

## CHAPITRE 1

### LA PROBLEMATIQUE

L'existence d'un Système Interactif d'Aide à la Décision (SIAD) dans la sécurité des bâtiments publics constitue un outil important dans la démarche des opérations d'urgence entreprises dans les minutes qui suivent le danger, pour prévenir ainsi les risques et assurer la sécurité des occupants. Ce système devra fournir des informations viables suivant les conditions du lieu pour s'appliquer à plusieurs types de bâtiment tout en respectant aux lois des différents pays où se trouve le bâtiment concerné. Lors d'un danger, pendant la panique, il faut prendre la bonne décision le plus vite possible avec sang froid, ce qui s'avère presque impossible pour le responsable de sécurité lorsqu'il s'agit de la première fois et que le cas présent est très grave. Le système à concevoir doit donc clarifier les choses et offrir les meilleures différentes alternatives.

Suite à notre étude qui sera présentée plus loin, nous avons constaté que peu de SIAD de ce genre existe, encore moins, d'une manière publique. Dans cette optique, nous considérons important la création d'un outil qui regroupe la liste des dangers et des procédures d'urgence, d'évacuation et des solutions aux problèmes en correspondance, applicable à plusieurs pays différents et à plusieurs bâtiments publics variés.

Un autre point essentiel de la démarche de création de ce genre de SIAD est que nous n'avons pas encore trouvé un ouvrage qui consiste à regrouper et synthétiser les informations permettant à n'importe quel administrateur de pouvoir de manière instinctive comprendre comment construire et compléter le système suivant de nouveaux paramètres.

Pour comprendre la nécessité d'un outil d'aide à la prise de décision dans le cadre de la sécurité pour des situations d'urgence dans un bâtiment public, il est nécessaire de connaître l'état de la situation de la sécurité nationale dans le monde et même de présenter divers systèmes interactifs déjà existant.

### **1.1 État de la situation en sécurité**

Depuis plus de cent ans, des normes et des codes de la construction sont écrits, présentés et suivis pour assurer avant tout la sécurité des occupants dans des bâtiments. L'édifice doit être construit suivant les règles de l'art pour ne présenter aucune menace par des défauts structurels. Il doit aussi fournir un refuge et des voies de déplacement et de sortie pour permettre aux personnes présentes de se protéger et de s'éloigner d'un risque ou un danger. Ainsi, un réseau de gicleurs limite la progression d'un foyer d'incendie ou encore le système d'aération assure le désenfumage et la circulation de l'air pour atténuer des fuites ou des sources de gaz toxique. Et depuis peu, de plus en plus d'édifices publics, des immeubles et des gratte-ciel se pourvoient d'un réseau de télésurveillance qui contrôle les entrées et sorties des individus mais qui offre aussi un moyen de détecter et de voir des dangers presque n'importe où dans le bâtiment.

Par ailleurs, depuis une dizaine d'année seulement, il y a eu un regain d'intérêt pour les environnements intelligents (COOK et DAS, 2005) qui offrent de grandes possibilités en interactivité entre l'homme et la maison et donc une meilleure rapidité dans les réponses face aux dangers. Des recherches ont été présentées durant la conférence MANSE (Conference on Managing Interactions in Smart Environments) en 1999. Celles-ci définissent un environnement intelligent comme un réseau d'appareils de mesure, de contrôle ou encore électroménager qui sont capables d'analyser les données grâce à des senseurs intelligents afin de prendre certaines décisions dans le but d'améliorer le confort des occupants ou assurer les économies d'énergie à travers l'éclairage, le chauffage ou la climatisation. Cette interactivité entre les appareils est aussi applicable

avec des réseaux sans fil utilisant le Wi-Fi pour faciliter le contrôle à distance pour la sécurité. Un exemple parfait de bâtiment intelligent qui utilise cette technologie est l'École des Technologies Supérieure (ETS) à Montréal. Comme il est indiqué sur son site Web (ETS, un bâtiment intelligent), cette école comporte l'optimisation des quatre éléments : (a) la structure; (b) les systèmes de protection, de climatisation, d'alimentation électrique; (c) les services de télécommunication, de courrier électronique, de vidéoconférence,... et (d) la gestion d'énergie, de surveillance, d'entretien, de comptabilité,... . Ainsi grâce à un réseau complexe de détecteurs sophistiqués, l'édifice peut détecter toute variation brusque de température, mesurer la composition chimique de l'air ambiant dans une salle pour interpréter la présence d'un risque ou d'un danger et lancer automatiquement l'alarme correspondante.

Aux États-unis, l'Institut National des Normes et des Technologies (NIST en anglais) a travaillé avec les entreprises de construction et la sécurité publique et les technologies d'information pour développer des normes et des conventions pour l'élaboration d'un immeuble intelligent qui puisse donner un maximum d'information dans les plus brefs délais aux premiers secours pour assurer la protection des occupants ("Washington Update", 2006). Néanmoins, un bâtiment intelligent ou l'ETS ne peut lancer une alerte automatique si et seulement si le danger a été détecté. Il ne peut agir qu'envers des dangers mesurables. Mais qu'en est-il des dangers non quantifiables comme des intrusions, une alerte à la bombe ou tout simplement une personne qui arrive et menace avec une bombe ? Le système de sécurité seul est incapable de gérer des situations de crise impliquant des attaques terroristes.

L'attaque du 11 septembre 2001 sur les tours jumelles du World Trade Center représente un moment clé qui a précipité le monde dans la course vers la sécurité des personnes et des bâtiments. A cette date, deux Boeing 767 se sont abattus sur chacune des tours de 110 étages. Le feu généré par les 91,000 litres de carburant n'a laissé aucune chance à l'intégrité de la structure, causant la chute des deux tours et la mort de 2,092 personnes

prises au piège dans les étages au-dessus de la zone d'impact et qui n'avaient plus aucun moyen de fuir (SUNDER, 2006). Suivant des rapports, les escaliers aux quatre coins de la tour sont construits pour permettre l'évacuation en une heure au mieux. Ce qui s'est passé constituait une situation inattendue et d'une ampleur extrême qui a dépassé les systèmes de sécurité (NICHOLSON, 2001). D'autre part, l'évacuation était d'autant plus difficile que le poste de commandement de sécurité était anéanti par le choc avec l'avion, la plupart des systèmes de gicleurs et d'aération étaient endommagés et la communication était alors très désordonnée. Des annonces contradictoires ont amenés plusieurs retards dans les déplacements et procédures d'évacuation (SUNDER, 2006). Cela s'explique en partie par le fait que la procédure normale pour les immeubles de grande taille (« Defend in Place ») consiste à n'évacuer que l'étage touché par un feu tandis que les autres personnes présentes doivent rester à leur étage correspondant dont la structure étaient censée offrir un refuge suffisant le temps que les secours arrivent. La procédure normale a l'avantage de faciliter une évacuation ordonnée avec une circulation fluide dans les voies de sortie. Mais l'ampleur de l'attentat du 11 septembre 2001 défiait toute prévision et l'initiative de certains employés à inciter une évacuation générale dans le calme qui intéresse beaucoup la NFPA (National Fire Protection Association) qui est l'organisme responsable des codes de construction et de sécurité dans l'Amérique du Nord. L'intérêt est d'autant plus grand que c'est la NFPA elle-même qui a mis en place la procédure « Defend in Place » qui ne s'adaptait pas du tout à ce moment (NICHOLSON, 2001). D'un autre côté, les exercices de sécurité imposés et répétés ainsi que le sang froid ont assuré, contrairement à ce qu'on pourrait croire, la survie de plus de 87% des approximativement 17,400 occupants présents. L'attentat à la bombe en 1995 du bâtiment fédéral Alfred P. Murrah à Oklahoma City a en quelque sorte préparé plusieurs autres immeubles d'affaire. Les procédures ont été révisées et les exercices accrues pour éviter une évacuation désordonnée et dans le noir qui a engendré un certain stress et état de panique durant cet attentat à la bombe. En conséquence, plusieurs rapports ont depuis souligné l'importance d'améliorer les technologies et moyens d'évacuation, les réponses aux premiers secours avec les communications

d'urgence avec le centre de commandement. En parallèle, il est vital de réviser et d'actualiser les plans, les exercices, les procédures standard SOPs (Standard Operating Procedures) et de tirer leçons des événements pour tenter de prévoir l'inattendu (NICHOLSON, 2001; SUNDER, 2006).

Une entrevue avec Danielle POITRAS, ing. qui est une ancienne chargée de projet en sécurité dans les hôpitaux de Montréal (POITRAS, 2006) nous donne une description rapide des procédures d'urgence durant une crise pour des hôpitaux au Québec. Et il s'agit plus particulièrement des cas d'attaques chimiques. Depuis, les premières attaques de type chimique pendant la guerre du Golf (17 janvier – 3 mars 1991) et l'attentat au gaz sarin en mars 1995 dans un métro de Tokyo, le gouvernement du Québec et des autres pays dans le monde s'est intéressé à la réaction la plus adaptée pour protéger et sauver au maximum les blessés. Une cellule de crise doit porter secours que ce soit des résidences, des bâtiments civils ou des édifices nécessitant une urgence. Cette cellule est composée de la sécurité civile, la santé publique, la police (Sécurité au Québec (SQ), Service de Police de la Ville de Montréal (SPUM)), du Service de Prévention des Incendies (SPIM) et l'Urgence Santé (POITRAS, 2006). Lors d'une crise d'une telle envergure, un centre hospitalier doit limiter son périmètre à un seul accès qui est la zone « chaude » ou de contamination qui permet de faire le tri des blessés qui sont ensuite transportés dans la zone « tiède » de décontamination et des urgences avec toutes les divers services correspondant au type de centre hospitalier avant de transférer le patient vers la zone « froide » des soins, là où sa vie n'est plus menacée. Aux États-unis, la NFPA et l'Administration Fédérale de la Gestion des Urgences (Federal Emergency Management Administration (FEMA) en anglais) ont créées de nouvelles directives en terme de recherche et de secours des blessés durant une crise, suite à l'attentat du 11 septembre 2001 (NICHOLSON, 2001). Les normes NFPA 1006 et 1670 ont pour but d'aider les autorités d'une juridiction à analyser et identifier le niveau de capacité opérationnelle face à un désastre avec des formations et des critères de sécurité. Ce sont surtout des mesures après le désastre et pour la crise sur le long terme pour venir en aide

aux victimes. Il y a même plusieurs procédures et des outils d'aide à la décision afin de mettre les meilleures dispositions pour réparer les dégâts, héberger les sinistrés et leur venir en aide pour les soins et la nourriture (DENIS, 2002). Ce qui est souvent le cas suite à une catastrophe naturelle aussi.

L'ouragan Katrina en août 2005 a causé des dégâts considérables et de nombreuses victimes dans le sud du Texas à cause surtout de l'échec de l'évacuation de personnes âgées et des familles défavorisées qui n'avaient pas suffisamment confiance aux autorités. Ces dernières étaient averties de fuir mais ne savaient dans quelle direction aller et n'avaient pas forcément un moyen de locomotion comme une banale voiture. Les décisions ont été inefficace quant à avertir certaines populations à cause d'un manque de compréhension sur un niveau social (CORDASCO et WOOD, 2006). Des efforts sont réalisés pour améliorer la réactivité des mesures de recherches et de sauvetage, une aide pour l'évacuation des personnes handicapées dans l'urgence, de meilleurs avertissements et des informations préventives. Lorsqu'une localité se retrouve isolée du reste du monde suite à un sinistre et une coupure des communications, celle-ci doit alors fonctionner de manière autonome avec ses propres sources de connaissances en matière d'urgence et de sécurité. Il faut alors fournir un maximum d'aide aux décisions et d'information préventivement pour qu'elle puisse tenter de gérer au mieux la crise (STYRON, 2006).

De même, quelques paragraphes plus haut, on a parlé d'environnement intelligent et des alarmes automatiques. Un réseau de détecteurs, aussi sophistiqués soient-ils pour analyser les données recueillies, n'est pas à l'abri d'une fausse alerte. Bien qu'interdit par la loi, la fumée de cigarette peut déclencher sous certaine condition l'alarme à incendie. Plusieurs erreurs ont été constatées à l'ETS suivant l'avis de spécialiste en sécurité travaillant dans l'établissement. Nous avons même vu que le système de sécurité seule ne pourrait intervenir pour protéger 600 personnes dans le hall principal durant l'ISIE 2006 face à l'intrusion d'un terroriste menaçant avec une bombe si on prend un

cas d'exemple extrême. Par conséquent le facteur humain reste vital dans ce genre de situation. L'homme, le responsable de sécurité, est le seul apte à prendre les bonnes décisions car il s'adapte au mieux à la situation et sait corriger les fausses alertes.

Une recherche américaine sur les sciences sociales sur plus de 50 ans a montré que les êtres humains réagissent tous de manière similaire face à une situation extrême telle un ouragan, un tremblement de terre, un accident de centrale nucléaire ou une attaque terroriste. La première réaction du public serait un choc émotionnel avec une certaine désorientation car il cherche à trouver de nouveaux repères pour aider les proches ou pour fuir et se sauver. Mais ces gens recherchent aussi des conseils et des directives. Les organisations privées de sécurité ont besoin de communiquer avec le public pour assurer une coopération avec les secours (MILETI, 2001). Un Système Interactif d'Aide à la Décision (SIAD) pour assurer cette communication représente un outil très intéressant pour faire garder le sang-froid et éviter une panique. L'utilisateur de l'outil pourra être conseillé au mieux possible et obtenir très vite des informations pour supporter son analyse et effectuer les étapes d'urgence dans le calme. Le but de ce mémoire est alors de proposer un cadre de développement pour un SIAD répondant à tout type de danger dans l'urgence.

## **1.2 Les systèmes d'aide à la décision déjà existants**

Avant de présenter un quelconque cadre d'étude pour un SIAD en sécurité des bâtiments publics dans l'urgence, il est nécessaire de voir quels autres systèmes existent déjà ou sont en projet. Plusieurs centres d'excellence d'étude et de recherche en sécurité ont déjà travaillé sur de telles technologies. Pour la France, il y a l'Institut National de Recherche et de Sécurité (INRS) et le Centre Scientifique et Technique du Bâtiment (CSTB); au Québec, c'est le Ministère de la Sécurité Publique du Québec qui s'occupe aussi de la gestion de crise alors qu'en France, il s'agit de l'Observatoire National de la Sécurité. La NFPA et la FEMA sont des organismes responsables des codes de construction et des

directives de sécurité surtout pour l'Amérique du Nord. Selon la NFPA, des études suite à l'attentat du 11 septembre 2001 ont montré qu'une préparation de tous les acteurs, secours et employés de bureaux, est la clé de la réussite pour une urgence et une évacuation réussie en réponse à une attaque terroriste. L'association a souhaité faire prendre conscience au public visé du développement de nouvelles normes et codes en prévision aux crises et a lancé la mise en place de nouvelles prédisposition en construction. Elle a par la suite lancé plusieurs programme « d'éducation » du public envers le terrorisme (NICHOLSON, 2001).

Un des premiers projets intéressant à ce mémoire en Amérique du nord en 2001 correspondait au bâtiment intelligent qui a été discuté plus haut. Mais l'optique est surtout portée ici sur l'aide offert aux premiers secours par l'édifice. Cette dernière ne lance pas de procédure automatique mais doit surtout informer de la situation pour que les autorités (pompiers, police,...) puissent agir rapidement en conséquence. Un autre projet traité en 2001 était le développement d'un système de référencement en réponse pour l'urgence proposé par le « National Incident Management System » (NIMS). Le système permettrait de vérifier la certification et l'identité des personnes en charges pour la gestion d'un risque afin que le public puisse prendre confiance aux ordres données par cette personne identifiée comme professionnel agréé ("Washington Update", 2006).

Au Canada et dans la province du Québec, selon Danielle POITRAS (POITRAS, 2006), tous les hôpitaux sont équipés d'un ordinateur indépendant et autonome qui s'occupe exclusivement de la gestion de la sécurité du bâtiment contre les incendies. C'est un ordinateur imperméable à tout autre programme, disposant de sa propre source d'énergie par des générateurs de secours en cas de panne électrique, qui s'occupe de toutes les procédures et des alarmes. Le programme mère envoie un pré signal vers les pompiers si un détecteur anti-incendie est déclenché. Cet ordinateur qui est imposé avec une telle configuration par l'ULC (Underwriter's Laboratories of Canada) ne peut recevoir aucune interaction ou connexion de l'extérieur et ne fait qu'envoyer des informations



aux préposés qui devra confirmer les décisions et procédures d'alerte. D'autre part, après une visite dans le centre commandement de sécurité de l'hôpital Notre-Dame à Montréal, des experts en sûreté confirment que la plupart des autres établissements similaires disposent en plus de cet ordinateur de l'ULC, contre l'incendie d'un autre ordinateur pour assurer d'autres tâches comme la surveillance et la sécurité contre les intrusions. A partir de là ils estiment intéressant d'intégrer un outil d'aide à la décision qui puisse regrouper les directives générales regroupées pour divers dangers. En effet, ces dernières consignes sont bien souvent affichées sur des notices ou des panneaux et peuvent nécessiter une petite manipulation pour les consulter. Un SIAD qui fournirait à la demande des conseils à plusieurs intéressés dans le même temps devient alors profitable.

Par contre, à chaque risque ou problème grave, il n'existe pas systématiquement un appareil de contrôle imposé par le gouvernement. C'est notamment le cas pour des chambres d'isolation. L'entrevue avec un responsable d'installation de ces chambres nous signale qu'il existe bien un moniteur surveillant la pression intérieure de la chambre d'isolement pour éviter les fuites d'air et donc les risques de contamination. Par contre, le logiciel n'est pas imposée par une loi comme ULC mais son fonctionnement doit suivre des directives de sécurité imposées par la corporation de l'hébergement du Québec ou encore le « Control Disease Center » (CDC) dans le monde, auquel le constructeur doit respecter. En cas de danger, il y a un arrêt des systèmes d'évacuation et de ventilation mais ces derniers sont installés et fonctionnent suivant les réarrangements et raccordements dictés par l'ingénieur conseil. C'est pour cela que contrairement aux procédures anti-incendie qui suivent des règles bien strictes, dans le cas des chambres d'isolement. Cela dépendra au cas par cas suivant la disposition dans le centre hospitalier correspondant. Il ne faut donc pas croire qu'à chaque problème il y a toujours des règles strictes mais plutôt des procédures qui s'adoptent au mieux à la situation et même qui se mettent à jour au fur et à mesure que des défauts sont trouvés.

Nous avons vu des appareils installés et avec une fonction exclusive. Il existe par ailleurs des SIAD s'utilisant à travers Internet, il s'agit par exemple du logiciel AGRIOPA de la société française au même nom (système, 2006). Ce dernier apporte aux acteurs de la sécurité des magasins de grande distribution des informations préventives, des outils et des conseils adaptés pour lutter contre toute forme de démarque (différence entre le chiffre d'affaire théorique et réel). C'est un outil d'aide pour un secteur économique pour optimiser et protéger le rendement avant l'apparition du risque ou pour régler des problèmes à travers le Web par des spécialistes. L'outil présente une interactivité intéressante pour transmettre l'aide à travers plusieurs magasins dans le monde du moment que ceux-ci disposent d'un accès Internet, ce qui devient presque une normalité dans les secteurs développés.

D'autres SIAD constituent une aide uniquement pour des secteurs privés ou qui nécessitent une surveillance et une sécurité particulière. Un projet d'outil d'aide à la décision pour l'évaluation du risque chimique a été mené par le département Métrologie des polluants. L'outil présente des listes triées suivant les directives européennes afin de hiérarchiser parallèlement les risques pour la santé, la santé et les impacts environnementaux (VINCENT et BONTHOUX, 2002). Le secteur chimique présente des sites sensibles avec des risques élevés pour l'environnement et la santé qu'il faut à tout prix éviter et maîtriser. Une autre étude française vise une gestion intégrée des risques et une gestion optimale des situations de crises grâce au concept SARA (Système d'Analyse des Risques Accidentels en situation de crise) qui est basé sur l'analyse des dangers inhérents au système étudié (DUSSERE et coll., 2003). L'idée est d'aider à la gestion de crise en agissant avant, pendant et après la crise. Le concept fait donc une évaluation des dangers, de leurs conséquences ainsi que l'analyse des barrières de protection et de la vulnérabilité pour aboutir sur un cycle d'analyse qui se complète afin de donner des mesures préventives, de modéliser le danger pour le lutter et atténuer les risques.

Dans le même ordre d'idée de risque lié avec l'environnement, l'ADEME (Agence de l'Environnement et de la Maîtrise de l'Énergie) en France a voulu en 1999 mettre en place une aide à la décision en matière de prévention de la pollution atmosphérique dans des entreprises. Et comme pour l'exemple précédent du concept SARA, l'outil fait un pré diagnostic et un diagnostic pour étudier les techniques et des analyses qualitatives pour proposer des programmes d'action (DUESO, 1999). Mais d'autres outils ont été développés en réponse à des catastrophes naturelles ou des attaques terroristes. Peu de temps après l'attentat du 11 septembre, des études ont montré une déficience dans les plans d'urgence et d'évacuation et qu'il manquait clairement une alarme compréhensive pour avertir des dangers menaçant la sécurité publique. Le manque d'information et des plans a amené une certaine crainte du public à rester dans la confusion et glisser vers la panique au moment d'une crise. Et même qu'une étude récente a prouvé que 90% du public aux États-unis ne suivraient pas les directives d'évacuation mais chercheraient des informations complémentaires par des autorités afin de mieux connaître la situation. L'intérêt des individus se porte aussi bien vers le secteur privé ou tous les niveaux de gouvernement pour obtenir des informations et donc une aide souhaité pour prendre des décisions (DORY, 2003). Il est alors nécessaire de créer un outil qui puisse informer le public pour les éduquer et préparer en leur communiquant des actions de protection spécifiques à chaque type de danger. Fournir une réponse globale présente plusieurs risques dans des situations dangereuses où la dynamique reste complexe et ne suit pas forcément un scénario prédéfini. Ainsi, le site de la croix rouge (Red Cross, 2006; , "Internet Pages", 2001) met à disposition plusieurs pages Web expliquant les risques de certaines attaques terroristes ainsi que les mesures conseillées à suivre. Le DHS (Department of Homeland Security) américain a aussi mis en place depuis mars 2003 des pages Web donnant des instructions contre le terrorisme avec des systèmes comme EAS (Emergency Alert System). Plusieurs organismes « entraînés » peuvent alors se communiquer et intervenir dans une réponse au désastre (DORY, 2003). De plus, une étude sur les évacuations dans les hôpitaux a montré qu'il vaut mieux préparé dans tous

les cas le personnel aux procédures présentes afin de faire face aux dangers et d'être prêts lors de prises de décisions importantes (HSU et coll., 2004).

Les catastrophes naturelles nécessitent aussi une intervention rapide pour venir en secours aux victimes ou pour annoncer le danger. WAPMERR (World Agency of Planetary Monitoring and Earthquake Risk Reduction) mène des recherches pour améliorer les modèles avancés sur le déroulement des tremblements de terre afin d'accroître l'efficacité des systèmes qui doivent prévoir l'apparition ou évaluer leurs impacts et conséquences ("WAPMERR A New Approach to World-Wide Earthquake Risk Reduction", 2001). En Allemagne, le Système de Planification des Informations d'Urgence en Allemagne (deNIS) permet de prévoir des risques météorologiques comme des tempêtes mais surtout des débordements de fleuve ou des risques d'inondation (KLEI-FIQUET, 2005). Le programme est lié avec un système de gestion des désastres (SDA) qui utilise des données géographiques par Internet. En couplant toutes les informations et mesures des divers organismes de recherches et de sécurité à travers le Web, et l'interaction entre les divers outils, deNIS permet de lancer une alerte très tôt, tout en informant et en conseillant le public touché. Le système ne fait que donner des renseignements pour annoncer la planification, assurer une prévention grâce à diverses fiches sur des sites Web accessibles gratuitement au public. Mais il permet aussi surtout d'aider à gérer une crise après une catastrophe. Cet outil d'aide présente plusieurs avantages sur l'accessibilité des données par les intéressés avec une interactivité sur le Web. Néanmoins il n'a qu'une fonction exclusive pour les catastrophes naturelles en Allemagne.

Nous avons vu qu'aucun système intelligent ne peut gérer automatiquement un danger non quantifiable faisant intervenir le facteur humain comme une intrusion ou une attaque terroriste. La présence d'un acteur humain, le responsable de sécurité, est vitale car l'homme est le seul à pouvoir s'adapter à temps à la situation et prendre les bonnes décisions. Plusieurs SIAD ont été développés afin de donner des mesures

préventivement pour avertir le public ou pour faciliter la gestion de crise après la catastrophe afin de secourir les blessés. Cependant, il n'existe pas vraiment de système qui puisse aider à gérer dans l'urgence une catastrophe dans la minute qui suit son déclenchement dans des bâtiments publics. Il y a bien des systèmes de ce type mis surtout dans le cadre privé ou par des militaires ou pour des sites où la sécurité est une composante majeure. La mémoire a donc pour objectif de proposer un SIAD qui puisse répondre à tout type de danger dans l'urgence pour différents types de bâtiments public et qui a la prétention d'être disponible dans divers pays ou provinces grâce à Internet.

### **1.3 Les objectifs**

Ce mémoire propose un cadre de développement pour la réalisation d'un SIAD permettant de conseiller les opérations nécessaires pour assurer la protection des occupants d'un édifice public dans les minutes qui suivent le danger.

Plus particulièrement, ce cadre de développement comprendra :

- a. l'élaboration d'une méthodologie de création d'un SIAD;
- b. l'élaboration d'une base de connaissances du SIAD;
- c. la proposition d'un fonctionnement de ce SIAD;
- d. l'adaptabilité du système proposé pour un fonctionnement sur Internet.

Ce travail décrira la possibilité de développement d'un outil facile à compléter et à utiliser qui guiderait le responsable de sécurité à identifier rapidement le type de danger et lui donnerait les conseils essentiels pour gérer au mieux le danger, tout en assurant la protection des personnes présentes. La disponibilité sur Internet rendrait ce SIAD profitable dans le monde et offrirait une interactivité de mise à jour. En théorie, chaque pays pourrait alors rajouter ses propres règles suivant sa législation propre ou des rapports d'études pour informer le public ou le comité de sécurité.

Dans les chapitres suivants, nous présentons et détaillons plusieurs éléments constitutifs de ce SIAD. Il sera surtout question du développement d'une méthode relativement simple pour construire une première version théorique d'un SIAD opérationnel. Il ne suffira plus alors que réitérer la méthodologie afin de compléter l'outil. A la fin de ce mémoire, nous obtiendrons alors :

- a. une première base de connaissances utilisable et paramétrable par le logiciel ACCESS;
- b. le développement d'une codification et une hiérarchisation des procédures d'urgence;
- c. une proposition de fonctionnement possible de SIAD.

MCours.com