N° d'ordre : 02/2020-D/G-C

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITÉ DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOUMEDIENE
FACULTÉ DE GÉNIE CIVIL

THÈSE DE
DOCTORAT en SCIENCES

Pour l'obtention du grade de Docteur

EN GÉNIE CIVIL
Spécialité : Construction

Par

AMIN BENMOKHTAR

Thème

PROPOSITION D'INTÉGRATION DES INFRASTRUCTURES ESSENTIELLES DANS LA STRATÉGIE ALGÉRIENNE DE PRÉVENTION CONTRE LES RISQUES MAJEURS ET LA GESTION DES CATASTROPHES

Soutenue publiquement le 26 septembre 2020 devant le jury suivant :

M. Amar NECHNECH	Professeur à l'USTHB	Président
M. Djillali BENOUAR	Professeur à l'USTHB	Dir. de thèse
M. Abderrahim BALI	Professeur à l'ENP	Examinateur
M. Hamid AFRA	Dir. Recherche à la DNRM	Examinateur
M. Hakim BECHTOULA	Dir. Recherche au CGS	Examinateur
Mme Fattoum KHARCHI	Professeur à l'USTHB	Examinatrice
M. Adel RAHMOUNE	M. Conférence A à l'UMBB	Invité

REMERCIEMENTS

Ce travail a vu le jour sous la direction de M. Djillali BENOUAR, Professeur à la Faculté de Génie Civil de l'Université des Sciences et de la Technologie Houari Boumediene. Qu'il trouve ici l'expression de mes sincères remerciements pour avoir accepté de me diriger afin de mener à bien cette thèse. Pour ses conseils utiles, ses critiques fructueuses, je tiens à lui exprimer ici ma profonde reconnaissance.

Je remercie le professeur Amar NECHNECH d'avoir bien voulu m'honorer en acceptant de présider le jury chargé d'examiner ce travail.

Aussi, je remercie les professeurs Fattoum KHARCHI, Abderrahim BALI, Hamid AFRA et Hakim BECHTOULA d'avoir accepté d'examiner ce travail malgré leurs nombreuses charges et préoccupations et je les remercie pour l'intérêt qu'ils ont accordé à cette thèse.

Que le professeur Mohamed DEBYECHE, Ex-directeur de l'École Nationale Polytechnique (ENP) soit particulièrement remercié pour son aide et son soutien.

Je ne saurais oublier l'aide si précieuse de Messieurs Abdel Fateh ZENATI, Adel RAHMOUNE, Mohamed OUADJAOUT, Djamel BOUKHETALA, Belkacem MOUSSAI ainsi que, Faycal RAHMOUNE. Qu'ils acceptent ma profonde considération.

Un grand merci également pour Nabila mon épouse, pour son soutien, sa précieuse aide, son inestimable affection mais surtout pour sa patience durant ces dernières années de préparation de cette thèse. Je remercie également mes enfants Manar, Ali et Walid pour leur patience et leur compréhension.

Un merci doit être adressé aux membres de ma famille, mes parents, mes sœurs, mes frères, mes gendres, à mes collègues de l'ENP et à mes étudiants.

Je ne peux pas non plus oublier le support que de nombreux amis m'ont apporté. Je tiens à remercier, vivement, Djamila HARIK, Mohamed BENBRIKA et Mokhtar BOULOUDENE pour leurs conseils et leur soutien moral.

Ma grande reconnaissance va à tous les enseignants qui ont contribué à ma formation.

Enfin, je tiens à reconnaître le support logistique du Laboratoire des Sciences et Techniques de l'Environnement de l'ENP. Je remercie particulièrement la directrice du Laboratoire professeur Naima BELHANECHE. Merci beaucoup à tous.

À toutes les personnes qui m'ont assisté de près ou de loin, qu'ils trouvent dans ce modeste document, l'expression de mes sincères remerciements.

DÉDICACE

À toi qui me manque tant,

Mon père (Benzekri).

Que Dieu tout puissant t'accorde sa sainte miséricorde et t'accueille en son vaste paradis.

À Allah nous appartenons et à lui nous retournons.

Je dédie ce modeste travail en signe de respect et de reconnaissance à :

- *Ma mère*
- *Mon épouse Nabila et mes enfants Manar, Ali et Walid ☺*
- *Mes chers frères, sœurs et gendres ;*
- *Toute ma grande famille et tous mes proches.*

RÉSUMÉS

ملخص:

الهدف من هذا العمل هو اقتراح مقاربة منهجية ووضع نمذجة رياضية لآثار الاضطرابات ورصدها، مما يساهم في فهم نظم البنى التحتية الحيوية (ب ت ح) في عملها قبل وقوع كارثة أو أثناءها أو بعدها (الفيضانات والزلازل، وما إلى ذلك). سيتم تطوير سيناريوهات الفشل واستخدامها من قبل المصممين الحضريين في نهج استباقي. تساهم النمذجة في إنشاء إطار نظري لخلق قنوات تعاونية بين الجهات الفاعلة في المدينة. كما تم تقديم اقتراح موجه إلى السلطات العامة بشأن تعريف **ب ت ح** وجردها التي سيتم تشريعها. ويقترح وضع مؤشر متوسط إجمالي لتدهور مهمة **ب ت ح.** تم أخذ تدهور مهمة شبكة المياه بعد الفيضان كمثال وتمت مناقشته للتحقق من صحة النموذج. الغرض من هذه الدراسة هو المساهمة في تعزيز صمود المدينة، من خلال تأمين **ب ت ح،** وتوعية السلطات العامة للنظر في أوجه ضعفها في استراتيجياتها لإدارة الكوارث وللتنمية الإقليمية والحضرية، وضع إجراءات لتعزيز صمود المناطق الحضرية.

كلمات مفتاحية: البنية التحتية الحيوية، الاضطراب، نمذجة الانتشار، إدارة المخاطر، صمود المدينة

Abstract:

The objective of this work is to propose a methodological approach and a modelling of disturbance effects for their monitoring which will contribute to the understanding of CISs and their function before, during or after a disaster (flood, earthquake, etc.). Failure scenarios will be developed and used by urban designers in a proactive manner. Modelling contributes to the establishment of a theoretical framework for the creation of a collaborative space between the actors of the urban site. A proposal, directed towards the public authorities, concerning the definition and inventory of these CISs to be legislated is also made. An overall weighted average mission degradation index of a CIS is proposed. The degradation of a water system's mission following a flood was taken as an example and discussed to validate the model. The purpose of this study is to contribute to the strengthening of the resilience of a city, by securing its CISs, and sensitize governments to consider their vulnerabilities in their disaster management and territorial and urban development strategies and to establish a process of resilience building.

Key words: Critical infrastructure, Failure, Propagation modeling, Risk management, Urban resilience.

Résumé :

L'objectif de ce travail est la proposition d'une approche méthodologique et d'une modélisation des effets de perturbations pour leurs suivis, ce qui contribuera à la compréhension des systèmes d'infrastructures essentielles (critiques) SICs et leurs fonctionnements avant, pendant ou après une catastrophe (inondation, tremblement de terre, etc.). Des scénarios de défaillance seront élaborés et utilisés par les concepteurs urbains dans une démarche proactive. La modélisation contribue à l'établissement d'un cadre théorique pour la création d'un espace collaboratif entre les acteurs de la ville. Une proposition, en direction des pouvoirs publics, concernant la définition et l'inventaire de ces SICs pour être légiférées est également faite. Un indice moyen pondéré global de dégradation de mission d'un SIC est proposé. La dégradation de la mission d'un réseau d'eau suite à une inondation a été prise comme exemple et discutée pour valider le modèle. La finalité de cette étude est de contribuer au renforcement de la résilience d'une ville, par la sécurisation de ses SICs, et sensibiliser les pouvoirs publics à considérer leurs vulnérabilités dans leurs stratégies de gestion de risque de catastrophes et de développement territorial et urbain et d'instaurer un processus de renforcement de la résilience.

Mots clés : Infrastructure critique, Perturbation, Modélisation de propagation, Gestion des risques, Résilience urbaine.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES ABRÉVIATIONS

AdD	Arbre de Défaillances
AdE	Arbre d'Évènements
AMDEC	Analyse des Modes de Défaillance et de leurs Effets et leurs Criticités
ANL	*Argonne National Laboratory.*
APR	Analyse Préliminaire des Risques
CEIS	Compagnie Européenne d'Intelligence Stratégique
CGS	Centre National de Recherche Appliquée en Génie Parasismique
CIAO	*Critical Infrastructures Assurance Office*
CIP/DSS	*Critical Infrastructure Protection/Decision Support System*
CIPMA	*Critical Infrastructure Protection Modelling and Analysis*
CIS	*Critical Infrastructure System*
CNAD	Centre National d'Aide à la Décision
CNVA	*Computer Network Vulnerability Assessment*
CRAAG	Centre de Recherche en Astronomie, Astrophysique et Géophysique
CSA	*Canadian Standard Association*
CSIRO	*Commonwealth Scientific and Industrial Research Organisation*
DHS	*Department of Homeland Security -USA*
DNRM	Délégation Nationale aux Risques Majeurs
FPM	Faculté Polytechnique de Mons
G.A.	Gouvernement Algérien
G.F.	Gouvernement Français
GC	Gestion des Catastrophes
GRC	Gestion de Risque de Catastrophe
GovCERT.au	*Australian Government Computer Emergency Readiness Team*
IAC	*Infrastructure Assurance Center*
IC	Infrastructure Critique
IDNDR	*International Decade for Natural Disasters Reduction*
IE	Infrastructure Essentielle
INHES	Institut National des Hautes Études de Sécurité
LANL	*Los Alamos National Laboratory*

MEDD	Ministère de l'Environnement et du Développement Durable français
MSP	Ministère de la Sécurité Publique du Québec
NIPC	*National Infrastructures Protection Center*
NISAC	*National infrastructure Simulation and Analysis Center*
ONU	Organisation des Nations Unies
ORSEC	Organisation de Secours
OSCQ	Organisation de Sécurité Civile du Québec
PDAU	Plans Directeur d'Aménagement et l'Urbanisme
PIB	Produit Intérieur Brut
POS	Plans d'Occupation des Sols
REX	Retour d'expérience
RSV	Réseaux de Support à la Vie
SCADA	*Supervisory Control And Data Acquisition*
SEAAL	Société des Eaux et de l'Assainissement d'Alger
SIC	Système d'Infrastructure Critique
SNL	*Sandia National Laboratories*
SONELGAZ	Société Nationale de l'Électricité et du Gaz
SPC	Sécurité Publique Canada
SPPCC	Sécurité Publique et Protection Civile Canada
TISN	*Trusted Information Sharing Network*

LISTE DES SIGLES

As	Activités
C	Criticité
ED	Éléments dangereux
EI	Évènement initiateur
ENS	Évènements non souhaités
ER	Évènement redouté
G	Gravité de conséquences
Is	Infrastructure
MG	Mission globale
Ms	Missions
Os	Opérations
P	Probabilité d'occurrence
Rs	Ressources
SD	Situation Dangereuse
SG	Système Global

INTRODUCTION

Nos milieux urbains dépendent de plus en plus, des réseaux de distribution et de transmission pour garantir la disponibilité et la fourniture des ressources essentielles : les transports, les ressources énergétiques, les communications, le raccordement et l'acheminement de l'eau potable, l'évacuation et le traitement des eaux usées ; sont considérés comme des Système d'Infrastructures Critiques (SICs). Ainsi, les villes sont des systèmes complexes et interdépendants, extrêmement vulnérables aux menaces des aléas naturels et du terrorisme. En effet, l'aspect structural et architectural, la concentration et la densité de la population, les espaces et lieux de rassemblement et les systèmes d'infrastructures interconnectés exposent les villes aux perturbations dues aux inondations, séisme, ouragan et voir même aux attaques terroristes (Godschalk, 2003).

Les ICs présentes dans ces milieux urbains, sont considérées comme étant des systèmes et des actifs, physiques ou virtuels, dont l'importance est telle que la destruction totale ou partielle de ces dernières aurait un impact grave sur la sécurité, la sécurité économique, la santé publique, etc. (Robert *et al*., 2003).

Les pays du monde entier ont été confrontés à plusieurs événements générés par diverses causes affectant les ICs (Too, 2011). Le séisme de Boumerdès en mai 2003 et les inondations de Bab El Oued en novembre 2001, ont montré d'une manière claire, la vulnérabilité de nos Systèmes Infrastructures Critiques (SICs). Ces derniers ont été hors usage, pendant plusieurs jours, compliquant fortement les actions de rétablissement et prolongeant la durée du retour à la normale. Les gouvernements ont reconnu que les ICs jouent un rôle crucial dans la fonction urbaine surtout celle liée à la vie (travail, soutien de l'économie, sécurité et le bien-être sociétal, etc.) (Tian *et al*., 2010). En effet, le bon fonctionnement de l'énergie, du transport, des usines d'eau, des télécommunications, des services financiers et autres, est vital pour toutes les communautés et tous les pays (Canzani, 2016).

Dans un territoire urbain, les ICs ne sont pas isolées les unes des autres. Les relations entre elles doivent être identifiées pour effectuer des analyses réalistes (Rinaldi, 2004). Plusieurs ICs peuvent être en relation, entraînant des défaillances à répercussions multiples par le biais d'effets dominos (Plate, 1996 ; Allen, 1997 ; Moses, 1998 ; Lemperiere, 1999). Leurs dispositions et emplacement doivent être bien conçus lors de l'aménagement du

territoire urbain pas juste pour assurer les services vitaux et améliorer le cadre de vie des habitants mais aussi les sauver en cas de catastrophe.

La caractérisation complète de la vulnérabilité des ICs, contribue à l'évaluation de la vulnérabilité de nos milieux urbains face aux différentes perturbations d'origine naturelle ou anthropique. Ceci nécessite de modéliser la dynamique de l'écoulement des grandeurs physiques dans le réseau ou dans un Système d'Infrastructure Critique (SIC) (Zio et Sansavini, 2011). Par conséquent, les SICs doivent être modélisés dans le cadre d'un processus global d'analyse de la sécurité et déterminer les points de faiblesse ou les zones de vulnérabilité (Pye et Warren, 2006). Cela implique, non seulement de prendre en compte l'interaction, entre les caractéristiques structurelles et architectural et les aspects dynamiques, mais aussi de l'ensemble de transformation au sein des composantes des ICs. Ces dernières dépendent d'autres ressources (Rs) pour pouvoir véhiculer l'élément transporté à travers le SIC. Par conséquent, la mission principale de ce dernier est garantie par l'accomplissement des missions des différentes ICs. Une mission correspond à une fonction pour laquelle un SIC a été conçu et construit, et correspondant à un besoin de la population (Robert *et al*., 2007).

L'intérêt de la recherche sur les SICs est de ne plus les considérer comme de simples systèmes isolés mais comme des systèmes multiples, interconnectés et dépendants, tout en évaluant l'influence qu'imposent les infrastructures en interaction sur les conditions d'exploitation de chaque IC (Zimmerman, 2001). L'interdépendance, les effets dominos et la vulnérabilité liés aux SICs sont les trois aspects qui forment cette problématique.

Justement, dans le milieu urbain, l'atténuation des risques et le rétablissement ont traditionnellement mis l'accent sur la prévention, la protection et la résistance plutôt que sur la résilience. (Allan et Bryant, 2011)

Ce travail de recherche vise à modéliser la propagation des effets, suite à une ou plusieurs perturbations dans un SIC, tout au long de ses ICs. L'interdépendance inter-ICs sera prise en considération lors de la décomposition des ICs en composantes et plus exactement au niveau de leurs ressources (Rs). Ce travail est orienté essentiellement sur les conséquences des perturbations dans les ICs causées, par le dysfonctionnement technique, l'erreur de l'intervention humaine ou même l'aléa naturel.

L'Algérie est bien dotée de mécanismes juridiques corroborant la gestion des risques majeurs, notamment la loi cadre 04/20 (GA, 2004), relative à la prévention des risques majeurs et à la gestion des catastrophes dans le cadre du développement durable. Les études pour la sauvegarde des ICs sont rares, ce qui ne ferait qu'amplifier la difficulté de gestion des risques pour ce genre d'infrastructure.

L'objectif de ce travail est la compréhension et le suivi, de la propagation des effets d'une ou plusieurs perturbations, de même que le comportement des SICs, face aux différents risques (industriels et de transformations) et aléas (naturel et anthropique) et ce pour une parfaite intégration de la planification du rétablissement et de l'urbanisme lors de la conception. En effet, il existe un lien fort entre la structure urbaine d'une ville et sa capacité à récupérer après un tremblement de terre (Allan et Bryant, 2011). Ceci contribuera par exemple à l'enrichissement des cartes des risques sismiques (Benouar *et al*., 1996).

L'autre objectif est de contribuer à l'instauration d'un cadre méthodologique pour faciliter la création d'espace de collaboration entre les concepteurs urbains et les ingénieurs en planification de rétablissement pour des fins d'échange d'informations dès la phase de conception d'études pour concevoir finalement des villes résilientes et renforcer celles qui le sont moins.

Une nouvelle approche pour la gestion du risque, dans son volet analyse est proposée. Cette approche « par effet » se base sur le suivi des effets d'une ou plusieurs perturbation(s) bien avant la rupture de la mission d'un système. L'approche en question se démarque du reste des méthodes d'analyse de risque et permet de préconiser des mesures, de prévention pour renforcer le niveau de résilience des sous-systèmes les plus vulnérables.

Une approche méthodologique sera décrite, et accompagnée d'une modélisation de la propagation de ces effets. Aussi, une simulation de perturbation à l'intérieur et à travers les SICs sera faite, offrant ainsi une contribution pour le développement d'un cadre méthodologique pour une ville résiliente joignant la conception, la fonctionnalité et la planification des mesures d'urgences et de rétablissement.

Un exemple, de la propagation des effets de deux perturbations suite à une inondation d'un réseau d'eau dans une zone urbaine, composé de quatre ICs est traité et discuté.

Notre thèse comporte six chapitres. Le premier chapitre est consacré au contexte général de la recherche, qui s'inscrit parfaitement dans la stratégie algérienne de gestion des risques de catastrophe, ce qui nous permet de définir la problématique à vouloir traiter dans le cadre du présent travail en fixant les objectifs et la démarche méthodologique.

Dans le deuxième chapitre, nous exposons les définitions et les notions de bases entourant les ICs et leurs problématiques spécifiques. La compréhension de ces concepts nous amènera à nous intéresser aux liens inter-ICs vu l'importance qu'ils jouent dans l'accomplissement de la mission d'un SIC.

Dans le chapitre trois, nous abordons les aspects théoriques sur la gestion des risques et l'intérêt de l'analyse de risque.

Le quatrième chapitre est exclusivement dédié à la revue de littérature abordant au début, la modélisation des liens inter-ICs, suivie par une synthèse d'écris sur la résilience et la résilience urbaine ensuite nous passons en revue les travaux effectués dans le monde.

Dans le chapitre cinq, nous présentons les principes méthodologiques pour modéliser les liens inter-ICs et ce pour évaluer la dégradation de leurs missions en cas de perturbations. La méthodologie, proposée, est basée sur la transformation des ressources d'entrée, en une mission par l'entremise des activités et des opérations propres à l'IC. Notre cadre méthodologique sera utilisé par les gestionnaires des ICs, dans un cadre collaboratif, que nous proposons. En effet, cette démarche va fortement contribuer à l'intégration de la problématique des SICs dans la stratégie algérienne de la gestion des risques de catastrophes.

Enfin, le sixième chapitre présente une application du modèle proposé sur un SIC (réseau d'eau). Une discussion est également engagée autour des résultats, obtenus, suite à une simulation d'inondation, survenue dans un milieu urbain et de quelles actions nous pouvons disposer pour rendre ce milieu résilient face à son propre SIC.

Chapitre 1

CHAPITRE 1 CONTEXTE DE RECHERCHE, PROBLÉMATIQUE ET OBJECTIFS

Le point de départ de notre recherche est directement lié à la stratégie algérienne de gestion des risques de catastrophe, son origine et ses objectifs, que nous abordons dans ce premier chapitre dans lequel nous mettons également en évidence l'importance que les pouvoirs publics algériens accordent aux Infrastructures Critiques (ICs). La problématique et les objectifs de recherche sont ensuite présentés et le chapitre finit par une illustration méthodologique pour la réalisation des objectifs assignés.

L'élément important qui nous a fortement encouragés à entamer le présent travail, est la volonté de l'État Algérien à renforcer les capacités présentes dans ses structures appelées à répondre, efficacement, aux besoins en cas d'urgence extrême afin de sauver et préserver des vies humaines par l'entremise de sa stratégie de gestion des catastrophes. En effet, l'adoption de la loi algérienne relative à la prévention des risques majeurs et à la gestion des catastrophes dans le cadre du développement durable s'inscrit dans cette vision.

Ainsi, cette mise en contexte, nous permettra d'explorer les outils, sur lesquels repose cette loi, entre autre la mise en place des mécanismes juridiques, pour la gestion des catastrophes (GC) et nous permettra, également de mettre en évidence le point d'ancrage de notre problématique.

En effet, nous assistons à un accroissement de la complexité de ces infrastructures. De plus, des vulnérabilités supplémentaires naissent des défaillances en cascades entre les infrastructures suite à des perturbations.

1.1 Stratégie algérienne de gestion des risques de catastrophe

L'Algérie a connu de nombreuses catastrophes « naturelles » et industrielles qui ont occasionné la perte de milliers de vies humaines, d'énormes dégâts matériels et des atteintes à l'environnement. Ainsi, les dégâts résultant du séisme de Chlef en octobre 1980, des inondations de Bab el Oued en novembre 2001 et du séisme de Boumerdès en mai 2003 pour ne citer que cela, font partie de la mémoire contemporaine de la société algérienne.

Afin d'assurer la protection des vies humaines et des biens, ainsi que le développement durable, les pouvoirs publics algériens sont devenus de plus en plus conscients de la nécessité de réduire les dommages, par l'introduction dans un premier temps d'actions préventives et ensuite par la mise en place d'un système de gestion des risques efficient.

À cet effet, nous débuterons cette section par ce qui était à l'origine de la mise en place des différents mécanismes de gestions de catastrophe. Nous présenterons aussi la dernière loi (04/20) relative à la prévention des risques majeurs et à la gestion des catastrophes dans le cadre du développement durable. Ainsi, cette partie permettra de passer en revue toutes les mesures existantes en matière de gestion de catastrophes et de l'importance de la gestion de risque de catastrophe (GRC).

1.1.1 Origine de la prise de conscience

De grandes catastrophes ont hautement concouru à une nouvelle prise de conscience des pouvoirs publics algériens, permettant ainsi la relance de certains programmes et d'actions considérés comme pilier de la stratégie algérienne en matière de la GRC. Avant d'explorer la stratégie sur laquelle elle se base et ses objectifs, nous avons trouvé utile de citer quelques catastrophes qu'avait connues l'Algérie comme les séismes et les inondations.

1.1.1.1 Séismes

La société algérienne a connu trois grands séismes durant les quarante dernières années à savoir :

- ✓ Séisme d'El Asnam (Chlef actuellement) : survenu le 10 octobre 1980 d'une magnitude 7,5 sur l'échelle de Richter. Ce séisme a touché l'ensemble de la région de Chlef. Le bilan général des dégâts enregistrés s'élevait à 3.500 morts, 8400 blessés, 350 disparus, 29.000 logements détruits et 478.950 sinistrés (Benouar, 1994). Le coût des dommages a été évalué à plus de 2 milliards de dollars US (Belazougui, 2018). Ce séisme est considéré comme étant le plus meurtrier de la région dans l'histoire algérienne.
- ✓ Séisme de Mascara : survenu le 18 août 1994 avec une magnitude de l'ordre de 5,7. Ce séisme a occasionné 171 morts, 289 blessés et avec plus de 1328 habitations détruites (Ayadi *et al.*, 2002).
- ✓ Séisme de Boumerdès : survenu le 21 Mai 2003, d'une magnitude de 6,8, provoquant la mort de 2.278 personnes et a occasionné 11.450 personnes blessées, 200.000 personnes sans-

abris et des centaines d'infrastructures détruites (Benouar et Meslem, 2007), soit plus de 3 Milliards de dollars US de dégâts (Belazougui, 2018).

1.1.1.2 Inondations

✓ Alger (Bab-El-Oued) en date du 10 novembre 2001. Provoquant le décès de plus de 700 personnes, 115 disparus, 311 blessés, plus de 1.500 familles sans abri, et des dégâts importants sur les infrastructures (routes, cratères de plus de 10 mètres de diamètre, réseaux d'assainissement endommagés, rues envasées, etc.) (Benouar, 2004) soit plus de 400 Millions de Dollars US de pertes (Belazougui, 2018).

1.1.2 Objectifs de la stratégie

La stratégie algérienne se base principalement sur la loi 04/20. En effet, à la lecture de cette dernière, nous pouvons clairement identifier les multiples objectifs escomptés par cette stratégie, à savoir (GA, 2004) :

✓ La compréhension, l'identification et l'évaluation des aléas et des risques pour les besoins de la cartographie des risques ;
✓ L'information et l'éducation du public ;
✓ Le renforcement des capacités des institutions et des organismes dont les missions concourent à la prévention et à la protection contre les risques ;
✓ L'encouragement des pratiques de collaboration et de concertation entre les institutions et les organismes concernés par la GC ;
✓ La promotion et le développement d'une coopération multiforme à l'échelle régionale et internationale.

1.1.3 Cadre réglementaire et organes d'exécution

Le cadre réglementaire et les organes d'exécution sont à la base de la stratégie algérienne. Ainsi, le premier cadre englobe l'ensemble des lois régulant cette stratégie et le deuxième représente les instruments à même d'exécuter ces même lois et règlements, dans son double volet prévention des risques, protection et interventions.

1.1.3.1 Cadre réglementaire

Nous considérons que l'origine du cadre réglementaire corroborant la GC trouve ses racines dans la constitution algérienne bien qu'aucune indication directe à la GC ne soit mentionnée. Néanmoins, des articles de la constitution de 1996 (GA, 1996) et modifiée en 2016, rendent l'État entièrement responsable de la sécurité des biens et des personnes et de la protection de nature, ces articles sont (GA, 2016) :

- ✓ Article 19 : « L'État garantit l'utilisation rationnelle des ressources naturelles ainsi que leur préservation au profit des générations futures.
  - L'État protège les terres agricoles.
  - L'État protège également le domaine public hydraulique.».
- ✓ Article 26 : « L'État est responsable de la sécurité des personnes et des biens.».
- ✓ Article 66 : « Tous les citoyens ont droit à la protection de leur santé.
  - L'État assure la prévention et la lutte contre les maladies épidémiques et endémiques.».
- ✓ Article 68 : « Le citoyen à droit à un environnement sain.
  - L'État œuvre à la préservation de l'environnement.».

Le séisme d'El Asnam de 1980 est considéré comme le point de départ pour la mise en place des premiers mécanismes juridiques portant sur la GC et donnant lieu à la classification des différents types de risques. Ainsi, le groupe de travail installé juste après ce séisme avait identifié quatorze (14) types de risques naturels et technologiques auxquels pourrait être exposée l'Algérie. Parmi ces risques sept (7) sont de types naturels comme l'indique le Tableau 1-1.

Tableau 1-1: Classement algérien par type de risque (Belazougui, 2018)

Types de risques naturels et technologiques (14)	
Naturels (7)	Technologiques (7)
▪ Séisme ▪ Inondations ▪ Mouvement de terrains, affaissement et tassement ▪ Tempêtes et vents violents ▪ Sécheresse ▪ Feu de forêt ▪ Acridien	▪ Incendie et explosion ▪ Catastrophes maritimes ▪ Catastrophes aériennes ▪ Désastres de chemin de fer et de route ▪ Accidents radiologiques ▪ Pollution ▪ Catastrophes biologiques

En 1985, soit cinq années après le séisme d'El Asnam, seulement deux décrets ont été promulgués, n°85-231et n°85-232, pour la GC. En effet, ces deux derniers ont toujours servi de base pour la GC en Algérie sur une période de plus de 20 ans.

Le premier décret datant de 1985(GA, 1985a) définit les organisations et les procédures de réalisation des interventions et de l'assistance en cas de catastrophe. Il a d'ailleurs permis la mise en place des Plans d'Organisation de Secours (ORSEC) au niveau de commune et de wilaya. Ce dernier a été abrogé en 2019 (Février) et remplacé par le décret exécutif n^{0}19-59 (GA, 2019). Quant au deuxième décret datant lui aussi de 1985(GA, 1985b) il concerne la prévention des risques naturels et technologiques.

La contribution de l'Algérie à la décennie internationale pour la réduction des catastrophes naturelles l'*International Decade for Natural Disasters Reduction* (IDNDR), 1990-1999, sous l'égide de l'Organisation des Nations Unies (ONU), avait permis aux comités interministériels, installés à l'occasion et en accord avec l'ONU, l'identification de quatorze (14) types de risques majeurs dont dix (10) concernent plus particulièrement l'Algérie, telle que classés au Tableau 1-2 (Lechat,1990), (Belazougui, 2018).

Tableau 1-2 : Classement par type de risque Onusien (IDNDR, 1999).

Naturels (5)	**Technologiques (4)**	**Autre (1)**
▪ Tremblements de terre et risques sismiques et géologiques. ▪ Inondations. ▪ Risques climatiques. ▪ Feux de forêt. ▪ Risques menaçant directement la santé humaine.	▪ Risques industriel et énergétique. ▪ Risques radiologique et nucléaire. ▪ Pollution atmosphérique, tellurique, marine et hydrique. ▪ Risque menaçant la santé animale et végétale.	▪ Catastrophes dues à des regroupements humains importants.

1.1.4 Mesures de réduction des risques de catastrophe

L'ensemble des mesures en GC a été principalement orienté vers le risque sismique. Vu que ce dernier est très présent depuis 1980 en Algérie (huit tremblements de terre dont les magnitudes dépassaient les 5,4 sur l'échelle Richter).

Ces mesures ont permis la mise en place de (Belazougui, 2018) :

✓ Réseau de surveillance sismique télémétré au niveau du Centre de Recherche en Astronomie, Astrophysique et Géophysique (CRAAG) composé de plus de 60 stations sismographiques ;

✓ Réseau national d'accélérographes du centre national de génie parasismique (CGS) composé actuellement de 400 appareils installés successivement, à travers le territoire national (Belazougui, 2018) ;

✓ Une dizaine de sismographes mobiles au niveau du CGS et autant au niveau du CRAAG et qui ont été déployés pour la première fois dans la région de Boumerdès pour enregistrer les répliques du séisme du 21 mai 2003 ;

✓ Équipements mobiles et fixes d'essais dynamiques des structures au niveau du CGS dont une « table vibrante » (*Shaking* table) de 6m x 6m à 6 degrés de liberté de dernière génération.

En plus de la mise en place de ces réseaux, les pouvoirs publics algériens ont élaboré plusieurs cartes et études comme (Belazougui, 2018) :

✓ Cartes de l'aléa sismique nationale (actualisée en 2018) et régionale (carte d'iso-accélérations avec des périodes de retour de 100, 200 et 500 ans) ;

✓ Cartes de "micro zonage" sismique d'une cinquantaine d'agglomérations urbaines des régions de Chlef, Ain Defla, Alger, Tipasa, Boumerdès, Constantine, Mascara et Aîn Témouchent, et de plusieurs sites d'ouvrages importants (barrages, centrales électriques, hôpitaux, etc.).

✓ Étude de la vulnérabilité sismique, pour le renforcement, de certains bâtiments stratégiques Alger, Constantine et Blida ;

✓ 2 Études de la vulnérabilité sismique de la capitale Alger.

De plus, les deux décrets déjà cités ont permis de se pencher sur des risques autre que le risque séismique par l'élaboration de plusieurs plans nationaux de préventions et d'alerte à l'échelle de l'Algérie. Ainsi, nous pouvons dénombrer ce qui suit (Belazougui, 2018) :

✓ Les plans de prévention et de lutte contre les incendies de forêts ;

✓ Plan national contre la désertification (avec adaptation à la convention internationale de lutte contre la désertification) ;

- ✓ Plan national de lutte antiacridien (avec une carte spéciale pourvue des indices des zones à végétation potentielle d'émeute des insectes nuisibles, couvrant l'Algérie du sud et les zones jusqu'au nord du Mali et du Niger) ;
- ✓ Plan national d'urgence contre la pollution maritime (Tel Bahr National) ;
- ✓ Plan de prévention et d'intervention pour tous les risques économiques et industriels.

Pour couvrir la majorité des risques, les pouvoirs publics algériens se sont forcés également de mettre en place des plans d'alerte comme (Belazougui, 2018) :

- ✓ Système national d'alerte par radio pour les incendies de forêts ;
- ✓ Système national et international de surveillance et d'alerte des invasions acridiennes ;
- ✓ Système national d'alerte rapide pour les déversements massifs d'hydrocarbures ;
- ✓ Système national d'alerte rapide par radio des déversements ou ruptures de barrages ;
- ✓ Systèmes pilotes de prévision et d'alerte aux crues du bassin versant du Sébaou (Région de Tizi-Ouzou) et du bassin de l'Oued El Harrach (Wilaya d'Alger) ;
- ✓ Systèmes d'alerte rapide spécialisés pour les grandes zones industrielles (pétrochimiques et pétrolières en particulier) ;
- ✓ Système d'alerte météorologique pour la prévention des tempêtes et vents violents.

En dépit, des diverses mesures prises par les pouvoirs publics algériens, le tremblement de terre de la ville de Boumerdès en 2003 a fait ressortir le manque d'efficience des plans de GC algériens. C'est ce qui a accéléré la promulgation d'une loi plus globale que nous aborderons dans la prochaine section. À travers l'examen de cette loi, nous mettrons l'emphase sur les bases, les buts escomptés ainsi que les nouveautés que cette dernière introduit. Le but recherché est d'ancrer et de positionner l'actuel travail de recherche dans son contexte voir même considérer cette loi comme le point de départ de notre recherche.

1.1.5 Loi algérienne relative à la prévention des risques majeurs et à la gestion des catastrophes dans le cadre du développement durable

Il s'agit de la loi n° 04-20 promulguée le 25 décembre 2004 et orientée vers la prévention des risques et la gestion des catastrophes dans le cadre du développement durable. Les inondations de Bab el Oued (2001) et le séisme de Boumerdès (2003) ont effectivement accéléré la promulgation de cette loi. Dans ce que suit nous allons aborder les principes de

bases, les buts, organes d'exécutions et les nouveautés qu'apporte cette loi. Nous aurons aussi à mettre en exergue le manque de quelques mécanismes juridiques pour renforcer la loi en question.

1.1.5.1 Principes de bases

Avant d'aborder les buts escomptés par la loi, il y'a lieu de citer ces principes de bases :

- ✓ Préparation et précaution ;
- ✓ Concomitance (simultanéité, synchronisme) ;
- ✓ Actions préventives et correctives aux sources des problèmes potentiels ;
- ✓ Participation des citoyens ;
- ✓ Intégration des nouveaux éléments techniques.

1.1.5.2 Buts

La loi dont il est question prévoit d'atteindre plusieurs objectifs comme :

- ✓ L'amélioration des connaissances sur les risques, le renforcement de l'étude et de la prédiction ainsi que le développement de l'information préventive sur les risques ;
- ✓ La prise en considération des risques dans l'acte de construction ainsi que la réduction de la vulnérabilité de la population ;
- ✓ L'implantation des moyens de sécurisations cohérents, intégrés et adaptés pour faire face aux catastrophes naturelles et technologiques.

1.1.5.3 Nouveautés

Les nouveautés apportées par cette loi sont d'une grande importance dans la mesure où elle accorde beaucoup d'intérêt à l'information du citoyen et à sa formation à la prévention des risques majeurs et à la GC. En plus, elle personnalise les mesures à prendre face à chaque risque majeur ainsi que pour les risques particuliers.

La loi fixe également et pour la première fois les mesures stratégiques pour les routes et les télécommunications de secours ainsi que pour les bâtiments à valeur stratégique et patrimoine et prévoit des mesures de prévention dans le domaine d'assurance, d'expropriation et d'utilité publique. Justement, l'objectif du présent travail de recherche est de contribuer dans le sens de préserver nos infrastructures stratégiques (Infrastructures Essentielles) que nous appellerons infrastructures critiques (ICs).

Concernant la GC, la loi institue un système national s'occupant de :

- ✓ La planification des secours et des aides adaptées à tous les niveaux ; national, inter-wilaya, wilaya et communal, ainsi qu'aux sites critiques à travers les plans ORSEC ;
- ✓ Les mesures structurelles pour les interventions : approvisionnement stratégique, restauration des dommages, institutions spécialisées notamment la création d'une Délégation Nationale aux Risques Majeurs (DNRM).

En somme, la loi n° 04-20 représente le moyen le plus important pour toutes les mesures permettant la GC aussi bien dans ses phases de prévention que dans ses phases de protection et d'interventions.

Le cadre organisationnel a été, également, renforcé par plusieurs dispositions réglementaires touchant l'aménagement et l'urbanisme. Ces dispositions sont :

Adoption et publication de la loi 04-05 du 14 Août 2004 modifiant et complétant la loi 90-29 du 1° décembre 1990 relative à l'aménagement et à l'urbanisme ;

- ✓ Publication de l'ordonnance du 26 août 2003 relative à l'obligation d'assurance des catastrophes naturelles et à l'indemnisation des victimes ;
- ✓ Promulgation en 1981 des premières règles parasismiques algériennes (RPA) et enrichies depuis par des versions successives (1983, 1988, 1999, 2003) ;

Pour la loi n° 04-05 du 14 août 2004 modifiant la loi n° 90-29 et la complétant concernant l'aménagement du territoire et le développement urbain en instaurant également :

- ✓ Les Plans d'Occupation des Sols (POS) ;
- ✓ Les Plans Directeurs d'Aménagement et l'Urbanisme (PDAU) ;
- ✓ Nouvelles règles pour l'obtention du permis de construire.

Enfin, et pour permettre la mise en application effective de la loi cadre sur la GC, d'autre décrets ont été promulgués dans ce sens, à savoir :

- ✓ Le décret exécutif n°19-59 du 2 février 2019 fixant les modalités d'élaboration et de gestion des plans d'organisation des secours ;
- ✓ Le décret exécutif n°15-71 du 11 février 2015 fixant les conditions et modalités d'élaboration et d'adoption des plans particuliers d'intervention pour les installations ou ouvrages ;

- ✓ Le décret exécutif n°09-335 du 20 octobre 2009 fixant les modalités d'élaboration et de mise en œuvre des plans internes d'intervention par les exploitants des installations industrielles ;
- ✓ Le décret exécutif n°04-181 du 24 juin 2004 relatif à la création de la commission de communication liée aux risques majeurs naturels et technologiques ;
- ✓ Le décret exécutif n°04-268 du 29 août 2004 relatif à l'identification des événements naturels à couvrir par l'assurance et aux méthodes de déclaration de l'état de catastrophes naturelles.

En outre, ces deux décrets exécutifs viennent compléter d'autres décrets existants à savoir :

- ✓ Le décret exécutif n°03-332 du 8 octobre 2003 relatif à la création et à l'organisation du Centre National opérationnel d'Aide à la Décision (CNAD) mais dissous en avril 2013 ;
- ✓ Le décret exécutif n°90-402 du 15 décembre 1990 portant organisation et fonctionnement du fonds de calamités naturelles et de risques technologiques majeurs.

1.1.5.4 Organes d'exécutions

Plusieurs organismes et institutions, sont chargés de la GC et l'atténuation des différents risques, ces organismes sont situés principalement à plusieurs niveaux, que ce soit au niveau central, local ou national (Belazougui, 2018) :

- ✓ Niveau central

Il englobe tous les départements ministériels impliqués dans la GC. Il s'agit donc des directions se trouvant aux différents ministères telles que le ministère de l'intérieur, des collectivités locales et de l'aménagement du territoire, le ministère de l'habitat, de l'urbanisme et de la ville, et le ministère de la santé, de la population et de la réforme hospitalière pour ne citer que ceux-là.

- ✓ Niveau local

Il englobe les autorités locales des wilayas et communales avec l'aide et l'assistance technique des services déconcentrés des ministères et des organismes techniques spécialisés. On citera, à titre d'exemple, les directions sectorielles sous l'autorité du Wali : la direction de la santé et de la population de Wilaya, la direction de ressources en eau de Wilaya et la direction de l'urbanisme, de l'architecture et de la construction de Wilaya.

- ✓ Niveau national

Création en octobre 2003 du CNAD pour renforcer les organes d'exécutions. Ce centre est chargé de gérer un système de veille permanente concernant les différents risques majeurs mais dissous en avril 2013. En juin 2004 il y'a eu la création de la Commission Nationale de Communication relative aux Risques Naturels et Technologiques Majeurs. La même année, soit en juillet 2004, l'Agence Nationale des Sciences de la Terre, a connu le jour. Il y'a lieu de noter que cette Agence est restée sans activité depuis sa création. Quant à la DNRM, le texte juridique qui fixe son organisation et son fonctionnement a été promulgué le 22 mai 2011 (GA, 2011).

1.1.5.5 Ce qui manque

L'absence de quelques décrets d'application handicape la mise en place effective d'une stratégie globale de GC.
Ces décrets d'applications concerneraient le mode de planification pour l'étude de la vulnérabilité des bâtiments stratégiques ainsi que l'élaboration de leurs plans de renforcement pour l'amélioration de leurs résiliences, et aussi, le mode de planification pour la prise en considération des SICs et leurs infrastructures.

Les autres textes manquants concernent l'enrichissement de l'actuel plan ORSEC en développant le mode opérationnel (même après la promulgation du décret exécutif n°19-59) :

- ✓ De réquisition des personnes et matériels essentiels pour la GC ;
- ✓ D'utilisation des réserves stratégiques.

Nous pouvons constater que dans la stratégie algérienne, en dépit des grands efforts déjà déployés, l'importance est donnée au risque sismique et que les moyens sont plus orientés vers l'intervention que vers la prévention et la planification.

Souvent la prise de conscience et les efforts d'amélioration en matière de GC sont consentis après la survenue de catastrophes.

L'examen de la loi (04/20) fait ressortir l'absence de texte réglementaire cadrant les ICs et qu'aucun inventaire de ces dernières n'est mentionnées.

Malgré, l'existence de larges structures et d'un cadre réglementaire, il y'a lieu de renforcer les mécanismes juridiques, sur lesquels s'appuie la stratégie algérienne, par la mise en place des décrets d'applications et de faire une nette différence entre les infrastructures sensibles et les ICs.

Pour cela, un de nos objectifs serait de proposer quelques définitions en liens avec les ICs et une classification de ces dernières. Ces propositions seront proposées à la DNRM pour une éventuelle légifération à l'instar des autres pays.

1.2 Enjeux de la sécurisation des systèmes d'infrastructures critiques

Sécuriser les SICs est une mission complexe qui ne peut être, totalement, accomplie que si les liens inter-infrastructures sont bien établis. Comme il s'agit avant tout de phénomènes physiques, la compréhension de ces liens peut être obtenue par une modélisation. Ainsi, la modélisation des interdépendances entre ICs apportera une contribution capitale pour la sécurisation de ces dernières par l'amélioration de leurs niveaux de résilience car nous assistons aujourd'hui à :

- ✓ La complexité croissante de la technologique utilisée dans les SICs (interférence de technologies, électronique, logiciel) ;
- ✓ L'exigence des utilisateurs des SICs en matière de qualité et de fiabilité de la ressource fournie ;
- ✓ L'accroissement des coûts induits par la dégradation de mission après une perturbation ;
- ✓ La responsabilité légale du gestionnaire, quant à la maitrise des risques ; associée à l'utilisation de ces SICs, qui reste en tout temps engagée.

1.3 Problématique

Nos milieux urbains dépendent, de plus en plus, des réseaux de distribution et de transmission pour garantir la disponibilité et la fourniture des ressources essentielles : les transports, les ressources énergétiques, les communications, le raccordement et l'acheminement de l'eau potable, l'évacuation et le traitement des eaux usées, considérés comme des Infrastructures Critiques (ICs). Ces dernières sont très souvent organisées en réseaux (SIC) complexes, de plus en plus interconnectés entre eux (Rinaldi, Peerenboom, et Kelly, 2001).

Nous avons vu, que le séisme le plus meurtrier qu'a connu l'Algérie post indépendante est celui d'El Asnam en 1980. Cependant, il n'est pas sans intérêt de se référer à celui de Boumerdès en mai 2003 puisqu'il permet, un quart de siècle environ après la catastrophe de Chlef, de constater que les différentes structures en charge de la GC ne sont toujours pas assez prêtes faute de gestion efficiente.

Vouloir aborder l'ensemble des impacts des catastrophes sur toute une société ainsi que les modalités de leurs atténuations est une tâche qui n'est pas possible dans un seul projet de recherche. Dans le présent travail de recherche, nous nous concentrerons essentiellement sur les conséquences résultant d'une perturbation, suite à une catastrophe, impactant les SICs et ceci dans le but d'intégrer la problématique de ces derniers, pour être traitée, dans la stratégie algérienne de gestion des risques de catastrophe. Ce choix est motivé par le fait que ces systèmes sont des structures primordiales en raison de leurs caractères indispensables aux milieux urbains. En effet, la rupture ou la dégradation d'une mission d'un SIC peut entraîner de graves conséquences (Petit *et al*., 2004)

Bien que l'Algérie dispose de mécanismes juridiques encadrant la gestion des risques de catastrophe, les textes d'application ne sont pas totalement élaborés voire inexistants à l'exemple de ceux traitant les (Infrastructures essentielles) SICs. Cet état de fait ne ferait qu'amplifier les difficultés dans la gestion des risques en cas de perturbation.

Par ailleurs, la parfaite compréhension des liens inter-ICs d'un SIC, la propagation des effets d'une perturbation et le degré de dégradation de la mission d'un SIC reste problématique en absence de modèle simple.

La sécurisation des SICs passe par l'analyse des risques associés aux perturbations touchants ses ICs. Ce qui revient à répondre aux questions suivantes :

- Comment une composante perturbée affecte la mission propre de l'IC à laquelle elle appartient ?
- Comment une IC affectée influe sur d'autres ICs ?
- Comment une IC affectée influe par la suite sur le SIC (système global) ?

1.4 Objectifs

Tout en se situant dans une phase de planification, notre projet de recherche a pour objectif la contribution pour l'établissement d'une approche permettant l'intégration de la problématique liée aux ICs, dans la stratégie algérienne de gestion des risques de catastrophe. L'objectif escompté est de sensibiliser nos pouvoirs publics à prendre en considération la notion de vulnérabilité des SICs,

Cet objectif s'avère très simple, mais son accomplissement demeure difficile pour deux raisons. La première est qu'il fait intervenir plusieurs notions souvent nouvelles et complexes et la deuxième est que le domaine abordé reste nouveau en Algérie. D'ailleurs, peu d'études abordant les problématiques en lien avec les SICs sont disponibles.

La prise en charge de ces problématiques, dans la stratégie algérienne de gestion des risques de catastrophe, ne peut se réaliser que par la compréhension, et le suivi de la propagation des effets d'une ou plusieurs perturbations, et du comportement des SICs, face aux différents risques (industriels et de transformations) et aléas (naturel et anthropique).

En effet, ces compréhensions permettront une parfaite intégration de la planification du rétablissement lors de la conception du milieu urbain mais aussi après une catastrophe. D'ailleurs, il existe un lien fort entre la structure urbaine d'une ville et sa capacité à récupérer après un tremblement de terre par exemple (Allan et Bryant, 2011).

Finalement sécuriser les SICs ne peut pas se faire sans cette compréhension. L'amélioration de cette dernière est possible grâce à la modélisation des liens fonctionnels et dysfonctionnels existants entre ICs d'un même SIC. Il s'agit de modèles simples et

souples, fortement adaptables (pouvant être utilisé à tout type de SICs) et non couteux pour évaluer la dégradation de la mission d'un SIC suite à une ou plusieurs perturbations.

Les modèles mathématiques, une fois, développés contribueront certainement à l'instauration d'un cadre méthodologique pour faciliter la création d'un espace d'échange et de collaboration entre les concepteurs urbains, les gestionnaires des ICs et des SICs et les ingénieurs en planification de rétablissement et ce pour des fins d'échange d'informations. Dans une démarche de prévention, le cadre d'échanges et de collaboration sera utile dès la phase de conception et études de ces infrastructures. Les objectifs de cette modélisation sont de répondre aux trois questions posées dans notre problématique.

La légifération des lois permettant l'identification et l'inventaire des ICs, l'utilisation de notre cadre méthodologique dans l'espace collaboratif contribuera à l'enrichissement de l'actuelle démarche de prévention et ainsi conduire à une meilleure prise de décision unie et commune.

La finalité de notre recherche est la contribution par l'intégration effective des problématiques en liens avec les SICs dans la stratégie algérienne de gestion des risques de catastrophe. Ainsi, nous aurons à concevoir des villes résilientes et renforcer celles qui le sont moins. À juste titre la loi algérienne 04/20 insiste sur l'aspect collaboration entre les différents acteurs de la ville.

En somme, nos objectifs coïncident et s'accordent, avec ceux du développement durable notamment l'objectif n° 9 visant à atteindre à l'horizon 2030 et au principe n°15 arrêté lors du sommet de la terre de Rio de Janeiro, Brésil (SFDR, 2015-2030). En effet, l'objectif 9 insiste sur le renforcement de la résilience des infrastructures quant au principe 15 attire l'attention sur l'apport des mesures de précaution pour protéger l'environnement.

1.5 Démarche méthodologique

Pour atteindre les objectifs cités et apporter des éléments de réponse à notre problématique, le processus suivi repose sur quatre grandes étapes, pour la réalisation de ce travail de recherche, comme montré dans la Figure 1-1.

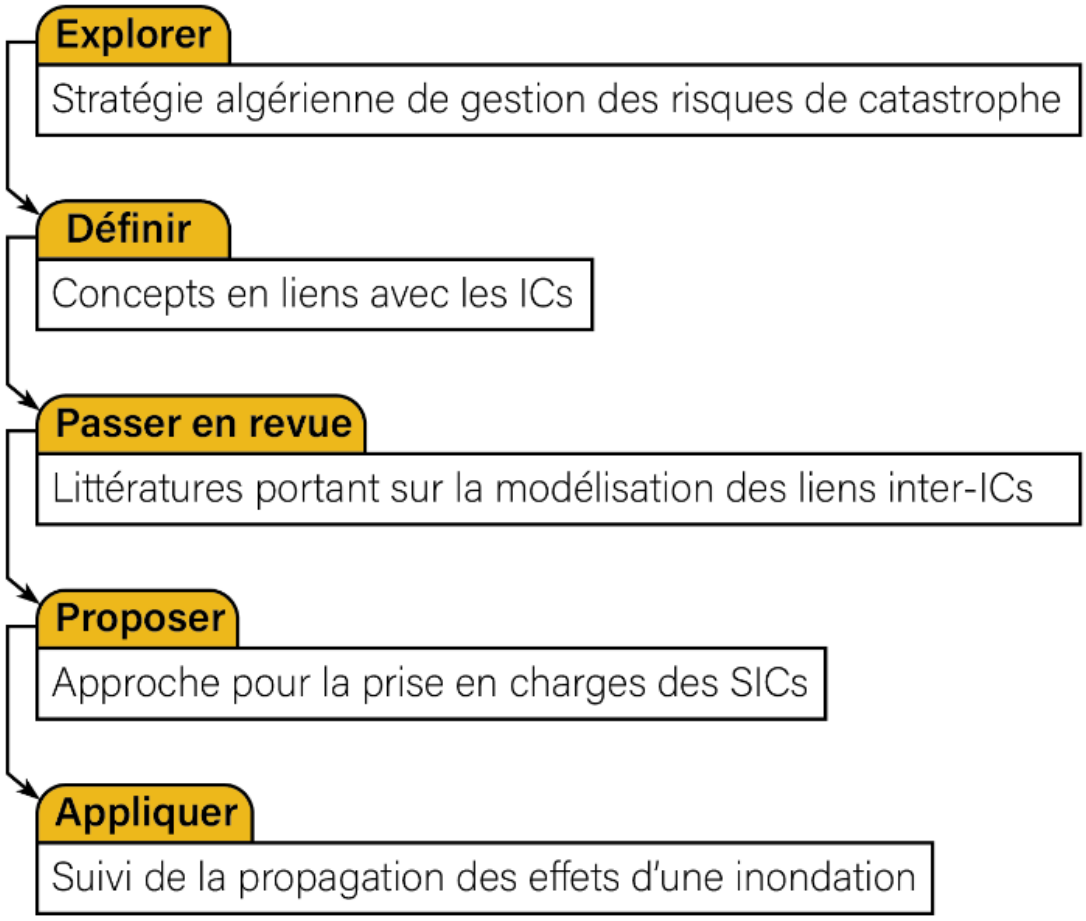


Figure 1-1 : Démarche méthodologique

Ces quatre étapes consistent en une :

1. Exploration de la stratégie algérienne de gestion des risques de catastrophe et la place des ICs dans cette dernière pour justifier l'intérêt de notre recherche ;

2. Définition de concepts en liens avec les ICs et quels sont les aspects à considérer pour pouvoir contribuer à leurs sécurisations ;

3. Revue de littérature sur la modélisation des liens inter-ICs et sur les travaux de recherche sur les SICs ;

4. Proposition d'une approche pour contribuer à l'intégration de ces SICs dans la stratégie algérienne de gestion des risques de catastrophe.

Les chapitres suivants aborderont plus en détails ces étapes.

En définitive, le contexte de ce travail concerne donc l'utilisation des ICs et leurs sauvegardes non seulement contre les effets de perturbations mais aussi contre les SICs avec lesquels ils sont en relation.

Ces objectifs nécessitent de bien corroborer l'ensemble des problématiques entourant les SICs et de bien valoriser l'apport de la modélisation des liens inter-ICs, dans la sécurisation de ces dernières. À cet effet, il y a lieu de prendre connaissance de la stratégie algérienne de gestion des risques de catastrophe et que préconise cette stratégie pour protéger ces SICs. Pour ce faire nous allons, dans ce qui suit, préciser les définitions et les concepts de base nécessaires à l'accomplissement de notre travail de recherche.

Chapitre 2

CHAPITRE 2 INFRASTRUCTURES CRITIQUES : DÉFINITIONS ET NOTIONS DE BASES

Avant d'aborder les notions de base propres aux ICs et pour se situer dans le temps, nous donnerons d'abord un bref historique sur ces ICs puis nous donnerons leurs différentes définitions et leurs classifications dans le monde.

Il est à noter que les auteurs, ayant abordé les SICs, utilisent souvent des appellations différentes les unes des autres. Cependant, toutes ces appellations visent à indiquer et à ressortir le caractère vital de ces infrastructures. Nous, nous joignons à l'avis de Pageon (2008) qui ne trouve aucune différence concernant l'utilisation terminologique des termes : Infrastructure Essentielle (IE), Infrastructure Critique (IC) ou Réseau Support à la Vie (RSV) car l'utilisation de ces derniers est justifiée seulement par le souhait de marquer leurs complexités et leurs importances vitales. D'ailleurs ces dénominations sont très proches de l'appellation anglaise *Lifline* ou *Critical Infrastructure System* (CIS) (Pageon, 2008).

Dans le cadre de cette étude, nous désignons un SIC (réseau de distribution des eaux, réseau électrique, réseau ferroviaire, réseau téléphonique, etc.) comme étant un regroupement d'ICs corrélées et inter-reliées, réparties dans le milieu urbain, dans le but d'accomplir une mission, bien définie, et dont la sécurité et le bien-être de la population dépend.

Les deux appellations (SIC et IC) seront donc utilisées dans la présente recherche.

2.1 Histoire et origine

Les ICs, sont plus que nécessaires pour le bon fonctionnement de nos milieux urbains, et ce sur plusieurs plans. Vu cette nécessité, leurs sauvegardes deviennent de plus en plus une priorité pour beaucoup de pays à travers le monde.

Les événements catastrophiques de cette dernière décennie, aussi bien en Algérie qu'à travers le monde, ont montré que ces infrastructures sont de plus en plus vulnérables et provoquent d'énormes pertes et de graves conséquences et parfois incontrôlables.

Nous avons déjà évoqué, les effets qu'a généré le séisme de Boumerdès en 2003 comme conséquence sur la société (Benouar et Meslem, 2007). En 2003, au mois d'août, l'Amérique

du Nord a connu un *blackout* suite à un arrêt total de la distribution de l'électricité qui a touché le Canada (province de l'Ontario) et huit autres États américains, New York, New Jersey, Connecticut, Vermont, Massachusetts, Michigan, Ohio, et la Pennsylvanie. Cette panne a non seulement touché plus de 50 millions de personnes sur une superficie de plus de 25 000 kilomètres carrés, mais elle a aussi empêché les autres systèmes d'infrastructure à accomplir leur missions (Zimmerman et Restrepo, 2006).Cette panne électrique est considérée comme la plus importante dans l'histoire de l'Amérique du Nord.

Selon les écris que nous avons explorés, les américains étaient les premiers à s'être intéressés à la problématique entourant les ICs. En effet, bien avant les attaques terroristes du *World Trade Center* en 2001, une démarche nationale avait été alors initiée.

En juillet 1996, l'administration du président des États-Unis d'Amérique (USA), Bill Clinton, ordonnait une étude nationale au sein d'une commission appelée : *The President's commission on critical infrastructure protection*, faisant associer le gouvernement et l'ensemble des intervenants dans la gestion des SICs. Cette étude avait comme objectif l'analyse des vulnérabilités et l'identification des éléments (Infrastructures) critiques pour le bon fonctionnement et la continuité normale de la vie sociale.

Le rapport résultant de cette étude, publié en 1997, démontrait irréfutablement la complexité et l'incompréhension des vulnérabilités de ces SICs dus essentiellement, à l'utilisation de l'information et à son partage entre intervenants. (U.S. DHS, 2004*)*. En mai 1998 et suite à ce dernier rapport, que la directive présidentielle américaine n° 63 qui encadre la stratégie américaine globale portant sur la protection des ICs publiques et privées, a été promulguée (U.S. G, 1998).

Cette stratégie était supportée par deux structures d'échelle fédérale à savoir :

✓ Le *Critical Infrastructures Assurance Office* (CIAO) qui coordonne les initiatives fédérales (niveau central) ;

✓ Le *National Infrastructures Protection Center* (NIPC) chargé de la collecte d'informations, de la surveillance et de l'alerte.

Suite aux attentats du *World Trade Center* de 2001, le Président des USA, Georges Walker Bush, met en place par décret le 17 décembre 2003 (U.S. G, 2003b), un plan national pour protéger les ICs et les ressources clés (stratégique) des USA. Ce plan repose essentiellement sur deux stratégies (Zimmerman et Horan, 2004) :

✓ Le *National Strategy for the Physical Protection of Critical Infrastructures*, qui définit les objectifs que les USA doivent atteindre ;

✓ Le *National Strategy to Secure Cyberspace* qui responsabilise chaque américain à sécuriser son propre espace cybernétique.

2.2 Infrastructures critiques et système d'infrastructures critiques

Après avoir expliqué dans quel contexte les américains ont commencé à se préoccuper des ICs., il est important de passer en revue les définitions, les plus utilisées, données aux ICs.

2.2.1 Définition et classification

Nous retrouvons dans la littérature plusieurs définitions des SICs et chacune d'elle met l'emphase sur quelques caractéristiques comme : la gestion de ces derniers, la nature des liens inter-infrastructures et certaines introduisent la notion de service essentiel.

En effet, les SICs sont un ensemble d'infrastructures civiles reliées physiquement, contrôlées par des opérations et dont la défaillance des missions affecte à plus ou moins long terme la santé et la sécurité de la collectivité. Un SIC transporte un élément qui peut être soit un service, soit une substance (Robert *et al*., 2003). Aussi, les SICs sont reparties sur un territoire donné, avec des liens directs ou indirects, qui assurent le bon fonctionnement d'une société par l'apport de services essentiels sur le plan de la santé de la sécurité et de l'économie (Robert *et al*., 2003).

Dans un milieu urbain, un réseau transporte un élément qui peut être soit une prestation de service, soit un élément physique (substance). De ce fait, les réseaux sont assimilés donc à un ensemble d'infrastructures reparties sur un environnement urbain ou un territoire donné, avec des liens directs ou indirects, qui assurent le bon fonctionnement d'une société par l'apport des services essentiels aux populations et ce sur le plan de la santé, de la sécurité, et de l'économie (Robert *et al.*, 2003).

Les réseaux sont en harmonies (liens spatial et fonctionnel) selon un aménagement bien établi, leurs développements et leurs évolutions rapides, la technologie utilisée, et la distribution géographique des populations qu'ils desservent, sont à même de créer des perturbations de plus en plus importantes.

La congestion de la circulation routière, les coupures de courant électrique et les pannes majeures des systèmes de communication provoquent des interruptions des services publics de première nécessité aux conséquences sociales considérables. En somme, les accidents deviennent de plus en plus imprévisibles (Perrow, 1984). Il est inutile de démontrer la gravité induite d'un dysfonctionnement quelconque suite aux perturbations (inondation, séisme, etc.).

Nous verrons dans ce qui suit comment sont définies et classées les ICs aux États-Unis et au Canada puis nous examinerons comment, ce type d'infrastructures, est considéré et défini en Algérie.

2.2.1.1 États-Unis d'Amérique

Le gouvernement américain considère les ICs comme étant des systèmes et des actifs, physiques ou virtuels, dont l'importance est telle que la destruction, totale ou partielle, de ces dernières aurait un impact grave sur la sécurité, la sécurité économique, la santé publique, ou toute autre combinaison de ces domaines (U.S. DHS, 2013).

Pour sa part et pour pouvoir les recenser, la *National strategy for the physical protection of cretical and key Assets* publiée en 2003 par la maison blanche (U.S. G, 2003a) recense 11 secteurs et 5 catégories d'ouvrages et d'ouvrages d'art.

Les onze Secteurs sont :

1 - L'Agriculture et l'alimentation
2 - L'eau
3 - La santé publique
4 - Les services d'urgence
5 - Les bases industrielles de défense
6 - Les télécommunications
7 - L'énergie
8 - Les transports
9 - Les services bancaires et financiers
10 - Les matériaux chimiques et dangereux
11 - Les postes et les services d'expédition

Les cinq Ouvrages sont :

1 - Les monuments nationaux et symboliques
2 - Les centrales nucléaires
3 - Les barrages
4 - Les édifices gouvernementaux
5 - Les édifices et les infrastructures commerciaux clés.

La catégorie des ouvrages a été rajoutée à la liste après les attentats du *World Trade Center*, de 2001 (U.S. G, 2003a).

2.2.2 Canada

Le département d'infrastructure canadien considère que le concept d'« Infrastructure » est fondamentalement dynamique : il évolue et s'étend de manière à englober de nouvelles catégories de biens qui sont essentiels au fonctionnement de l'économie et de la société. Dans son sens le plus strict qui est aussi son sens historique, l'expression « infrastructure » fait référence à ce qui est construit, soit l'infrastructure « matérielle », comme les routes et les égouts, etc. Au cours des 30 dernières années, le terme a pris un sens plus large pour inclure les biens construits mais mobiles, comme les trains et les véhicules servant au transport en commun, ainsi que les réseaux de biens construits, tel que les systèmes de distribution de l'eau potable et les systèmes de communication continentaux et mondiaux.

En effet, la défaillance de ces SICs peut entraîner de graves conséquences (Petit *et al*., 2004). D'ailleurs la Sécurité Publique Canada (SPC) recommande de leur donner toute l'attention nécessaire (SPC, 2008a).

La Sécurité Publique du Canada définit leurs ICs comme étant des installations, réseaux, moyens et biens physiques et ceux de la technologie de l'information, dont la défaillance ou la destruction entraînerait de graves répercussions sur la santé, la sécurité ou le bien-être économique des Canadiens et des Canadiennes, ou encore sur le bon fonctionnement des gouvernements du pays. Le Tableau 2- 1 nous montre les 10 secteurs et les domaines concernés.

Tableau 2-1 : Classification des SIC (SPC, 2008b)

Secteurs	Domaines
Énergie et services publics	Systèmes de production d'énergie électrique, de gaz naturel et de pétrole ainsi que leurs réseaux de transport
Technologie de l'information et des communications	Systèmes, logiciel, matériel et réseaux de télécommunications et de radiodiffusion, y compris l'internet
Finances	Système bancaires (Opérations, transactions, ..) valeurs mobilières et investissements
Soins de santé	Hôpitaux, établissements de soins de santé et de réserve de sang, laboratoires et produits pharmaceutiques
Nourriture	Sécurité, distribution, agriculture et industrie alimentaire
Eau	Eau potable et gestion des eaux usées
Transports	Voies aériennes, ferroviaires, maritimes et terrestres
Sécurité	Sécurité contre les armes chimiques, biologiques, radiologiques et nucléaires, matières dangereuses, recherche et sauvetage, secours d'urgence et barrages
Gouvernement	Services, installations, réseaux d'information, biens gouvernementaux et sites et monuments nationaux privilégiés
Fabrication	Base industrielle de la défense, industrie chimique

À la lecture du Tableau 2-1, nous remarquons aisément que les ICs touchent une panoplie de secteurs à buts différents mais contribuent effectivement tous au bien-être de l'individu.

Une étude des services de sécurité publique et protection civile Canada (SPPCC), portant sur la caractérisation et la hiérarchisation des liens inter-SICs, fait ressortir deux notions importantes qui nous permettront de comprendre la base de la caractérisation de ces infrastructures (SPPCC, 2003), ces notions sont :

✓ Le Réseau (Système d'infrastructure) : Un réseau peut être défini globalement selon deux principes distincts :

- L'ensemble d'infrastructures et de liens qui se ramifient et s'entrecroisent physiquement ou virtuellement comme :
    - Le réseau de distribution des eaux ;
    - Le réseau électrique ;
    - Le réseau ferroviaire ;
    - Le réseau téléphonique.

- L'ensemble d'infrastructures réparties sur un territoire donné, en relation directe ou indirecte les unes avec les autres et régies généralement par des directives similaires. comme :
    - Le réseau hospitalier ;
    - Le réseau d'alimentation ;
    - Le réseau routier ;
    - Le réseau aéroportuaire.

✓ Critiques : Ces réseaux remplissent des missions primordiales pour le bon fonctionnement d'une société, en assurant des services essentiels sur le plan de la santé, de la sécurité des populations et le bon fonctionnement de l'économie.

Les services de SPPCC ont identifié des critères pour classer ces réseaux. Ces critères ont une relation avec (SPPCC, 2003) :

✓ La définition du réseau et de ces composantes ;
✓ La mission pour laquelle un réseau donné a été conçu ;
✓ Le maillage ;
✓ L'interaction avec d'autres réseaux.

Le Tableau 2-2 indique en détail ces critères.

Tableau 2-2 : Caractérisation des réseaux par critères (SPPCC, 2003).

Critères	Interprétations
Maillage	Maillées ou réparties sur un territoire
Élément transporté	Transporter et contenir une substance (eau, gaz, pétrole, nourriture, etc.) ou fournir un service
Interaction entre réseaux	Interactions et liens avec d'autres réseaux (SIC)
Conséquences sur les populations	L'ampleur de la défaillance d'un réseau et des conséquences directes ou indirectes sur la vie des populations.

À partir de ces quatre critères, cinq (05) classes de SIC ont été identifiées par ce même groupe de recherche. Ces classes sont :

Tableau 2-3 : Caractérisation des SICs par classe (SPPCC, 2003).

Classe	Spécifications	Types de SIC
Classe A	Infrastructures maillées, supportant les fournitures de service avec de très nombreuses interactions avec d'autres réseaux.	Électrique Télécommunication Informatique Transport en commun
Classe B	Infrastructures maillées, permettant le transport d'une substance avec de nombreuses interactions avec d'autres réseaux.	Gaz naturel Carburants liquides Transport ferroviaire Eaux usées
Classe C	Infrastructures maillées, permettant le transport d'une substance et ayant de faibles interactions avec d'autres réseaux. Cette classe se distingue des précédentes par le fait que les conséquences d'une défaillance de ces réseaux ont un impact direct sur la population.	Eau potable
Classe D	Infrastructures réparties, pour la fourniture de service ayant des interactions avec d'autres réseaux variables. Les conséquences d'une défaillance de ces réseaux ont un impact direct sur la population.	Alimentation Hospitalier.
Classe E	Réseaux particuliers, infrastructures réparties ou maillées, conçus pour le transport de personnes et de substances variées et multiples ; ils ont des interactions avec d'autres réseaux variables. Les conséquences d'une défaillance de ces réseaux sont indirectes sur les populations.	Routier Aéroportuaire Maritime financier et banquier (maillé ou réparti) Sécurité publique Gouvernemental

La classification est d'une importance capitale faisant ressortir deux aspects. Le premier en relation avec la nature physique du SIC (maillé ou réparti) alors que le deuxième-fait ressortir les conséquences sur les populations (directes ou indirectes).

Le Tableau 2-4, en plus des aspects déjà cités, donne un aperçu plus général de la classification des SICs en mettant en évidence l'élément transporté et la nature de l'interaction entre SIC.

Tableau 2-4 : Synthèse de la caractérisation (SPPCC, 2003).

Critères	Classe des SICs				
	A	**B**	**C**	**D**	**E**
Élément transporté	Service	Substance	Substance	Service	Service ou substance
Maillage	Infrastructures maillées	Infrastructures maillées	Infrastructures maillées	Infrastructures réparties	Infrastructures réparties ou maillées
Interaction entre SIC	Très nombreuses	Nombreuses	Faibles	Variables	Variables
Conséquences populations	Indirectes	Indirectes	Directes	Directes	Indirectes
Classification du SIC	Électrique Télécom. Informatique Transport en commun	Gaz naturel Carburants Liquides Ferroviaire Eaux usées	Eau potable	Alimentation Hospitalier	Routier Aéroportuaire Maritime Financier Sécurité publique Gouvernement

Au cours des quinze dernières années, la notion d'infrastructure s'est encore élargie pour inclure :

✓ L'infrastructure immatérielle comme le capital humain ;

✓ L'infrastructure fondée sur le savoir, à la fois matérielle et immatérielle, comme les bases de données publiques, les établissements et les données de recherche et d'éducation, les réseaux de milieux d'affaires et d'universités.

Actuellement les SICs sont globalement catégorisés afin de les différencier d'autres réseaux qui ne sont pas autant reliés aux activités socio-économiques. Mais cette différentiation ne tient pas compte des spécificités de ces réseaux en termes de conséquence ou d'impact pour la société.

Le Tableau 2-5 ci-dessous illustre les 17 réseaux considérés comme essentiels (critiques) par les services de sécurité publique canadienne.

Tableau 2-5 : Caractérisation des SICs (SPC, 2008b).

Nº	SIC	Infrastructures/opérations
1.	Électrique	Production, transport et distribution de l'électricité. (gaz, hydraulique, nucléaire, etc.).
2.	Télécommunication	Communications par câbles, de satellites, d'ondes, de radios, etc.
3.	Informatique	Transfert de données et de connaissances codifiées numériquement. Les réseaux de contrôle à distance
4.	Transport en commun	Transport de passagers dans une zone urbaine. Routier ou ferroviaire.
5.	Gaz naturel	Extraction, stockage, transport distribution de gaz naturel.
6.	Carburant liquide	Extraction, stockage, transport distribution des carburants liquides.
7.	Ferroviaire	Transport, entreposage et la distribution de marchandises et de personnes par rails de trains.
8.	Maritime	Transport, entreposage et la distribution de marchandises et de personnes par bateaux sur la mer, fleuve ou lac
9.	Eau usée	La collecte, le transport et le traitement des eaux usées.
10.	Eau potable	Alimentation, le traitement et la distribution en eau potable de la population.
11.	Alimentation	La production, l'entreposage, le transport et la distribution de marchandises nécessaires à l'alimentation humaine.
12.	Santé	Soins de santé à la population (hôpitaux, cliniques, ambulances, etc.).
13.	Routier	Transport de marchandises et de personnes par le biais de routes, autoroutes, ponts, échangeurs, viaducs, etc.,
14.	Aéroportuaire	Transport de marchandises et de personnes par le biais d'avions.
15.	Financier	Agences bancaires, les bourses, guichets automatiques, etc.
16.	Sécurité publique	Sécurité et la protection des biens et des personnes (police, gendarmerie, pompier, etc.).
17.	Gouvernemental	Administration publique

En examinant le Tableau 2-5, nous remarquons que tous ces réseaux ont une relation directe ou indirecte avec la population et ceux pour ses besoins vitaux d'où la notion du SIC.

En effet, ces derniers sont multiples et variés par leurs natures, mais aussi par leurs fonctions, et ils peuvent offrir des prestations et transporter une panoplie d'éléments et de substances (eau, gaz, etc.).

2.2.3 Algérie

L'Algérie n'adopte aucune définition pour ses ICs et elle ne dispose d'aucune liste permettant leurs identifications ou leurs inventaires. Aussi, la dernière loi (04/20) relative à

la prévention des risques majeurs et à la gestion des catastrophes dans le cadre du développement durable aborde les infrastructures, sans traiter leurs problématiques, encore moins la définition qu'elle donne à ces dernières. Néanmoins, et dans le cadre des dispositifs de sécurisation stratégiques ladite loi évoque sommairement l'importance des infrastructures suivantes (G A, 2004) :

- ✓ Routières et autoroutières ;
- ✓ Télécommunications et liaisons stratégiques ;
- ✓ Bâtiments stratégiques.

Deux éléments sont à constater en examinant la loi, mentionnée ci-dessus. Le premier est que cette dernière est restée sans la promulgation de la totalité des textes d'applications, du moins pour ce qui est de la sécurisation des ICs, le deuxième est que les infrastructures citées dans la loi n'englobent pas la totalité des ICs, comparées à celles inscrites dans la liste américaine ou canadienne et encore moins la manière de prendre en charge leurs vulnérabilités.

Après avoir passé en revue la manière avec laquelle les chercheurs à travers le monde et les fonctionnaires du SPPCC abordent la notion d'ICs et leurs caractérisations, nous aurons certainement à adapter ce type de classification à la réalité algérienne. En effet, dans le cadre de notre recherche une définition et une liste d'ICs, inspirées de celles déjà recensées, seront proposées aux autorités algériennes concernées.

2.3 Fonctionnement d'un SIC

Le fonctionnement d'un SIC dépend particulièrement de la ressource transportée et des liens inter-ICs. Dalleurs, Wallace *et al* rappellent qu'il est important de comprendre ces liens pour mettre en place les bons mécanismes de gestion afin d'assurer la continuité de services en cas d'incident. Les SICs sont un assemblage d'éléments physiques avec des activités associées qui correspondent aux tâches nécessaires pour opérer les éléments physiques (Wallace *et al*., 2001).

Petit *et al* admettent qu'il est possible de caractériser les SICs selon leurs fonctionnements par la mise en valeur, l'importance et l'efficience de leur mission principale (fonction pour laquelle un IC est conçue), de leurs opérations (actions directes ou indirectes

sur l'ensemble ou des parties du réseau afin de réaliser les missions) et de leurs infrastructures (installations nécessaires à la réalisation des opérations) (Petit *et al.*, 2004).

La Figure 2-1 présente un schéma de fonctionnement global d'un SICs (infrastructure essentielle) composé d'infrastructures et d'opérations dédiées à la réalisation de missions.

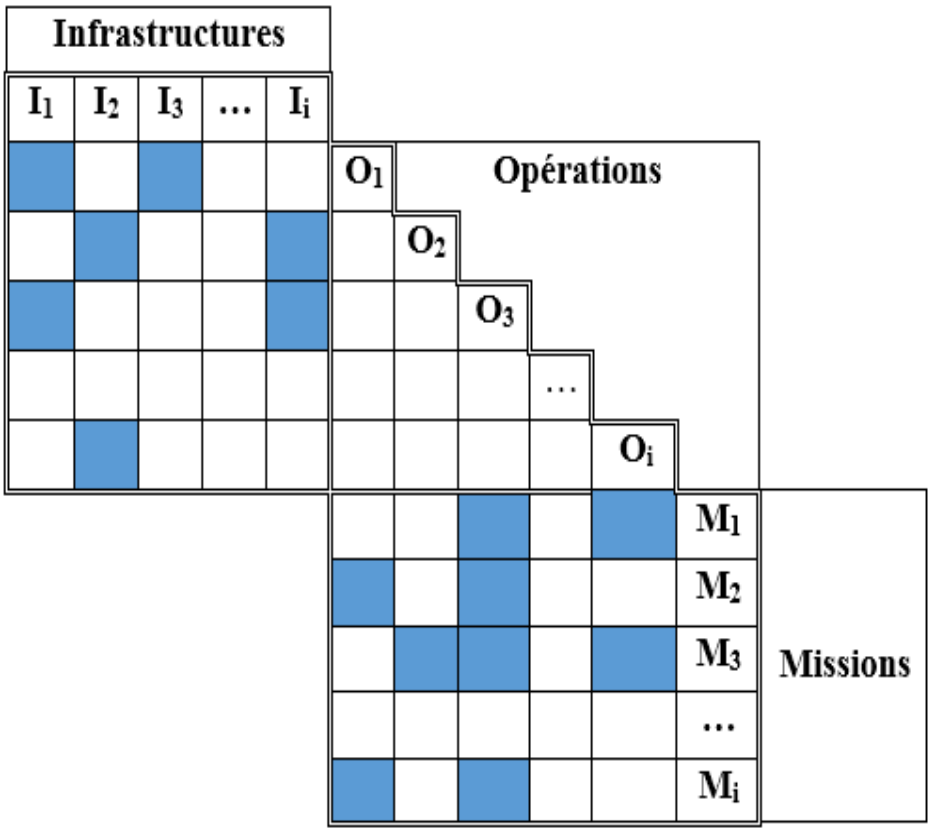


Figure 2-1 : Caractérisation d'un SICs (Robert *et al.*, 2004).

Ainsi, par exemple pour la réalisation de la Mission M_2, nous aurons besoins de 2 Opérations [O_1 et O_3]. Ces deux dernières Opérations sont respectivement soutenues par les Infrastructures [I_1 et I_2] et [I_1 et I_i]. Infrastructure, Opération et Missions sont dépendantes et tous les ICs peuvent se décomposer ainsi.

Nous donnerons l'exemple du réseau d'eau comme illustré par le Tableau 2-6 ci-dessous.

Tableau 2-6 : Décomposition d'un réseau d'eau (*inspiré :* Robert et *al.*, 2003).

Désignation	**Domaine**
Missions	Fournir une eau de qualité pour la consommation humaine, fournir de l'eau (volumes et pressions) lutte contre l'incendie.
Infrastructures	Barrage, canalisations, station d'épuration, réservoirs, système de pompes, etc.
Opérations	Exploitation, Pompage, régulation, vidanges des réservoirs, des conduites, etc.
Activités	Maintenance, Réparation, détections des fuites.

Ainsi, pour remplir la mission de disponibilité d'eau de qualité pour la consommation humaine, des infrastructures sont nécessaires comme les usines de traitement de l'eau potable et le réseau de distribution. Pour mener à bien cette mission dans le temps, des opérations (pompage, traitement, etc.) et des activités sont nécessaires (d'entretiens, réparation, etc.).

Le tableau 2-7 illustre d'une manière générale la décomposition d'un SIC.

Tableau 2-7 : Décomposition d'un réseau SIC (Robert *et al*., 2003).

Réseau				
Ressources (R)	Infrastructure (I)	Operations (O)	Activité (A)	Mission (M)
Éléments matériels, opérationnels, humains et naturels permettant la réalisation des activités.	Composantes matérielles conçu pour assurer le fonctionnement des activités du réseau. Ces installations sont nécessaires à la réalisation des opérations.	Processus technique actions directes ou indirectes sur l'ensemble ou des parties du réseau pour réaliser les missions. Automatisées (informatique-électronique) ou manuelles,	Actions nécessaires et devant être exécutées pour permettre la réalisation des missions.	Mission pour laquelle un SIC a été conçu et réaliser.

2.3.1 Défaillance d'un SIC

Selon Plamondon Marie. E. Parent, 2004, les SICs permettent de réaliser toutes les activités socio-économiques en temps dit normal. Elles peuvent les paralyser lorsqu'émerge une défaillance résultant d'une perturbation, et ainsi générer des conséquences graves (Plamondon, 2004). Nous pouvons alors distinguer deux types d'origines : les aléas internes (humains et techniques, etc.) et les aléas externes (naturels, malveillants, etc.) tel que mentionnée dans la Figure 2-2.

Un SIC entre en défaillance lorsqu'il ne remplit plus ou partiellement ses missions, suite aux dysfonctionnements d'une ou plusieurs opérations et/ou activités.

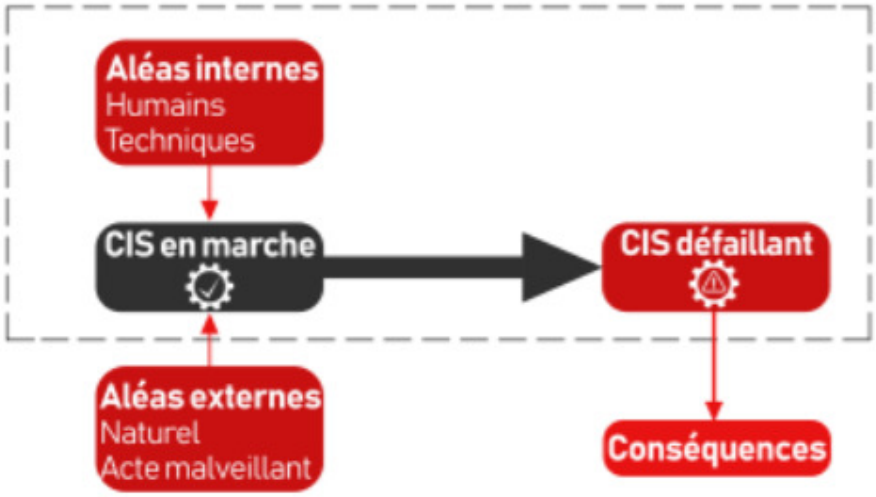


Figure 2-2 : Défaillance d'un SIC suite aux différents aléas

Petit explique également qu'une défaillance découle d'une vulnérabilité du SIC, c'est-à-dire lorsqu'une opération d'une infrastructure n'est plus efficiente (Petit, 2008). Ainsi, l'ampleur de la vulnérabilité dépend de l'importance des infrastructures, non efficientes, impliquées dans l'accomplissement de la mission d'un SIC.

2.4 Missions et différents états de fonctionnement d'un SIC

Tout dépend de la nature de l'aléa et de la perturbation, induite, à laquelle il peut faire face, la mission principale d'un SIC peut être compromise et son fonctionnement altéré. L'altération peut s'accentuer dans le temps et dans l'espace.

Dans ce qui suit nous examinons comment se comporte un système soumis à des perturbations.

2.4.1 État de fonctionnement

Petit rappel la prépondérance de la notion d'état d'un système dans la gestion des risques. Il insiste sur le fait que la caractérisation de l'état du système est au centre de l'analyse des risques qui englobe la vulnérabilité du système, l'aléa et la résilience (Petit,

2009). En effet, ce dernier concept implique la capacité d'un système à s'adapter, résister et à rebondir et reprendre un état optimal une fois affecté.

Petit en s'intéressant aux différents états que peut connaître un système vis à vis de la mission qu'il doit assurer, identifie alors trois états (Petit, 2009) :

✓ L'état de fonctionnement « normal » pour lequel le système a la capacité de remplir sa mission ;

✓ L'état de fonctionnement « dégradé » pour lequel le système fonctionne avec certaines composantes dégradées sans qu'il y ait un impact considérable sur sa mission ;

✓ L'état de fonctionnement « défaillant » pour lequel, le système ne remplit plus sa mission ce qui a des conséquences sur son environnement.

Le passage d'un état à l'autre se fait selon des seuils fixés en fonction d'un système donné. En conséquence, il y aurait le seuil de dysfonctionnement entre deux états « normal » et « dégradé » et le seuil de défaillance entre les états « dégradé » et « défaillant ».

Dans la prochaine section nous aurons à caractériser les ICs selon deux états (fonctionnel et dysfonctionnel).

2.5 Caractérisation des infrastructures critiques

Pour atteindre les objectifs de notre recherche, pour des fins de caractérisation des SICs, nous aurons à identifier les effets d'impact des perturbations sur le fonctionnement de ces SICs que nous caractérisons par deux états, un fonctionnel et l'autre dysfonctionnel.

2.5.1 États fonctionnels

La caractérisation des infrastructures (fonctionnelles) est faite par plusieurs propriétés comme (Mc Daniels *et al*., 2007) :

- **L'Opérabilité** exprimée en pourcentage (0-100%) indiquant également la qualité de service fournie au réseau donc au SIC ;
- **L'Intégrité** définie par au moins un seuil de service fourni et peut également être appliquée au réseau et à ses services échangés ;
- **Les Mesures d'atténuations** permettant le maintien minimal du service ;

- **Les « Entrées »** est une faible variable indépendante de la sortie. Elles sont souvent référées aux ressources reçues (matières premières) ou en tant que services reçus (eau, énergie électrique, etc.) ;
- **Les « Sorties »** est une variable dépendante de l'entrée et des processus internes de l'infrastructure et également de la demande formulée pour satisfaire le besoin de la ville ;
- **Les Processus internes** concernent les activités de transformation et des opérations au sein de l'infrastructure elle-même.

Au sein de l'infrastructure, un ou plusieurs processus peuvent avoir lieu pour transformer les entrées en sorties (Rowell et Wormley, 1997). Cette caractérisation sera utilisée, dans notre modèle, pour formaliser la génération de la mission d'une IC. En effet, ces processus transforment les ressources d'entrées en une mission principale bien définie.

Lors de l'aménagement, d'un espace urbain, les différents états des missions d'une IC doit être pris en considération pour développer des moyens palliatifs, nécessaires à la continuité d'activités d'une ville, en cas de perturbations survenant après une catastrophe.

2.5.2 États dysfonctionnels

Plusieurs auteurs décrivent que les états dysfonctionnels, possibles, des SICs dépendent de la nature d'interdépendance et des effets dominos induits. Ces états créent des vulnérabilités et peuvent générer des conséquences selon une certaine criticité.

- L'interdépendance est considérée comme une relation bidirectionnelle entre deux ICs dont l'état de l'une est influencé ou est en corrélation avec l'état de l'autre (Rinaldi *et al.*, 2001), (Peerenboom, 2001). Le Tableau 2-8 illustre les quatre catégories.

Tableau 2-8 : Type d'interdépendance (Rinaldi *et al.*, 2001).

Interdépendances			
Physiques	Cybernétiques	Géographiques	Logiques
Lien matériel utilisé pour recevoir des ressources ou pour émettre un produit dont le SIC est supposée fournir	Informatique comme support d'échange	Deux SICs ou plus se partagent un espace limité. L'appartenance à cet espace génère souvent des effets entre systèmes.	Liens financiers ou réglementaires.

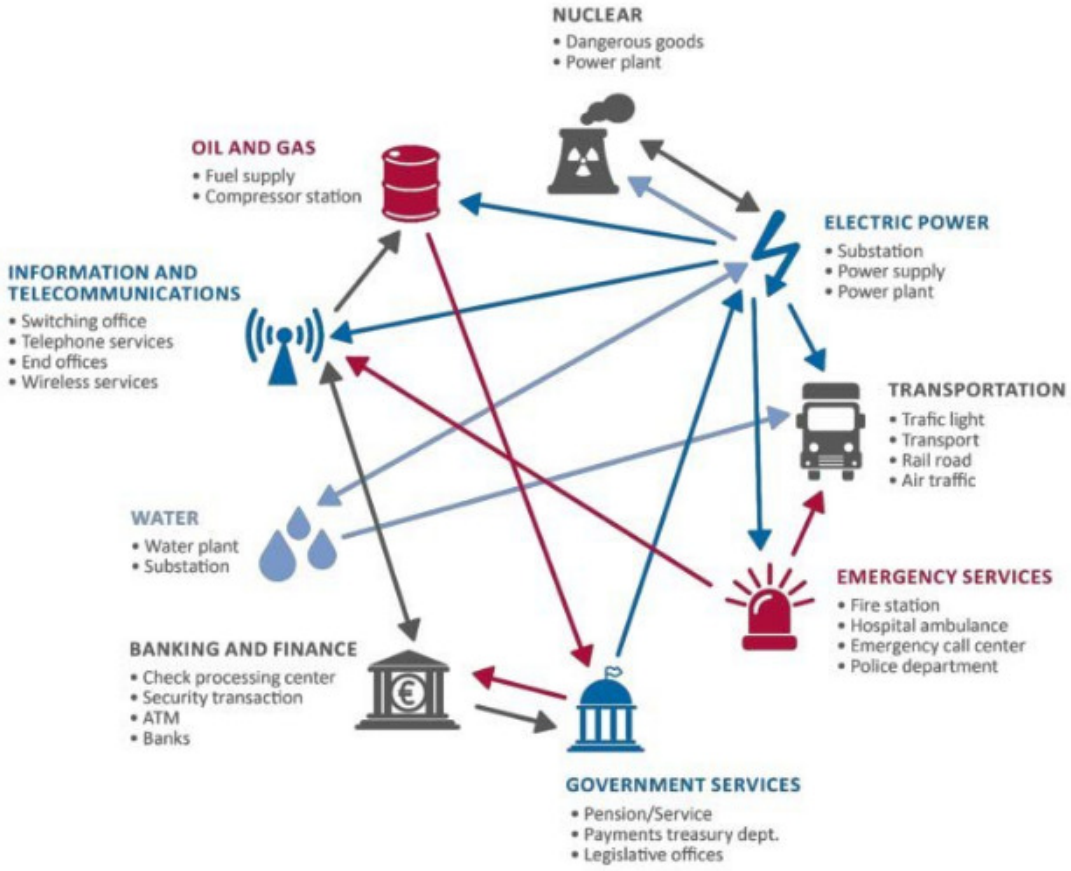


Figure 2-3 : Représentation d'interdépendances inter-SICs (Peerenboom, 2001)

Nous constatons que la Figure 2-3 met en évidence le besoin de chaque SIC vers d'autres SICs pour fonctionner. Comme c'est le cas, des réseaux d'électricité et des télécommunications où l'un ne peut fonctionner sans l'autre. La protection totale de notre société ne peut se faire sans, entre autre, la compréhension du comportement des SICs face à leurs dépendances et leurs interdépendances.

Les interdépendances font partie intégrante de la conception et du fonctionnement d'une infrastructure, mais peuvent générer une vulnérabilité d'une ampleur beaucoup plus grande que n'importe quel système isolé : l'interdépendance entre ICs provoque également la propagation des perturbations (Schneider, 1999). En outre, ces interdépendances ne cessent d'augmenter, cet état de fait accroit les risques de défaillance en cascade.

Il est plus qu'utile d'intégrer les méfaits des dépendances des SICs dans la stratégie algérienne.

- **Les Effets dominos**, d'après ce que nous avons relaté, sont véhiculés par les liens existants entre les ICs appartenant à un même SIC mais aussi entre SICs. En effet, suite à ces liens des défaillances, à répercussions multiples, par le biais d'effets dominos naissent (Plate, 1996 ; Allen, 1997 ; Moses, 1998 ; Lemperiere, 1999). Ces derniers causent une amplification de la vulnérabilité de nos villes.

Les ICs possèdent des liens d'interdépendances, de type physique, les effets dominos possibles sont une suite d'événements en cascade où les conséquences d'un accident antérieur sont augmentées jusqu'à provoquer un accident majeur (Reniers et Cozzani, 2013).

Nous reconnaissons deux types d'effets dominos ; internes et externes. Les effets dominos internes commencent dans l'IC elle-même alors que les externes débutent dans le voisinage de ces ICs (Reniers et Cozzani, 2013). Le terme propagation est alors utilisé. Ce dernier signifie, que l'impact est ressenti sur plus d'un système, souvent selon un effet domino (Zimmerman, 2002).

Il y'a lieu de mettre en place immédiatement des moyens dans le but de se protéger face aux effets dominos (Amin, 2002).

La protection des SICs face aux effets dominos se trouve être une mission difficile. Cette difficulté réside dans la complexité de ces derniers, l'accès aux paramètres à prendre en compte, la multitude des intervenants, le nombre élevé d'interactions et le manque d'un modèle mathématique permettant la prise en charge des difficultés citées (Amin, 2002). Nous pouvons ainsi identifier les difficultés qu'il faut rayer afin de pouvoir donner une réponse adéquate pour la protection des SICs interdépendants.

Pour ce qui est de l'Algérie, et d'après les rencontres que nous avons eu avec les différents gestionnaires des principaux réseaux (eau, gaz, etc.), aucun de ces gestionnaires ne nous a mentionné l'existence de procédures permettant de faire face aux effets dominos externes ni l'interdépendance entre les ICs, d'où la nécessite de prendre en compte les effets d'interdépendances et leurs effets dominos dans la stratégie Algérienne. Il apparaît donc indispensable de mettre en place des mesures pour protéger les SICs des risques de défaillances en cascades.

- **La Vulnérabilité** de la ville est accentuée par ses propres SICs et de leurs interdépendances. En effet, en prenant seulement trois réseaux (électriques, télécommunications et le transport), nous parviendrons à affirmer qu'il y a effectivement un accroissement de la vulnérabilité lors de l'arrêt de l'un de ces 3 réseaux (Amin, 2002).

En plus, l'accélération de l'urbanisation et le progrès technologique rend nos villes toujours plus vulnérables à des défaillances en cascades causées par des événements naturels, environnementaux et techniques (Lewis et Mioch, 2005).

D'ailleurs, les attaques terroristes contre le *World Trade Center* en 2001 (Mendonça et Wallace, 2006), et la panne d'électricité de 2003 en Amérique du Nord avait paralysé les télécommunications, les transports et même le secteur financier et les banques, ce qui a entrainé un dérèglement généralisé du fonctionnement de la société sur un laps de temps non négligeable avec tous les désagréments que cela peut engendrer.

Les réseaux algériens ont leurs propres spécificités, vu que certaines infrastructures sont relativement jeunes, simples dans leur conception et leur gestion (technologie simple). Penser à étudier la vulnérabilité de nos réseaux, en ce moment, nous éviterait d'énormes problèmes, étant donné que l'Algérie a connu, ces vingt dernières années, une forte édification de plusieurs nouvelles infrastructures (autoroute, centrale électrique, etc.).

- **La criticité** est liée aux conséquences d'une perturbation du fonctionnement d'une infrastructure (Herder et Thissen, 2003). Cela explique les grandes divergences sur l'appréciation de la criticité ou voire même le degré d'essentialité de ces ICs. Pour cette raison, la modélisation de tous les aspects en lien avec les ICs reste un travail difficile à faire. La criticité des infrastructures est due à (Amin, 2000) :

  - La multi-échelle, multi-composantes, hétérogène et la distribution dans l'espace urbain et surtout sur les aires d'influence ;

- La vulnérabilité aux perturbations se propageant instantanément ;
- Aux points d'interaction multiple en augmentation avec le nombre de participants.

La caractérisation des ICs, faite dans cette section, est d'une importance capitale dans la mesure où elle permet une première compréhension du fonctionnement et de l'importance des ICs. Néanmoins, toute infrastructure peut être considérée comme critique dans certaines circonstances et conditions.

2.6 Condition de fonctionnement

La norme *Canadian Standard Association* (CSA) CAN/CSA Z1600 (CSA, 2008), portant sur la gestion des mesures d'urgence et de la continuité des activités, s'agissant des seuils de tolérance entre des états, mentionne que les organisations industrielles, pour fonctionner, doivent définir leurs exigences minimales non seulement en termes de ressources (le personnel, les infrastructures, les installations) mais aussi en termes de temps afin de garantir la disponibilité de leurs produits, prestations et services.

De même, les travaux, de Rinaldi *et al.*, sont très importants dans la mesure où nous pouvons avoir un réseau en difficulté ou en voie d'être défaillant, car les auteurs nous indiquent que l'état de fonctionnement d'un SIC varie d'un niveau optimal à un niveau de défaillance, et selon eux, un SIC peut fonctionner dans un état qui n'est pas optimal, sans impact sur les utilisateurs, selon certaines conditions (Rinaldi *et al*, 2001). À cet effet il y a lieu de préciser que les méthodes d'analyse essayent d'identifier les causes pouvant, par exemple, rendre un SIC défaillant ou hors usage dans la mesure où il ne remplit plus sa mission.

Cet état se situe entre un niveau optimal et un niveau défaillant. Il évoluerait selon des critères ou facteurs (Rinaldi *et al*, 2001) :

- ✓ De fonctionnement : toutes les procédures permettant la sauvegarde de l'infrastructure en cas de dysfonctionnement ;
- ✓ Organisationnels : tout ce qui a trait à l'environnement interne de l'organisation et de son mode de fonctionnement ;
- ✓ Temporel : l'infrastructure peut avoir de différents flux dans le temps (dynamiques). Le facteur temps nous renseigne sur la nature de l'interdépendance ;
- ✓ Spatial : l'infrastructure peut influer sur un espace géographique.

Les éléments apportés montrent bien que la connaissance, des conditions de fonctionnement, et de l'état de fonctionnement et de dysfonctionnement d'un SIC est un élément central et nécessaire pour la gestion des risques pour ce genre d'infrastructure. Le prochain chapitre traitera les concepts généraux de la gestion des risques.

Chapitre 3

CHAPITRE 3 CONCEPTS GÉNÉRAUX DE GESTION DE RISQUES

Dans ce chapitre, nous abordons les différents aspects entourant la gestion de risque, nous définissons également quelques termes afin de faciliter la compréhension de notre cadre d'étude.

La sécurisation des SICs passe par une parfaite gestion des risques. Cette dernière se base fondamentalement sur l'analyse de ces mêmes risques. Une nouvelle approche pour la gestion de risque, dans son volet analyse, est donc proposée.

Cette approche « par effet » se base sur le suivi des effets d'une perturbation bien avant la rupture de la mission d'un système. L'approche en question se démarque du reste des méthodes d'analyse de risque et permet de préconiser des mesures, de prévention, pour renforcer le niveau de résilience des sous-systèmes les plus déterminants dans la réalisation de la mission d'un SIC.

À cet effet, il est important de signaler que les risques à analyser, peuvent-être la propagation des effets (dominos) d'une ou plusieurs perturbations impactant les ICs. Ces effets en question génèrent à leurs tours d'autres risques comme : la dégradation, non accomplissement voire même la perte (cessation) de la mission globale d'un SIC. Les risques cités peuvent avoir des conséquences sur la population occupant une zone urbaine donnée.

Le but recherché est la contribution, par l'instauration d'une méthode, pour la gestion de ces risques contre les aléas susceptibles d'altérer la mission d'un SIC, basée sur les liens inter-ICs, par la mise en place de mesure de sécurité et le renforcement de la résilience de ces ICs.

3.1 Description d'une infrastructure

Cremona (2002) considère qu'une infrastructure ou un système génie civil (ouvrage ou ensemble d'ouvrages) peuvent être définis d'une part, par ses éléments structurels (sous-systèmes) qui les composent et d'autre part, par les fonctions qu'ils accomplissent ou tout simplement par les missions qu'ils sont censés accomplir.

À chaque niveau de décomposition du système, les éléments structurels remplissent à leur tour des fonctions qui contribuent à la réalisation des fonctions globales de

l'infrastructure comme l'illustre l'exemple (Figure 3-1). Ainsi, le barrage comme infrastructure (système) et son masque, en amont, comme sous-système, illustre la notion de mission et de sous mission que nous venons d'expliquer (Cremona, 2002). Cette décomposition sera utilisée plus tard pour formaliser la mission d'une IC avec et sans dégradation. Ainsi, Cremona (2002) mentionne deux types d'analyses permettent de définir une infrastructure : une structurelle et une autre fonctionnelle.

La performance est l'aptitude d'une infrastructure à remplir les fonctions pour lesquelles elle a été conçue. Ainsi, les performances d'une infrastructure sont amenées à évoluer durant sa vie. Nous pouvons constater que les fonctions initialement prévues lors de la construction peuvent être modifiées volontairement par le gestionnaire ou encore par des événements extérieurs et des perturbations peuvent aussi dégrader ou altérer les missions initiales. Ces perturbations peuvent être causées entre autres par des catastrophes d'origine multiples.

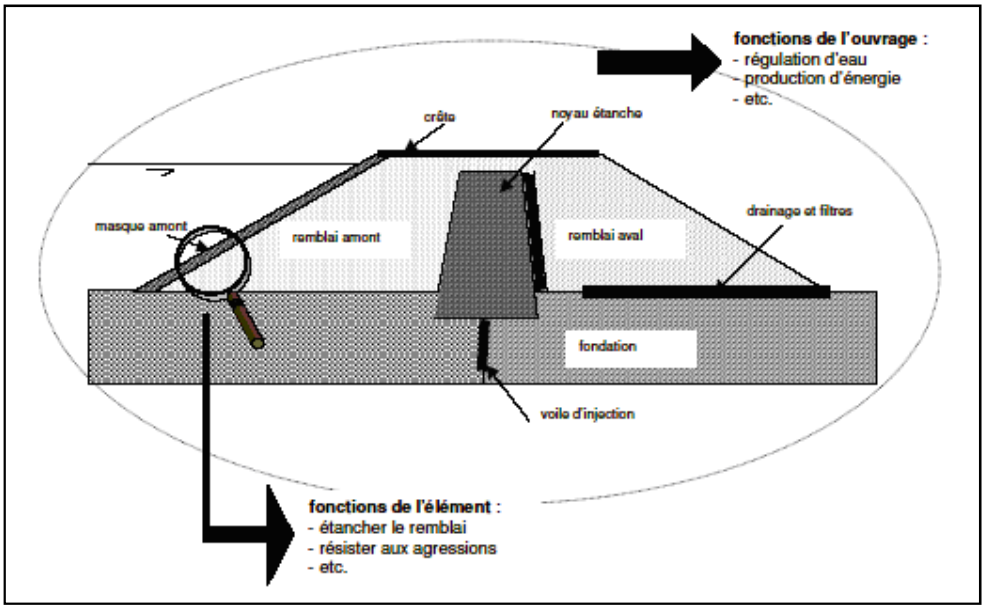


Figure 3-1 : Composants et fonction d'un système : Barrage en terre (Peyras, 2002)

Selon le même auteur, trois principales causes peuvent provoquer la dégradation de la mission d'une infrastructure affectant par la suite sa performance : (Cremona, 2002)

- ✓ Vieillissement de l'infrastructure ;
- ✓ Erreurs humaines ;
- ✓ Évènements extérieures prévus ou imprévus.

Dans notre approche méthodologique, nous considérons ces trois causes (aléas internes et externes), comme l'origine des perturbations, possibles auxquelles les SICs peuvent faire face.

Deux catégories de perte de performance sont considérées comme l'illustre la Figure 3-2 :

✓ La dégradation liée à une diminution de la performance d'une fonction (mission) restant néanmoins supérieure au seuil fonctionnel ou à l'état-limite (état ou phénomène que l'on souhaite éviter) (Cremona, 2002). Renforcer la résilience d'un système serait, justement, de le maintenir dans cette catégorie en cas de perturbations.

✓ La défaillance liée à « l'altération ou la cession de l'aptitude d'un système à accomplir sa ou (ses) fonction(s) requise(s) avec les performances définies dans les spécifications techniques » (Cremona, 2002). Dans ce cas, une au moins des performances est inférieure au seuil fonctionnel.

Pour réunir les deux catégories de performance nous proposons la définition suivante : la défaillance se réfère à un certain niveau variable (augmentation, dégradation, altération, rupture) de l'aptitude d'un système à remplir sa ou ses missions requises avec les performances nominales. Ainsi, même une variation positive de performance, par rapport aux spécifications, serait considérée comme une défaillance.

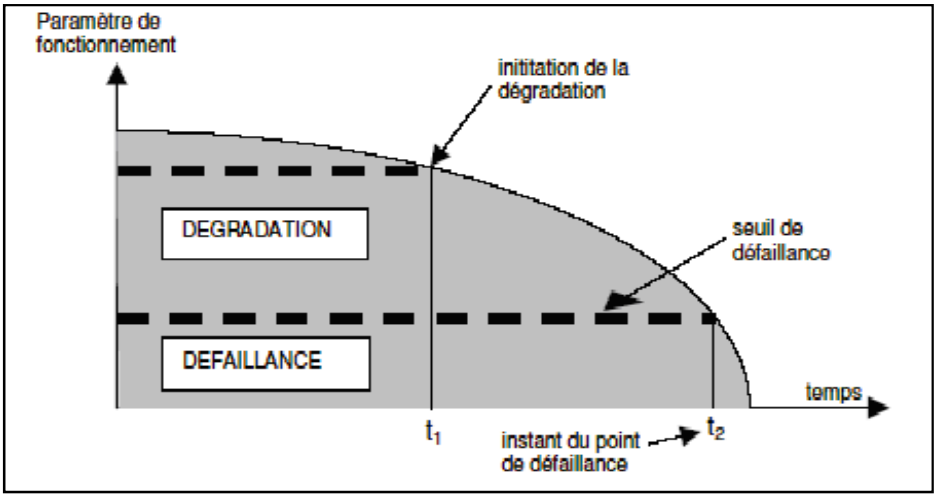


Figure 3-2 : Dégradation et défaillance (Zwingelstein, 96)

La performance d'un système est caractérisée par plusieurs critères, définis par la norme française (NF X60-500), notamment :

✓ La fiabilité est l'aptitude de l'infrastructure à assurer ses fonctions, dans des conditions données, pendant une période de temps donnée ;

✓ La durabilité est l'aptitude à demeurer en état d'accomplir ses fonctions, dans des conditions données d'utilisation et de maintenance, jusqu'à ce qu'un état limite soit atteint.

Cette façon d'approcher la performance d'une infrastructure est plus qu'intéressante, car elle nous permet de bien appliquer notre modèle, et nous renseigne également sur la localisation des principales causes, de perturbation, pouvant provoquer la dégradation de la mission d'une IC.

3.2 Définitions

Dans le but de bien cerner notre travail, il est nécessaire de bien définir les notions de risque, danger, aléa et vulnérabilité.

3.2.1 Risque

Le risque est un concept qui a évolué dans le temps et qui reste aujourd'hui très nuancé selon le domaine auquel il se rattache. En effet, il n'est pas aisé de trouver une définition générale susceptible d'être retenue et chaque domaine de recherche donne sa propre définition du risque. Cependant, nous pouvons dire que le risque est la possibilité qu'un ou plusieurs faits ou évènements non souhaités (ENS) surviennent ainsi que les conséquences induites à toutes ces possibilités, mais nous retrouvons plusieurs autres définitions dans la littérature scientifique :

Villemeur considère que le risque mesure le danger « Le risque est une mesure d'un danger associant une mesure de l'occurrence d'un événement indésirable et une mesure de ses effets ou conséquences » (Villemeur, 1988).

La loi cadre 04-20 (algérienne) définit le risque majeur comme toute menace probable pour l'homme et son environnement pouvant survenir du fait d'aléas naturels exceptionnels et/ou du fait d'activités humaines (GA, 2004).

La directive « Seveso II » définit le risque comme : « la probabilité qu'un effet spécifique se produise dans une période donnée ou dans des circonstances déterminées. De ce fait, un risque se caractérise par deux composantes : la probabilité d'occurrence d'un

événement donné et la gravité des effets ou conséquences de l'événement supposé pouvoir se produire » (Council Directive, 1996).

Nous retenons, dans le cadre de cette recherche, que le risque est la probabilité d'occurrence d'un ENS causant des effets, ayant des conséquences variables, sur des cibles. Dans notre cas, les ENS proviennent des aléas internes et externes qui affecteront les ICs plus exactement aux niveaux de leurs composantes.

Dans une démarche de sécurisation, le risque est un concept clé autour duquel gravitent d'autres notions qui le complètent, notamment le danger, la vulnérabilité et l'aléa.

3.2.2 Danger

Le danger est un événement ou une situation susceptible d'entraîner des conséquences négatives ou dommages à l'homme et/ou à l'environnement (Villemeur, 1988).

Cette définition est plus qu'intéressante dans la mesure où les perturbations affectant les SIC ont des impacts sur la population plus exactement dans ses besoins.

3.2.3 Aléa

Ce mot d'origine latine qui signifie "coup de dé", peut se définir comme un " hasard favorable ou non ; un risque d'incident défavorable, d'inconvénients " (Petit Larousse), ou encore un " aspect imprévisible que peut prendre une activité " (Encyclopédie Hachette).

Ces définitions, issues des dictionnaires, montrent que le terme de risque rentre dans la définition de l'aléa, alors que la communauté scientifique différencie nettement entre ces deux notions (Henry, 2004).

Depuis que la recherche fondamentale et appliquée s'intéresse au problème des risques, elle a cherché à préciser son langage et à fixer des définitions claires quant aux caractéristiques des événements considérés. D'autres définitions méritent d'être citées comme :

Gendreau (1999) considère l'aléa, comme une menace caractérisée par des propriétés physiques et une probabilité d'occurrence. Cette définition est en adéquation avec celle des Nations Unies (UN *International Strategy for Disaster Reduction*), qui évoque l'événement

menaçant ou probabilité d'occurrence dans une région et au cours d'une période donnée d'un phénomène pouvant engendrer des dommages.

Dauphiné (2001) préconise d'ajouter à la probabilité d'occurrence d'un phénomène, l'intensité et la durée de ce dernier et aussi l'espace qu'il affecte.

3.2.4 Vulnérabilité

Selon les auteurs, les définitions données à la vulnérabilité considèrent plusieurs paramètres : géographiques, sociaux ou économiques. Ces paramètres font naitre de larges divergences dans la définition de la vulnérabilité. Parmi les définitions existantes, on peut retenir :

Celle de Gendreau, qui caractérise la vulnérabilité comme étant la fragilité des installations humaines dans l'absolu (Gendreau, 1999). Cette notion s'appréciera de la même façon pour un élément donné quels que soient sa position et le risque considéré. Elle est mesurée par une période de retour, ce qui s'accorde avec la dimension de l'aléa (Henry, 2004).

Avoir à statuer sur une définition générale de la vulnérabilité est une tâche difficile car elle fait intervenir de multiples facteurs : les dimensions physiques, économiques, sociales, matérielles, etc.

Néanmoins, nous considérons, dans le cadre de ce travail de recherche, que la vulnérabilité est la sensibilité active (temps et espace) d'un système face aux perturbations pouvant compromettre sa fonction requise.

3.3 Risques et milieu urbain

Le milieu urbain génère des risques endogènes (technologiques, sociaux, sanitaires, sociétaux) et tend à aggraver et accélérer la survenue des risques naturels. Le risque est encore plus accru vu la forte concentration humaine sur des espaces urbains réduits.

Metzger et D'Ercole considèrent que les risques urbains sont souvent considérés comme majeurs étant donné le fort endommagement en ville. En effet, Il existe beaucoup plus d'éléments exposés aux aléas, la population étant en premier rang, mais les villes sont aussi le cœur localisé et matérialisé de systèmes économiques, politiques, institutionnels et logistiques, éléments essentiels non seulement du fonctionnement urbain mais des sociétés modernes en général (Metzger et D'Ercole, 2011). L'accroissement de la vulnérabilité de nos

milieux urbains, est dû à la rapidité de la croissance urbaine et la forte implantation des SICs, pour répondre aux divers besoins de la population.

3.4 Approches méthodologiques pour la gestion des risques

Le risque est un problème multi face et doit être étudié avec des méthodes appropriées pour aider à la prise de décision. Pour évaluer les risques, les chercheurs en gestion des risques utilisent des processus très systémiques. En effet, l'approche méthodologique proposée pour le suivi des effets de perturbations le long d'un SIC se base sur cette vision systémique.

Par ailleurs, Mitchell *et al* (2004), soulignent qu'il est primordial de commencer par comprendre le risque avant de passer à son évaluation (Figure 3.3). La phase de compréhension est décisive. Les sources des ENS (évènement redouté) ainsi que leurs fréquences permettent d'approcher le risque à sa juste valeur.

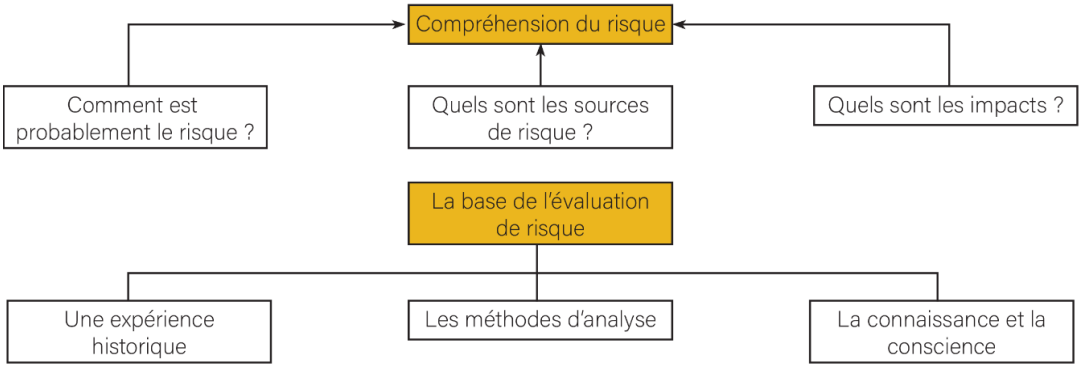


Figure 3-3 : Élément de base pour la compréhension du risque (Mitchell *et al*., 2004).

3.4.1 Gestion des risques

La gestion du risque se décompose en plusieurs étapes et phases d'analyse chacune obéissant à certaines règles et exigences pour justifier la mise en place de mesures et d'actions de maitrises (ISO 31000). La gestion des risques intervient tout au long de la vie d'un système.

Selon toutes ses formes, la gestion de risque aboutirait, principalement, à la réalisation des deux éléments de base suivants :

✓ La prévention qui est le processus amont fondé sur la modélisation des transformations et l'observation régulière de variables représentatives d'un système ;

✓ L'anticipation débutant dès que les indicateurs atteignent des valeurs définies pouvant mener à des conséquences graves (seuils d'avant dégradation, seuils de dégradation, etc.).

Dans la présente recherche, la prévention et l'anticipation seront réalisées consécutivement par la modélisation de la propagation des effets suite à des perturbations et par le renforcement de la résilience des ICs.

3.4.1.1 Étapes

La gestion des risques est un processus dont le but est de prévenir et résoudre les problèmes en matière de sécurité que présente un système ou un sous-système. Ainsi, la finalité est la maitrise de ces risques selon l'environnement et les conditions d'exploitation qui s'imposent. La Figure 3-4 présente les quatre phases de la gestion des risques qui sont :

1. Identification des sources de dangers ;
2. Estimation du risque ;
3. Évaluation du risque ;
4. Réduction du risque inacceptable.

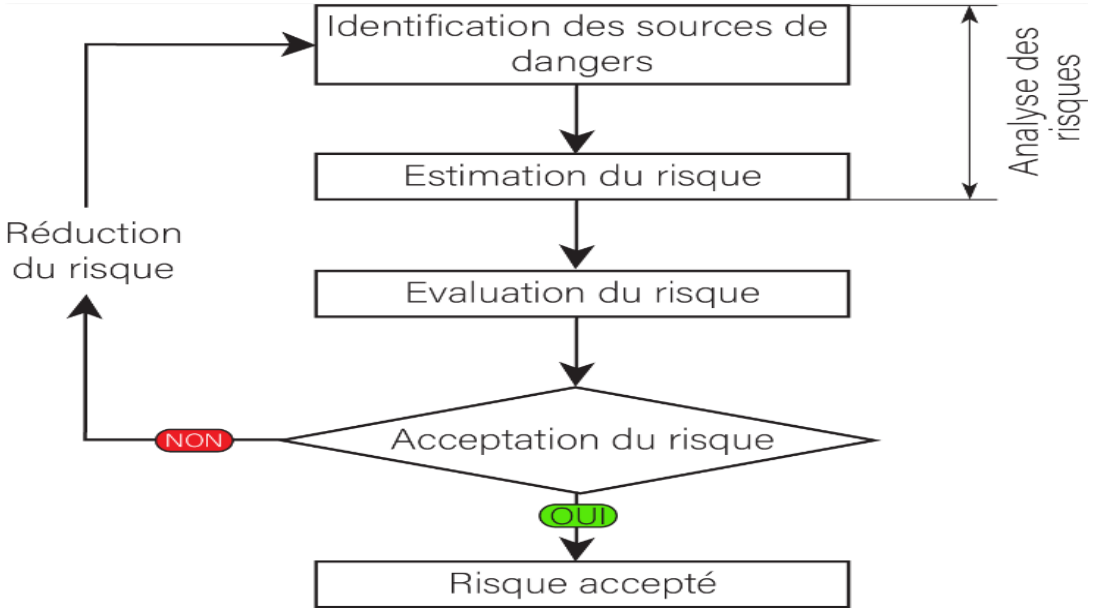


Figure 3-4 : Processus de la gestion des risques, adapté de (AFNOR, 1988)

L'analyse de risque se trouve au cœur de la gestion des risques. Elle précède l'évaluation qui déterminera si le risque est accepté ou non et dans ce cas s'il y'a lieu de le maîtriser ou le réduire.

Un aperçu de quelques méthodes d'analyse est donné dans ce qui suit.

3.5 Outils d'analyse des risques

La mise en place des mesures de sécurisation des infrastructures passe, entre autres, par une analyse du risque de dégradation de leurs missions. Elle permet d'étudier les effets induits suite à d'éventuelles perturbations. Pour mener cette étude, une nouvelle approche est utilisée.

Avant de présenter le cadre méthodologique de cette approche, il est judicieux d'explorer quelques méthodes d'analyse de risque les plus souvent utilisées en ingénierie.

Nous donnons une brève description des principales méthodes d'analyse utilisées dans une démarche de la gestion de risques. Ces méthodes se divisent, principalement, en deux catégories comme le montre la Figure 3-5 :

- Méthodes qualitatives ;
- Méthodes quantitatives.

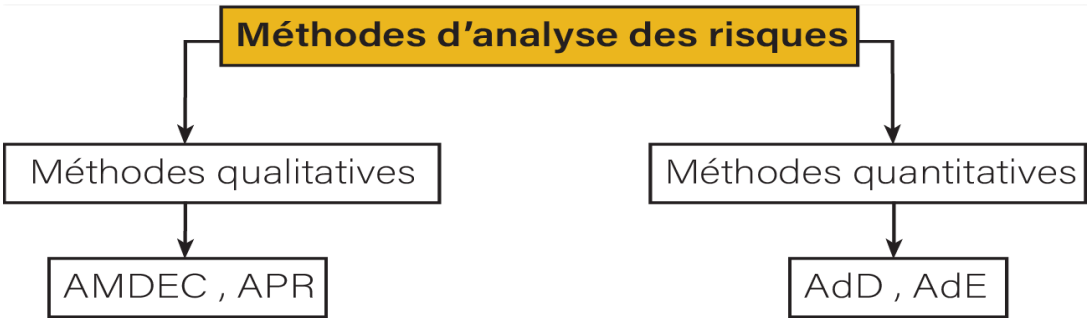


Figure 3-5 : Types de méthode d'analyse des risques

3.5.1 Méthodes qualitatives

L'analyse qualitative des risques constitue un préalable à toute autre analyse. En effet elle permet la bonne compréhension et la connaissance systématique du système étudié et de ses composants. Pour une bonne évaluation qualitative du risque, cette approche ne s'appuie pas explicitement sur les données chiffrées, mais elle se réfère à des observations pertinentes sur l'état du système et surtout sur le retour d'expérience (REX) et les jugements

d'expert. Cette approche nécessite alors une très bonne connaissance des différents paramètres et causes liés au système étudié. Dans quelques études de gestion de risque, cette approche peut être suffisante pour atteindre les objectifs voulus si elle est bien menée et justifiée (Mazouni, 2008).

L'Analyse Préliminaire des Risques (APR) et l'Analyse des Modes de Défaillance et de leurs Effets et leurs Criticités (AMDEC) font partie des nombreux outils d'analyse et d'évaluation des risques à caractère qualitatif. Ces deux dernières méthodes sont détaillées dans ce qui suit :

3.5.1.1 Analyse Préliminaire des Risques

La norme CEI-300-3-9, décrit l'APR comme étant une technique d'identification des fréquences de danger « L'Analyse Préliminaire des Risques (APR) est une technique d'identification et d'analyse de la fréquence du danger qui peut être utilisée lors des phases amont de la conception pour identifier les dangers et évaluer leur criticité ». Un bref descriptif de cette technique d'analyse sera présenté ci-dessous (CEI 300-3-9, 2015) :

- ✓ **Domaine d'application**

L'APR est applicable à tout type de système et comme son nom l'indique, c'est une méthode généralement utilisée afin d'identifier les risques au stade préliminaire de la conception d'un système. Cette méthode est aussi appliquée dans le cadre des études de danger car elle ne nécessite pas une connaissance approfondie du système étudié (Debray *et al*., 2006).

En ce sens, cette méthode s'avère pertinente dans les phases de conception d'un système et de son exploitation.

- ✓ **Principe**

L'APR s'occupe, en un premier temps, de recenser les éléments dangereux relatifs au système étudiée et cela après avoir effectué une décomposition fonctionnelle de ce dernier en sous-système. Ces éléments dangereux peuvent être (Debray *et al*., 2006) :

- Un produit transporté ou stocké (eau, inflammable, explosive, etc.), mélange de produits susceptibles de provoquer un phénomène dangereux ;
- Des équipements dangereux, par exemple : réservoir de grande capacité, pompe, etc. ;

- Des opérations dangereuses, par exemple : vidange rapide, opération d'urgence, traitement (par une substance) interne d'un château d'eau.

Pour chaque élément dangereux préalablement recensé, l'APR vise à identifier une ou plusieurs situations dangereuses (SD) susceptibles de se produire en présence d'une source de danger ou d'un élément causant la SD.

Cette dernière peut engendrer un ENS lorsqu'elle est suivie d'un évènement initiateur ou un élément causant un autre ENS.

Pour chaque SD, il faut envisager les causes susceptibles de provoquer l'ENS et les conséquences qui découlent de leur apparition. Ensuite l'APR est appelée à identifier les sécurités existantes sur le sous-système étudié. Si ces dernières sont jugées insuffisantes pour réduire le risque à un niveau acceptable, des propositions d'amélioration doivent être envisagées.

✓ **Étapes de déploiement**

Schématiquement, la méthode est classée parmi les méthodes mixtes (inductives et déductives) qui consistent à déterminer les accidents potentiels que peuvent provoquer les ENS.

Le support utilisé pour le déroulement de la méthode est un tableau (Mortureux, 2002). Le Tableau 3-1 en est un exemple mettant en évidence le déploiement de la méthode :

Tableau 3-1 : Déploiement de l'APR.

Sous-système	Élément Dangereux	Situation Dangereuse	Cause	Conséquence	P	G	C	Mesure de prévention	P'	Mesure de protection	G'	C'	Proposition

En se basant sur le REX et les connaissances des experts, chaque sous-système identifié dans la phase de décomposition fonctionnelle a été revu, et les SD ont été examinées de manière systématique.

À partir du Tableau 3-1, une démarche systématique est suivie sous la forme suivante :

- **Étape 1 :** Décomposition fonctionnelle de chaque système, L'APR s'appuie au début, sur la décomposition fonctionnelle du système étudié en sous-systèmes détaillés afin de faire ressortir les parties pouvant être à l'origine d'un ENS.

- **Étape 2 :** Énumération des éléments dangereux (ED). À partir de cette décomposition, les ED qui constituent un danger pour le système sont énumérés. Ce dernier peut être un équipement ou un produit transporté ou approprié au sous-système.
- **Étape 3 :** Identification des SD, elle se fait sur la base de REX et la connaissance des experts pour identifier les SD réelles se rapprochant du sous-système en question.
- **Étape 4 :** Identification d'un évènement non souhaité (ENS). Après l'apparition de chaque SD en présence d'un évènement initiateur, résulte un événement non souhaité susceptible d'infliger un dommage à des cibles vivantes ou matérielles.
- **Étape 5 :** Détermination des causes et conséquences. L'énumération des causes susceptibles de provoquer directement une SD et un ENS est un élément essentiel pour faire ressortir les conséquences qui en découlent.
- **Étape 6 :** Évaluation du risque par calcul de la criticité (C). Une probabilité d'occurrence (P) de l'ENS et la gravité de ses conséquences (G) sont attribués, sans prise en compte des barrières de sécurité existantes et en utilisant des échelles de cotation. Cela permet ensuite de calculer la criticité (C) à l'aide de la grille de criticité pour positionner le risque (risque acceptable, tolérable, inacceptable).
- **Étape 7 :** Réévaluation du risque par calcul de la criticité (C'). La réévaluation se fait après avoir considéré la mise en place des mesures de prévention et de protection qui permettent la réduction de la criticité d'un risque (niveau acceptable ou tolérable). Cette réévaluation permet de nous assurer le niveau de confiance des barrières de sécurité.
- **Étape 8 :** Proposition donnée sous forme de mesures de maîtrise des risques pour améliorer le niveau de sécurité. En dernier, si tous les enchainements ont été étudiés, le choix d'un nouvel ED pour le même sous système s'impose, sinon lorsque tous les ED appropriés au sous-système ont été examinés, il faut procéder au choix d'un nouveau sous-système ou d'un système.
- **Étape 9 :** Classification des risques identifiés sur la grille de criticité, afin de positionner les risques dans leur niveau approprié. Ces grilles permettent de faire apparaître les risques inacceptables et critiques qui doivent être traités par des approches spécifiques.

3.5.1.2 Analyse des Modes de Défaillance et de leurs Effets et leurs Criticités

En 2007 et selon Landy, qui considère l'Analyse des Modes de Défaillance et de leurs Effets et leurs Criticités (AMDEC) comme étant une technique fondamentale d'identification et d'analyse de la fréquence des dangers qui analyse tous les modes de

défaillances d'un système donné et leurs effets tant sur les sous-systèmes que sur le système lui-même. En effet, l'AMDEC est une analyse de problème potentiel et non pas une analyse de problème avéré (Landy, 2007).

- ✓ **Domaine d'application**

L'AMDEC se trouve parmi les méthodes les plus répandues en ingénierie du fait, qu'elle s'adapte à l'étude des défaillances de matériaux et d'équipements et peut s'appliquer aussi à des systèmes et des infrastructures de différentes technologies (électrique, mécanique, hydraulique…).

- ✓ **Principe**

Cette analyse vise d'abord à identifier l'impact de chaque mode de défaillance des composants d'un système sur ses diverses fonctions et ensuite hiérarchiser ces modes de défaillances en fonction de leur facilité de détection et de traitement (Debray *et al*., 2006).

L'AMDE(C) traite des aspects détaillés pour démontrer la fiabilité et la sécurité d'un système. Elle s'articule autour de quatre (04) parties primaires :

1. Identification des modes de défaillance ;
2. Identification des causes potentielles de chaque mode ;
3. Estimation des effets engendrés ;
4. S'il s'agit d'une AMDEC : évaluation de la criticité de ces effets.

L'analyse commence toujours par l'identification des défaillances potentielles des modes opérationnels. Elle se poursuit, par des inductions afin d'identifier les effets potentiels de ces défaillances (SD, évènement dangereux et dommages). Une fois les effets potentiels établis, le risque, en spécifiant les actions de contrôle, est estimé.

- ✓ **Déroulement**

Le déroulement de l'AMDEC est donné dans le Tableau 3-2 (Ridoux, 2002) :

Tableau 3-2 **:** Déploiement de l'AMDEC.

Sous-système	Composant	Fonction	Mode de défaillance	Causes	Effets	P	G	D	C	Mesure de prévention	P'	C'

Les étapes de l'AMDEC sont :

- **Étape 1** : Choisir les éléments ou composants du sous-système identifié lors de la décomposition fonctionnelle. Les sous-systèmes sont choisis selon leur importance dans la réalisation de la mission du système.
- **Étape 2** : Décrire la fonction du composant choisi pour l'analyse afin de déterminer ses liens avec les autres équipements.
- **Étape 3** : Retenir un mode de défaillance susceptible d'apparaitre dans le composant en question. La définition du mode possible de défaillance pour un équipement peut être réalisée à partir du REX et des connaissances d'experts.
- **Étape 4** : Identifier les causes de chaque mode de défaillance ainsi que les conséquences tant au niveau sous-système que sur tout le système.
- **Étape 5** : Procéder à l'évaluation de la criticité de ce mode de défaillance en termes de probabilité et de gravité. Ensuite positionner les modes de défaillance sur une grille de criticité pour situer leurs classements.
- **Étape 6** : Prévoir des mesures ou moyens supplémentaires si l'évaluation du risque le recommande.
- **Étape 7** : Réévaluer après mise en place des mesures de sécurité et vérifier que le couple (P, G) peut être jugé acceptable et enfin, envisager un nouveau mode de défaillance et reprendre l'analyse. Si tous les modes de défaillances ont été examinés, le choix d'un nouveau composant s'impose.

3.5.2 Méthodes quantitatives

L'analyse quantitative des risques, quand elle est possible, contribue à la bonne prise de décision pour la maitrise de certains risques. Cette approche consiste à caractériser les différents paramètres d'analyse des risques par des mesures probabilistes.

L'analyse passe généralement par un traitement mathématique en prenant en compte les données relatives aux différents paramètres évalués et aussi aux informations qui sont de nature quantitative.

Dans la perspective de l'application de cette démarche, une attention particulière aux données utilisées, à leur origine et à leur adéquation aux cas étudiés doit être portée car une simple erreur remettra en cause l'étude (Mazouni, 2008).

3.5.2.1 Arbre de défaillance

L'analyse par Arbre de Défaillances (AdD) est employée pour identifier les causes relatives aux événements redoutés (ER) selon une démarche déductive (effet à causes). En partant d'un événement unique, il s'agit de rechercher les combinaisons d'événements conduisant à la réalisation de ce dernier. L'analyse par AdD peut également être utilisée dans le cadre d'une reconstitution des causes d'un accident (Debray *et al*., 2006).

La méthode consiste en une représentation graphique des multiples causes d'un ER. Elle permet de visualiser les relations entre les défaillances des sous-systèmes, les erreurs humaines et les facteurs environnementaux qui peuvent conduire à des accidents. Les facteurs reliés aux aspects organisationnels peuvent être eux aussi considérés.

L'analyse par AdD se déroule généralement en trois étapes :

- Spécification du système et de ses frontières ;
- Spécification des ER préalablement identifiés
- Construction des arbres de défaillances : Les ER, sont considérés un par un et les successions ainsi que les combinaisons d'événements de base permettant de les atteindre sont identifiés.

En outre, un événement de base doit être :

- Indépendant des autres événements de base ;
- Non décomposable en éléments plus simples ;
- Fréquence évaluable.

Le calcul de la probabilité de l'événement sommet se fait à travers la propagation des probabilités d'occurrence des événements de base vers le sommet. Le calcul des coupes minimales peut s'effectuer avec le même principe en essayant de trouver les plus petits ensembles d'événements de base pouvant mener à un ER. Ceci permettrait de hiérarchiser les événements et d'implanter stratégiquement les barrières de défense afin d'améliorer la fiabilité et la sécurité en même temps.

Une coupe minimale représente la plus petite combinaison d'évènements (chemin critique) pouvant conduire à un événement indésirable (intermédiaire) ou redouté (final). Plus l'ordre d'une coupe minimale est petit, plus l'occurrence de l'événement final suivant ce chemin critique peut paraître probable.

L'affectation des probabilités des événements de base se fait par extraction des bases de données, essais, REX, jugement d'experts, audits, etc.

3.5.2.2 Arbre d'évènement

L'analyse par Arbre d'Évènements (AdE) est une technique d'identification et d'analyse de la fréquence des dangers moyennant un raisonnement inductif (causes à effets) pour convertir différents événements initiateurs en conséquences éventuelles, relatives au fonctionnement ou à la défaillance des dispositifs techniques / humains / organisationnels de sécurité (Debray *et al*.,2006).

À l'inverse de l'analyse par AdD, l'analyse par AdE suppose la défaillance d'un composant ou d'une partie du système et s'attache à déterminer les évènements qui en découlent.

L'analyse par AdE se déroule en plusieurs étapes préliminaires :

- Considération d'un événement initiateur (EI) ;
- Identification des fonctions de sécurité prévues pour contrôler son évolution ;
- Construction de l'arbre ;
- Description et exploitation des séquences d'évènements identifiées.

Il serait plus pertinent d'élaborer une Analyse par l'AdE à l'issue d'une première analyse identifiant les accidents potentiels comme l'APR.

Les fonctions de sécurité doivent être assurées par des barrières ayant pour objectif d'empêcher le processus de matérialisation d'un accident provoqué par un EI.

La construction de l'arbre consiste à envisager soit le bon fonctionnement soit le dysfonctionnement de la première fonction de sécurité en partant de l'EI.

La suite de la méthode consiste à examiner le développement de chaque branche en considérant systématiquement le fonctionnement ou la défaillance de la fonction de sécurité jusqu'à l'atteinte d'un accident potentiel. La propagation des probabilités d'occurrence des évènements initiateurs permet de calculer la probabilité de l'évènement catastrophique.

3.6 Discussion autour des méthodes d'analyse de risque

Les méthodes d'analyses (quantitative et qualitative) que nous venons de voir nous permettent d'écrire les scénarios plausibles d'accidents. Ainsi, un scénario est un enchaînement d'événements allant d'un événement initiateur à un accident, dont la séquence et les liens logiques découlent de l'analyse de risques.

Souvent, seuls les scénarios les plus dévastateurs sont pris en considération. Ces scénarios sont estimés en combinant la probabilité d'accident et la gravité des conséquences.

Une telle façon d'estimer le risque de dégradation ou de perte de mission d'un SIC a des inconvénients.

En effet, le fait de ne considérer que les conséquences très graves (pire scénario) implique l'utilisation de très faibles valeurs de probabilités. Comme la gravité des conséquences, de ces évènements, sont très importante sur le milieu urbain. Le risque, une fois évalué, correspond au produit d'une faible probabilité par une très grande gravité et cela sous-estime le risque analysé. Aussi, le fait de ne considérer que le pire scénario fait abstraction des situations intermédiaires, plus probables, mais avec des conséquences moins graves, qui pourraient conduire à la perte de la mission d'un SIC. De telles situations peuvent survenir avec le vieillissement des ICs, ou les dysfonctionnements de ses composantes. En plus, l'ignorance de la forte interdépendance des infrastructures provient du fait que la majorité des types de perturbation qui causent de graves effets en cascade font partie des événements «à faible probabilité et à impact élevé» (Dunn, 2005).

Pour une analyse de risque plus complète il y'a lieu de considérer la propagation des effets tout le long des ICs d'un SIC.

Une approche dite « par effet » est proposée, basée sur le suivi des effets d'une perturbation bien avant la rupture de la mission d'un système. La modélisation des liens inter-ICs est plus que nécessaire pour le dit suivi.

Après avoir exploré les méthodes d'analyse de risque, nous passons dans le chapitre qui suit à la présentation de nos travaux de recherche appuyé par une revue de la littérature sur les ICs.

Chapitre 4

CHAPITRE 4 REVUE DE LITTÉRATURE SUR LA MODÉLISATION DES LIENS INTER-ICs

La revue de littérature qui suit, nous permettra de corroborer tous les aspects entourant les ICs et nous indiquera de quelle façon les approcher pour les sécuriser.

Ensuite, elle nous éclairera sur la manière d'intégrer, réellement, ces aspects, dans la stratégie algérienne, en s'inspirant, bien sûr, de la grande expertise qu'ont de nombreux pays dans ce domaine. Cette revue de littérature passe par la présentation, dans un premier temps, des écrits portant sur l'interdépendance et les effets dominos au sein des ICs et leurs modélisations. Dans un deuxième temps nous explorons quelques travaux scientifiques réalisés et nous finissons en abordant le concept de résilience et la résilience urbaine.

4.1 Interdépendances et effets dominos

Après avoir passé en revue les définitions attribuées aux SICs pour montrer la valeur de ces réseaux pour la société, nous tenons à souligner l'importance des interdépendances et des effets dominos qui les caractérisent. Cet état de fait met en évidence le niveau de complexité de ces derniers.

4.1.1 Liens inter-ICs

Little (2002) indique que malgré les menaces dont font l'objet les ICs, un grand nombre des défaillances trouve l'origine dans la complexité de ces systèmes, eux-mêmes, et de leurs nœuds. En effet, ces derniers sont des points d'intersections créant une dépendance entre les systèmes.

Cette section nous permettra de comprendre comment un lien inter-ICs peut agir directement sur l'état de fonctionnement et par voie de conséquence sur la mission du SIC.

Robert *et al.* mentionnent que la propagation de la vulnérabilité est le résultat d'un dysfonctionnement qui trouve son support dans les liens entre les infrastructures « Cette interrelation permet la répercussion d'une vulnérabilité d'un réseau origine à un réseau de destination par le biais d'infrastructures et/ou d'opérations » (Robert *et al.*, 2003).

Little trouve que des interdépendances sont générées quand il y'a la transmission d'effets de rupture d'une infrastructure à une autre et que cette dernière générera encore plus d'impact sur une troisième infrastructure et ainsi de suite (Little, 2002).

Quant à Rinaldi *et al*. (2001), ils rappellent que les dépendances et les inters-connexions font que les ICs forment des systèmes encore plus complexes. Ils soulignent également que la nature du lien influe fortement sur leurs caractéristiques opérationnelles. À cet effet, ignorer ces liens peut avoir des conséquences non seulement supplémentaires mais aussi compromettantes (une source de dangers supplémentaires) pour le bon fonctionnement de la société.

Robert *et al*. (2003) décrivent qu'un lien direct peut être unidirectionnel comme le transfert de substance d'un réseau (origine) vers un autre réseau (destination), pour ce qui est du lien bidirectionnel, c'est le transfert qui se fait dans deux sens c'est à dire origine/destination et vice-versa. En effet, les liens favoriseront la propagation des défaillances et de ses effets.

4.1.2 Interdépendances et effets dominos

Robert préconise une démarche de prévention, appliquée aux interdépendances et aux effets dominos, qui se préoccupe plus de l'anticipation des conséquences néfastes et de la communication entre ICs dans un espace de coopération et de collaboration entre les intervenants basé sur l'échange d'informations (Robert, 2008). Donc, il devient plus aisé d'évaluer la vulnérabilité des SICs dans une perspective de sécurisation.

Ainsi, les gestionnaires des SICs doivent emprunter une attitude proactive devant des défaillances ou les interdépendances sont les principales causes.

C'est pour cela, que le dernier auteur recommande de reconnaître les liens et que les gestionnaires des ICs appartenant à l'espace de coopération doivent s'informer (en temps et lieu) de l'état de la ressource véhiculée par un SIC donné (eau, gaz, électricité, etc.).

La difficulté d'accomplir une mission est considérée comme une défaillance, nous assistons alors à une altération ou une dégradation de la mission et par voie de conséquence une détérioration de la qualité de la ressource fournie.

Quant à Michel-Kerjan (2003), il regarde les SICs comme des systèmes, complexes, d'éléments en perpétuel interaction, qui deviennent de plus en plus concentrés et connectés. Et selon lui, certains de ses éléments (ICs) sont plus critiques et pourraient, en cas de défaillance, affecter toute une région ou un pays tout entier (Michel-Kerjan, 2003).

4.2 Modélisations des liens inter-infrastructures critiques

C'est au début du XXIe siècle que Rinaldi, Peerenboom, et Kelly (Rinaldi *et al.*, 2001) ont initié les recherches sur les interdépendances des ICs, en proposant des dimensions encadrant les principaux aspects d'interdépendances. Leurs recherches ont fait surgir de nouvelles interrogations. Certaines de ces questions ont eu des réponses mais d'autres sont restées posées. Le caractère confidentiel, des données, entourant les ICs a rendu les écrits non publics et rares. C'est pourquoi, la plupart des premiers travaux ne se sont concentrés que sur les aspects qualitatifs du problème d'interdépendance (Popescu et Simion, 2012). Par ailleurs, d'autres chercheurs ont proposé des approches afin de quantifier les impacts en cascades dans les ICs (Zimmerman et Restrepo, 2006).

Min Ouyang dans sa revue des différentes approches utilisées dans la modélisation et la simulation des interdépendances liées aux SICs, avait recensé cinq approches : empiriques, basées sur les agents, basées sur la dynamique des systèmes, basés sur la théorie économique et basés sur les réseaux (Ouyang, 2013).

4.2.1 Approches empiriques

Ces approches analysent les interdépendances des ICs en fonction des données historiques des accidents ou des catastrophes et de l'expérience des experts, pour identifier des modèles de défaillances fréquents et significatifs et pour quantifier les liens d'interdépendance par l'entremise de différents indicateurs.

Ces approches aident à identifier les modèles d'interdépendance potentiellement importants et établissent des espaces de collaboration entre les concepteurs urbains et les gestionnaires de plans d'urgences. Par contre, quelques faiblesses sont à noter :

- Impartialité et rétention dans la déclaration des échecs et des défaillances ;
- Absence d'un cadre méthodologique unifié pour la définition d'un SIC et la collecte de données d'échec ;

- Lenteur dans l'analyse des données d'échecs.

4.2.2 Approches basées sur un agent

Ces approches considèrent les composantes d'un SIC comme des agents et modélisent les comportements des décideurs et des principaux gestionnaires des SICs interdépendants. Elles permettent également de prendre en charge tous les types d'interdépendances entre les SICs par des simulations à événements discrets sous forme de scénarios. Toutefois, quelques faiblesses sont à noter :

- La qualité de la simulation dépend fortement des hypothèses de départ ;
- L'étalonnage des paramètres de simulation est un défi par manque de données pertinentes et des difficultés à modéliser le comportement humain.

4.2.3 Approches basées sur la dynamique du système

Ces types d'approches utilisent une méthode descendante pour gérer et analyser les systèmes adaptatifs complexes impliquant des interdépendances (Sterman, 2000) ; (Kollikkathara et Huan Feng, 2010) ; (O'Reilly *et al*., 2007). Elles modélisent les SICs interdépendants par un diagramme en boucle causale en considérant l'influence causale entre différentes variables et par un diagramme stock-et-flux elles décrivent le flux d'informations et de produits à travers le système (Brown *et al*., 2004), (Stapelberg, 2008).

En effet, ces approches modélisent le comportement dynamique et évolutif des SICs interdépendants en considérant les causes et les effets importants dans des scénarios perturbateurs et en considérant d'autres effets (facteurs de gestion et technique) pour refléter l'évolution du système à long terme et fournir des recommandations d'investissement. Les faiblesses de ce type d'approches sont :

- Diagramme de la boucle causale : établi en fonction des connaissances d'experts, (méthode semi-quantitative) ;
- Paramètres et fonctions dans les modèles qui nécessitent un étalonnage et ayant besoin de données difficilement accessibles pour des raisons de sécurité ;
- Utilisation d'équations différentielles pour décrire les comportements au niveau du SIC. Cette approche ne peut analyser la dynamique au niveau des composantes (ajustement ou changement des topologies d'infrastructure) ;
- Difficulté d'obtenir des données pertinentes, donc, les efforts de validation consistent plus en une validation conceptuelle pour les variables descriptives importantes de

chaque SIC afin de déterminer si le modèle donne une réponse raisonnable suite aux perturbations. Ce qui rend la validation du modèle relativement limitée.

Ces faiblesses nécessitent l'intégration d'autres approches de modélisation dans un cadre d'analyse uniforme pour l'aide à la décision globale.

4.2.4 Approches basées sur la théorie économique

La plupart des chercheurs utilisent la théorie économique en se basant sur le modèle entrée-sortie (I-O) de Leontief (Leontief, 1966). Ce modèle décrit le degré d'interconnexion des différents secteurs économiques.

$$\mathbf{x} = \mathbf{A}\mathbf{x} + \mathbf{c} \Leftrightarrow \forall \mathbf{i}\,, \left\{\mathbf{x_i} = \sum_{\mathbf{j=1}}^{\mathbf{n}} \mathbf{a_{ij}}\mathbf{x_j} + \mathbf{c_j}\right\} \qquad (4\text{-}1)$$

Dans cette équation, x_i est la sortie d'opération totale du secteur i. Le coefficient a_{ij} décrit le rapport de l'apport du secteur i au secteur j par rapport aux besoins totaux du secteur j. c_j décrit la demande pour le secteur i qui n'a pas été exprimée par des interconnexions de secteur à secteur.

Haimes et un groupe de chercheures ont utilisé un modèle d'entrée-sortie d'inopérabilté pour ces infrastructures basées sur la théorie de Leontief (Haimes et al., 2005).

Le modèle suppose que les différents types d'interdépendances puissent être modélisés par des interactions financières et le degré d'interdépendance est spécifié par le pourcentage de consommation de chaque secteur par rapport aux productions des autres secteurs. L'autre aspect de ce modèle est la grande difficulté pour écrire un modèle complet.

Il est fort possible qu'au fur et à mesure, le nombre de secteurs concernés augmente, la complexité des modèles, tels que celui présenté par Haimes *et al*., (2005), augmentera considérablement, et par conséquent compliquera le processus de modélisation et de simulation.

4.2.5 Approches basées sur le réseau

Ces approches décrivent les SICs comme des réseaux, où les nœuds représentent les différentes composantes, et leurs liens imitent les connexions physiques et relationnelles

entre elles. En fonction de la modélisation du flux de particules sur les SICs, les méthodes sont :

- **Méthodes basées sur la topologie :** Ces méthodes modélisent les SICs interdépendants uniquement en fonction de leurs topologies, avec des états discrets pour chaque composante (nœud ou lien) et généralement avec deux états : défaillant et normal.

Les nœuds peuvent rentrer en défaillance directement à partir des dangers, ou indirectement en raison des déconnexions des nœuds-source dans le même SIC (Patterson et Apostolakis, 2007) ou en raison des défaillances simultanées de leurs nœuds dépendants d'un autre SIC, aussi en raison d'autres facteurs, tels que des défaillances des systèmes de sauvegarde (Adachi et Ellingwood, 2008). La modélisation des topologies des SICs, peut être analysée par des méthodes analytiques et par des méthodes de simulations :

- **Méthodes analytiques** : Ces méthodes de modélisation ne tiennent pas compte de l'hétérogénéité des nœuds (nœuds-source, nœuds de transmission et nœuds puits). Chaque SIC peut alors être caractérisé par sa distribution de degré de nœuds représentée par une fonction génératrice.

- **Méthodes de simulation** : Ces méthodes considèrent principalement les caractéristiques topologiques des SICs interdépendants tout en identifiant les composantes critiques du SIC, et fournissent des suggestions sur les améliorations de robustesse du point de vue topologique. En dépit de la topologie du système qui détermine sa fonctionnalité, des études récentes ont montré que le modèle topologique seul ne peut pas fournir suffisamment d'informations sur les performances de flux des SICs réels (Ouyang, 2013).

Par conséquent, ces méthodes ne peuvent pas être utilisées seules comme outils de gestion des SICs. Elles nécessitent l'intégration d'autres approches de modélisation dans le cadre d'aménagement urbain et spécifique à chaque IC, c'est-à-dire sa mission, sa position spatiale et la force de lien inter-ICs et ce pour la mise en place d'un support décisionnel global dans le cadre collaboratif impliquant tous les acteurs de la ville. La complexité de la modélisation de l'interdépendance contraint les chercheurs à ne considérer qu'une seule infrastructure (Eusgeld *et al.*, 2009), ou quelques-unes d'entre elles (O'Reilly *et al.*, 2007).

Récemment, l'approche des ICs en tant que « système des systèmes » (Eusgeld, *et al.*, 2011) et l'approche «réseau des réseaux » (Gao *et al.*, 2014), ont fait avancer la compréhension des dépendances et les interdépendances entre les ICs.

4.3 Travaux de recherche en lien avec les ICs

Nous pouvons dire que l'analyse, de vulnérabilité des ICs, a commencé en 1996. Depuis cette date à nos jours, plusieurs études et analyses ont été réalisées à travers le monde. Nous explorons dans ce qui suit, quelques-uns de ces travaux

Petit s'est penché sur les travaux réalisés à ce jour dans le but d'apporter des éléments de réponses à la problématique des ICs. Il décompose alors ces travaux en deux : intersectoriels et sectoriels (Petit, 2009).

4.3.1 Travaux intersectoriels

Il s'agit des travaux de recherche qui se penchent sur le comportement des réseaux (SICs) qui n'arrivent pas à accomplir leurs missions principales. L'objectifs de ces travaux est de déterminer et de caractériser les liens existants entres les différents SICs, étant donné que ces derniers sont fortement liés comme le souligne Rinaldi *et al.*

Pour satisfaire les besoins divers et quotidiens de la société en eau, électricité, gaz, etc., une grande partie des SICs ont des besoins mutuels appelés « Interdépendance » par les chercheurs. Cette dernière peut être entre deux infrastructures ou multiples entre plusieurs ICs. Des exemples de telles interdépendances sont illustrés à la Figure 4-1.

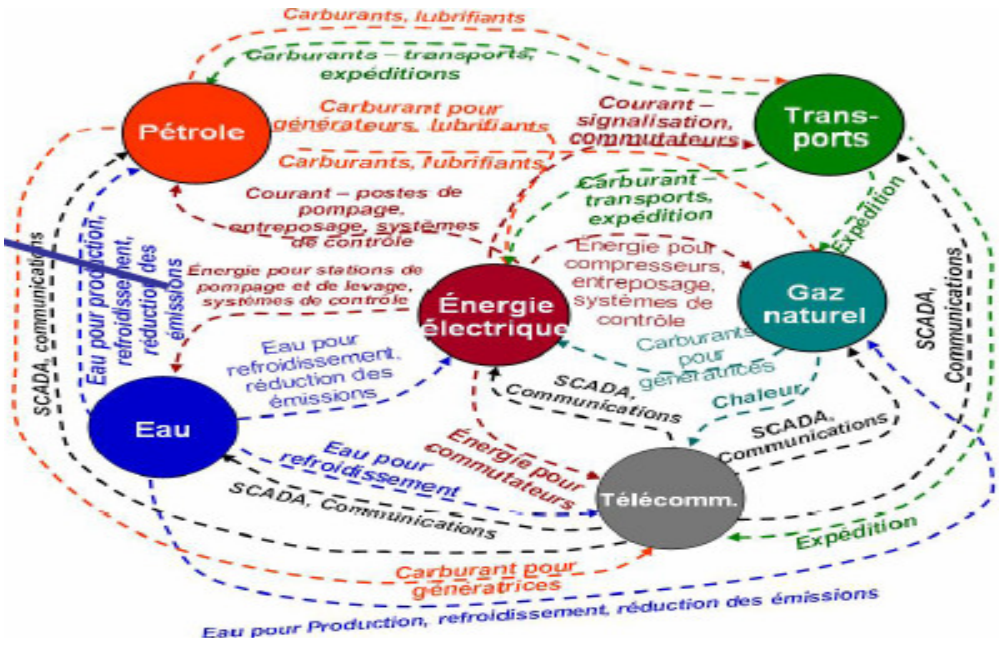


Figure 4-1 : Interdépendances entre SIC (Rinaldi *et al.*, 2001)

Les interdépendances sont également présentes dans les ICs d'un SIC. Ainsi, l'interdépendance inter-ICs peut conduire à des défaillances en cascade lorsque la défaillance d'une infrastructure conduit à la défaillance d'autres infrastructures et à des défaillances en escalade et lorsqu'une défaillance mineure dans une infrastructure provoque rapidement une panne grave de la même infrastructure (Amin, 2003). La panne est considérée lors de la rupture totale de la mission d'un SIC. D'autre part, la taille importante d'un SIC fait naitre de nouvelles vulnérabilités.

4.3.1.1 États-Unis

Aux États-Unis, c'était le *National Infrastructure Simulation and Analysis Center* (NISAC), le premier centre à avoir abordé la problématique des ICs et plus précisément leurs interdépendances. Le NISAC a vu le jour, en 1999, suite au partenariat entre *Los Alamos National Laboratory* (LANL) et le *Sandia National Laboratories* (SNL) et sous la tutelle du *Department of Homeland Security's Preparedness Directorate*.

Le NISAC a été désigné en octobre 2001 (juste après les attaques du 11 septembre 2001) comme source de compétence, par le congrès américain, pour tout ce qui est protection des SICs, et support pour les activités visant à contrer le terrorisme, dans le but d'évaluer les menaces et d'en apporter les outils d'atténuations des risques (Brown, 2007). Par ailleurs, le NISAC s'est fixé comme mission, l'élaboration des modèles et des simulations adaptées à l'analyse des SICs, de leurs interdépendances et de leurs vulnérabilités.

La modélisation des interdépendances des réseaux se base essentiellement sur l'expertise développée par le SNL relative à la simulation des systèmes complexes. Le NISAC dans sa démarche, cherche avant tout, à cartographier les « nœuds critiques » dans les SICs. Ensuite, il quantifie les conséquences physiques et économiques d'un risque pour la sécurité des systèmes des infrastructures nationales.

Petit, signale que les travaux de recherche du NISAC sont élaborés selon deux aspects : la modélisation des interdépendances et l'analyse des conséquences (Petit, 2009).

Ces vingt dernières années, Le NISAC a développé des méthodes de simulation informatisée permettant de prédire, en temps réel, les conséquences d'événements perturbateurs sur les SICs.

Les méthodologies développées semblent permettre la modélisation d'événements perturbateurs et d'impacts affectant les SICs. Cependant, elles risquent de comporter des inconvénients, plus précisément, avec ce qui a trait aux ressources nécessaires à son application et leurs déploiements (sur l'ensemble du territoire). En effet, pour fonctionner, les approches du NISAC nécessitent l'utilisation d'ordinateurs très puissants pouvant supporter les simulations de divers systèmes (Brown, 2007).

À cet effet, Petit fait remarquer aussi que la méthodologie du NISAC est basée sur une approche par scénario qui rend plus difficile la prise en considération de la totalité des événements conduisant à la défaillance d'un SIC par effets dominos. Leurs approches sont plus adaptées à l'étude des transferts d'aléas (Petit, 2009).

Pour ce qui a trait à l'évaluation des conséquences, le NISAC a développé des approches en complément à celles que nous venons de voir. Ces approches ont mené plus à établir des techniques déductives, comme l'analyse par l'AdD, et celles pour décomposer d'une manière systémique chaque conséquence en une série de causes susceptibles de générer des conséquences dommageables. En effet, cette analyse a pour avantage de combiner les causes de défaillance d'une infrastructure sans pour autant faire sortir la totalité des causes.

Les travaux de recherche du NISAC se sont intéressés particulièrement aux secteurs d'activités bien spécifiques. Comme les réseaux de finance, en étudiant les effets de la congestion des systèmes de payement bancaire et interbancaire (Beyeler *et al*., 2006), le réseau de l'énergie en cherchant à modéliser le réseau de gaz naturel (Ellison, 2007) et des télécommunications en cherchant de quelle façon ils peuvent être eux aussi modélisés comme l'illustre le travail de Conrad et O'Reilly (Conrad et O'Reilly, 2007).Dernièrement, des études ont été également lancées, abordant les indicateurs des dépendances. Il est à remarquer que la plupart des travaux de ce centre (NISAC) se préoccupe plus sur l'estimation du risque du point de vue économique, ne considérant que les liens de type cybernétique.

D'autres travaux du NISAC, comme le développement du *Critical Infrastructure Protection/Decision Support System* (CIP/DSS), se font conjointement avec d'autres laboratoires de recherche, comme L'ANL. Le CIP/DSS se trouve être pertinent, dans la mesure où il vise à supporter la prise de décision des gestionnaires pour la protection des ICs (Conrad et O'Reilly, 2007). Pour ce faire, il simule les interdépendances directes entre ICs en se basant non seulement sur les ressources clés utilisées ou produites par ces

infrastructures, mais aussi sur les conséquences environnementales, économiques et sur la santé humaine. Le concept de ressources clés est très avantageux car, il permet d'analyser le système en se focalisant sur ses besoins, mais aussi sur ses apports à la société (Conrad et O'Reilly, 2007).

D'autres entités de recherches s'intéressent aussi aux interdépendances inter-ICs. Nous citerons l'Argonne *National Laboratory* (ANL). Les travaux de ce dernier sont développés au sein d'un de ses centres de recherche comme l'*Infrastructure Assurance Center* (IAC) qui a pour objectif le soutien aux organisations publiques et privées impliquées dans les mesures d'urgence dans ces trois volets, (prévention, préparation, intervention et rétablissement), pour sécuriser les SICs contre toute menace chimique, biologique, terroriste, radiologique et nucléaire (Nozick, 2005). En effet, les recherches de ce centre se sont principalement orientées vers la sécurité et la fiabilité des ICs américaines, notamment le secteur énergétique et des missions essentielles qu'elles fournissent aux USA. Pour cela, le centre de recherche, avantage une approche intégrant à la fois trois aléas naturels, techniques et sociaux et considérant les conséquences sur la santé humaine, l'économie et la sécurité nationale. Il attache beaucoup d'importance, dans leurs analyses, sur le type de lien caractérisant les interdépendances.

Quatre types de liens ont été définis :

- ✓ Physique (lien direct : une infrastructure utilise une ressource fournie par une autre infrastructure) ;
- ✓ Cybernétique (électronique, informationnel, *Supervisory Control And Data Acquisition* (SCADA) ;
- ✓ Géographique (espace commun) ;
- ✓ Logique (dépendance par l'entremise des marchés financiers, règlement, etc.).

La caractérisation des liens se trouve être la même que celle donnée par Rinaldi *et al*. (2001).

L'ANL donne une autre définition du risque intégrant les aléas, les vulnérabilités et les conséquences pouvant affecter les liens entre ICs. Ainsi, la vulnérabilité est abordée sous l'angle de la sensibilité du fonctionnement des ICs au regard des différents liens qui les relient. L'analyse de risque s'articule principalement autour des interdépendances et la nature des liens existant entre les ICs (Petit, 2009).

En outre, plusieurs outils informatiques ont été développés par l'ANL dans le but d'identifier les interdépendances et pour partager les informations pertinentes entre les parties prenantes (Peerenboom et Fisher, 2007).

Les chercheures de l'ANL tentent alors de répondre aux questions suivantes :

- ✓ Connaissez-vous vos fournisseurs et leurs chaînes d'approvisionnement ?
- ✓ Connaissez-vous les effets dominos qui pourraient résulter d'une défaillance ?
- ✓ Connaissez-vous les systèmes de relève (palliatif) qui sont en place ?
- ✓ Connaissez-vous l'autonomie de ces systèmes de relève ?
- ✓ Savez-vous où trouver de l'information concernant les priorités de rétablissement des infrastructures ?

Afin de partager adéquatement ces informations, le *Department of Homeland Security* (DHS) a mis en place un programme d'échange d'informations entre le secteur privé et le gouvernement, le *Protection Critical Infrastructure Information* (U.S. DHS, 2009).

Les informations et données collectées des questionnaires déjà cités seront utilisées ultérieurement comme des entrants aux profits des différents outils informatiques développés par l'ANL. La majorité de ces outils sont des systèmes d'informations géographiques (SIG) servant à la représentation cartographique de l'état des ICs à l'échelle du pays (Petit, 2009).

4.3.1.2 Australie

Le Ministère de la Sécurité publique du Québec (MSP) se base sur la législation australienne et néo-zélandaise, à savoir la norme de gestion des risques (AS/NZS 4360), pour élaborer son cadre de référence pour la gestion des risques (MSP, 2007). Ce qui nous renseigne de la qualité des travaux australiens. D'ailleurs, ces derniers sont partagés avec les américains et les britanniques (Scott, 2007) ; (Cobb, 1999). Il est à noter que les australiens, de par leurs travaux, se trouvent être les pionniers dans le domaine de l'analyse et de la gestion des risques des ICs à l'instar des travaux des USA.

En Australie, un programme est conçu spécialement pour les ICs. Il s'agit du *Critical Infrastructure Protection Modelling and Analysis* (CIPMA) mis en place par le département de la justice (Attorney-General), en collaboration avec *Geoscience Australia* et le

Commonwealth Scientific and Industrial Research Organisation (CSIRO), pour analyser et modéliser les défaillances en cascade de ses infrastructures (Petit 2009).

L'approche préconisée requiert la collaboration de l'ensemble des partenaires industriels (privés), si nous constatons que ce sont eux les principaux propriétaires (90%) des ICs (Scott, 2007). Cette approche est inductive et se concentre sur l'analyse géomatique à grande échelle de scénarios de danger (CSIRO, 2008). Donc, à partir d'un aléa naturel ou humain donné, les outils informatiques développés permettent de modéliser les défaillances en cascade en intégrant la notion de vulnérabilités des ICs.

(Petit, 2009) qui s'est penché sur les approches développées par l'Australie, constate que leurs travaux se basent sur la mise en œuvre d'un réseau de travail, le *Trusted Information Sharing Network* (TISN), de façon à favoriser un climat de confiance entre les différents partenaires pour permettre l'échange de données confidentielles du point de vue sécurité. En effet, la confidentialité des données est souvent une contrainte majeure pour tisser un réseau collaboratif contraignant ainsi le partage de l'information.

L'objectif visé par la démarche australienne est de définir :

- ✓ Le comportement des ICs ;
- ✓ Le degré d'affection de la population et de l'économie ;
- ✓ La durée de cette affection ;
- ✓ Le secteur affecté.

L'auteur trouve cette approche pertinente, car elle considère les effets dominos surtout dans sa dimension triptyque aléas/vulnérabilités/conséquences pour définir le risque. Sauf que l'application de cette dernière se trouve concentrée sur les secteurs d'énergie, les finances et les télécommunications.

Il existe un autre programme australien appelé, le *Computer network vulnerability assessment program* (CNVA), dirigé par l'*Australian Government Computer Emergency Readiness Team* (GovCERT.au). Ce programme est dédié à l'étude des vulnérabilités et des défaillances reliées aux ICs du secteur des technologies de l'information et des télécommunications (TISN, 2008). Aussi, ce programme traite plus la vulnérabilité du point de vue cybernétique. Robert et Cloutier trouvent que les deux programmes Australiens sont dispendieux et requièrent beaucoup d'informations pour une meilleure exploitation (Robert et Cloutier, 2007). De plus, le partage d'informations reste le grand obstacle vu la sensibilité des données.

Cette approche n'est donc possible que si le pouvoir public l'endosse. En effet, la mise en place de tels programmes reste possible en Algérie, et pourrait être envisageable vu que la sécurité des biens et des personnes est de la responsabilité de l'État et que les ICs lui appartiennent en grande majorité.

4.3.1.3 Canada

Au Canada, les ICs sont la propriété de l'état mais aussi du privé. C'est ainsi, que Petit rappelle la stratégie canadienne pour prendre en charge la problématique des SICs. Cette stratégie est essentiellement conduite par les pouvoirs publics. Cependant, elle responsabilise aussi, et pleinement, les propriétaires privés quant à leurs devoirs de protéger leurs propres infrastructures en se conformant aux exigences de prévention, d'atténuation et de préparation aux risques. La même stratégie insiste, également, sur l'établissement d'un climat de confiance entre les différents partenaires (Petit, 2009). La Sécurité Publique du Canada définit cette démarche comme étant un processus continu, anticipatoire et systématique permettant de comprendre, de gérer, et de diffuser les menaces, les risques, les vulnérabilités et les interdépendances dans l'environnement des ICs (SPC, 2008a).

En effet, le Québec s'est engagé sur une démarche visant précisément la résilience de ses SICs. L'Organisation de Sécurité Civile du Québec (OSCQ) (protection civile) a pris en charge cette démarche. C'est ainsi, qu'en février 2009, le gouvernement du Québec venait d'agréer un cadre de référence.

La méthode a comme point de départ l'identification des SICs de leurs dépendances en terme de besoins en ressources et de leurs missions (ce qui sont censés fournir). De même, cette méthode propose d'analyser les conséquences de la perte de ressources utilisées, par elle-même, et pour les autres utilisateurs c'est-à-dire d'autre SICs.

Pour atténuer les effets des perturbations, mises en évidence lors de l'analyse des conséquences, la démarche propose, également, de déterminer les mesures adéquates afin que les systèmes accomplissent bien que mal leurs missions (continuité d'activité) en tout temps. La mise en place de ces mesures doit être faite en étroite collaboration avec les différents gestionnaires de ces systèmes. (Dufour *et al*., 2009)

Petit (2009) considère les SICs comme étant des systèmes évoluant dans un environnement et en interrelation les uns avec les autres. L'analyse des risques se fait de plus en plus complexe et de nouvelles vulnérabilités peuvent apparaitre. À cet effet, il y'a lieu d'adapter les modes de gestion et la mise en place de nouveaux dispositifs. Ces

considérations impliquent également la collaboration des gestionnaires des ICs pour une meilleure connaissance des risques afin de préconiser des mesures d'atténuations efficientes. Justement, la proposition de la mise en place d'un espace collaboratif, dans le cadre de cette recherche, doté de simple modèle mathématique pour la sécurisation des SICs, serait d'une grande utilité.

4.3.1.4 Europe

Selon un rapport de la commission européenne préparé dans le cadre de l'élaboration d'une stratégie globale visant à renforcer la protection des ICs, ladite commission définit ces dernières comme étant des installations physiques et des technologies de l'information, les réseaux, les services et les actifs qui, en cas d'arrêt ou de destruction, peuvent avoir de graves incidences sur la santé, la sécurité ou le bien-être économique des citoyens ou encore le travail des gouvernements des États membres (COM, 2004).

Ainsi, les ICs se trouvent dans de nombreux secteurs de l'économie (bancaire et les finances, les transports et la distribution, l'énergie, les services de base, la santé, l'approvisionnement en denrées alimentaires, les communications, et les services administratifs de base). Le Tableau 4-1 nous donne un aperçu sur les secteurs concernés.

Tableau 4-1 : Infrastructures critique par secteur (COM, 2006).

Secteurs	Sous-secteurs
I. Énergie	1 Production pétrolière et gazière, raffinage, traitement, stockage et distribution par oléoducs et gazoducs 2 Production et transport d'électricité
II. Industrie nucléaire	3 Production et stockage/traitement de substances nucléaires
III. Technologies de l'information et des communications (TIC)	4 Protection des systèmes d'information et des réseaux 5 Systèmes d'instrumentation, d'automatisation et de contrôle (SCADA, etc.) 6 Internet 7 Fourniture de services de télécommunications fixes 8 Fourniture de services de télécommunications mobiles 9 Radiocommunication et radionavigation 10 Communications par satellite 11 Radiodiffusion
IV. Eau	12 Fourniture d'eau potable 13 Contrôle de la qualité de l'eau 14 Systèmes de digues et contrôle quantitatif des eaux
V. Alimentation	15 Fourniture de vivres et sécurité alimentaire
VI. Santé	16 Soins médicaux et hospitaliers

	17 Médicaments, sérums, vaccins et produits pharmaceutiques 18 Laboratoires de biologie et agents biologiques
VII. Finance	19 Systèmes de paiement, de compensation et de règlement des opérations sur titres 20 Marchés réglementés
VIII.Transports	21 Transports par route 22 Transport ferroviaire 23 Transport aérien 24 Navigation intérieure 25 Transport hauturier et transport maritime à courte distance (cabotage)
IX. Industrie chimique	26 Production et stockage/traitement de substances chimiques 27 Transport de substances dangereuses (chimiques) par pipelines
X. Espace	28 Espace
XI. Installations de recherche	29 Installations de recherche

Il est également utile d'énoncer sur quels critères se base la communauté européenne pour considérer qu'une Infrastructure est critique. Trois critères sont suggérés pour l'identification de l'infrastructure potentielle critique le Tableau 4-2 nous montre l'importance de chaque critère.

Tableau 4-2 : Critère de classification (COM, 2006).

Critères	**Désignation**	
Étendue	La perte d'une IC est mesurée en fonction de l'étendue de la région géographique susceptible d'être touchée – de dimension internationale, nationale, provinciale/territoriale ou locale.	
Degré de gravité	L'incidence ou la perte peut être nulle, minimum, modérée ou élevée.	Incidence sur le public nombre de personnes touchées, décès, maladies, dommages corporels graves, évacuation.
		Incidence économique, effet sur le PIB, importance de la perte économique et/ou de la dégradation de produits ou services.
		Incidence environnementale (impact sur le public et sur l'environnement).
		Dépendance (à l'égard d'autres ICs).
		Politique (confiance dans les capacités du gouvernement).
L'effet dans le temps	Détermine à quel moment la perte d'un élément pourrait avoir une incidence grave (immédiatement, après 24-48 heures, une semaine, autre).	

Une autre dimension est à relever d'une manière plus accentuée c'est que non seulement les ICs sont interdépendants à l'intérieur même des États membre de la communauté européenne mais ils sont aussi interdépendants entre les États à l'instar des réseaux de transport, réseau d'énergie, etc.

- **France**

Comme nous l'avons déjà mentionné, les états européens et notamment la France s'intéresse plus, particulièrement, à la vulnérabilité des ICs face à la menace terroriste.

C'est le ministère de l'Intérieur et le Ministère de la Transition Écologique (gouvernement juillet 2020), qui sont en charge de l'ensemble des questions en matière de sécurité civile. Deux lois corroborent les principales préoccupations sécuritaires, celle du 30 juillet 2003 portant sur la prévention des risques technologiques et naturels et à la réparation des dommages et celle du 13 août 2004 portant modernisation de la sécurité civile. (GF, 2003) et (GF, 2004).

Selon l'étude de Lasbordes sur la sécurité des systèmes d'information, l'État a la responsabilité, en relation avec les représentants des secteurs stratégiques économiques, de la protection des infrastructures vitales (Lasbordes, 2006).

Les secteurs d'activités d'importance vitale sont ceux ayant trait à la production et la distribution de biens ou de services indispensables à la satisfaction des besoins essentiels pour la vie des populations, à l'exercice de l'autorité de l'État, au fonctionnement de l'économie, au maintien du potentiel de défense et à la sécurité de la nation, dès lors que ces activités sont difficilement substituables ou remplaçables, ou peuvent causer un danger grave pour la population (Lasbordes, 2006). Nous remarquons que la notion de vitale est toujours présente, en France, pour désigner les infrastructures, objet de notre étude.

Les principales infrastructures vitales sont l'énergie électrique, les télécommunications, les transports, la chaîne de transactions interbancaires, le réseau de vigilance sanitaire, la chaîne des prestations sociales et la distribution d'eau potable (Lasbordes, 2006).

La France n'a réellement commencé à se préoccuper de la protection de ses ICs qu'en 2003. En effets, en se basant sur les travaux de Viellard et Ribnikar, cet intérêt survient dans un contexte de défense nationale et de continuité de l'état faisant suite à la crainte des actions terroristes (Viellard et Ribnikar, 2003). De ce fait, l'identification des ICs susceptibles d'être touchées par ce genre d'actes malveillants se trouve à la base de toute évaluation de leurs

niveaux de protection. Ainsi, il serait aisé d'estimer l'impact possible sur la société dans le cas de la survenue d'action terroriste.

L'étude « La protection des infrastructures critiques face aux menaces asymétriques »réalisée, en 2003, par la Compagnie Européenne d'Intelligence Stratégique (CEIS) a montré que certaines ICs n'avaient pas pris en compte leurs degrés de vulnérabilités face à un acte terroriste et par conséquent aucune mesure de protection appropriée n'a été préconisée (Viellard et Ribnikar, 2003). Pire encore, les risques résultant de l'interdépendance de ces réseaux n'étaient pas encore considérés à cette époque.

Ces derniers auteurs mettent en évidence la nécessité d'examiner les ICs dans leurs ensembles. De plus, une prise de conscience de l'ensemble des pouvoirs publics s'avérait nécessaire de manière à développer des processus de sensibilisation et d'entraînement à la gestion de crise impliquant les ICs (Viellard et Ribnikar, 2003).

Petit (2009) pense qu'en 2003, la France avait plus une vision politique et économique sur ce qui avait trait à la protection des ICs. Donc, c'est le bon fonctionnement de l'État qui compte plus qu'autre chose, justifié par le fait que les gestionnaires des réseaux avaient leurs propres processus de gestion de risque pour le maintien et la continuité des opérations. Cependant, l'état intervient si les effets des perturbations touchent un réseau impactant la totalité ou une partie de la société.

Petit en 2009, en se basant sur les travaux de Viellard et Ribnikar (2003), souligne la nécessité de développer des exercices de simulation basés sur des scénarios pour pousser les pouvoirs publics à conduire des analyses de risques spécifiques aux défaillances des ICs. Il est à noter cependant, que le traitement que préconise les français face à la problématique des ICs est purement stratégique et sécuritaire, n'accordant que peu d'intérêt au côté opérationnel (Petit, 2009). En effet, l'après septembre 2001, le traitement sécuritaire prévalut pour un certain nombre d'États.

Néanmoins, d'autres travaux plus opérationnels se développent également. Nous mentionnons plus particulièrement les travaux de MIBS, Infrastructure & Services et ceux de l'Institut National des Hautes Études de Sécurité (INHES). Les travaux de MIBS Infrastructure & Services se concentrent particulièrement sur la sécurité informatique puisque les systèmes d'informations jouent un rôle primordial en tant que réseau

d'informatique, mais aussi en tant que moyen de gestion à la disposition des différents acteurs responsables des autres réseaux. Donc, ce sont plutôt des études portant sur la gouvernance du système d´information et toutes les problématiques de sécurité (MIBS, 2006).

Quant aux travaux de l'INHES, ils s'articulent autour de l'aspect gestion et sur l'aspect sécurité économique. Ils se fixent comme objectifs la parfaite compréhension du risque (exploration et analyse de nouveaux risques) (INHES, 2008).

Malgré les avancées des chercheurs dans le domaine des ICs les travaux français comparés à ceux des autres pays restent à son stade embryonnaire.

4.3.2 Travaux sectoriels

Les travaux à caractère sectoriel sont ceux qui étudient les risques dans un secteur donné, comme par exemple l'énergie (réseaux électriques, nucléaires, etc.), les transports (aéronautique, route, etc.), ou encore la fabrication (industrie chimique, alimentaire, etc.).

Les défaillances comme la panne électrique de 2003 en Amérique du Nord, l'accident chimique de Seveso en Italie en 1976 etc. pour ne citer que ceux-là, ont été les propulseurs pour que les organisations développent des approches d'analyse des risques pour faire face à ce genre de défaillances.

Ainsi, la Faculté Polytechnique de Mons (FPM) en Belgique, notamment, son *Major Risk Research Centre* (division du contrôle des risques chimiques), a été fortement impliquée dans des projets de recherches, axés sur le développement de la connaissance autour de domaines spécifiques. Un de ces travaux est le projet d'examen de la méthodologie « DOMINO » pour caractériser les enchaînements de défaillances menant à une réaction en chaîne par l'établissant d'une méthodologie pour l'identification et l'évaluation des effets dominos.

Le résultat de cette recherche est largement utilisé dans les études de danger pour les installations classées. La FPM défini un effet domino comme étant une cascade d'accidents dans laquelle les conséquences des accidents précédents sont accrus par les accidents suivants, conduisant à un ou des accidents majeurs.

Ainsi, la FPM a adapté cette définition à l'industrie chimique. Pour ce faire, elle définit comme primaire un premier accident qui va alors concerner un équipement primaire. Pour

considérer les effets dominos, elle définit que les effets primaires induisent la défaillance d'un second équipement alors qualifié de secondaire qui est à son tour le siège d'un accident qualifié de secondaire (FPM, 1998).

Petit (2009) considère que la méthode développée a pour but d'essayer de définir les enchaînements d'événements exceptionnels de type explosion ou incendie entre les industries utilisant des produits chimiques ; sauf qu'elle ne permet pas de considérer l'ensemble des vulnérabilités d'une IC. Cette approche ne prend pas en considération la propagation des effets de perturbations avant l'accident ou avant la perte de mission d'une IC donnée. En effet, nous estimons qu'avant que la défaillance touche la mission principale d'un SIC, elle touche la mission propre de l'IC appartement au SIC.

Aux USA et selon Petit, qui en reprenant les travaux de Mili, Qiu et Phadke (2004), considère que ces derniers auteurs abordent la problématique des défaillances en cascades d'IC, en s'intéressant plus particulièrement aux systèmes électriques (Petit, 2009). Leurs méthodes consistent à développer des algorithmes pour évaluer les risques dans les réseaux électriques en considérant surtout les points faibles des systèmes de protection. C'est alors une approche statistique qui s'appuie surtout sur des données historiques (Mili *et al*., 2004).

Les travaux de recherche que nous venons de voir visent dans un premier temps à faire connaitre les risques en lien avec la problématique des ICs. Pour cela il faudrait que les pouvoirs publics endossent la volonté de considérer ces ICs en intégrant leurs problématiques dans la stratégie algérienne de gestion des risques de catastrophe. Dans un second temps, d'élaborer une méthode de prise en charge de cette problématique dans toutes ces dimensions.

4.4 Résilience et résilience urbaine

Comprendre le concept de résilience urbaine ne peut se faire que si nous abordons la notion de résilience et de son origine.

Le terme résilience est souvent employé en psychologie et en génie. La résilience, utilisée dans la littérature, pour traiter des changements environnementaux mondiaux, est généralement attribuée à l'écologiste C.S. Holling (Brown, 2014). Meerow et Newell (2016), Holling définissent la résilience comme la capacité d'un écosystème à maintenir des caractéristiques fonctionnelles de base lors d'une perturbation. Holling caractérise les

écosystèmes comme ayant plusieurs états stables et dans un état de flux constant, tout en faisant une distinction entre la résilience statique « d'ingénierie », en lien avec la capacité d'un système à rebondir à son état antérieur, et la résilience dynamique « écologique » (Meerow et Newell, 2019). En effet, la résilience, met l'accent sur le maintien des fonctions clés lorsqu'elles sont perturbées (Meerow *et al.*, 2016).

Cette définition est plus qu'intéressante dans la mesure où ses fonctions clés peuvent être assurées par les SICs pour fournir ce qui est vital aux populations en eaux, électricité, gaz, etc. pour garantir la continuité des activités de la ville. Ceci ne peut se faire que par un aménagement urbain résilient.

Il existe plus d'une vingtaine définitions se rapportant à la résilience urbaine dans la littérature scientifique, ce qui instaure une certaine ambigüité (Meerow *et al.*, 2016).

La définition que donne Godschalk semble plus adaptée pour comprendre les concepts de la résilience urbaine. Ce dernier considère qu'une ville résiliente est un réseau, durable, de systèmes physiques et de communautés humaines. Les systèmes physiques sont les éléments construits (routes, bâtiments, infrastructure, installations) mais aussi naturels (faune et flore) formant l'environnement de la ville.

Lors d'une catastrophe, ces systèmes physiques doivent survivre et fonctionner sous des contraintes extrêmes. Si un bon nombre d'entre eux subissent des pannes, qui ne peuvent être réparées, les pertes augmentent et la reprise ralentit. Les communautés humaines sont les composantes sociales et institutionnelles de la ville. Une ville sans systèmes physiques, comme les SICs résilients, sera extrêmement vulnérable aux catastrophes (Godschalk, 2003)

Le concept de résilience offre une vision plus large du système urbain et des perturbations auxquelles il fait face. Ainsi, la résilience urbaine est dans cette perspective, vue comme l'aptitude des parties pérennantes (acteurs de la ville et gestionnaire des systèmes physiques) a concilier leurs efforts dans le sens durabilité mais aussi pour un retour rapide à la normale suite à des perturbations, depuis la conception des systèmes urbains jusqu'à leurs utilisations.

Cette revue bibliographique nous a permis d'apprécier l'intérêt de la modélisation des liens inter-ICs et son apport dans la sécurisation et dans le renforcement de leurs résiliences des SICs.

En nous basant sur les résultats de cette revue bibliographique, nous présentons dans le prochain chapitre une nouvelle conceptualisation de relations existantes entre les différentes

infrastructures d'un réseau, basée sur notre approche « par effet », pour une modélisation de la propagation d'effet d'une ou plusieurs perturbations.

Chapitre 5

CHAPITRE 5 PRINCIPES ET CONCEPTS MÉTHODOLOGIQUES

Les concepts de base entourant les ICs ayant été définis, la méthodologie d'analyse de la vulnérabilité des SICs et les effets des perturbations sur la mission de ces ICs peut être présentée.

La gestion des risques est plus orientée sur les conséquences plutôt que sur les causes de défaillances (Hémond, 2008). Cette démarche est fastidieuse et très lente à réaliser. En plus, elle ne considère aucun effet domino, encore moins les vulnérabilités.

L'analyse des risques des SICs, telle que les réseaux stratégiques (eau, gaz, électricité, etc.), est effectuée par des méthodes qui considèrent le risque comme étant le produit de la « probabilité d'occurrence (P) » d'un événement, par la gravité des « conséquences (G) » qu'il engendre (Benmokhtar, 2019 ; Kaplan, 1997). Cette approche est pénalisante du fait que seuls les scénarios les plus catastrophiques seront considérés.

Le principal risque analysé serait autour de la disponibilité de la ressource transportée par le SIC. Il y'a lieu de concevoir des réseaux résilients pour renforcer la résilience territoriale et urbaine.

5.1 Concepts et principes méthodologiques

L'IC est composée de plusieurs composantes permettant son existence et son fonctionnement comme : les **Activités (As)**, les **Opérations (Os)** supportées par des **Infrastructure (Is)** (bâtiment, aménagement hydraulique, etc.).

5.1.1 Composante des SICs

Les SICs sont considérées comme un système fonctionnant grâce à ses ICs. Ceux- ci nous ramènent à dire que ces ICs soutiennent la mission principale du réseau. Pour cela, il est préférable de parler de système au lieu de considérer ces infrastructures comme des entités indépendantes. Il y a lieu de les approcher comme des systèmes complexes regroupant plusieurs sous-systèmes.

Dans son état fonctionnel, l'IC par l'entremise de ses **Activités (As)** et de ses **Opérations (Os)** transforment les **Ressources (Rs)** et ce pour garantir les **Missions (Ms)** utiles pour la population. La schématisation que nous proposons dans la Figure 5-1 et le

Tableau 5-1 illustre ces composantes et leurs relations. Ainsi, l'ensemble des ICs constitue un SIC (Figure 5-4), dont le bon fonctionnement dépend de l'aptitude des ICs à accomplir chacune de ses missions. Cette vision a pour avantage la contribution à l'analyse de risques des SICs, à travers une parfaite connaissance de leurs composantes et l'évaluation de leurs résiliences.

Cet état de fait, pourrait prémunir les utilisateurs contre le risque de dégradation ou de rupture de la mission principale d'un SIC.

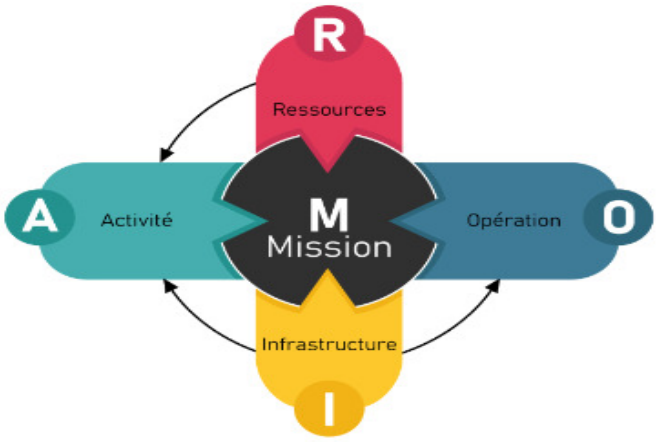


Figure 5-1 : Composante d'une IC

Aussi, il est primordial d'identifier les ICs, leurs principales composantes et leurs Ms.

Les ICs vont être décomposées selon la même démarche utilisée dans la décomposition d'un SIC. Le Tableau 5-1 reprend cette décomposition.

Tableau 5-1 : Décomposition d'une IC (*inspiré* de Robert *et al*., 2003).

IC (sous-système)				
Ressources (Rs)	Infrastructures (Is)	Operations (Os)	Activités (As)	Mission (Ms)
Éléments matériels, opérationnels, humains et naturels permettant la réalisation des As.	Éléments matériels (bâtiment, aménagement hydraulique, etc.) conçus pour assurer le fonctionnement des As de l'IC. Ces éléments sont nécessaires à la réalisation des Os.	Processus technique actions directes ou indirectes sur l'ensemble ou des parties de l'IC pour réaliser les Ms. Automatisées (informatique-électronique) ou manuelles.	Actions nécessaires et devant être exécutées pour permettre la réalisation des Ms.	La fonction pour laquelle une IC a été conçue et réalisée pour satisfaire un besoin.

Nous proposons dans la figure 5-2, ci-dessous, une illustration de la réalisation de la mission globale d'un SIC.

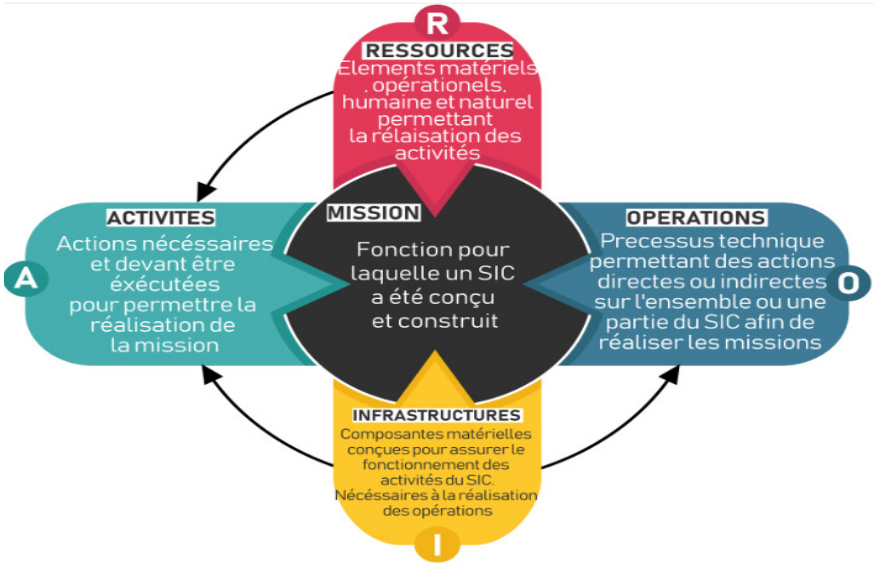


Figure 5-2 : Réalisation d'une mission d'SIC

En outre, dans un état dysfonctionnel suite à des aléas, externes ou internes, nous assistons a des perturbations le long du SIC qui auront des effets sur la mission de ce dernier et des conséquences sur les utilisateurs. Dans la Figure 5-3 une illustration des effets de cette propagation est proposée.

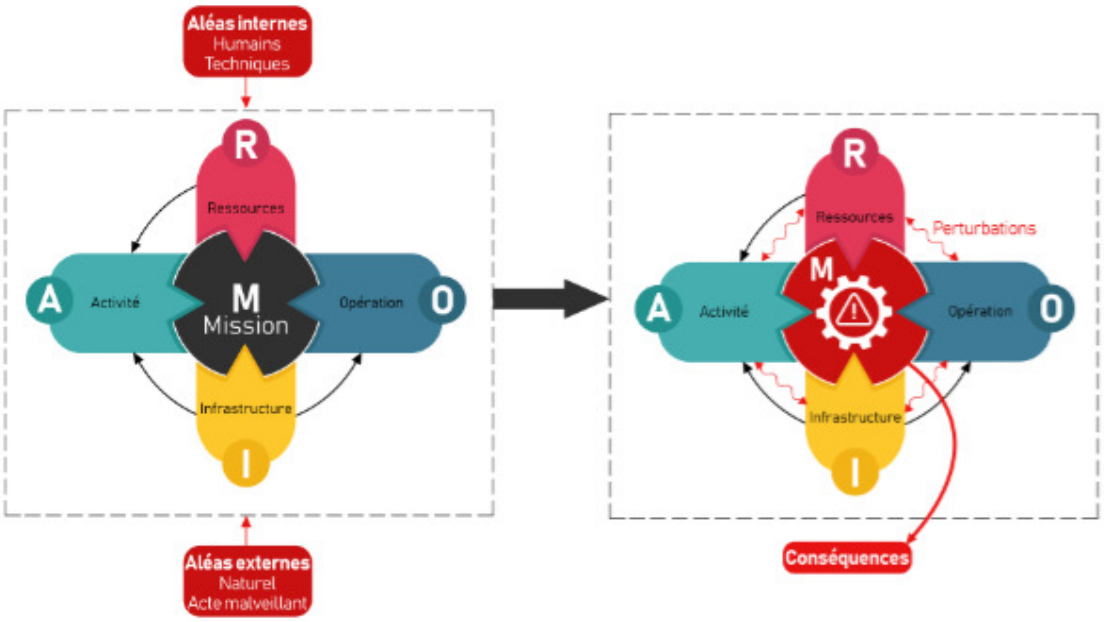


Figure 5-3 : Dégradation d'un SIC

Le modèle développé se base sur le principe des flux (Figure 5-4). De même, chaque SIC a sa propre mission dite Mission Globale (MG) pour satisfaire un besoin vital dans l'aménagement urbain tout en ayant lui-même besoin des produits des autres ICs et éventuellement des autres SICs (d'autre ressources), pour accomplir pleinement sa mission.

Aussi, chaque IC a sa propre M qui sera considérée et diffusée comme étant une R aux ICs subséquentes. Dans la Figure 5-4, nous proposons une illustration d'un flux inter-IC possible.

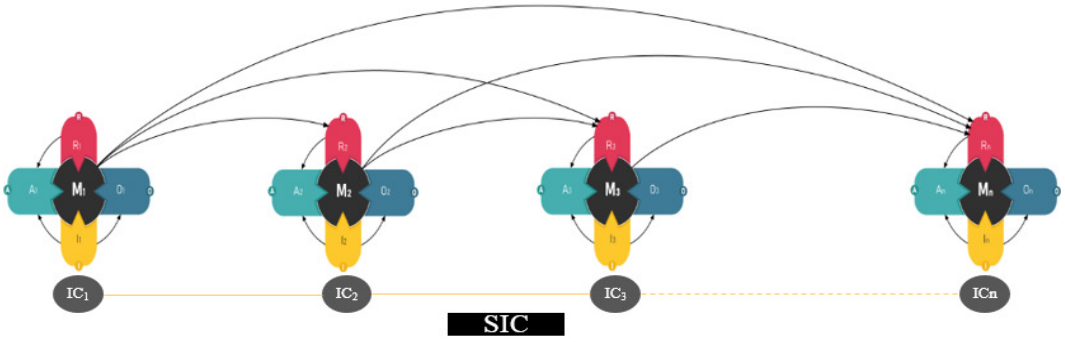


Figure 5-4 : Exemple du flux inter-ICs

Dans ce qui suit, nous formalisons la mission propre à un sous-système appelé $\mathbf{m_{kSi}}$ et la ressource d'entrée appelé $\mathbf{r_{Kei}}$.

5.1.2 Méthodologie proposée

La sécurité des SICs passe par l'analyse des risques associés aux perturbations touchants ses ICs. Ce qui revient à répondre aux trois (3) questions découlant de notre problématique.

La réponse à ces questions passe par la modélisation, de la propagation des effets d'une perturbation, tout au long d'un SIC suivant l'état des missions de ses ICs. De ce fait, de bonnes décisions pourront être prises pour atténuer les effets d'une perturbation. De cette manière les difficultés, qu'il faut enrayer afin de sécuriser les SICs par la protection des composantes d'ICs interdépendantes, sont identifiées. Il est donc indispensable de se doter de mesures, pour se prémunir, contre le risque de propagation des effets suite aux perturbations. Cela se fait par le suivi, le plus fidèlement possible, de ces propagations.

La méthodologie élaborée passe par l'étude des interrelations des SICs fortement interdépendantes d'un même réseau. Une méthodologie est alors proposée, reprenant la démarche et représentée dans la Figure 5-5 ci-dessous :

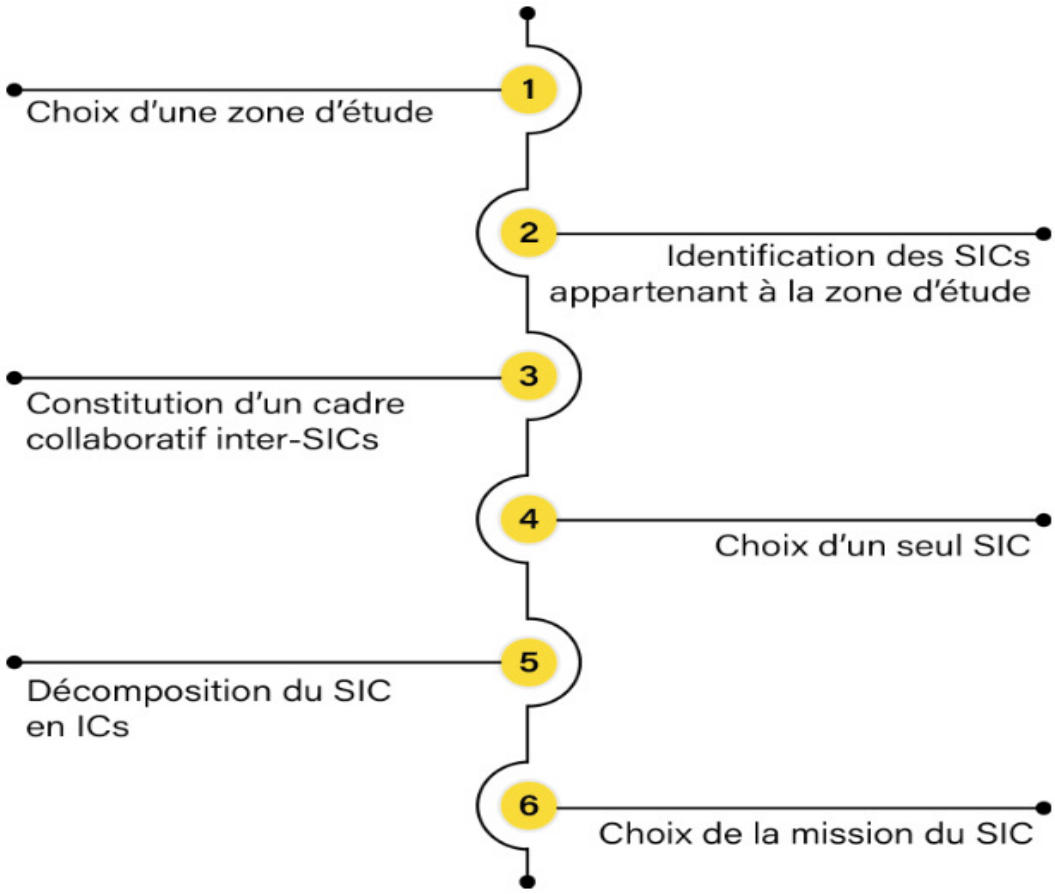


Figure 5-5 : Démarche suivie

Plus en détail la démarche consiste à :

1. **Choisir une zone d'étude pour** identifier les SICs et leurs ICs associées, avec une parfaite connaissance de leurs missions respectives et pour schématiser les liens inter-ICs formant un SIC donné. Le choix se fait selon la densité des ICs dans la zone considérée (au moins, trois ICs par zone) ;
2. **Identifier les SICs et leurs missions** tout en recensant l'ensemble des ICs et leurs composantes, pour identifier les intervenants d'un SIC donné. Il y a lieu de mentionner à chaque fois si ce même SIC est aussi fournisseur d'un autre SIC. Par exemple, le SIC_1 (Eau-fournisseur) fournit de l'eau dans la zone urbaine, mais lui-même, est client du SIC_2 (Électricité-client) ;
3. **Constituer un cadre collaboratif** et ce pour le bon déroulement de la méthodologie. Le gestionnaire de chaque IC aura la responsabilité de transmettre ses données. De ce fait, le problème de confidentialité ne se posera pas, vu que les gestionnaires sont de la même organisation (SEAAL, SONELGAZ, etc.) ;
4. **Choisir un seul SIC** car vouloir traiter tous les SICs, de la zone d'étude, complique la tâche. Nous considérons SIC par SIC (réseau d'eau, réseau de gaz, électricité, etc.). Cependant, une indication sera donnée au moment où la ressource véhiculée par le SIC_1, objet de l'étude, est utilisée par un autre SIC_2. Par exemple signaler quand un SIC-fournisseur devient client d'un autre SIC ;
5. **Décomposer le SIC en IC** (sous-systèmes) et ensuite en composantes. Le niveau de décomposition dépend de la nature du SIC et des informations recherchées. Ainsi, le SIC choisi sera considéré comme un système global (SG) et ses ICs comme étant des sous-systèmes avec indication des missions de chaque sous-système ;
6. **Choisir une mission du SIC** pour la formaliser et pour contribuer à son analyse. Le risque à analyser, peut-être la dégradation, le non accomplissement voire même la perte (cessation) de la MG. Ainsi, nous pouvons déterminer l'effet de la dégradation sur la fonction urbaine. La MG peut être désagrégée en plusieurs missions propres à chaque ICs. En d'autre terme, la MG ne peut se réaliser que par l'accomplissement des missions de chaque IC. Il est inutile d'examiner la totalité de ces missions à la fois. Donc, les missions seront considérées les unes après les autres pour évaluer les effets d'une perturbation à la fin du SIC. Ceci permettra le suivi des effets résultants d'une perturbation donnée tout au long du SIC.

5.1.3 Mission d'une IC

La Mission de chaque IC et sa relation avec les Ressources inter-ICs est déterminée pour chaque sous-système i donné, la mission k de sortie m_{kSi} est alors induite.

K ∈{K_1, K_2, K_3}, K_1= Mission principale, K_2= Mission secondaire et K_3= Mission tertiaire

Seule la mission K_1 sera considérée dans cette étude. Pour concrétiser le flux inter-ICs, la M de sortie d'une IC se transforme en R pour l'IC subséquent. La Figure 5-6 illustre le flux inter-ICs et le transfert de la M en R.

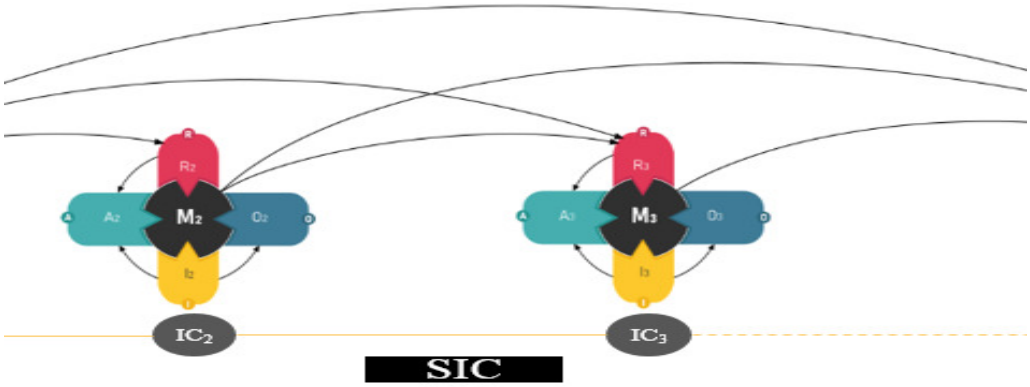


Figure 5-6 : Transformation de la Mission en Ressource

Les ressources d'entrée r_{kE_n} de chaque sous-système i :

$$\begin{cases} r_{kE_1} = a, \text{pour i} = 1, \text{le 1er sous} - \text{système} \\ r_{kE_2} = m_{kS_1}(s_1/ss_2) \\ r_{kE_3} = m_{kS_1}(ss_1/ss_3) + m_{kS_2}(ss_2/ss_3) \\ r_{kE_i} = \sum_{j=1}^{i} m_{kS_j}(ss_j/ss_i) \end{cases} \quad (5\text{-}1)$$

Avec : m_{kSi} : Mission de sortie et r_{kE_n} : Ressource d'entrée

La valeur de la ressource d'entrée d'une IC_i est calculée en fonction de la valeur de la mission de sortie d'une IC_{i-1}

Le flux inter-IC ne se fait pas tout le temps de la même manière mais selon une certaine dépendance.

Pour $i \neq 1$ l'expression des ressources d'entrée r_{kE_i} est donnée par :

$$\boldsymbol{r_{kE_i} = \sum_{j=1}^{i} \varepsilon_{kji} m_{kS_j}(ss_j/ss_i)} \quad (5\text{-}2)$$

ε_{kji} : Pourcentage du flux inter-ICs dans l'intervalle $[0,1]$. Nous proposons 5 natures de flux comme indiqué dans le Tableau 5-2.

Tableau 5-2 : Nature du flux inter-ICs

Nature du flux	ε_{kji}
Aucun	**0**
Mineur	**0.25**
Modéré	**0.5**
Important	**0.75**
Plein	**1**

Nous remarquons que la mission d'une IC dépend de la transformation de la ressource d'entrée et de la nature du flux inter-ICs**.**

5.1.4 Formaliser la contribution des activités et des opérations

L'accomplissement d'une mission M d'un SIC est réalisé par l'ensemble des transformations au sein des composantes des ICs par les Os et les As. Ces dernières dépendent, eux aussi, d'autres Rs (ressources d'appoints et humaines), afin de véhiculer l'élément transporté à travers le SIC. Cet élément est dans la plupart du temps en volume très variable dans l'espace et dans le temps. Nous considérerons l'élément cité comme étant ressource principale.

Finalement, la mission m_{ki} d'une IC dépend de son I, de ses As, de ses Os et de ses Rs d'entrée.

$$m_{ki} = \text{Fonction}\left((A_{ki}),(O_{ki}),(R_{ki})\right) \quad (5\text{-}3)$$

Donc, la m_{ki} d'une IC_i est la transformation de la R (réceptionnée du sous-système i-1) avec une série de transformations obtenues grâce à la contribution des As et des Os. Une pondération de ces dernières serait établie pour suivre et apprécier le flux après transformation. Nous écrivons, la nouvelle expression, de la mission d'une IC comme suit :

$$m_{ki} = \left(coef_{ki,1}(A_{ki}) + coef_{ki,2}(O_{ki})\right)\left(\sum_{j=1}^{i} \varepsilon_{kji} m_{kSj}(^{ss_j}/_{ss_i})\right) \quad (5\text{-}4)$$

La mission k d'un sous-système i est :

$$\boldsymbol{m_{kS_j}(ss_j/ss_i) = m_{kji}} \quad (5\text{-}5)$$

m_{kji} : Est la mission k sortante d'un sous-système j allant vers le sous-système i

$coef_{ki,1}(A_{ki})$ Contribution As dans la réalisation de la m_k

$coef_{ki,2}(O_{ki})$ Contribution Os dans la réalisation de la m_k

Ainsi, l'équation exprimant la mission m_{ki} d'une IC s'écrit en fonction de la contribution des As et des Os pour la transformation des ressources en mission selon la nature du flux inter-ICs.

La mission m_{ki} d'une IC est une fonction affine des As et Os. D'autre part, elle augmente quand les valeurs des As et Os augmentent.

Le SIC dans son fonctionnement normal est censé garantir une MG. Cette dernière résulte de l'ensemble des missions m_{ki} tel que : V_{0k} est la valeur nominale de la mission k, lorsque i =n.

V_{01} : Valeur nominale de la mission de l'IC_1 notée $m_{1,1}$ et V_{0n} : Valeur nominale de la mission de l'IC_n notée $m_{1,n}$.

La MG est la mission globale du SIC représentée par un vecteur unidimensionnel de n lignes.

$$Mg(SIC) = \begin{pmatrix} V_{01} \\ V_{02} \\ V_{03} \\ V_{0n} \end{pmatrix} \quad (5\text{-}6)$$

En conclusion, la concrétisation de la mission d'une IC dépend de la forte contribution des As et des Os après réception de la ressource.

5.1.5 Générer des perturbations

La perturbation peut prendre origine dans l'Infrastructure (I) elle-même ; ceci aura une répercussion sur les As et les Os. C'est pourquoi seules les perturbations touchant ces deux dernières composantes seront considérées.

Le modèle proposé évalue le degré d'altération ou de dégradation de la MG à la fin du SIC en prenant en considération l'ensemble des besoins en ressources. C'est-à-dire, même si certaines Os et As d'une IC appartenant à un SIC sont perturbées, le système peut toujours être en mesure d'accomplir sa mission en fournissant des services et en répondant relativement à la demande. Ainsi, les effets d'une perturbation dans une des composantes,

se font sentir sur le système global. Aussi, les effets sont en rapport avec l'importance de la composante et de la nature de ses liens avec d'autres composantes.

Les perturbations λ_{ki} et σ_{ki} sont localisées, respectivement, aux niveaux des As et des Os. Nous considérons que les perturbations sont comprises entre [0, 1] soit $0 \leq \lambda_{ki}, \sigma_{ki} \leq 1$.

Pour apprécier la mission dégradée, nous avons arrêté cinq(5) natures de perturbations comme l'illustre si bien le Tableau 5-3.

Tableau 5-3 : Ampleur de perturbation

Nature de la perturbation	Valeurs
Aucune	**0**
Mineure	**0.25**
Modérée	**0.5**
Sévère	**0.75**
Très sévère (Rupture)	**1**

Après perturbation, l'expression de la mission dégradée m'_{ki} est écrite comme suit :

$$\boldsymbol{m'_{ki}} = \left((\mathbf{1} - \boldsymbol{\lambda_{ki}})\boldsymbol{coef}_{\boldsymbol{ki,1}}(\boldsymbol{A_{ki}}) + (\mathbf{1} - \boldsymbol{\sigma_{ki}})\boldsymbol{coef}_{\boldsymbol{ki,2}}(\boldsymbol{O_{ki}})\right)\left(\sum_{\boldsymbol{j=1}}^{\boldsymbol{i}} \boldsymbol{\varepsilon_{kji}}\boldsymbol{m_{kji}}\right) \quad (5\text{-}7)$$

Pour $r_i = n$, m'_{ki} devient V_k.

Dans le cadre de notre recherche, nous considérons la valeur α comme étant le coefficient de perturbation.

$$\boldsymbol{\alpha} = \left((\mathbf{1} - \boldsymbol{\lambda_{ki}})\boldsymbol{coef}_{\boldsymbol{ki,1}}(\boldsymbol{A_{ki}}) + (\mathbf{1} - \boldsymbol{\sigma_{ki}})\boldsymbol{coef}_{\boldsymbol{ki,2}}(\boldsymbol{O_{ki}})\right) \quad (5\text{-}8)$$

La mission dégradée m'_{ki} d'une IC est une fonction affine au coefficient de perturbation α. Elle diminue quand α diminue.

Nous remarquons que l'accomplissement de la mission d'une IC est fortement lié au coefficient de perturbation. Ce dernier dépend de l'ampleur des perturbations impactant les As et les Os.

5.1.6 Évaluation et suivi de la propagation de l'effet de perturbation

Le suivi et l'évaluation des effets d'une perturbation nous permettra de déterminer ses conséquences sur la MG du SIC.

V_k est la valeur de la mission perturbée m'_{1n} , avec : V_{11} est la valeur de la mission perturbée m'_{11} de l'IC_1. Ainsi, V_{1n} est la valeur de la mission perturbée m'_{1n} de l'IC_n.

Nous préconisons pour chaque IC un indicateur de dégradation de mission que nous appellerons $dm_{1,n}$. Ce dernier est calculé par :

$$\boldsymbol{dm_{1,n}} = \frac{\boldsymbol{V_{0n} - V_{1n}}}{\boldsymbol{V_{0n}}} = 1 - \frac{\boldsymbol{V_{1n}}}{\boldsymbol{V_{0n}}} \qquad (5\text{-}9)$$

Il en ressort que l'indicateur de dégradation de mission est fortement lié à la valeur de la mission perturbée. De ce fait, pour renforcer la résilience d'un SIC, il y'a lieu de ramener l'indicateur de dégradation de tous les ICs d'un système à zéro.

De même, ces indicateurs de dégradation de mission seront pondérés selon l'importance et l'essentialité des ICs respectives, dans l'accomplissement de la MG du SIC dans la zone choisie.

β_k Coefficient de pondération selon l'importance de la contribution de la mission k dans la MG. La dotation du coefficient importance est laissée au gestionnaire de l'IC.

$\beta_k \in \{1, 2, 3, 4\}$. Nous proposons dans le Tableau 5-4 les différentes valeurs que peut prendre β_k .

Tableau 5-4 : Importance de la mission d'une IC/MG

Importance de la mission	Peu importante	Assez importante	Importante	Essentielle
β_k	1	2	3	4

Nous définissons $\overline{M}$ comme étant l'indicateur moyen pondéré de dégradation de la MG du SIC, appelé aussi ampleur de l'effet de la perturbation du SIC dans la zone étudiée.

$$\overline{M}\left(\mathbf{dm_{i,k}}\right) = \frac{\sum_{k=1}^{n} \mathbf{dm_{i,k} \cdot \beta_k}}{\sum_{k=1}^{n} \boldsymbol{\beta_k}} \qquad (5\text{-}10)$$

Cette moyenne est obtenue grâce à la sommation des indicateurs, de dégradations pondérées, de tous les ICs divisée par la somme de toutes les valeurs de pondération.

Ainsi, cette moyenne dépend fortement de l'importance de la mission d'une IC et de l'indicateur de dégradation relative à l'une ou l'autre IC. Il est important de noter qu'une petite dégradation de mission dans une IC à importance essentielle aura un grand impact sur la MG du système.

5.1.7 Établissement des classes d'impact de perturbation

Une typologie d'indice de dégradation de mission suite à une perturbation sur le SIC est proposée. Nous avons arrêté l'indice en question entre modéré et sévère, le Tableau 5-5 illustre les différents cas.

Tableau 5-5 : Indice de dégradation de mission du SIC

Indice de dégradation moyen pondéré de mission %	Modéré	Assez important	Important	Sévère
$\overline{M}$	0-30	30-50	50-80	80-100

Selon l'équation 5-9

$$dMi = 1- \frac{M_1^{'}}{M1} \quad (5\text{-}11)$$

Avec :

$$M_1 = (coef_{ki,1}(A_{ki}) + coef_{ki,2}(O_{ki}))\, a \quad (5\text{-}12)$$

et

$$M_1' = ((1 - \lambda_{ki})coef_{ki,1}(A_{ki}) + (1 - \sigma_{ki})coef_{ki,2}(O_{ki}))\, a \quad (5\text{-}13)$$

$$\text{Alors } dMi = 1 - \frac{(\mathbf{1-\lambda_{ki}})\mathbf{coef_{ki,1}}(\mathbf{A_{ki}})+(\mathbf{1-\sigma_{ki}})\mathbf{coef_{ki,2}}(\mathbf{O_{ki}})}{(\mathbf{coef_{ki,1}}(\mathbf{A_{ki}})+\mathbf{coef_{ki,2}}(\mathbf{O_{ki}})} \quad (5\text{-}14)$$

Cette équation se lit : l'indice de dégradation d'une M_i est une fonction affine de la valeur de la mission dégradée d'une IC exprimée au numérateur. Il s'annule quand il n y a pas de dégradation de mission et il est égal à 1 quand la dégradation est totale.

$$Q_i = \frac{(1-\lambda_{ki})coef_{ki,1}(A_{ki})+(1-\sigma_{ki})coef_{ki,2}(O_{ki})}{(coef_{ki,1}(A_{ki})+coef_{ki,2}(O_{ki})} \quad (5\text{-}15)$$

Un SIC peut accomplir sa mission malgré une perturbation modérée. Selon le Tableau 5-5, l'indice de dégradation, moyen pondéré, de la mission globale est modéré si $0 \leq dM_i \leq 0.3$

$$\text{L'équation 5-14 devient : } dM_i = 1 - \frac{\sum_{k=1}^{n} Q_i \cdot \beta_k}{\sum_{k=1}^{n} \beta_k} \quad (5\text{-}16)$$

Avec $Q_i \leq 1$

De cette équation, et par minoration, nous avons :

$$\begin{cases} \sum_{k=1}^{n} Q_i \cdot \beta_k \geq \text{Min } Q_i \left(\sum_{k=1}^{n} \beta_k \right) \\ \dfrac{\sum_{k=1}^{n} Q_i \cdot \beta_k}{\sum_{k=1}^{n} \beta_k} \geq \text{Min } Q_i \end{cases} \quad (5\text{-}17)$$

$$\text{Donc : } 1 - \frac{\sum_{k=1}^{n} Q_i \cdot \beta_k}{\sum_{k=1}^{n} \beta_k} \leq 1 - \text{Min } Q_i \quad (5\text{-}18)$$

Par utilisation de l'équation (5-9), et par majoration, nous obtenons :

$$\begin{cases} \dfrac{\sum_{k=1}^{n} Q_i \cdot \beta_k}{\sum_{k=1}^{n} \beta_k} \leq \text{Max } Q_i \\ 1 - \dfrac{\sum_{k=1}^{n} Q_i \cdot \beta_k}{\sum_{k=1}^{n} \beta_k} \geq 1 - \text{Max } Q_i \\ 0 < 1 - \text{Max } Q_i \leq 1 - \dfrac{\sum_{k=1}^{n} Q_i \cdot \beta_k}{\sum_{k=1}^{n} \beta_k} \end{cases} \quad (5\text{-}19)$$

L'indice de dégradation moyen pondéré de la mission globale du SIC doit être :

$$1 - \text{Max } Q_i \leq 1 - \frac{\sum_{k=1}^{n} Q_i \cdot \beta_k}{\sum_{k=1}^{n} \beta_k} \leq 1 - \text{Min } Q_i \quad (5\text{-}20)$$

Nous déduisons que l'indice dégradation moyen pondéré est une quantité bornée, encadrée par [1 - Max Q_i et 1- Min Q_i].

L'équation 5-20, nous permet d'avoir une estimation instantanée de l'indice de dégradation, moyen pondéré, de la mission globale du SIC. Ainsi, au moins une des ICs n'est pas perturbée et qu'une des ICs le Min $Q_i \geq 0.7$ et ce pour rester dans la zone de dégradation modérée de la mission.

Dans ce chapitre, nous avons élaboré deux modèles : le premier modélise la mission d'une IC et le deuxième modélise la mission dégradée d'une IC suite à une perturbation. Un indice moyen pondéré global de dégradation de mission d'un SIC a été également proposé.

Dans le chapitre suivant, une application pour déterminer les effets d'une inondation sur la mission d'un réseau d'eau sera présentée suivie d'une discussion sur les résultats obtenus.

Chapitre 6

CHAPITRE 6 APPLICATION DU MODÈLE, DISCUSSIONS ET RECOMMANDATIONS

Le SIC (réseau d'eau) a été choisi pour l'application du modèle développé. Cependant il reste valable pour d'autres SICs comme l'électricité ou le gaz, ce qui diffèrera sera juste le choix des ICs et l'identification des missions de ces dernières.

6.1 Application

Les réseaux d'eaux conditionnent l'activité et le développement des agglomérations. Ainsi, ces réseaux constituent un SIC d'une ville ou d'un milieu urbain. Ce SIC est choisi pour illustrer la propagation des effets de deux perturbations causés par une inondation le long du réseau. Cet exemple est orienté vers la planification de mesures d'urgence pour mettre en place les meilleures actions pour un retour à la normal.

La mission principale de ces SICs n'est pas juste l'approvisionnement de la population en eau potable, mais aussi d'autres SICs comme le réseau de gaz ou le réseau électrique servant tous une même aire d'influence. C'est pourquoi il est nécessaire de s'assurer de son bon fonctionnement. Un réseau d'eau est composé essentiellement des infrastructures suivantes (voir Figure 6-1), IC_1 : Barrage, IC_2 : Station de traitement, IC_3 : Station de pompage et IC_4 : Château d'eau.

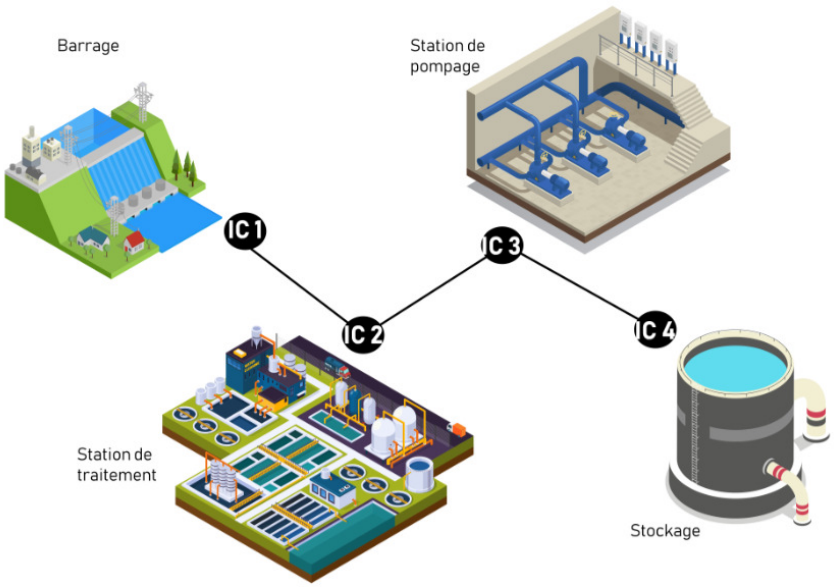


Figure 6-1 : Système d'infrastructure critique (réseau d'eau)

Un réseau d'eau a pour mission, principale, l'acheminement d'eau potable. La quantité, la qualité, la pression et l'emmagasinement font partie de cette mission. Les dites missions sont supportées par des ICs constituants ce SIC. Ces missions sont exprimées comme suit :

- m_1 : Disposer d'une quantité Q (m^3) par l'entremise de l'IC_1 : Barrage,
- m_2 : Offrir une qualité Qa (taux de coliformes) par l'entremise de l'IC_2 : Station de traitement,
- m_3 : Fournir une pression P (mPa) par l'entremise de l'IC_3 : Station de pompage,
- m_4 : Stoker une quantité C (m^3) par l'entremise de l'IC_4 : Château d'eau.

La mission globale du réseau d'eau serait dégradée si une des missions de ses ICs est dégradée ou altérée suite à une ou plusieurs perturbations. Dans notre cas, deux perturbations ayant comme origine une inondation, affectant les deux stations de traitement et de pompage, sont considérées.

- **Mission de chaque IC et relation avec la R inter-ICs**

Pour chaque sous-système i donné, la mission k de sortie m_{kSi} est induite. Juste K_1 = mission principale qui est considérée, pour chaque IC qui sont : m_1, m_2, m_3, et m_4. Pour concrétiser le flux inter-ICs (Figure 6-2), la M de sortie d'une IC se transforme en R pour l'IC subséquent.

- Les ressources d'entrées de chaque sous-système i sont :

  r_{1E1}= a, pour i=1

  $r_{2E2}= m_{1S1}(ss_1/ss_2)$

  $r_{1E3}= m_{1S1}(ss_1/ss_3) + m_{1S2}(ss_2/ss_3)$

  $r_{1E4}= m_{1S1}(ss_1/ss_4) + m_{1S2}(ss_2/ss_4) + m_{1S3}(ss_3/ss_4)$

- **La M d'une IC dépends de son I, de ses As, de ses Os et de ses Rs d'entrées.**

  V_{01} est la valeur nominale de la mission 1 : $m_{1,1}$ de l'IC_1,

  V_{02} est la valeur nominale de la mission 2 : $m_{1,2}$ de l'IC_2,

  V_{03} est la valeur nominale de la mission 3 : $m_{1,3}$ de l'IC_3,

  V_{04} est la valeur nominale de la mission 4 : $m_{1,4}$ de l'IC_4.

- La MG est la mission globale représentée par un vecteur unidimensionnel de 4 lignes.

$$Mg\ (\ SIC\ ) = \begin{pmatrix} m_{1,1} \\ m_{1,2} \\ m_{1,3} \\ m_{1,4} \end{pmatrix} \qquad (6\text{-}1)$$

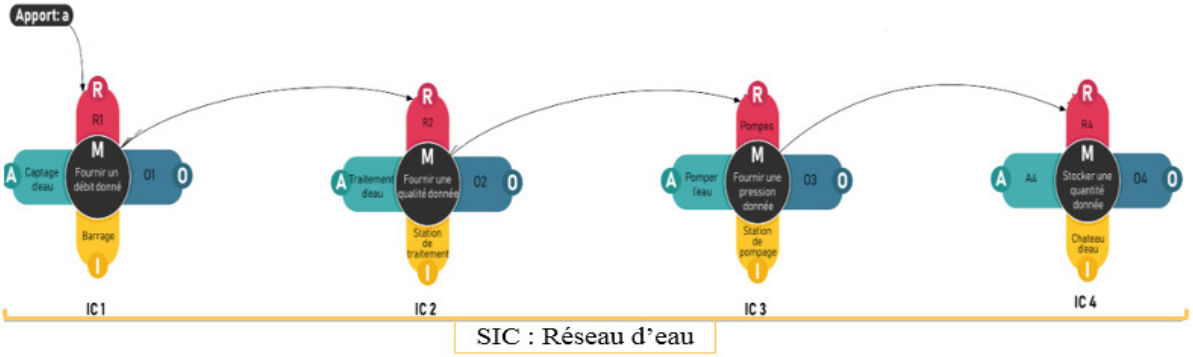


Figure 6-2 : Flux inter 4 ICs

6.2 Résultats et discussions

Considérons r_{1E1}= 1000 m^3, comme l'apport **a**, disposé dans l'IC_1. Les liens et les flux inter-ICs sont paramétrés tel que indiqués dans le Tableau 6-1. La contribution des activités et des opérations relatives à l'accomplissement de chaque mission de l'IC est fixée. Une pondération est aussi attribuée selon l'importance de l'IC dans le SIC.

Tableau 6-1 : Paramètres par IC

Désignations	**IC_1**		**IC_2**		**IC_3**		**IC_4**	
Coef β_k d'importance	3		3		4		3	
Flux inter-ICs ε_{kji}	$\varepsilon_{11,1}$=1		$\varepsilon_{12,1}$=1		$\varepsilon_{13,2}$=1		$\varepsilon_{14,3}$=1	
Ressources	r_{1E1}= a, **1000**		r_{1E2}= $m_{1S1}(ss_1/ss_2)$		r_{1E3}= $m_{1S2}(ss_2/ss_3)$		r_{1E4}= $m_{1S3}(ss_3/ss_4)$	
Contribution : Activités et Opérations (%)	$coef_{11,1}(A_{11})$	$coef_{11,2}(O_{11})$	$coef_{12,1}(A_{12})$	$coef_{12,2}(O_{12})$	$coef_{13,1}(A_{13})$	$coef_{13,2}(O_{13})$	$coef_{14,1}(A_{14})$	$coef_{14,2}(O_{14})$
	0.65	0.30	0.55	0.40	0.50	0.45	0.65	0.30

La valeur des missions de chaque IC est alors déterminée (voir le Tableau 6-2)

Tableau 6-2 : Valeurs par mission - État fonctionnel

Désignations	IC_1	IC_2	IC_3	IC_4
Valeurs nominale des missions V_0	**950**	**902.5**	**857.38**	**814,51**

- Une simulation d'une inondation est alors considérée et qui affectera l'IC_2 et l'IC_3 comme suit :
  - L'IC_2 : Les activités et les opérations sont affectées respectivement de 50% et 25%,
  - L'IC_3 : Les activités et les opérations sont affectées les deux de 25%.
- La valeur des missions de chaque IC après l'inondation est alors calculée (voir Tableau 6-3).

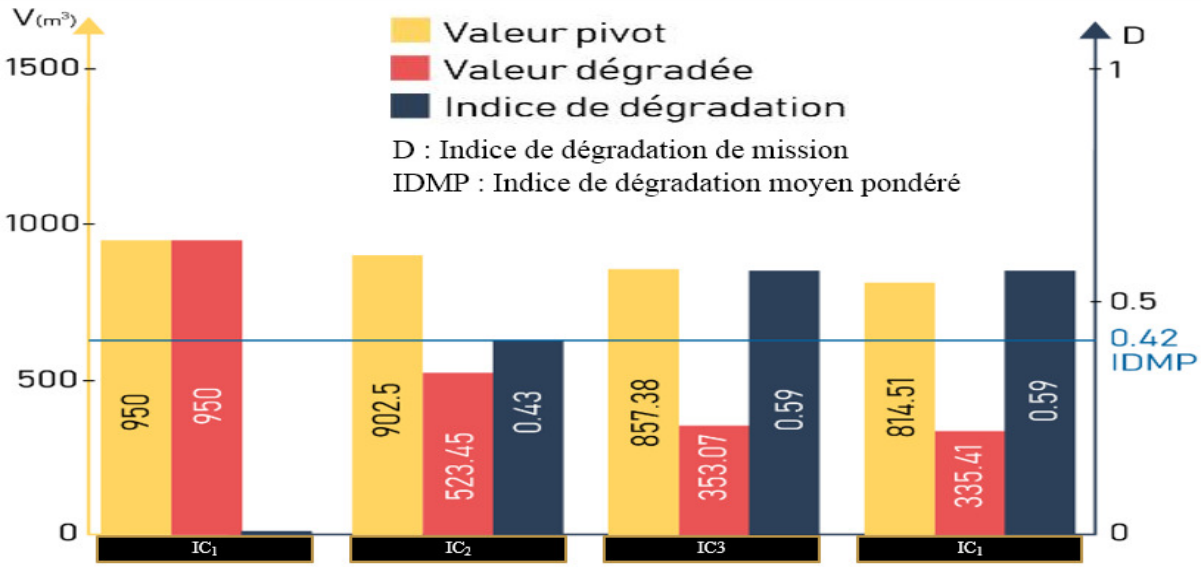
Tableau 6-3 : Valeurs de mission après l'inondation- État dysfonctionnel

Infrastructure	IC_1	IC_2		IC_3		IC_4
Perturbation	/	✓		✓		/
Impact de l'inondation		Activité	Opération	Activité	Opération	
		$\lambda_{ki} = 0.5$	$\sigma_{ki} = 0.25$	$\lambda_{ki} = 0.25$	$\sigma_{ki} = 0.25$	
Coefficient de perturbation	$0.95 - (0.65\,\lambda_{ki} + 0.3\,\sigma_{ki})$	$0.95 - (0.55\,\lambda_{ki} + 0.4\,\sigma_{ki})$		$0.95 - (0.5\,\lambda_{ki} + 0.45\,\sigma_{ki})$		$0.95 - (0.65\,\lambda_{ki} + 0.30\,\sigma_{ki})$
Valeurs des missions après l'inondation	**950**	**523.45**		**353.07**		**335.41**

L'inondation a eu des impacts sur le réseau d'eau, pour cela pour chaque IC, un indicateur de dégradation de mission est alors estimé et représenté dans le Tableau 6-4 et l'ensemble des résultats sont schématisés dans le Graphe 6-1.

Tableau 6-4 : Indice de dégradation de mission par IC et SIC

Infrastructures	IC_1	IC_2	IC_3	IC_4
D indice de dégradation de mission	0	0.43	0.59	0.59
Indice de dégradation moyenne pondérée de la MG du réseau d'eau	**0.42**			



Graphe 6-1 : Valeurs de missions par IC avant / après l'inondation et indice de dégradation

L'inondation a causé deux perturbations aux niveaux des IC_2 et IC_3 une dégradation sévère de la mission principale du réservoir de stockage de l'ordre de 0.59 est observée. Le déficit en ressource d'eau est de 479,1 m^3. La dégradation moyenne pondérée de la mission globale du SIC de l'ordre de 0.42est considéré comme étant importante. Cette dégradation aura des impacts en termes de disponibilité de la ressource aux populations et à d'autres utilisateurs. Dans notre cas, des mesures doivent être prises pour améliorer l'indice de dégradation du SIC. Ces mesures toucheront l'IC_4 par le remplacement intégral du déficit en eau traitée (479.1 m^3) ce qui ramènerait cette moyenne à 0.28. L'intervention sur IC_4 est justifiée par le fait que c'est au niveau de cette infrastructure que l'indice de perturbation de l'ordre de 0.59, est le plus important. En plus, l'infrastructure en question est le point de départ de la distribution de la ressource transporté par le SIC, donc techniquement l'apport de ressource comme moyen palliatif reste faisable. Finalement, l'apport en ressource améliorera l'indice moyen de dégradation de la mission globale du SIC, d'important à modéré. Pour rester dans l'intervalle modéré un apport minimum de 405.79 m^3, d'eau traitée, dois être garanti. Ces mesures ne seront que provisoires de façon que l'inondation n'aille pas paralyser les activités de la ville cela la rendrait résiliente. Ainsi, les mesures préconisées doivent être prises par les ingénieurs planificateurs des mesures d'urgence.

Quant à la faisabilité de ces mesures, ils sont du ressort du l'urbaniste d'où la nécessité de collaboration entre les deux spécialités étant donné que la faisabilité de ces mesures est cautionnée par la prédisposition de l'aménagement et des espaces.

6.3 Recommandations, propositions et perspectives

Au terme de ce travail, de recherche, nous avons à proposer deux définitions (IC et SIC) et une liste de secteur, d'activité, pouvant abrités un certain nombre de SIC. Cette proposition sera faite aux autorités compétentes. Une fois les mécanismes juridiques établis, par la légiférations des définitions et de la liste des SIC proposées, l'instauration des espaces collaboratifs, entre gestionnaires des ICs, serra fait. Ces espaces pourront ainsi utiliser notre cadre méthodologique pour le suivi des effets de perturbation dans les SICs.

En perspective, une piste de recherche pouvant être dégagé pour évaluer les effets de l'indisponibilité de la ressource humaine, en cas de pandémie, dans l'accomplissement de la mission d'une IC.

6.3.1 Infrastructure critique

Les ICs sont des installations (physique ou virtuelle), de structures, d'équipements, de moyens et biens matériels indispensables à la fourniture d'une prestation vitale et qui permet de transformer des éléments d'entrés en éléments de sorties.

6.3.2 Système d'infrastructure critique

Un SIC (réseau de distribution des eaux, réseau électrique, réseau ferroviaire, réseau téléphonique, etc.) est un regroupement d'ICs corrélées et inter-reliées, réparties ou maillées dans un environnement, et véhiculant un élément physique ou virtuel, dans le but d'accomplir une mission en terme de fourniture de ressource essentielle, et dont dépend la sécurité, le bien-être de la population et le bon fonctionnement de l'État.

6.3.3 Proposition de liste

La liste de dix (10) secteurs est proposée. Cette dernière est inspirée de la liste du Ministère de la Sécurité Publique du Canada et adapté à l'Algérie selon nos différents secteurs (gouvernement juin 2020).

Tableau 6-5 : Liste des réseaux par secteurs et ministères selon Gouvernement 2020

N⁰	Secteurs	Ministères	Réseaux et systèmes
1	Gouvernement	· Ministre de la Numérisation et des Statistiques · Totalité des ministères	Services de première nécessité, installations, réseaux d'information, biens gouvernementaux et sites stratégiques
2	Soins de santé	· Ministre de la Santé, de la Population et de la Réforme hospitalière · Ministre de l'Enseignement supérieur et de la Recherche scientifique · Ministre de l'Éducation nationale · Ministre de la Formation et de l'Enseignement professionnels · Ministre du Tourisme, de l'Artisanat et du Travail familial · Ministre des Affaires religieuses et des Wakfs	Réseaux : Hôpitaux, établissements de santé de proximité, capacité de prise en charge, établissement public, réserve de sang, laboratoires d'analyse de sang et produits médicaux
8	Sécurité	· Ministre de la Défense nationale · Ministre de l'Intérieur, des Collectivités locales et de l'Aménagement du territoire · Ministre des Finances · Ministre de l'Habitat, de l'Urbanisme et de la Ville · Ministre de l'Environnement · Ministre de l'Agriculture et du Développement rural · Ministre de la Jeunesse et des Sports	Sécurité des biens et des personnes (police, gendarmerie et protection civil) contre tous risques et les infrastructures nécessaires pour sécuriser les populations
3	Énergie	· Ministre de l'Énergie · Ministre de la Transition énergétique et des Énergies renouvelables · Ministre des Mines	Installation pour la production d'énergie électrique, de gaz naturel (autre source d'énergie). Moyens et réseaux de transport de ces ressources

4	Finances	· Ministre des Finances	Réseau banquier Opérations bancaires (liquidité d'argent) et échanges
6	Eau	· Ministre des Ressources en eau	Réseaux d'Eaux potable (réserve et distribution)
5	Nourriture	· Ministre du Commerce · Ministre de l'Agriculture et du Développement rural · Ministre de l'Industrie	Distribution, réseau de réserve et industrie alimentaire (première nécessité)
7	Transports	· Ministre des Transports · Ministre des Travaux publics	Voies aériennes, ferroviaires, maritimes et terrestres
9	Fabrication	· Ministre de l'Industrie pharmaceutique · Ministre de l'Industrie	Réseau d'industrie en lien avec les services de santé et la production alimentaire
10	Technologie de l'information et des communications	· Ministre de la Poste et des Télécommunications · Ministre de la Communication	Réseaux de télécommunications et d'information

6.3.4 Piste de recherche

Le modèle développé et les différents concepts sur lesquels il repose, peut être rattaché au volet ressource tertiaire comme la ressource humaine car nous avons vu que lors d'une pandémie, comme celle du COVID19, la disponibilité de la mission globale d'un SIC peut être affectée suite à une convalescence ou au décès du personnel en charge de la gestion de ces SICs.

CONCLUSION

Sécuriser les SICs ne peut pas se faire sans la compréhension de leur fonctionnement. L'amélioration de cette compréhension est possible grâce à la modélisation des liens fonctionnels et dysfonctionnels existants entre ICs d'un même SIC. La notion de résilience offre également une aide précieuse pour la compréhension du lieu et du moment et aussi de la façon d'intervenir. Le rétablissement s'appuie principalement sur l'aspect spatial. En effet, le concept de la résilience favorise, déjà lors des études, la conception d'espaces pour un rétablissement efficient.

La résilience d'une ville dépend de la pérennité et la performance de ses systèmes d'infrastructures critiques (SICs). Sécuriser ces derniers passent inévitablement par l'évaluation de l'état de leurs missions et par le suivi des effets de défaillances en cas de perturbations au niveau de leurs ICs qui affectent non seulement la mission globale (MG) du SIC, mais aussi les missions propres de ses ICs. L'effet d'une perturbation touchant une IC se fait ressentir en terme de dégradation de la mission globale du SIC. Cette dégradation est surtout induite par l'importance de l'IC touchée et par l'ampleur de la perturbation affectant cette dernière.

Une nouvelle approche pour la gestion de risque, dans son volet analyse, est utilisée. Cette approche « par effet »se base sur le suivi des effets d'une perturbation bien avant la rupture de la mission d'un système. L'approche en question se démarque du reste des méthodes d'analyse de risque et permet de préconiser des mesures, de prévention, pour renforcer le niveau de résilience des sous-systèmes.

Dans notre recherche une méthodologie, en six étapes, a été proposée pour étudier les liens inter-ICs. Ainsi, deux modèles mathématiques ont été élaborés :

- Le premier modélise l'accomplissement de la mission m_{ki} d'un SIC en fonction de la contribution des activités As et des opérations Os pour la transformation des ressources R en mission selon la nature du flux inter-ICs.
- Quant au second, il modélise la mission dégradée m'_{ki} d'un SIC qui est fortement liée au coefficient de perturbation α. Ce dernier dépend de l'ampleur des perturbations impactant les activités As et les opérations Os.

Les modèles développés permettront d'effectuer une analyse montrant l'interdépendance causale entre les différents sous-systèmes qui affectent la mission principale d'un réseau et ce d'une manière instantanée, ce que ne permettent pas les autres méthodes existantes. Ceci constitue l'originalité de ce travail, et facilite l'identification des ICs pour renforcer leurs résiliences.

Nous avons préconisé pour chaque IC, un indicateur de dégradation de mission $dm_{1,n}$. Ce dernier est fortement lié à la valeur de la mission perturbée. De ce fait, pour renforcer la résilience d'un SIC, il y'a lieu de ramener l'indicateur de dégradation de tous les ICs d'un système à zéro.

Pour une zone donnée un indicateur $\overline{M}$ moyen pondéré de dégradation de la MG du SIC a été proposé et nous permet d'évaluer la vulnérabilité de la zone étudiée.

Les modèles proposés sont donc des outils d'aide à la décision dédiés non seulement au suivi des effets provoqués par des perturbations pour anticiper les effets dominos, dans un système donné, mais constitue aussi une contribution à la gestion des risques de catastrophe (prévention, protection, planification du rétablissement, etc.) par la mise en place des mesures de maitrise des risques pour rendre l'espace urbain plus résilient. En plus, ils offrent un cadre méthodologique pour instaurer un espace collaboratif entre les acteurs de la ville.

Les résultats donnés par ces modèles sont de types semi-quantitatifs et ne prennent en considération que la ressource principale qui est l'élément transporté. Les modèles développés peuvent être supportés par des applications informatiques (simple) et utilisées comme un tableau de bord par les acteurs de la ville et les gestionnaires des ICs. Ces modèles permettent aussi de simuler un certain nombre de perturbation et de déterminer les infrastructures les plus, critiques pour préconiser les actions de sécurités soit en phase conception ou en planification du rétablissement. De ce fait, l'établissement de l'espace collaboratif entre concepteur urbain, ingénieur de planification de mesures d'urgence et gestionnaire des ICs serait d'une grande utilité.

Le présent travail peut être élargi au reste des ressources comme la ressource d'appoint et la ressource humaine afin d'éviter une rupture de la mission d'une bonne partie des SICs en cas de pandémie comme celle provoquée par le *Covid19* suite aux décès ou la convalescence des gestionnaires de ces systèmes.

En guise de contribution pour l'intégration des ICs dans la stratégie algérienne de gestion des risques de catastrophe nous proposons :

- Des définitions en liens avec les SICs et une classification de ces dernières pour être légiférées. Ces propositions seront faites en direction de la DNRM.
- La formation d'un espace collaboratif, impliquant tous les gestionnaires des SICs d'une zone urbaine donnée. Cet espace adoptera, en autre, notre démarche méthodologique comme cadre de travail pour sécuriser nos infrastructures et améliorer la résilience de nos villes.

Finalement, pour sécuriser les SICs nous utilisons quatre notions :

- Suivi instantané de la propagation des effets suite à des perturbations ;
- Échange d'information entre les gestionnaires des ICs ;
- Renforcement de la résilience des ICs les plus déterminants dans la réalisation de la mission d'un SIC ;
- Mise en place de mesures organisationnelles pour la continuité des prestations pour la population.

Au terme de ce travail, il serait assurément irréaliste de prétendre parvenir à cerner, au travers d'une seule recherche, l'ensemble des mécanismes de propagation d'effets responsables de la perte et de la dégradation de mission des SICs qui forment notre milieu urbain.

Il n'en demeure pas moins que nous sommes convaincus d'avoir réalisé une contribution significative pour l'intégration des ICs en Algérie et à la connaissance des liens inter-ICs dans une perspective de protection par l'amélioration entre autre de leurs résiliences, étant donné le très faible nombre d'études réalisées dans ce domaine surtout en Algérie.

RÉFÉRENCES

Adachi T., Ellingwood B. R. (2008), *Serviceability of earthquake-damaged water systems: effects of electrical power availability and power backup systems on system vulnerability*, Reliability Engineering and System Safety **93(1)**:78-88.

Allan P., Bryant M. (2011), *Resilience as a framework for urbanism and recovery*, Journal of Landscape Architecture **6(2)**:34–45.

Allen H. (1997), *Making a business of dam safety*, International Water Power Dam Construction **49(8)**:20-21.

Amin M. (2000), *National infrastructures as complex interactive networks*, in: Automation, Control and Complexity: An Integrated Approach, T. Samad and J. Weyrauch (Eds.), John Wiley and Sons Ltd., NY, USA, pp. 263-286.

Amin M. (2002), *Toward secure and resilient interdependent infrastructures*. *Journal of Infrastructure Systems*, *8*(3), 67-75.

Amin M. (2003), *North America's electricity infrastructure : Are we ready for more perfect storms*? IEEE Security & Privacy, 1(5), 19-25.

Ayadi A., Ousadou-Ayadi F., Bourouis S., Benhallou H. (2002), *Seismotectonics and seismic quietness of the Oranie region (Western Algeria): The Mascara earthquake of August 18th 1994, Mw = 5.7, Ms = 6.0*. Journal of Seismology, 6: 13–23.

Belazougui M. (2018), *La politique nationale de gestion des risques de catastrophes*, rencontre national sur la gestion des risques de catastrophes - Ministre de l'Intérieur, des Collectivités locales et de l'Aménagement du territoire. 22, 23 octobre 2018 Alger, Algérie.

Benmokhtar A. (2019), *Risk management related to the handling of explosive products* [in French]. In: Second Conference of Industrial Security, National Defense Minister, Military manufacturing department, October 2019. Algiers, Algeria.

Benouar D., Molas G. L., Yamazaki F. (1996), *Earthquake hazard mapping in the Maghreb countries: Algeria, Morocco, Tunisia*, Earthquake Engineering and Structural Dynamics 25(10):1151-1164.

Benouar D. (1994), *Materials for the investigation of the seismicity of Algeria and adjacent regions during the twentieth century*.

Benouar D. (2004), *La catastrophe du 10 novembre 2001 à Alger*. Du PNUD, p28.

Benouar D., Meslem A. (2007), *Seismic risk in existing school buildings in Algeria*. Regional Development Dialogue, 28(2).

Beyeler W. E., Glass R. J., Bech M., Soramäki K. (2006), *Congestion and Cascades in Payment Systems. Federal Reserve Bank of New York, Staff Reports no. 259, September 2006, New-York, USA, 39 p.*http://www.ny.frb.org/research/staff_reports/sr259.html.

Brown K. (2014), *Global environmental change I: A social turn for resilience?*, Progress in Human Geography **38(1)**:107–117.

Brown T. (2007), *Multiple modeling approaches and insights for critical infrastructure protection, Computational models of risks to infrastructure*, NATO Security through Science Series D-Information and Communication Security 13:23.

Brown T. J., Beyeler W. E., Barton D. (2004), *Assessing infrastructure interdépendances : the challenge of risk analysis for complex adaptive systems*, International Journal of Critical Infrastructure **1(1)**:108-117.

Canadian Standard Association (CSA) (2008), CSA Z1600-08, *Emergency management and business continuity programs*, Canada.

Canzani E. (2016), *Modeling dynamics of disruptive events for impact analysis in networked critical infrastructures*, In: 13th International Conference on Information Systems for Crisis Response and Management, ISCRAM, Rio de Janeiro, Brazil.

Cobb A. (1999), *Critical infrastructure attack: An investigation of the vulnerability of an OECD country*. In Bosch, J.M.J., Luiijf, H.A.M., Mollema, A.M. (Eds.) NL ARMS – *Netherlands Annual Review of Military Studies 1999: Information Operations, Tilburg University Press, Tilburg, Netherlands, pp. 201- 222.*COM/2006/786 final.

Commission Des Communautés Européennes (COM) (2004), *Communication de la commission au conseil et au parlement européen lutte contre le terrorisme : préparation et gestion des conséquences*. Bruxelles.

Commission Des Communautés Européennes (COM) (2006), *Communication de la commission sur un programme européen de protection des infrastructures critiques. Concernant le recensement et le classement des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection.* Bruxelles.

Commonwealth Scientific and Industrial Research Organisation (CSIRO) (2008), *Protecting Australia's critical infrastructure with CIPMA*http://www.csiro.au/partnerships/CIPMA.html.

Conrad S. H., O'reilly G. P. (2007), *An Overview of Energy and Telecommunications Interdependencies Modeling at NISAC. Computational Models of Risks to infrastructure. IOS Press, 8 p.*

Conrad, S. H., LeClaire R. J., O'Reilly G. P., Uzunalioglu H. (2006), *Critical national infrastructure reliability modeling and analysis*. Bell Labs Technical Journal, 11(3), 57-71.

Council Directive (1996), *96/82/EC of 9 December 1996 the control of major-accident hazards involving dangerous substances*, Official Journal L 010, 14 January 1997, p13-33.

Cremona C. (2002), *Applications des notions de fiabilité à la gestion des ouvrages existants*, Presses de l'École Nationale des Ponts et Chaussées. France.

Dauphiné A. (2001), *Risques et catastrophes*. Observer-Spatialiser-Comprendre-Gérer. Paris, Armand Colin, 288 p.

Debray B., Chaumette S., Descouriere S., Trommeter V. (2006), *Méthode d'analyse des risques générés par une installation industrielle*, INRIS-DRA-2006-P46055-CL47569, Ω7.

Dufour D., Neault J., Robert B. (2009), *Démarche gouvernementale de résilience des systèmes essentiels - Colloque sur la sécurité civile 2009* - Ministère de la Sécurité publique du Québec. Sécurité civil Québec.

Dunn M. (2005), The socio-political dimensions of critical information infrastructure protection, International Journal of Critical Infrastructures 1(2-3) :258-268.

Ellison J. (2007), *Modeling the US Natural Gas Network*. Institute of Industrial Engineers (IIE) Transactions *39, 6 p.*https://www.sandia.gov/nisac-ssl/publications/

Eusgeld I., Kröger W., Sansavini G., Schläpfer M., Zio E. (2009), *The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures*, Reliability Engineering and System Safety **94(5)**:954-963.

Eusgeld I., Nan C., Dietz S. (2011), *"System-of-systems" approach for interdependent critical infrastructures*, Reliability Engineering and System Safety **96(6)**:679-686.

Faculté Polytechnique De Mons (1998), *Méthodologie pour l'identification et l'évaluation des effets domino*. Ministère Fédéral de l'Emploi et du Travail, Administration de la sécurité du travail, Direction risques chimiques, Métatechnique, CRC/MT/003, première édition, 93 p.

Gao J., Li D., Havlin S. (2014), *From a single network to a network of networks*, National Science Review **1(3)**:346-356.

Gendreau N., 1999, *L'évaluation de la vulnérabilité et des enjeux : la méthode inondabilité*, In : Hubert G. et Ledoux B. (dirs), Le coût du risque, l'évaluation des impacts socioéconomiques des inondations, Paris, Presses de l'école nationale des Ponts et Chaussées, pp. 123-127.

Godschalk D. R. (2003), *Urban hazard mitigation : creating resilient cities*, Natural Hazards Review **4(3)**:136-143.

Gouvernement Algérien (1985a), *Décrets n°85-231 du 29 mai 1985 relatif à l'organisation des interventions et secours en cas de catastrophe*, Journal Officiel de la République Algérienne Démocratique et Populaire 36 : 832-836.

Gouvernement Algérien (1985b), *Décrets n°85-232 du 29 mai 1985 relatif à la prévention des risques de catastrophe*, Journal Officiel de la République Algérienne Démocratique et Populaire 36: 836-837.

Gouvernement Algérien (1996), *Loi 96-438 du 07 décembre 1996 portant sur la constitution algérienne*, Journal Officiel de la République Algérienne Démocratique et Populaire 76:5-27.

Gouvernement Algérien (2004), *Loi 04-20 du 25 décembre 2004 relative à la prévention des risques majeurs et à la gestion des catastrophes, dans le cadre du développement durable*, Journal Officiel de la République Algérienne Démocratique et Populaire 43 : 13-21.

Gouvernement Algérien (2011), Décret exécutif n° 11-194 du 22 mai 2011 *portant missions, organisation et fonctionnement de la délégation nationale aux risques majeurs*, Journal Officiel de la République Algérienne Démocratique et Populaire 29 : 7-9.

Gouvernement Algérien (2016), *Loi 16-01 du 6 mars 2016 relative à la modification de la constitution algérienne*, Journal Officiel de la République Algérienne Démocratique et Populaire 25 : 5-38.

Gouvernement Algérien (2019), *Décret exécutif n° 19-59 du 2 février 2019 fixant les modalités d'élaboration et de gestion des plans d'organisation des secours*, Journal Officiel de la République Algérienne Démocratique et Populaire 10 : 6-11.

Gouvernement Français (2003), *Loi n° 2003-699 des 30 juillet 2003 relative à la prévention des risques technologiques et naturels et à la réparation des dommages*, Journal Officiel De La République Française, n°175 .p.13021.

Gouvernement Français (2004), *Loi n° 2004-811 du 13 août 2004 portant modernisation de la sécurité civile,* Journal Officiel De La République Française, Texte n° 3 p14626.

Haimes Y. Y., Horowitz B. M., Lambert J. H., Santos J. R., Lian C., Crowther K. G. (2005), *Inoperability input-output model for interdependent infrastructure sectors. I: Theory and methodology*, Journal of Infrastructure Systems **11(2)**:67-79.

Hémond Y., Robert B. (2014), *Assessment process of the resilience potential of critical infrastructures*, International Journal of Critical Infrastructures **10(3-4)**:200-217.

Henry J-B. (2004) : *Systèmes d'information spatiaux pour la gestion du risque d'inondation de plaine*. Thèse de Doctorat. L'Université de Strasbourg I.

Herder P. M., Thissen W. A. H. (2003), *Critical infrastructures: a new and challenging research field* In: Critical Infrastructures State of the Art in Research and Application.

Institut National des Hautes Études de Sécurité (INHES) (2008), *Rapport : Le marché de la sécurité privée en France*. France p340.

Kaplan S. (1997), *The words of risk analysis*, Risk Analysis **17(4)**:407-417.

Kollikkathara N., Feng H., Yu D. (2010), *A system dynamic modeling approach for evaluating municipal solid waste generation, landfill capacity and related cost management issues*, Waste Management 30(11):2194-2203.

Landy G., (2007), AMDEC : Guide pratique, Edition AFNOR 2007.

Lasbordes P. (2006), *La sécurité des systèmes d'information : un enjeu majeur pour la France*. La documentation française, collection des rapports officiels, Paris, France, 200 p.

Lechat, M. F. (1990), *The international decade for natural disaster reduction: background and objectives*. Blackwell.

Lemperiere F. (1999), *Risk analysis: What sort should be applied and to which dams?*, Hydropower and Dams **6**:128-132.

Leontief W. (1966), *Input-output economics*, Oxford University Press, Oxford, United Kingdom.

Lewis D., Mioch J. (2005), *Urban vulnerability and good governance*, Journal of Contingencies and Crisis Management **13(2)**:50-53.

Little R. G. (2002), *Controlling cascading failure: Understanding the vulnerabilities of interconnected infrastructures*. Journal of Urban Technology, *9*(1), 109-123.

Mazouni M. H. (2008), *Pour une meilleure approche du management des risques : de la modélisation ontologique du processus accidentel au système interactif d'aide à la décision*, Doctorat de l'institut National Polytechnique de Lorraine, p.47.

Mc Daniels T., Chang S., Peterson K., Mikawoz J., Reed D. (2007), *Empirical framework for characterizing infrastructure failure interdependencies*, Journal of Infrastructure Systems **13(3)**:175-184.

Meerow S., Newell J. P. (2019), *Urban resilience for whom, what, when, where, and why?*, Urban Geography **40(3)**:309-329.

Meerow S., Newell J. P., Stults M. (2016), *Defining urban resilience: A review*, Landscape and Urban Planning **147**:38-49.

Mendonça D., Wallace W. A. (2006), *Impacts of the 2001 world trade center attack on new york city critical infrastructures*. Journal of Infrastructure Systems, 2006, vol. 12, no 4, p. 260-270.

Metzger P., D'Ercole R. (2011), «*Les risques en milieu urbain : éléments de réflexion* », *EchoGéo* [En ligne], 18 |2011, en ligne le 06 décembre 2011.

MIBS (2006), Les infrastructures critiques : bien maîtriser le socle du patrimoine informatique de l'entreprise. Livre blanc, MIBS Infrastructure & Services, 23 p.

Michel-Kerjan E. (2003), *Risques catastrophiques et réseaux vitaux : de nouvelles vulnérabilités*. Flux, (1):6-15.

Mili L., Qiu Q., Phadke A. G. (2004), *Risk assessment of catastrophic failures in electric power systems*. International Journal of Critical Infrastructures, 1(1): 38-63.

Ministère de la Sécurité Publique du Québec (MSP) (2007), *Cadre de référence pour la gestion desrisques*, Québec, Canada, 34 p.

Mitchell C., Decker C., (2004), *Applying risk- based decision- making methods* Applying Risk-based Decision-making Methods/Tools to U.S. Navy Antiterrorism Capabilities.

Mortureux Y. (2002), *Sécurité et gestion des risques- méthode d'analyse des risques- Maîtriser les concepts et méthodes nécessaire à la sécurité et à la gestion des risque- Analyse Préliminaire des risques.* Technique de l'ingénieur.

Moses F. (1998), *Probabilistic-based structural specifications*, Risk Analysis **8(4)** :445-454.

Norme CEI 300-3-9 (2015), Gestion de la sûreté de fonctionnement. CEI.

Norme NF X 60-500 (1988), Terminologie relative à la fiabilité. NF.

Nozick L. K., Turnquist M. A., Jones D. A., Davis J. R., Lawton C. R. (2005), *Assessing the performance of interdependent infrastructures and optimizing investments*, International Journal of Critical Infrastructures **1(2-3)**:144-154.

O'Reilly G. P., Jrad A., Kelic A., LeClaire R. (2007), *Telecom critical infrastructure simulations: Discrete-event simulation vs. dynamic simulation how do they compare?*. In IEEE Global Telecommunications Conference p 2597-2601.

Organisation des Nations Unies (ONU) (1992), *Déclaration de Rio sur l'environnement et le développement*. Rio de Janeiro, Brésil.

Ouyang M. (2014), *Review on modeling and simulation of interdependent critical infrastructure systems*, Reliability Engineering and System Safety **121**:43-60.

Pageon, J. (2008), *Méthodologie d'évaluation de la vulnérabilité d'une MRC face aux ressources essentielles*, École Polytechnique de Montréal, Département de mathématiques et de génie industriel, Québec, Canada, 94 p.

Patterson S.A., Apostolakis G. E. (2007), *Identification of critical locations across multiple infrastructures for terrorist actions*, Reliability Engineering and System Safety **92(9):**1183- 1203.

Peerenboom J. P., Fisher R. E. (2007), *Analyzing cross-sector interdependencies*. In 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07) (pp. 112- 112). IEEE.

Peerenboom, J. P. (2001), *"Infrastructure Interdependencies: Overview of Concepts and Terminology,"* invited paper, National Science Foundation/Office of Science and Technology Policy Workshop on Critical Infrastructure: Needs in Interdisciplinary Research and Graduate Training; Washington, DC, June 14-15, 2001.

Perrow C. (1984), *Normal Accidents: living with high-risk technologies*, Basic Books, New York,USA.

Petit F. (2009), *La vulnérabilité cybernétique des infrastructures essentielles*. Thèse de Doctorat École Polytechnique de Montréal, Québec, Canada.

Petit F. (2008), *Concepts d'analyse de la vulnérabilité des infrastructures essentielles-prise en compte de la cybernétique* École polytechnique (Montréal, Québec).

Petit F., Robert B., Rousselle J. (2004), *Une nouvelle approche pour la caractérisation des aléas et l'évaluation des vulnérabilités des réseaux de support à la vie*. Revue Canadienne de Génie Civil, No. 31, pp. 333-344.

Peyras. L, (2002)**,** *Diagnostic et analyse de risques liés au vieillissement des barrages développement de méthodes d'aide à l'expertise*. Thèse doctorat. Université de la Méditerranée (Aix- Marseille II).

Plamondon M-E. P., (2004), *Méthodologie d'évaluation du degré d'essentialité appliquée à la planification des mesures d'urgence,* Thèse de maitrise École polytechnique de Montréal, Québec, Canada.

Plate E. J. (1996), *Dams and safety management at downstream valleys, Proceedings of the International* NATO Workshop Dams Safety Manage Downstream valley, Rotterdam, Betamio de Almeida and Viseu, pp. 27-43.

Popescu C. A., Simion, C. P. (2012), *A method for defining critical infrastructures*. Energy, 42(1), 32-34.

Pye G., Warren M. J. (2006), *Security management: Modeling critical infrastructure*, Journal of Information Warfare 5(1): 46-61.

Reniers G., Cozzani V. (2013), *Domino effects in the process industries: Modeling, Prevention and Managing*, Elsevier, London, UK.

Ridoux. M. (2002), *Sécurité et gestion des risques- méthode d'analyse des risques- Maîtriser les concepts et méthodes nécessaire à la sécurité et à la gestion des risque- Analyse des Modes de Défaillance leurs Effets et leurs criticités.*Technique de l'ingénieur

Rinaldi S. M. (2004), *Modeling and simulating critical infrastructures and their interdependencies*, Proceedings of Thirty-Seventh the Hawaii International Conference on System Sciences, Hawaii, pp.54-61.

Rinaldi S. M., Peerenboom, J. P., Kelly T. K. (2001), *Identifying, understanding, and analyzing critical infrastructure interdependencies*, IEEE Control Systems Magazine **21(6)**:11-25.

Robert B. (2004), *A method for the study of cascading effects within lifeline networks*, International Journal of Critical Infrastructures **1(1)**:86-99.

Robert B., Morabito L., Quenneville O. (2007), *The preventive approach to risks related to interdependent infrastructures*, International Journal of Strategic Emergency Management 4(2):166-182.

Robert B., Senay M. H., Plamondon M. E. P., Sabourin J. P. (2003), *Characterization and ranking of links connecting life support networks*, in: Public Safety and Emergency Preparedness, PSEPC, Canada.

Robert B., Cloutier I. (2007), *Geoinformation for Risk Prevention – The Challenges Facing Critical Infrastructure Protection.* Joint CIG/ISPRS Conference on Geomatics for Disaster and Risk Management, May 22–25, Toronto, Ontario, Canada.

Robert B., de Calan R., Morabito L. (2008), *Modelling interdependencies among critical infrastructures*. International Journal of Critical Infrastructures, 4(4), 392-408.

Rowell D., Wormley D. N. (1997), *System dynamics: an introduction*. Prentice Hall.

Schneider F. B. (1999), *Trust in Cyberspace,* National Academy Press, Washington DC, USA.

Scott, G. (2007), CIPMA – *Critical Infrastructure Protection Modelling and Analysis: Overview of CIP in Australia*. Séminaire technologique du *Centre risque & performance*, 15 novembre 2007, École Polytechnique de Montréal, Québec, Canada.

Sendai Framework for Disaster Risk Reduction (2015-2030), *Reports and publications*. United Nations Office for Disaster Risk Reduction.

Sécurité Publique Canada (SPC) (2008a), *Aller de l'avant avec la stratégique nationale et le plan d'action pour les infrastructures essentielles.* Sécurité Publique Canada.

Sécurité Publique Canada (SPC) (2008b). *Protection des infrastructures essentielles*. Sécurité publique Canada.

Sécurité Publique et Protection Civile Canada (SPPCC) (2003), *Programme national de fiabilité des infrastructures essentielles*. Site internet de la SPPCC, Canada.

Stapelberg R .F. (2008), *Infrastructure systems interdependencies and risk informed decision-making (RIDM): impact scenario analysis of infrastructure risks induced by natural, technological and intentional hazards*, Journal of Systemic, Cybernetics and Informatics **6(5)**:21-27.

Sterman J. D. (2000), *Business dynamics: systems thinking and modeling for a complex world*, Irwin/McGraw-Hill, Boston, Massachusetts, USA.

Tian G., Wu J., Yang Z. (2010), *Spatial pattern of urban functions in the Beijing metropolitan region*, Habitat International 34(2):249-255.

Too E. G. (2011), *Capability for infrastructure asset capacity management*, International Journal of Strategic Property Management **15(2)**:139-151.

Trusted Information Sharing Network (TISN) (2008), *Critical infrastructure protection project.* En ligne https://www.tisn.gov.au/critical-infrastructure : Australie.

U.S. Department of Homeland Security (DHS) (2004), *Launches Protected Critical Infrastructure Information Program to Enhance Homeland Security*, Facilitate Information Sharing, Homeland Security Digital Library.

U.S. Department of Homeland Security (DHS) (2009). *Protected Critical Infrastructure Information (PCII) Program*. Site Internet du Department of Homeland Security [En ligne], États-Unis. https://www.cisa.gov/pcii-program.

U.S. Department of Homeland Security (DHS) (2013). *National Infrastructure Protection Plan (NIPP) 2013: Partnering for critical infrastructure security and resilience*. [PDF file]. https://www.dhs.gov/sites/default/files/ publications/national-infrastructure-protection-plan 2013-508.pdf. p57.

U.S. Government, The White House (1998), *The Clinton Administration's Policy on Critical Infrastructure Protection*: Presidential Decision Directive 63. May 22, 1998, Washington, D.C.

U.S. Government, The White House (2003a). *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Washington, DC, February 2003.

U.S. Government, The White House (2003b), The White House: *Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection*, Washington, DC, December 17, 2003.

Viellard L., Ribnikar D. (2003), *La protection des infrastructures critiques face aux menaces asymétriques – Synthèse*. Compagnie européenne d'intelligence stratégique, 6 p.

Villemeur A. (1988), *Sûreté de fonctionnement des systèmes industriels : Fiabilité, facteur humain, informatisation*, Eyrolles, Paris.

Wallace W. A., Mendonça D., Lee E., Mitchell J., Chow J. (2001), *Managing disruptions to critical interdependent infrastructures in the context of the 2001 World Trade Center attack. Impacts of and Human Response to the September 11, 2001 Disasters: What Research Tells Us*.

Zimmerman R. (2001), *Social implications of infrastructure network Interactions*, Journal of Urban Technology **8(3)**:97-119.

Zimmerman R., Restrepo C. E. (2006), *The next step: quantifying infrastructure interdependencies to improve security*, International Journal of Critical Infrastructures **2(2-3)**:215-230.

Zimmerman R. (2002), *Enjeux et gestion des interactions entre les différents réseaux d'infrastructure*. Flux, (1), 54-68.

Zimmerman R., Horan T. A. (Eds.) (2004), *Digital Infrastructures: Enabling civil and environmental systems through information technology*. Psychology Press.

Zio E., Sansavini G. (2011), *Modeling cascading failures in "systems of systems" with uncertain behavior uncertain behavior*, in: International Conference on Applications of Statistics and Probability in Civil Engineering, Zurich, Switzerland. pp. 1858-1866.

Zwingelstein G. (1996), *La maintenance basée sur la fiabilité* – guide pratique d'application de la RCM, Hermes, Paris.