PolyPublie
Polytechnique Montréal

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Titre: Title:	Sûreté portuaire et solutions technologiques
Auteur: Author:	Anie Daniel
Date:	2005
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Daniel, A. (2005). Sûreté portuaire et solutions technologiques [Mémoire de maîtrise, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/7357/

Document en libre accès dans PolyPublie
Open Access document in PolyPublie

URL de PolyPublie: PolyPublie URL:	https://publications.polymtl.ca/7357/
Directeurs de recherche: Advisors:	Élisabeth Lefebvre
Programme: Program:	Non spécifié

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

https://publications.polymtl.ca

UNIVERSITÉ DE MONTRÉAL

SÛRETÉ PORTUAIRE ET SOLUTIONS TECHNOLOGIQUES

ANIE DANIEL
DÉPARTEMENT DE MATHÉMATIQUES ET DE GÉNIE INDUSTRIEL
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION DU DIPLÔME
DE MAÎTRISE ÈS SCIENCES APPLIQUÉES
(GÉNIE INDUSTRIEL)
FÉVRIER 2005

© Anie Daniel, 2005.

Library and Archives Canada
Bibliothèque et Archives Canada

Published Heritage Branch
Direction du Patrimoine de l'édition

395 Wellington Street
Ottawa ON K1A 0N4
Canada

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence
ISBN: 0-494-01301-X
Our file Notre référence
ISBN: 0-494-01301-X

NOTICE:
The author has granted a non-exclusive license allowing Library and Archives Canada to reproduce, publish, archive, preserve, conserve, communicate to the public by telecommunication or on the Internet, loan, distribute and sell theses worldwide, for commercial or non-commercial purposes, in microform, paper, electronic and/or any other formats.

The author retains copyright ownership and moral rights in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

AVIS:
L'auteur a accordé une licence non exclusive permettant à la Bibliothèque et Archives Canada de reproduire, publier, archiver, sauvegarder, conserver, transmettre au public par télécommunication ou par l'Internet, prêter, distribuer et vendre des thèses partout dans le monde, à des fins commerciales ou autres, sur support microforme, papier, électronique et/ou autres formats.

L'auteur conserve la propriété du droit d'auteur et des droits moraux qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

In compliance with the Canadian Privacy Act some supporting forms may have been removed from this thesis.

While these forms may be included in the document page count, their removal does not represent any loss of content from the thesis.

Conformément à la loi canadienne sur la protection de la vie privée, quelques formulaires secondaires ont été enlevés de cette thèse.

Bien que ces formulaires aient inclus dans la pagination, il n'y aura aucun contenu manquant.

Canada

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé :

SÛRETÉ PORTUAIRE ET SOLUTIONS TECHNOLOGIQUES

présenté par : DANIEL Anie

en vue de l'obtention du diplôme de: Maîtrise ès sciences appliquées

a été dûment accepté par le jury d'examen constitué de:

M. BOURGAULT Mario Ph.D., président

Mme. LEFEBVRE Élisabeth, Ph.D., membre et directrice de recherche

M. CASSIVI Luc, Ph.D., membre

REMERCIEMENTS

La réalisation de ce projet de maîtrise aurait été impossible sans l'apport précieux de nombreuses personnes que je tiens à remercier. Je souhaite remercier tout d'abord Madame Lefebvre, ma directrice de recherche, pour son aide tout au long de ce parcours. Sans cet appui important, ce projet n'aurait jamais vu le jour.

De plus, je tiens à remercier mes différents intervenants auprès des entreprises et des bureaux gouvernementaux visités, pour leur collaboration et leur participation dans ce mémoire. Leur disponibilité et leur ouverture d'esprit m'ont grandement impressionné. Leur apport a permis la réalisation de ce projet et a lui donné une saveur plus riche.

Par ailleurs, je remercie tous mes collègues au centre ePoly pour leur soutien, leur aide et leurs encouragements incessants. Véronique, Carl, Ygal, Harold et Samuel, merci! Par votre entraide, vous avez su rendre mon séjour parmi vous plus agréable.

Enfin, je voudrais remercier tout particulièrement mes parents qui m'ont toujours donné le meilleur d'eux-même et m'ont encouragé par leur amour et leur présence, ma grand-mère pour l'intérêt qu'elle a toujours porté à ce que je fais et son aide précieuse dans la révision de ce document et mes amis pour leur support moral et spirituel.

À mon Seigneur et Sauveur, Jésus, je rends toute la gloire car c'est Lui qui rend toutes choses possibles.

RÉSUMÉ

Les événements du 11 septembre 2001 ont changé à tout jamais le sens de sûreté des nations industrialisées dont les infrastructures et les méthodes de protection ne sont plus adaptées aux menaces des temps présents. De ce fait, les ports et les gouvernements les régissant, se voient dans l'obligation de sécuriser une chaîne d'approvisionnement mondiale complexe et stratégique. L'OMI, (Organisation Internationale Maritime) a rapidement réagi aux nouvelles donnes en établissant un code international auquel les pays souhaitant faire du commerce doivent se conformer. Ainsi, la toile de fond se dessine, des investissements énormes sont alloués pour solutionner un problème épineux, celui de la sécurisation des conteneurs et par extension des marchandises entrantes et sortantes.

Cette étude présente les différentes initiatives et les divers programmes mis sur pied dans le cadre d'amélioration de la sûreté maritime. Les différents risques attachés à la sûreté maritime ainsi que les couches qui forment l'approche de base des plans de sûreté des ports sont analysés. Les solutions technologiques en matière de sûreté portuaire sont examinées. L'une des technologies à haut potentiel qui permettrait une meilleure traçabilité est la technologie du RFID. En effet, certains avantages notables peuvent découler de son utilisation, tels que la réduction des délais et des marchandises égarées, une meilleure fiabilité et surtout une diminution de la vulnérabilité aux attaques terroristes.

Dans le cadre de cette réflexion, nous avons analysé comment deux entreprises abordent ce marché lucratif de la sûreté portuaire et réussissent à se positionner dans un marché compétitif. L'approche méthodologique retenue est une sur le terrain. De cette étude, des pistes d'action pertinentes pour les deux entreprises ayant fait le sujet de cette recherche ont été mises de l'avant et des recommandations ont été apportées.

Bien que les défis pour proposer des solutions efficaces et innovantes sont de taille, la technologie du RFID et son application sur des conteneurs pour les rendre plus 'intelligents' se dessine comme viable et à forte valeur ajoutée. Cependant, force est d'admettre que la technologie, bien qu'utile et essentielle, exige des changements structurels importants.

ABSTRACT

September 11th has forever changed the sense of security of industrialized nations that have to improve the protection of their infrastructures. By their importance in the dynamic role they bring to the economy, harbours have the obligation to secure a global supply chain which has become more complex and strategic. The International Maritime Organization (IMO) legislating ports and marine infrastructures, has quickly reacted to bring about a new code by which nations wishing to engage in commerce must comply with. Hence, huge investments are made to solve a major problem in this new era i.e., securing containers and merchandises.

Through this study, the programs put about to improve maritime security in the U.S. are reviewed. The risks attached to maritime security and the layers which are the basis for securing ports are presented, while technologies in use for decision making are then examined. RFID emerges as a technology that offers great potential in improving tracing and that could generate certain notable advantages, from a reduction in delays, improved accuracy to most notably, a reduction in vulnerability to terrorist attacks.

We have analysed how two different companies are providing port and maritime solutions and how they position themselves in such a competitive market. The methodological approach retained here is field research. Recommendations are brought forward for both companies. Despite many technical and non-technical challenges, RFID emerges as a value-added solution to improved harbour and maritime security.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

INTRODUCTION

Durant la seconde moitié du 20ième siècle, la libre circulation des marchandises et des échanges mondiaux à travers un système maritime bien établi, a largement contribué à l'amélioration de la prospérité des pays. De plus, grâce à une diminution des obstacles aux échanges et une baisse des droits de douanes, l'économie mondiale à pris son envol et est devenu plus interconnectée. Ainsi, les échanges s'étant développés, fournisseurs et fabricants ont mis au point des processus de production rapides et efficients, réduisant ainsi les stocks au minimum. Toutefois le 11 septembre, l'équilibre de l'économie de marché s'est fragilisé et au lendemain des attentats, les dirigeants du monde entier se sont concertés pour évaluer les vulnérabilités du secteur maritime qui sous-tend le dynamisme des économies mondiales. De l'altération de l'intégrité des cargaisons et des navires jusqu'à la fraude de documents, les vulnérabilités sont multiples et de natures diverses. Par conséquent, l'Organisation Maritime Internationale (OMI) a mis en place plusieurs mesures visant à réduire ses risques à travers toutes les étapes du réseau de transport maritime.

Le but de ce mémoire consiste donc à analyser les caractéristiques du transport maritime, en identifier les risques et les failles majeurs, et de regarder de plus près les solutions présentes et en développement pour y pallier. Nous regarderons de plus près le cas de deux entreprises, intégrateurs de solutions de sûreté maritime, pour conclure sur les potentialités de ce marché et de la technologie du RFID. Les objectifs seront en premier lieu d'évaluer l'évolution de la technologie RFID et de son impact au sein du domaine maritime et portuaire, puis de proposer des stratégies technologiques à des entreprises oeuvrant dans le domaine de la sûreté portuaire pour tirer avantage des tendances actuelles. Nous répondrons à la question de recherche de ce mémoire: le RFID est-elle une technologie pertinente pour la sûreté maritime et portuaire ?

Ce mémoire est composé de trois chapitres. Le premier chapitre introduit les infrastructures portuaires américaines et canadiennes et conclut sur les différences. Le 11 septembre ayant eu un impact notable sur le transport maritime et les ports mondiaux, une liste des menaces et des risques est passé en revue tandis que les programmes de sûreté ayant été mis sur pied d'abord par les É.U. dans l'objectif de sécuriser leur territoire national, puis par les Nations Unis comme cadre de référence à l'échelle, sont présentés.

Le deuxième chapitre se propose de regarder de près les méthodes et les moyens utilisés pour combattre le plus efficacement possible le terrorisme en matière de transport maritime. D'une part, une vue globale des technologies les plus avant-gardistes employées sera passée en revue. D'autre part, la technologie du RFID sera présentée comme une solution potentielle et intéressante permettant l'amélioration de la sûreté dans les ports. En conclusion, les différentes couches qui forment la sûreté maritime et leur mise en application à tous les niveaux de la chaîne de valeur clôturera notre aperçu du tableau globale du transport maritime.

Le troisième chapitre présentera l'étude de terrain ayant été menée afin de traiter le sujet présent. Le cadre conceptuel de Burgelman étant le cadre utilisé dans cette étude, il sera possible de saisir les motivations ayant aiguillé l'usage de telle technologie versus une autre, et de comprendre les forces et les faiblesses de chaque entreprise étudiée face à ses compétences fondamentales, actuelles et futures, dans le but de survivre ou de croître dans un marché hautement compétitif. Des pistes d'action spécifiques aux deux entreprises retenues pour ce mémoire viendra enrichir notre conclusion sur l'apport des RFID et de leur pertinence dans le marché de la sûreté maritime.

CHAPITRE 1
LES INFRASTRUCTURES PORTUAIRES ET LA SÛRETÉ

1.1. L'importance des infrastructures portuaires

1.1.1 Le transport maritime aux États-Unis

Afin de bien saisir les concepts mis de l'avant dans cette étude, il est important de définir quelques notions de base pertinentes à ce domaine d'étude. Lorsque nous parlons de sûreté il s'agit d'une combinaison des mesures ainsi que des moyens humains et matériels visant à protéger le transport maritime contre des actes d'intervention illicite par opposition au concept de sécurité qui correspond à l'absence ou la faiblesse relative de risques d'accidents. L'infrastructure portuaire correspond au port, les bâtisses adjacentes et le matériel nécessaire au bon fonctionnement de celui-ci.

En 2002, le commerce mondial s'est élevé à un montant astronomique de 6 270 trillions $ U.S. (World Trade Organization, 2003). Selon l'Organisation Mondiale du Commerce (OMC), l'économie de l'Amérique du nord s'est accrue de 2.5% en 2002. Tandis que les exportations ont légèrement diminué pour atteindre 946 G$ soit une diminution de 4%. Celles-ci ont diminué de 2% à 3% vers l'Asie, le Moyen-Orient et les économies de transition tandis que pour l'Amérique latine, l'Europe de l'Ouest, et l'Afrique, elles ont diminué de 7%, 10% et 12% respectivement. En revanche, les importations de l'Asie, l'Europe de l'Ouest et l'Amérique latine ont augmenté. Les données disponibles de l'Administration Maritime Américaine (Maritime Administration, MARAD) indiquent que le trafic de conteneurs n'a fait que croître depuis les quatre dernières années à un rythme de 7% annuellement pour atteindre 15.6 millions de EVP (équivalent vingt pieds pour conteneurs qui renferment des marchandises) en 2002 (MARAD, 2003). De plus, le nombre de cargos conteneurisés aux É.U. en 2003 a atteint un peu plus de 21millions

dont 83% provient de ses 25 plus importants partenaires d'échange. Le tableau 1.1 présente les 10 plus importants partenaires d'échanges internationaux. Il est à souligner que les cinq premières places en matière de cargos conteneurisés sont détenues par des pays asiatiques.

Tableau 1.1: Les 10 plus importants partenaires d'échanges américains

Commerce maritime américain pour le cargo conteneurisé **Année 2003** **(milliers de EVP, conteneur cargo de 20 pieds)**				
Partenaires	**Total**	**Export**	**Import**	**Rang**
Chine	5 656	1 209	4 447	1
Hong Kong	1 619	327	1 292	2
Japon	1 603	880	722	3
Taiwan	946	295	651	4
Corée	898	429	469	5
Allemagne	650	183	467	6
Italie	602	129	473	7
Brésil	533	145	388	8
Thaïlande	496	118	378	9
Royaume Uni	429	223	206	10

Adapté de Port Import/Export Reporting Services (PIERS), 2004

1.1.2 Le transport maritime au Canada

Le Canada possède un système de transport sophistiqué ce qui lui permet d'être relié au reste du monde par un système d'échange efficace. Le système maritime du Canada comprend environ 200 000 km de littoral, s'étend sur 200 miles marins au large du littoral et s'avance sur plus de 3 700 km au cœur du continent grâce au réseau des Grands Lacs et de la Voie maritime du Saint-Laurent. En 2000, la valeur du commerce maritime était d'environ 100 G$ d'un total de 740 G$ dont l'impact économique est

évalué à 20 G$. Le secteur maritime du Canada emploie plus de 30 000 personnes et génère des revenus annuels de 2.6 G$, tandis que 250 ports transigent 3.5 M de conteneurs annuellement et 200 M de tonnes de marchandises (Transport Canada, 2004). De ces portes d'entrée, les importations entrent au Canada et sont distribuées à travers l'Amérique du Nord. Par ailleurs, 4 000 navires étrangers de plus de 500 tonnes visitent les ports canadiens chaque année tandis que 100 navires canadiens de plus de 500 tonnes font des voyages internationaux. Ainsi, les ports maritimes sont des nœuds critiques d'un système complexe de centres industriels et logistiques.

Dans le contexte de la globalisation, les ports doivent s'assurer de demeurer compétitifs pour garder leur positionnement de choix dans le commerce maritime et c'est pourquoi les efforts pour améliorer la sûreté doivent être équilibrés avec la nécessité de maintenir la libre circulation des échanges commerciaux et des gens, qui contribue à son tour à maintenir la position concurrentielle du secteur maritime du Canada de même que notre vitalité économique. Suite aux événements du 11 septembre, le gouvernement du Canada a pris des mesures afin de sécuriser le transport maritime notamment en obligeant le trafic trans-océanique de donner 96 heures de préavis avant de pénétrer les eaux canadiennes plutôt que les 24 heures habituelles. Une entente fut signée avec les É.U. pour faire une inspection au préalable des navires qui entreraient dans le système des Grands Lacs/St-Laurent, de même que la sélection des navires se ferait par les opérations conjointes des douanes des deux pays. De plus, afin d'accélérer le temps de réponse en cas de menace, des protocoles plus rigoureux ont été adoptés tandis que la présence policière a été renforcée sur les bateaux de croisière. Finalement, une évaluation des risques et des menaces face aux infrastructures portuaires doit être faite de façon régulière (Transport Canada, 2004).

Pour améliorer la sûreté du public et les capacités anti-terroristes, cinq priorités ont été établies par le gouvernement canadien : 1) garder les terroristes à l'extérieur du pays, 2) prendre action contre ceux-ci lorsque nécessaire, 3) améliorer les relations canadiennes-

américaines 4) encourager les initiatives internationales, 5) protéger les infrastructures tout en améliorant les plans d'urgence. C'est ainsi que le gouvernement canadien signa un accord avec les É.U., le Smart Border Declaration le 12 décembre 2001 afin d'améliorer la collaboration entre les deux pays et travailler ensemble sur la sûreté à la frontière pour maintenir le flux des marchandises et des personnes. Pour mettre en place ses priorités, le gouvernement du Canada débloqua 7.7 G$ sur six ans pour combattre le terrorisme et renforcer la sûreté publique tandis que, 172.5 M$ seront investis de 2003-2007 pour la sûreté maritime (Transport Canada, 2004). L'environnement de la sûreté maritime peut être considéré comme une série de zones autour du Canada. Celles-ci sont soit étrangères, internationales, canadiennes ou côtières. À l'intérieur de ces zones, les activités de sûreté maritimes peuvent être regroupées en 4 catégories dont les objectifs dépendent de la zone dans laquelle elles se déroulent: la vigilance dans le secteur maritime, la capacité d'intervention, la protection et la collaboration.

La vigilance dans le secteur maritime

Cette activité concerne la surveillance des zones maritimes ainsi que la collaboration avec les agences d'intelligence internationale. Dans ce secteur d'activité, les efforts de sûreté sont axés sur le principe que plus un aspect est vulnérable, plus les besoins en matière de renseignements du gouvernement du Canada seront grands et plus les renseignements devront être détaillés. Les principaux objectifs consistent à obtenir une connaissance exhaustive des personnes, conteneurs, marchandises et bâtiments à la première occasion qui se présente et la capacité de réaliser une intervention au moment opportun en cas d'incident.

Ainsi, afin d'accomplir cet objectif, le ministère de Pêche et des Océans recevra 2 M$ annuellement pour améliorer la surveillance maritime. Ces fonds permettront l'amélioration de la surveillance maritime et l'augmentation de la surface de la zone de patrouille. L'initiative d'identification des passagers et du personnel permettra

d'examiner de près les navires afin d'interdire les terroristes et les migrants illégaux. Ainsi 14.4 M$ seront employés sur 5 ans pour ce projet. Par ailleurs, 27 M$ seront investis sur 5 ans pour des systèmes d'identification automatique et l'identification des navires afin d'améliorer la reconnaissance des navires à distance. Et enfin, 43 M$ seront investis sur 5 ans pour le projet de (HFSWR) High Frequency Surface Wave Radar qui permet de suivre au radar la surface des océans (Transport Canada, 2004).

Capacité d'intervention

La capacité d'intervention désigne, les efforts d'application de la législation menés en collaboration avec les corps policiers et les organismes de sûreté afin d'intercepter et d'appréhender les terroristes éventuels et leurs engins.

Les activités correspondant à la capacité d'intervention sont fondées sur le principe que les mesures doivent être prises dès que possible et de préférence à une certaine distance du Canada et des Canadiens. Les principaux objectifs comprennent la capacité d'interdire l'accès aux personnes, conteneurs, marchandises et bâtiments représentant un risque élevé, la capacité d'appréhender les personnes précitées et de confisquer ces conteneurs, marchandises et bâtiments à la première occasion qui se présente, et, la capacité de réaliser une intervention au moment opportun en cas d'incident.

Pour développer le contre-terrorisme, 1 M$ sera investi par année de 2003 à 2007. Ceci permettra de développer la coordination et la coopération inter-agences pour répondre aux menaces terroristes de même qu'assister le département à remplir son mandat sous le Plan National de Contre-Terrorisme. Le but du Projet National des Ports est d'éliminer les capacités du crime organisé de contrôler des ports et de travailler avec des activités terroristes. Ainsi, 6.8 M$ sera injecté dans ce programme pour un projet pilote au Port de Montréal afin d'évaluer le potentiel de menaces du crime organisé sur la

sûreté nationale et de maintenir une présence constante de la RCMP sur les lieux (Transport Canada, 2004).

Protection

La protection comprend les mesures prises pour rehausser la sûreté matérielle des infrastructures maritimes ou d'autres infrastructures essentielles dans des zones maritimes ou à proximité de zones maritimes. La protection comprend également les mesures prises pour accroître le contrôle du personnel afin d'empêcher des engins terroristes de pénétrer au Canada ou d'avoir accès à notre système de transport maritime. Le principe clé qui guide les activités de protection repose sur le fait que le système maritime est aussi sûr que le plus faible de ses maillons. Les objectifs clés visent à assurer l'intégrité des infrastructures matérielles et technologiques et à empêcher l'infiltration de personnes et d'engins présentant des risques élevés dans le système maritime.

Par conséquent, 3.2 M$ seront investis pour s'assurer de la conformité avec les réglementations internationales, la protection des échanges commerciaux et maintenir la confiance des partenaires du Canada en matière d'échange. De plus, 14.5 M$ iront au renforcement des standards de sûreté sur les navires et les installations et ainsi protégera l'économie canadienne s'assurant ainsi que le Canada rencontre ses obligations auprès de l'Organisme Maritime International (OMI). Le programme de MFRAACP (Marine Facilities Restricted Area Access Clearance Program) protégera la sûreté des personnes aux ports, de même qu'il limitera l'accès aux facilités maritimes seulement à ceux qui auront la permission. Ce programme sera calqué sur le modèle des aéroports et recevra un montant de 11.8 M$ sur 5 ans pour l'élaboration de nouveaux règlements, l'achat et l'installation de nouveaux équipements, la formation du personnel et la revue des processus d'autorisation (Transport Canada, 2004).

Collaboration

La collaboration est le facteur clé pour assurer l'efficacité des activités de vigilance dans le secteur maritime de même que les activités de protection et la capacité d'intervention. La collaboration apporte un soutien aux trois aspects précités en assurant que les ministères, les organismes et autres organisations qui assument des responsabilités en matière de sûreté maritime et d'anti-terrorisme, y compris les instances homologues aux États-Unis et dans d'autres pays, partagent l'information efficacement et de manière sécuritaire, évaluent les risques et réalisent des interventions coordonnées sous réserve des dispositions législatives applicables. La collaboration repose sur le principe que le tout est plus grand que la somme de ses parties. Les principaux objectifs sont de susciter la plus grande vigilance possible au sein des ministères et organismes du gouvernement fédéral qui assument des mandats de lutte contre le terrorisme et d'obtenir un mécanisme de prise de décision de grande qualité permettant la prise de décisions en temps opportun par les ministères et organismes concernés.

Le groupe de travail interdépartemental de sûreté maritime (IMSWG, Interdepartemental Marine Security Working Group) coordonne la réponse fédérale à tout problème de sûreté maritime, analyse le système maritime et développe des initiatives possibles à la mitigation. Ce programme tente d'identifier les aspects du système de transport maritime qui requiert une revue et met le focus sur l'évaluation des risques au niveau de la sûreté et des mesures de mitigation pour le système maritime (Transport Canada, 2004).

Le 1er juillet 2004, Transport Canada a mis en application les réglementations sur la sûreté maritime régies par l'OMI qui a développé le code ISPS (International Ship and Port Facility Security). Sous ce code, tous les navires cherchant à entrer dans les eaux canadiennes devront se prémunir d'un certificat international de sûreté des navires. Les nouveaux règlements s'appliqueront aussi aux infrastructures maritimes et portuaires qui reçoivent ces navires. Les exigences vont améliorer la sûreté maritime au Canada et dans

le monde. Tous les navires commerciaux de 500 tonnes ou plus, ou dont le nombre de passagers est plus de 12 personnes et voyageant entre pays, seront soumis à de nouvelles réglementations qui incluent l'évaluation de sûreté, les plans de sûreté ainsi que la désignation d'officiers de sûreté.

La nouvelle réglementation canadienne surpasse les exigences de l'OMI en les étendant au navire cargo de 100 tonnes ou plus, les navires de charge qui tirent du cargo dangereux ainsi que les infrastructures maritimes et portuaires. Transport Canada travaille de près avec les partenaires internationaux de sûreté maritime incluant la garde côtière américaine pour assurer la mise en œuvre effective de ce nouveau régime de sûreté maritime. Le Canada et les É.U. vont offrir une reconnaissance réciproque et une acceptation de leurs plans respectifs de sûreté des navires. Cet arrangement permet de créer une approche harmonisée pour assurer que seulement les navires respectant le code ISPS puissent pénétrer dans les eaux canadiennes et les infrastructures portuaires (Transport Canada, 2004). Afin d'assister les infrastructures portuaires pour améliorer la sûreté, le ministère des Transport a débloqué 115 M$ sur 3 ans pour le nouveau programme de contribution à la sûreté des installations maritimes (Marine Facility Security Contribution Program). Cette initiative inclut l'amélioration de la surveillance, les clôtures, l'éclairage, et le contrôle d'accès, aspects auxquels les ports doivent se soumettre avec ce nouveau programme de contribution à la sûreté des installations maritimes, version canadienne du code ISPS, entrant en vigueur le 1er juillet 2004.

Collaboration: la coalition pour la sûreté et l'efficacité des échanges

La coalition pour la sûreté et l'efficacité des échanges a été formée par plus de 55 associations d'entreprises canadiennes et compagnies pour aider le gouvernement fédéral à être plus efficace face aux questions de sûreté et des frontières. Son propos est triple : tout d'abord elle doit pouvoir recommander les mesures pour faciliter le passage de marchandises à faible risque et des gens à travers les frontières canadiennes ; puis, elle doit faire des recommandations afin d'améliorer la sûreté canadienne, l'immigration

et la gestion de la frontière ; et enfin elle vise à accroître la coopération entre le Canada et les É.U. ainsi qu'avec d'autres alliés pour prévenir l'entrée de terroristes, d'immigrants illégaux, de contrebande et de marchandises illégales dans le pays.

La coalition pour la sûreté et l'efficacité des échanges est une des plus grandes coalitions formées dans l'histoire canadienne, et représente la vaste majorité des activités d'affaires au Canada. Ses membres proviennent de tous les secteurs de l'industrie et représentent des entreprises de tout gabarit (Rethinking our Borders: Beyond the Plan, 2004). La sûreté maritime implique une panoplie de partenaires. Grâce à une collaboration plus élevée avec les différents organismes, le gouvernement canadien tente de développer un système de transport plus sécuritaire pour le Canada et les canadiens.

1.1.3. Les rivalités entre ports pour les conteneurs du Canada et des É.U.

Les ports pour conteneurs nord-américains sont une plaque tournante clé du commerce international basée sur le transport rapide et efficace des navires qui déchargent la marchandise qui sera par la suite acheminée aux différents centre de distribution du pays. En 2001, 20,2 millions d'EVP chargés ont fait l'objet de manutentions dans les ports nord-américains dont 60% des EVP chargés en Asie et Océanie et 23% en Europe (O'Keefe, 2003). Si l'on étudie le nombre d'EVP chargés par région du globe, l'on remarque en effet que le marché est dominé par la côte Pacifique qui retient à elle seule un peu plus de 50% du trafic total. Le tableau 1.2 présente les EVP manutentionnés aux ports nord-américains en 2001.

Table 1.2: Millions d'EVP chargés manutentionnés aux ports nord-américains par région du globe/destination en 2001

Région du globe	Atlantique	Pacifique	Golf du Mexique	Total
Asie et Océanie	2,35	9,63	0,04	12,03
Europe	3,65	0,38	0,56	4,58
Amérique du Sud et Centrale	2,07	0,25	0,53	2,85
Moyen-Orient et Afrique	0,57	0,07	0,11	0,75
Total	8,64	10,33	1,24	20,21

Tiré de : O'Keefe, 2003

Trois ports canadiens offrent des portes d'entrée pour le marché nord-américain : Vancouver, Montréal et Halifax. D'après des statistiques de 2001, Vancouver est le 3^{ième} port nord-américain par ordre d'importance pour la manutention du volume de marchandises conteneurisées échangées avec l'Asie et l'Océanie. En effet, l'Asie et l'Océanie sont la région de commerce d'importance pour cette ville car la quantité de fret conteneurisé représente pas moins de 95% de tout le fret importé dans son port. Les principaux concurrents de Vancouver dans ce corridor commercial sont Seattle et Tacoma. En terme de croissance de marché, celui en 2001 n'avait augmenté que de 1% contre 11,1% l'année précédente.

Le port de Montréal est le principal port canadien pour la destination de l'Europe. Plus de 95% de son fret conteneurisé en 2001 provenait de cette destination tandis que le port de NY/NJ n'affichait que 40,8% de son volume de marchandise en provenance de l'Europe. Ensemble, Montréal et NY/NJ représentent quelque 40% du volume des marchandises conteneurisées en provenance/destination de l'Europe et sont des rivaux de longue date dans ce corridor commercial (O'Keefe, 2003).

Montréal est un centre majeur de transit de conteneurs entre l'Europe et l'Amérique du Nord. En effet, près de 40% des conteneurs venant du marché de l'Atlantique Nord (Europe du Nord jusqu'à la Méditerranée) destinés au Canada et aux régions du Nord-

Est et du Midwest américain passent par le port de Montréal. C'est environ 1 million de conteneurs qui entrent et sortent annuellement dans le port de Montréal. De ce million de conteneurs, plus de la moitié est dirigé vers les entreprises américaines du Nord-Est et du Midwest américain (America Montreal Close). Le tableau 1.3 présente le trafic annuel 2003-2002.

Tableau 1.3: Trafic annuel 2003-2002 (tonnes métriques)

Types de marchandises	**2003**	**2002**	**Variations tonnes**	**Variation %**
Ensemble du trafic				
Marchandises diverses :				
Conteneurisées	9 755 300	7 446 412	308 888	3,3%
Non conteneurisées	446 533	405 366	41 167	10,2%
Total	**10 201 833**	**9 851 778**	**350 055**	**3,6%**
Marchandises en vrac				
Solides				
Liquides	5 233 109	5 059 129	173 980	3,4%
	5 345 352	3 808 972	1 536 380	40,3%
Total				
	20 780 294	**18 719 879**	**2 060 415**	**11,0%**
Trafic à l'entrée				
Marchandises diverses				
Conteneurisées	5 085 530	5 102 775	-17 245	-0,3%
Non conteneurisées	371 732	305 366	66 366	21,7%
Total	**5 457 262**	**5 408 141**	**49 121**	**0,9%**
Marchandises en vrac	3 805 700	4 028 141	-222 441	-5,5%
Solides	3 891 042	2 430 539	1 460 503	60,1%
Liquides				
	13 154 004	**11 866 821**	**1 287 183**	**10,8%**
Total				

Trafic à la sortie				
Marchandises diverses				
Conteneurisées	4 669 770	4 343 637	326 133	7,5%
Non conteneurisées	74 801	100 000	-25 199	-25,2%
Total	**4 744 571**	**4 443 637**	**300 934**	**6,8%**
Marchandises en vrac				
Solides	1 427 409	1 030 988	396 421	38,5%
Liquides	1 454 310	1 378 433	75 877	5,5%
Total	**7 626 290**	**6 853 058**	**773 232**	**11,3%**

Tiré de Port de Montréal, Statistiques 2003

Le port de Halifax, en revanche, est classé 6^{e} parmi les ports nord-américains sur l'itinéraire commercial de l'Europe et 11^{e} sur celui de l'Asie et de l'Océanie. La répartition de son trafic est de plus de 58% pour le marché européen et un peu plus de 24% pour le marché d'Asie et Océanie en volume de marchandises conteneurisées. Il est à remarquer que le port de Halifax n'a pas été un concurrent majeur ni pour le marché asiatique, ni pour le marché européen puisque sa part de marché ne représente que moins de 6% du marché européen et 1% asiatique. En 2001, 96,6% du volume des marchandises transportées en conteneurs maritimes ont été manutentionnées dans les ports de Vancouver, Montréal, et Halifax.

D'après les études qui ont été menées par le passé, les ports canadiens disposent d'un fort potentiel de s'emparer de beaucoup plus de trafic grâce à leurs installations et à l'excellent accès par rail et par route à tous les principaux marchés nord-américains (O'Keefe, 2003). Cependant, plusieurs enjeux concurrentiels doivent être pris en compte pour les ports canadiens lorsqu'ils sont comparés aux ports américains. En effet, il est important de tenir compte du financement des investissements en capital, des coûts des prix du service, et des répercussions de l'intensification des mesures de sûreté à la

frontière canado-américaine. Afin de déterminer quels ports pour conteneurs une société d'expédition doit choisir, les coûts de traversée, d'opération au port et du transbordement et du voyage par voie de terre sont pris en compte. D'après une étude menée par l'administration maritime américaine (MARAD) auprès des principaux transporteurs, en comparant les ports américains et canadiens, les répondants ont préféré plusieurs caractéristiques des ports américains en notant toutefois que ceux-ci avaient le désavantage d'être souvent plus chers que les ports canadiens. Les aspects sûreté, disponibilité des châssis, et catégories de terminaux ont reçu les plus fortes cotes du côté américain tandis que les ports canadiens se sont démarqués en matière de coûts par déplacements (cost per move) et temps d'attente des camions à la barrière (truck gate time). Cependant, parmi les raisons ayant été citées dans le choix de l'utilisation des ports canadiens, le commerce de conteneurs, les liaisons avec l'arrière pays et le temps de transit ont été citées le plus souvent. Plusieurs répondants ont mentionné être influencés par les frais élevés de maintenance américains, ainsi que la congestion et les coûts de ces ports.

Selon une étude effectuée par la Australian Productivity Commission les tarifs moyens de transport ferroviaires canadiens seraient d'un peu moins de 10% inférieurs aux tarifs américains en valeur réelle. De plus, les droits des utilisateurs maritimes canadiens s'établissent à 19 cents la tonne versus 63 cents la tonne pour les droits des utilisateurs américains (O'Keefe, 2003). Enfin, les nouvelles mesures de sûreté entamées depuis le 11 septembre font craindre des embouteillages à la frontière canado-américaine ce qui pourrait être nuisible aux ports conteneurs canadiens, mais cela reste à être vérifié car les ports canadiens demeurent malgré tout une destination économique de choix pour le transport maritime. À la lumière de ces quelques données sur le trafic maritime dans les ports canadiens, nous saisissons donc mieux l'importance de ceux-ci de se doter de mesures et de technologies appropriées permettant de bien sécuriser leurs infrastructures portuaires afin de préserver l'intégrité de la marchandise transitant par ce maillon important que sont les ports canadiens.

1.2. Les initiatives en matière de sûreté des infrastructures portuaires

1.2.1. Les conséquences du 11 septembre pour les installations portuaires

Les attaques terroristes du 11 septembre et l'épisode des menaces par l'anthrax qui suivit en octobre, ont profondément changé l'approche des É.U. vis-à-vis la gestion d'urgence et les méthodes mises en application. Cinq grands changements ont pris place dans la façon que le gouvernement américain aborde le terrorisme : l'élaboration de protocoles, la préparation face aux actes terroristes, le financement de la guerre contre le terrorisme, la création du Département de Sûreté Nationale (Department of Homeland Security) et des efforts militaires accrus pour contrer le terrorisme.

Voici compilé dans au tableau 1.4, quelques données sur les effets du 11 septembre sur l'économie générale :

Tableau 1.4 : Liste partielle des pertes économiques causées par le 11 septembre

Impact	Coûts (en date du 12/2001)
Industrie Aérienne	
Pertes financières	4.5 G$
Pertes d'emploi Continental	12 000 personnes
Delta	13 000 personnes
American	11 000 personnes
Industrie Financière	
Compagnie d'assurance Berkshire Hathaway	2.3 G$
Lloyd's	1.8 G$
Munich 'Re'	1.8 G$
Allianz	0.9 G$
Assistance au désastre	
Fonds d'urgence	657 M$
Prêts personnels	164 M$
Perte d'emplois par industrie	
Hotels	46 000 personnes
Compagnies aériennes	100 000 personnes
Alimentation	42 000 personnes
Perte de vies humaines	3 021 personnes (9/2003)

Adapté de Haddow, Bullock, 2003

Ainsi, l'on remarque que les pertes lors de cette attaque terroriste ont été considérables. Les pertes d'emplois ont été importantes et dans le secteur privé plusieurs industries ont connu des baisses de profits dues au ralentissement de l'économie, des changements dans les habitudes de consommation, ainsi que des restructurations nécessaires pour s'ajuster aux marchés devenus fébriles. L'entreprise Berkshire Hathaway souligne d'ailleurs qu'en cas d'attaques terroristes, les pertes pourraient être de l'ordre de 1 trillion $, coûts que les compagnies d'assurance ne seront certainement pas en mesure

d'absorber. On comprend donc l'importance pour les gouvernements et les entreprises de se prémunir contre de telles catastrophes.

Depuis le 11 septembre, une attention accrue s'est portée sur la sûreté portuaire car les ports américains et ceux du monde entier pourraient être la cible potentielle d'attaques de la part de terroristes. Les experts demeurent soucieux que le système de transport maritime puisse être utilisé comme un moyen pour le trafic d'armes de destruction massive ou le transport de matériels dangereux. Les ports représenteraient non seulement une entrée pour le transit de la marchandise, mais constituent aussi des endroits privilégiés d'industries qui sont très souvent près des centres urbains, ce qui pourrait être un intérêt supplémentaire pour les terroristes cherchant à atteindre les populations. En 2002, la garde côtière canadienne intercepta dans le Golfe d'Oman deux membres suspects d'Al-Qaeda qui fuyaient Le HMCS Algonquin et le navire français Guepratte (Toronto Globe and Mail, 2002). Par ailleurs, certaines autorités croient que le groupe d'Al-Qaeda posséderait 15 navires qui pourraient être utilisés comme des bombes flottantes contre des navires de croisières ou tout autre bateau, pour transporter des armes de destruction massive ou des membres de leur organisation (Mintz, 2002 ; Rashbaum, Osler, 2001).

Pour ne citer que les É.U. comme exemple, le transport maritime est vital pour l'économie. En effet, plus de 95% de tout échange, hormis l'échange nord-américain, entre aux É.U. par les ports qui transigent respectivement plus de 740 G$ et 2 milliards de tonnes de frets domestiques et internationaux. Par ailleurs, les navires étrangers amerrissent 50 000 fois par an aux É.U. Pourtant, l'infrastructure du transport maritime fait face à une quantité de menaces vers lesquelles les autorités se penchent pour mitiger les risques.

En 1999, La Commission Clinton sur la Sûreté Portuaire (Clinton Port Security Commission) étudia de façon précise le crime et les menaces aux infrastructures critiques des villes portuaires. Suite à des recherches sur les différents ports du pays, elle

conclua qu'il n'y avait aucun standard de sûreté et de procédure parmi les différentes installations portuaires. De plus, les différents organismes en charge de la sûreté portuaire fonctionnaient si indépendamment les uns des autres que des criminels pourraient prendre avantage des failles du système. Cependant, malgré les recommandations qui furent faites, aucun changement pour améliorer la sûreté maritime ne fut entrepris à l'exception de la Floride. Depuis janvier 2001, cet état a entrepris rapidement des démarches et possédait plusieurs ports avancés en terme de sûreté portuaire car, cet état avait en effet mis en place des codes rigoureux de sûreté portuaire et maritime qui devinrent l'étalon pour le pays en entier en terme du combat contre la criminalité.

Antérieurement au 11 septembre, l'Organisation Standard Internationale (ISO) cherchait déjà à développer un standard maritime international. L'OMI, un sous-comité des Nations Unies avait déjà des standards d'entraînement et de certification pour les marins afin d'assurer la sûreté du personnel. En janvier 2002, la Garde Côtière Américaine (USCG) présenta un document à l'OMI intitulé le 'Prevention and Suppression of Acts of Terrorism against Shipping', dans le but d'améliorer la sûreté du personnel marin. L'une de ses recommandations était l'adoption de systèmes d'identification automatique internationale et des systèmes de signalisation d'urgence pour les bateaux.

Plusieurs risques existent en matière de transport maritime. Premièrement, les autorités craignent que certains de ces individus se soient échappés, sachant qu'ils possèdent des navires et que ces derniers soient utilisés dans le but d'amasser des fonds (Gordon, Rising, Lekic, 2002). Il est de notoriété publique que des navires pourraient effectivement être acquis facilement pour soutenir le terrorisme tandis qu'il est parfois plus difficile d'identifier les vrais propriétaires de ces flottes (King, 2004). Deuxièmement, certains pays transportent des armes de tout genre, y compris de destruction massive et l'on craint que ces pays cherchent à les destiner à des groupes terroristes. Troisièmement, le piratage est un cas qui n'est pas toujours punissable surtout lorsque l'acte commis se fait en eaux internationales, et demeure donc

problématique (Roach, 2004). En général, le piratage consiste à voler ou piller des navires. Mais, il existe des cas où des marins ont été pris en otage, ce qui laisse présager que des terroristes pourraient exploiter cette option à leur avantage. Quatrièmement, l'on estime le vol par des conteneurs cargo à 50 G$ annuellement. Finalement, plusieurs pays cherchent à combattre la migration illégale et dangereuse du trafic humain qui est estimé à 4 millions de personnes par an et qui génère un revenu de plus de 5 G$ U.S. par an (Nations Unies, 2000).

Notons que face à de tels risques, le trafic de drogue continue d'être un des fléaux les plus inquiétants et dont les ramifications ne cessent de se compliquer (Roach, 2004). Enfin, les conteneurs cargo demeurent l'aspect le plus vulnérable de la chaîne d'approvisionnement, car sur environ 15 millions de conteneurs en circulation seulement 2% sont inspectés pour des anomalies (United States Senate, 2003). C'est dans le but d'éviter que les cargos soient utilisés à des fins terroristes que les États-Unis ont mis sur pied les programmes sécurisant les cargos et les échanges. Tel que le mentionnait M. Flynn devant le Sénat américain, 'a modest investment by a terrorist could yield billions of dollars in losses to the U.S. economy by shutting down-even temporarily- the system that moves 'just in time' shipments of parts and goods.' En effet, en s'appuyant sur les résultats receuillis lors de la grève au port de West Coast en 2002, il a été déterminé qu'une attaque terroriste sur les ports américains créerait des pertes de l'ordre de 50 G$ U.S. et que la reprise des activités ne se ferait 3 mois que plus tard (Booz Allen Hamilton, 2003).

Les experts en sûreté et les agents gouvernementaux s'inquiètent de l'ampleur et de la probabilité des menaces aux navires et aux ports car les menaces sont réelles. Pour qu'une menace ne soit pas considérée critique, elle ne doit pas avoir de conséquence importante ou encore doit être difficile à exploiter par des terroristes en raison de la complexité de la mettre en oeuvre. Les experts estiment que les terroristes tendent à continuer à faire ce qui a été un succès par le passé, à savoir les enlèvements, détournements et détonations explosives. Transposé dans le domaine maritime, cela

correspond à prendre d'assaut un navire de croisière ou à cacher des engins explosifs dans la soute à bagages. C'est pourquoi les navires ont investi dans la sûreté et l'entraînement de leur personnel. Pour ce qui est des navires à cargo et des terminaux, on considère différents types de menaces. Par exemple, le nitrate d'ammonium, bien que celui-ci soit inoffensif à prime abord, car utilisé comme fertilisant, peut être également l'ingrédient de base dans la composition des explosifs. Ainsi, le risque qui lui est associé devient important. Le 1er juillet 2003, la garde côtière américaine publia une liste de scénarios maritimes et la magnitude des risques qui leur sont associés grâce à une méthode appelée le 'National Risk Assessment Tool (N-RAT)'. C'est ainsi que les traversiers internationaux sont cotés à risque élevé dû à la valeur de leur cargaison et à la facilité avec laquelle ils peuvent être attaqués.

Lorsque l'on étudie le transport maritime, il est important de prendre en compte les liens avec le transport par train et celui par camion. Pour étudier le risque dans le transport maritime, il faut déterminer le niveau de risque d'une situation avec sa valeur critique, en tenant compte des menaces et des vulnérabilités, c'est ainsi que l'on obtient l'équation : RISQUE = VALEUR x MENACES x VULNÉRABILITÉ. Cette méthode permet une évaluation des différents scénarios qui peuvent se présenter. Les pires scénarios seraient l'explosion d'une raffinerie de gaz naturel, la détonation d'une arme de destruction massive dans un terminal ou sur un navire amarré, un détournement, la destruction d'un navire de croisière ou encore l'utilisation d'un navire comme arme de collision. Pour reprendre l'exemple du capitaine Fred Evans (Maritime and Port Security, 2004) d'un navire transportant du gaz naturel qui exploserait, le risque qui lui est associé est élevé car la valeur de la marchandise est élevée, de plus, les terroristes réussiraient à s'attirer la couverture médiatique et par ailleurs il y aurait des impacts sur l'économie et plus spécifiquement sur les marchés boursiers qui réagiraient à une telle attaque. La composante menace consisterait en la capacité pour un groupe terroriste d'embarquer sur un tel navire et d'exploiter les vulnérabilités de celui-ci. Cependant, si l'environnement autour du navire transportant du gaz naturel est bien protégé et un

système de sûreté est en place pour en assurer les va-et-vient autour d'un certain périmètre, alors le niveau de risque baisse et devient acceptable.

Dépendamment des circonstances, la mitigation de risque peut comporter des éléments tel la localisation de conteneur grâce à un système satellite GPS (Global Positioning System), une base de données à jour sur les navires, un système de scanner (balayage électronique) de conteneurs et d'identification par images au point de chargement de la cargaison ou un système d'analyse des douanes permettant d'arrêter tous colis suspects. De plus, pour ce qui est des navires de croisière, il faut s'assurer de faire une vérification méticuleuse des bagages, pour pouvoir identifier indubitablement les passagers et les membres du personnel et s'assurer des meilleures méthodes de sûreté. Il est à remarquer que plus l'étau se resserre en terme de sûreté sur les avions, plus il devient difficile pour les terroristes d'exploiter ce domaine, ce qui rend le domaine du transport maritime plus attrayant et par conséquent vulnérable à des attaques. Bien que beaucoup d'améliorations en matière de sûreté portuaire aient été apportées depuis les événements du 11 septembre, beaucoup restent encore à être faites, car plusieurs des programmes ayant été mis sur pied restent encore sous-financés et n'ont pas été testés.

L'une des menaces les plus sérieuses reste la menace d'armes biologiques. Lorsque l'on étudie de plus près les moyens pouvant être exploités en matière de destruction, l'on se rend compte rapidement d'après le tableau 1.5 que six micro-organismes menaceraient sérieusement la santé du grand public.

Tableau 1.5: Les six micro-organismes les plus menaçants pour la santé

Bacillus anthracis (anthrax)	L'anthrax pourrait être propagé comme une arme biologique aérosol. L'aérosol serait sans odeur et invisible et pourrait voyager plusieurs kilomètres avant de disséminer. Peut être traité avec un vaccin si celui-ci est administré avant l'apparition des symptômes.
Variola major (variole)	La variole peut se propagé par contact avec des personnes infectées ou par contact avec des objets contaminés tels que de la literie ou des fluides humains contaminés. En de rares occasions, la variole s'est propagée à travers l'air dans des endroits clos. Un vaccin est disponible.
Yersinis pestis (peste)	La peste pourrait être utilisée comme attaque aérosol, ce qui causerait des cas de peste pneumonique. Les gens développeraient des symptômes un à six jours suite à la contamination. Peut être traité avec un vaccin si celui-ci est administré 12-24 hrs après l'apparition des symptômes.
Botulinum toxin (botulisme)	Le botulisme est potentiellement dangereux car il peut être transmis par nourriture contaminée. Peut être traité avec un vaccin si celui-ci est administré peu de temps suivant l'apparition des symptômes.
Francisella tularensis (tularaemie)	La tularaemie peut servir comme arme et être transmis dans l'air. Les gens développeraient des symptômes trois à cinq jours plus tard. Un vaccin est disponible.
Filovirus/ arenavirus (fièvre hémmoragique)	Les fièvres hémorragiques sont très infectieuses par les voies aérosols ex: la fièvre Ebola. La majorité sont stables comme aérosols et peuvent être utilisées comme arme. Il n'y a pas de vaccin pour la majorité des fièvres hémorragiques.

Adapté de Standing Senate Committee on National Security andDefense, March 2004

Santé Canada a déterminé qu'une attaque terroriste employant l'un de ces agents biologiques serait catastrophique. En utilisant un modèle CDC et des données canadiennes, il a été déterminé que sous certaines conditions, une attaque d'anthrax sur 100 000 personnes résulterait en un cas de 50 000 cas d'anthrax, 32 875 morts, 332 500

jours d'hospitalisation et coûterait dans l'ordre de 6,5 G$ *(National Emergencies : Canada's Fragile Front Lines, March 2004)*. Des six micro-organismes qui ont été cités, seul le cas de variole possède un cas spécifique d'urgence, les autres correspondant à des solutions génériques d'urgence. Afin de pallier à ces lacunes, Santé Canada doit remettre ses recommandations pour la fin mars 2005, car en matière de terrorisme le Canada serait vulnérable. En effet, la population du pays et sa richesse sont de plus en plus concentrées dans un petit nombre d'endroits.

1.2.2. La sûreté des conteneurs

Suite aux événements du 11 septembre , le service des douanes mit sur pied le programme d'Initiative de Sûreté des Conteneurs (Conteneur Security Initiative, CSI) dont le mandat est de vérifier la marchandise en destination des É.U. à leur port d'origine plutôt qu'à leur arrivée. Cette nouvelle démarche fut mise sur pied suite à la découverte que les terroristes chercheraient à cacher des engins explosifs de destruction massive à l'intérieur des cargos scellés. Ainsi, afin de garder leur compétitivité dans l'économie globale, les 20 plus importants ports au monde qui transigent 90% des conteneurs au monde, mirent ensemble leurs efforts et permirent aux douanes américaines le soin de vérifier la marchandise au port de destination. L'intérêt de ces mesures était non seulement de préserver la sûreté de la marchandise mais également de protéger leurs propres économies et l'économie américaine.

La sûreté CSI consiste en 4 éléments: 1) utiliser des systèmes d'identification automatique pour cibler les conteneurs à haut risque, 2) détecter les conteneurs à haut risque au port de départ, 3) utiliser des technologies de détection pour scanner ces conteneurs ciblés, et 4) développer des conteneurs difficiles à frauder (Evans, 2004). Le port de Singapore est l'un des plus gros au monde, et celui-ci est considéré le deuxième plus important en terme d'achalandage. En 2003, celui-ci s'est joint aux autres grands ports du monde pour sécuriser la marchandise transitant sur son territoire. Tel que le

disait M. Bonner, commissaire aux douanes américaines, 'CSI is essential to securing global trade against terrorist exploitation'. C'est ainsi que depuis le début 2002, CSI a été mis en pratique auprès des grands ports du monde faisant affaire avec les É.U. De plus, les douanes américaines sont en pourparler avec plusieurs gouvernements afin d'étendre ce code de sûreté aux ports localisés dans des endroits stratégiques, possédant les infrastructures et la technologie en place pour participer au programme et qui expédient une quantité importante de cargos vers les É.U. Des organisations internationales telles le World Customs Organization et le G-8 ont favorisé l'expansion de CSI en adoptant des résolutions qui supportent l'application de mesures de sûreté introduites par CSI à travers les ports du monde. Les bénéfices d'une telle adoption sont multiples, le CSI est un élément dissuasif pour des organisations terroristes cherchant à attaquer des ports étrangers. Incontestablement, cette initiative offre des mesures de sûreté substantielles pour les ports participants et permet d'emblée des échanges plus sécuritaires car tout export doit être rapporté 24hr à l'avance. Par exemple, si des terroristes attaquaient un port en utilisant un cargo, le système maritime d'échange s'arrêterait jusqu'à ce que le niveau de sûreté soit rétabli. Pour un port qui n'aurait pas le système de sûreté CSI, la reprise des activités serait beaucoup plus lente. C'est pourquoi le CSI est souvent évalué comme 'une police d'assurance contre les menaces d'attaques terroristes' et comme 'un avantage compétitif en terme de prévoyance'. Pour ce faire, la mise en pratique du CSI requiert du pays participant d'avoir des scanners rayons-X ou une technologie de détection rayons gamma. L'inspection des cargos se fait le plus tôt possible dans la chaîne d'approvisionnement afin de maintenir l'intégrité de l'expédition.

L'importance du transport par cargo ne doit pas être sous-estimée car, en effet, 90% de toute marchandise à travers le monde transite par cargo, et plus de la moitié des réceptions de marchandise aux É.U. arrivent par des cargos maritimes, ce qui représente 7 millions de cargos par année. Finalement, pour être exigible à la phase d'expansion du CSI, une nation candidate doit remplir certains standards minimaux. En effet, les

douanes doivent pouvoir inspecter le cargo d'origine, de transit, sortant ou expédié à travers le pays. L'équipement non-intrusif de détection (NII) et de radiation doit être disponible et utilisé pour effectuer des inspections rapides sans interrompre le flux des échanges. Deuxièmement, les ports doivent avoir un trafic cargo régulier et substantiel vers les É.U. Ensuite, le port doit se munir d'un système de gestion de risques afin d'identifier potentiellement les cargos à haut risque et en automatiser le système. Ce système doit inclure un mécanisme pour valider les menaces, cibler les décisions et identifier les meilleures pratiques. Les données d'importance et les renseignements sur la gestion de risque doivent être partagés avec les douanes américaines. D'autre part, une évaluation complète du port doit être faite régulièrement afin d'en déterminer les vulnérabilités et les failles en matière de sûreté. Enfin, des programmes d'intégrité doivent être mis en place pour prévenir tout problème d'intégrité auprès des employés et combattre les infractions.

1.2.3. La sûreté des cargos

À l'exemple des mesures prises pour la sûreté des conteneurs, l'on développa un programme de sûreté à l'échelle internationale en collaboration avec les plus importants ports du monde, soit l'Opération Sûreté Cargo (Operation Safe Cargo, OSC).

L'OSC est un effort de collaboration entre le gouvernement fédéral, les entreprises, et l'industrie maritime afin de développer et partager les meilleures pratiques pour le transport sécuritaire des cargos. Les objectifs de ce programme sont l'accroissement des mesures de sûreté dans les ports d'origine, l'utilisation de la haute technologie pour faire le suivi des cargos en transit et une meilleure communication entre les agences de sûreté américaines et internationales. De plus, ce projet analyse les pratiques existantes et teste les solutions de sûreté dans un environnement opérationnel. Ce projet est mené dans les trois plus grands ports des É.U. soit ceux de New York, Los Angeles, et Seattle.

La crainte sous-jacente à la création de ces programmes serait le fait que les groupes terroristes pourraient utiliser les différentes installations portuaires pour le transport cargo de matières dangereuses; l'utilisation de cargos comme armes de destruction, des attaques sur les avions en utilisant des missiles sur les navires près des ports ou encore des attaques sur des villes en utilisant des navires comme arme. En effet, l'un des maillons les plus faibles dans le système de transport est l'expédition de conteneurs qui peuvent être ciblés pour transporter illégalement de la drogue, des gens ou des armes. Afin de palier à ce problème, le Département de Sûreté Nationale (Homeland Security Department) a investi 58 M$ pour le projet pilote de l'OSC car comme le dit Mick Shultz, porte-parole du port de Seattle 'If you want to secure the economy, secure the supply chain'. Malheureusement, cette prise de conscience se fit suite à la découverte qu'Osama bin Laden possédait auparavant plusieurs navires marchands (plus d'une vingtaine à une certaine époque) et donc s'y connaîtrait très bien vis-à-vis des forces et faiblesses du domaine maritime et portuaire. C'est pourquoi l'OSC étudie les vulnérabilités des conteneurs entrant dans les 3 plus grands ports américains et teste les différentes combinaisons des pratiques sécuritaires pour une chaîne d'approvisionnement plus sécuritaire. Par exemple, des éléments de détection d'intrusion pour capter la lumière, les radiations, les éléments chimiques ou biologiques peuvent être placés à l'intérieur d'un conteneur. Des sceaux sécuritaires ou des puces pouvant communiquer avec ces détecteurs sont placés à l'extérieur et les données récoltées sont transmises à un système de gestion d'événement de la chaîne d'approvisionnement. Nous aborderons dans le dernier chapitre ces sceaux électroniques qui sont l'une des solutions de base pour les nouvelles technologies en mode d'essai et qui utilisent entre autre, la technologie RFID.

Ainsi, les employés agissent lorsqu'ils détectent une anomalie en accord avec les protocoles établis tandis que le système de gestion d'événements de la chaîne d'approvisionnement communique avec la garde côtière et les douanes. L'un des buts de ces initiatives est de développer des pratiques qui peuvent être adoptées comme standard à l'échelle internationale. Ainsi, lorsqu'en place, ces standards permettront un flux

efficace des échanges ce qui pourrait se traduire non seulement par des réductions de coûts dans les magasins de grande surface, mais aussi assurerait des cargos plus sécuritaires.

1.2.4. Le partenariat d'échange-douanes

Le Custom-Trade Partnership against Terrorism (C-TPAT), est une initiative conjointe entre le gouvernement et les entreprises pour protéger la sûreté des cargos entrant aux É.U. et maintenir le flux des échanges. En effet, le but de cette initiative est de sécuriser la chaîne d'approvisionnement et les frontières grâce à une coopération entre les douanes et les intervenants de la chaîne d'approvisionnement. À l'exemple des douanes dont le rôle est de protéger la frontière, les entreprises doivent pouvoir assurer la protection de leurs produits, leurs employés, et leurs clients. Ainsi, le C-TPAT permet aux entreprises de jouer un rôle d'importance dans la lutte contre le terrorisme en échange de quoi, les douanes promettent certains avantages, notamment une réduction des inspections et donc du temps moindre de transit à la douane des marchandises. Les experts sont d'accord pour dire que si les terroristes peuvent interrompre le flux des échanges économiques en forçant la création de mesures de sûreté trop sévères, alors ils auront réussi à ralentir le progrès et l'avancement de l'économie des pays développés. En effet, l'économie des pays industrialisés est fondée sur le principe du marché libre et ouvert, et donc doit demeurer ainsi. Pour garantir ce flux, les douanes américaines offrent maintenant des 'voies rapides' aux transporteurs et expéditeurs qui se munissent de mesures pour sécuriser leur marchandise. Ceci permet donc un transit plus rapide de la marchandise ce qui se traduit par un avantage compétitif pour la firme. Le C-TPAT requiert, d'autre part, des importateurs 'd'évaluer, faire évoluer, et communiquer de nouvelles pratiques' et donc de sécuriser leur chaîne d'approvisionnement.

En conclusion, l'Acte de la Sûreté des Transports Maritimes (MTSA), également connu sous le nom de S1214, fut signé en novembre 2002 par le président Bush et un mois plus

tard, par l'OMI. Se basant sur les recommandations américaines, cet acte passa un code pour la sûreté portuaire et l'expédition internationale. C'est ainsi, qu'il se développa au sein du domaine portuaire un consensus sur les règles et les procédures à suivre dans le but d'améliorer la sûreté des infrastructures.

1.2.5. L'Acte sur la Sûreté du Transport Maritime (MTSA)

En février 2002, le congrès américain créa un Fonds pour la Sûreté Portuaire (Port Security Grant) afin de pallier aux coûts inhérents de développements ainsi qu'au perfectionnement des mesures de sûreté adoptées, et en juillet 2002, 93 M$ furent donc alloués pour l'achat de nouveaux équipements afin d'améliorer la sûreté portuaire (Evans, 2004). L'année dernière, 442 projets dans 326 localités à travers les États-Unis, reçurent 179 M$ en subvention. En février 2004, le président Bush a réitéré son engagement dans la sûreté de son pays et a choisi d'augmenter de 13% le financement, soit débloquer 1.9 G$ spécifiquement pour la sûreté portuaire. Ces fonds inclus 102 M$ pour la garde côtière américaine afin d'implanter l'Acte de Sûreté du Transport Maritime de 2002 (Maritime Transportation Security Act) qui établit les standards de sûreté pour certains navires, les facilités portuaires et les plates-formes offshore d'importances. De plus, un total de 6.6 G$ sera alloué pour la maintenance et l'amélioration de la sûreté des frontières, ce qui correspond à une augmentation de 7% (White House Office of Communications, 2004).

De plus, la requête pour le budget 2005 est de 6.3 G$ pour la garde côtière américaine, soit une augmentation de 9% par rapport à l'an dernier (White House Office of Communications, 2004). Ainsi, cette initiative permettra à la garde côtière des standards de sûreté et des équipements lui permettant de sécuriser ses ports. Une portion de ce montant servira à renouveler sa flotte de navires et à installer des systèmes d'identification automatique (AIS).

Par le passé, les experts en matière de sûreté étaient d'accord pour dire que les menaces principales au commerce maritime étaient le piratage occasionnel, les passagers clandestins ou la contrebande, événements qui seraient plutôt le résultat d'un manque de vigilance de la part des responsables des navires ou des opérateurs (Evans, 2004). Plusieurs pensaient à l'époque que les attaques terroristes se produiraient d'avantage sur les avions commerciaux, puisque ceux-ci ont toujours été des cibles et que la couverture médiatique de tels événements suscite un grand intérêt. Les attaques terroristes d'Al Qaeda sur le U.S.S Cole, une frégate de la marine américaine se ravitaillant dans le port du Yemen en octobre 2000, servirent d'alerte que des événements se mijotaient. L'analyse de cet incident était presque finalisée lorsque les attaques du 11 septembre eurent lieu. Par la suite, un autre plan d'attaque sur un navire américain à Singapore fut découvert et fut presque mis en œuvre, mais il fut avorté grâce à des efforts conjoints de la communauté intelligente internationale et le travail de la police. C'est à ce moment que l'on découvrit les liens d'Osama bin Laden avec l'industrie de la navigation. En décembre 2002, cette fois-ci, un pétrolier français le *Limberg* explosa en entrant dans le port du Yemen. La détonation créa non seulement un désastre écologique, mais compromit les efforts de la diplomatie française dans la région du Moyen-Orient. Le message fut clair, l'industrie du commerce maritime serait la proie à des attaques terroristes. En réponse aux actes terroristes des dernières années, l'Acte sur la Sûreté du Transport Maritime (Maritime Transportation Security Act, MTSA), mis sur pied par le gouvernement fédéral américain, a cherché à transformer l'approche générale de la sûreté maritime. En effet, dorénavant la sûreté engloberait une meilleure planification, une sûreté du personnel accrue, et une plus grande vigilance des navires et des cargos. Des investissements en matière de système de détection des navires, l'identification des travailleurs et une méthode de détection des ports étrangers à risque pour les É.U., sont certaines mesures importantes ayant été prises. De plus, une approche systématique a été adoptée afin de pallier aux faiblesses des installations à l'échelle nationale car effectivement, celles-ci représentent des cibles intéressantes vu leur étendue, leur accessibilité par mer ou terre, et de leur proximité aux centres urbains et leurs réseaux de

transport complexe pour déplacer la marchandise efficacement. Par ailleurs, dans le voisinage l'on retrouve souvent des installations critiques pour l'économie d'un pays telles des raffineries, des manufactures et des centrales électriques.

Les maillons faibles auprès des installations et des navires sont multiples. Les terminaux des conteneurs, endroit où les conteneurs sont transférés des bateaux aux trains ou aux camions, doivent pouvoir examiner les véhicules entrant et vérifier régulièrement les cargos pour tout indice portant à croire à une manipulation illicite. Les manufactures chimiques, autres installations et des matériaux dangereux sont présents et on doit pouvoir en contrôler l'accès. Les navires également doivent pouvoir limiter l'accès à leur pont ou au centre de contrôle du navire. Pour mitiger tous ces risques potentiels, des barrières, des gardes de sûreté et des caméras peuvent être utilisés pour réduire les intrusions et prévenir toute exploitation des vulnérabilités mentionnées.

Bien que plusieurs décideurs des secteurs privés et publics soutiennent l'idée d'une plus grande sûreté, celle-ci ne vient pas sans impact sur l'économie générale. Les livraisons juste-à-temps ont effectivement besoin d'un flux régulier et sans goulot à travers le système de transport car des délais ou des interruptions dans la chaîne d'approvisionnement pourraient avoir des impacts économiques importants. C'est pourquoi, le MTSA oblige les opérateurs et propriétaires d'installations portuaires ou de navires, d'effectuer une évaluation des faiblesses de la sûreté en accord avec des objectifs bien précis. La date du 1er juillet 2004 a été imposée comme date de conformité avec les plans stipulés dans le MTSA et, en décembre 2002, les membres de l'OMI (International Maritime Organization) ont adopté le code international ISPS (International Ship and Port Facility Security) à mettre en place également pour le 1er juillet 2004.

Le code ISPS

Le code ISPS (International Ship and Port Facility Security Code) développé par l'OMI sous l'égide des Nations Unies, est un ensemble de procédures et de mesures adoptées en novembre 2001 afin de prévenir les actes de terrorisme qui menacent la sûreté des passagers, des membres d'équipage et des navires. Tel que déclaré lors du Sommet du G-8 en juin 2002, il s'agit d'améliorer la sûreté et protéger le commerce : 'cooperative actions to promote greater security of land, sea and air transport while facilitating the cost-effective and efficient flow of people, cargo and vehicles for legitimate economic and social purposes.' Une des résolutions d'importance ayant été adoptée est la conformité avec ce code pour tous les ports du monde pour le 1er juillet 2004. Certaines des mesures adoptées incluent des mesures pour améliorer la cueillette et l'échange de données, dont les données biométriques pertinentes au personnel marin, l'amélioration de la sûreté cargo, aérienne et le transport en général.

L'objectif de ce code est d'établir un cadre international pour la coopération entre les gouvernements, les agences gouvernementales, les administrations locales et l'industrie maritime et portuaire pour détecter les menaces et prendre les mesures nécessaires contre tout incident affectant les navires ou les facilités portuaires utilisées dans le cadre des échanges internationaux et offrir des plans et procédures pour réagir à différents niveaux de sûreté. Ces objectifs seront atteints grâce au personnel adéquat sur chaque navire, dans les ports et dans chaque entreprise de transport maritime afin de préparer et mettre en application les plans de sûreté (ISPS Code, 2003).

Plus précisément, le code stipule que chaque navire doit avoir à bord un plan de sûreté résultant de l'évaluation de la sûreté du navire. Ce plan doit être approuvé par l'administration du pavillon et/ou un organisme de sûreté reconnu (RSO). Le plan de sûreté du navire (SSP) doit prévoir des dispositions sur les procédures et les stratégies de

sûreté correspondant à chacun des trois niveaux d'alerte déterminés par les gouvernements contractants. Ce plan doit porter au moins sur ces éléments suivants :

- Les mesures visant à empêcher l'introduction à bord d'armes, de substances dangereuses et d'engins interdits qui peuvent être utilisés contre des personnes, de navires ou des ports.
- L'identification des zones d'accès restreint et des mesures visant à empêcher l'accès non autorisé à ces zones
- Des mesures visant à empêcher l'accès non autorisé au navire
- Des procédures pour faire face à une menace contre la sûreté ou une atteinte à la sûreté, y compris des dispositions pour maintenir les opérations essentielles du navire ou de l'interface navire/port.
- Des procédures pour donner suite aux consignes de sûreté que les gouvernements contractants peuvent donner au niveau de sûreté 3.
- Des procédures d'évacuation en cas de menace contre la sûreté ou d'atteinte à la sûreté.
- Les tâches du personnel du navire auquel sont attribuées des responsabilités en matière de sûreté et celles des autres membres du personnel du navire concernant les aspects liés à la sûreté.
- Des procédures d'audit des activités liées à la sûreté.
- Des procédures concernant la formation, les entraînements et les exercices liés au plan.
- Des procédures concernant l'examen périodique du plan et sa mise à jour.
- Des procédures de notification des incidents de sûreté.
- L'identification de l'agent de sûreté du navire.
- L'identification de l'agent de sûreté de la compagnie, y compris les coordonnées où il peut être joint 24 heures sur 24.
- Des procédures visant à garantir l'inspection, la mise à l'essai, l'étalonnage et l'entretien de tout matériel de sûreté prévu à bord.

- La fréquence de mise à l'essai ou de l'étalonnage de tout matériel de sûreté prévu à bord.
- L'identification des endroits où sont installés les commandes du système d'alerte de sûreté du navire.
- Les procédures, instructions et conseils concernant l'utilisation du système d'alerte de sûreté du navire, y compris sa mise à l'essai, son déclenchement, sa neutralisation et son réenclenchement et la manière de réduire le nombre de fausses alertes.

Tiré de l'OCDE, 2003

Les mesures prises pour palier aux lacunes en matière de sûreté des transports maritimes ont été négociées et approuvées à L'OMI ou prises à l'initiative des États-Unis. Voici sous forme de tableau les coûts estimés de ces mesures :

Tableau 1.6 Coûts des mesures de sûreté maritime

Tableau récapitulatif : coûts des mesures de sûreté maritime et évaluation des avantages autres que ceux liés à la lutte contre le terrorisme					
Mesure	**Coût initial approximatif (en millions dollars US)**	**Coût annuel approximatif (en millions dollars US)**	**Coûts indirects**	**Degré de certitude**	**Autres avantages**
SOLAS/Codes ISPS OMI					
Niveau gouvernemental d'alerte de sûreté	**faible**	**n.d.**	**Potentiellement élevé**	**faible**	+
Systèmes d'identification automatique	649.3	indéterminé	indéterminé	élevé	+++
Système d'alerte de sûreté des navires	**86.5**	**4.3**	**0**	**élevé**	
Numéro d'identification	21.6	n.d.	0	moyen	+

du navire					
Agent de sûreté de la compagnie (grandes compagnies)	514.6	514.6	indéterminé	moyen	+
Agent de sûreté de la compagnie (petites compagnies)	150	150	indéterminé	faible	
Évaluation de la sûreté du navire	103.9	faible	0	moyen	
Plan de sûreté du navire	51.9	faible	0	moyen	
Agent de sûreté du navire	29	29	0	moyen	+
Sûreté du navire: formation/exercices	16.8	16.8	0	moyen	
Équipement de sûreté du navire	304.4	15.2	0	élevé	+
Tenue de registre	faible	faible	0	élevé	
Évaluation de la sûreté des installations portuaires	27.9	0.8	0	faible	++
Plan de sûreté des installations portuaires	27.9	0.8	0	faible	++
Agent de sûreté des installations portuaires	indéterminé	indéterminé	indéterminé		++
Installations portuaires : formation/exercices	indéterminé	indéterminé	indéterminé		+
Sûreté des installations portuaires équip./personnel	indéterminé	indéterminé	indéterminé		+++
Mesures de sûreté maritime – États-Unis Maritime Transportation Safety Act de 2002	indéterminé	Potentiellement élevé	indéterminé		

Notification de l'arrivée 96 heures à l'avance	6.7	6.7	indéterminé	élevé	
Carte d'identité obligatoire pour les membres d'équipage (proposée)	**95 (au moins)**	**indéterminé**	**élevé**	**faible**	
Notification 24 heures à l'avance des manifestes	281.7 à 10 000	281.7 à 10 000	Indéterminé	faible	++
Initiative destinée à améliorer la sûreté des conteneurs	**indéterminé**	**indéterminé**	**indéterminé**		+
Partenariat entre les services des douanes et du commerce contre le terrorisme	indéterminé	indéterminé	indéterminé		+++

Tiré du rapport de l'OCDE, 2003

L'Organisation pour la coopération et le développement économique (OCDE) estime que les coûts de mise en œuvre des amendements SOLAS et du code ISPS sont de l'ordre de 1.3 G$ initialement et entraînent des charges récurrentes de 700 M$ par année : ces coûts correspondent aux systèmes de sûreté automatiques ainsi qu'aux officiers supplémentaires ayant été engagés. Cependant, bien que ces sommes puissent paraître astronomiques, elles sont infimes en comparaison à la valeur des échanges internationaux et des coûts qui s'ensuivraient si le commerce devait s'arrêter.

1.2.6. Le contrôle des navires par l'État du port

Le contrôle des navires par l'État du port (CNEP) est un programme d'inspection des navires dans le cadre duquel les navires étrangers qui s'engagent dans les eaux d'un État souverain sont arraisonnés afin de vérifier s'ils respectent les exigences des principales conventions maritimes internationales. Parmi ces dernières, mentionnons notamment la

Convention internationale pour la sauvegarde de la vie humaine en mer (SOLAS), la Convention internationale pour la prévention de la pollution par les navires (MARPOL), la Convention internationale sur les normes de formation des gens de mer, de délivrance de brevets et de veille (SCTW) et Convention de l'Organisation internationale du travail no 147 (OIT 147) (Sûreté maritime- contrôle des navires par l'État du port, rapport annuel 2002). Les programmes du CNEP ont un caractère régional. Cela signifie que plusieurs pays partageant des étendues d'eau communes sont regroupés en vertu d'un mémorandum d'entente (ME) pour que les navires faisant du commerce dans leur région se conforment aux normes internationales. Le Canada est signataire de deux mémorandums d'entente : le ME de Paris, qui réunit 19 pays (18 pays européens et le Canada) et le ME de Tokyo qui regroupe 18 pays de l'Asie-Pacifique.

Le Canada est devenu un membre associé au ME de Paris en avril 1998 et a été le premier pays non européen à avoir ce privilège. Par ailleurs, le Canada a été l'élément moteur de l'élaboration du ME de Tokyo dont il est membre depuis son entrée en vigueur en décembre 1993. Transport Canadaest responsable de toutes les activités de CNEP au Canada. Les inspections des navires étrangers sont effectuées dans tous les grands ports par des inspecteurs de la Direction de la sûreté maritime (Sûreté maritime-contrôle des navires par l'État du port, rapport annuel 2002).

À la fin de l'année 2002, le naufrage du navire-citerne Le Prestige, a provoqué un désastre écologique sur la côte espagnole après que le navire transportant 77 000 tonnes de pétrole se soit brisé en deux et a coulé au large de l'Espagne. Ce désastre démontra une fois de plus, l'importance du régime du contrôle par l'État du port et la nécessité d'inspecter les bâtiments étrangers qui font escale dans nos ports. Afin de garantir que les navires-citernes qui font escale dans les ports canadiens respectent les normes internationales, la direction de la Sûreté maritime de Transport Canadaa confirmé de nouveau en juillet 2002 une décision prise au début des années 1990 d'inspecter chaque navire-citerne étranger lors de sa première visite au Canada, puis sur une base annuelle par la suite. Grâce à la participation du Canada aux ME de Paris et Tokyo sur le contrôle

des navires par l'État du port, la collaboration avec la garde côtière américaine, et l'élaboration de programmes nationaux, la Canada continue à travailler en faveur de l'élimination des navires inférieurs aux normes afin de garantir que les navires faisant escale dans nos ports sont sécuritaires et écologiques (Sûreté maritime- contrôle des navires par l'État du port, rapport annuel 2002).

Données statistiques sur le contrôle des navires par l'État du port

Au Canada, les inspections de contrôle des navires par l'État du port sont menées conformément à la *Loi sur la marine marchande du Canada* et aux mémorandums d'entente de Paris et de Tokyo sur le contrôle des navires par l'État du port quand il s'agit de déterminer la conformité des navires étrangers aux conventions internationales. Au cours des cinq dernières années, le nombre d'inspections a fluctué et c'est en 2001 que le nombre des inspections a atteint un sommet. Grâce à un meilleur ciblage des navires et aux programmes spéciaux (notamment ceux de l'inspection des vraquiers et de l'inspection des navires-citernes), on a constaté une baisse du nombre des navires ne respectant pas les normes et pratiquant le commerce dans les ports canadiens.

En 2002, la proportion des navires présentant des anomalies était de quarante-cinq pour cent (45%) de l'ensemble des inspections, ce qui représente une réduction de sept pour cent (7%) par rapport aux chiffres de 2001. Parmi les navires présentant des anomalies, quatre pour cent (4%) de l'ensemble des navires inspectés ont été détenus. Comparativement aux détentions de 2001, le pourcentage était plus élevé, le taux de détention étant de huit pour cent (8%) (Sûreté maritime- contrôle des navires par l'État du port, rapport annuel 2002). Le tableau 1.7 présente une comparaison des navires inspectés, présentant des anomalies et détenus de 1998-2002.

Tableau 1.7 Comparaison des navires inspectés, des navires présentant des anomalies et des navires détenus au Canada au cours des cinq dernières années

Année	2002	2001	2000	1999	1998
Inspections	1 159	1 197	1 070	1 076	1 191
Présentant des défectuosités	525	634	583	563	587
Détentions	49	92	103	125	142

Tiré de Transport Canada, 2002

Pour soulever rapidement le type d'anomalies généralement rencontrées, on constate de nombreuses catégories distinctes. La catégorie de l'équipement de lutte contre les incendies affiche le plus fort pourcentage d'anomalies, soit 17,5% du total. En 2002, 2540 anomalies sur les 525 navires inspectés au Canada ont été relevées (Sûreté maritime- contrôle des navires par l'État du port, rapport annuel 2002). La catégorie 'Sûreté en général' se classait au deuxième rang des anomalies constatées, ce qui représente 17,1% du total des anomalies signalées. La catégorie 'Sûreté en général' énumère notamment les anomalies de structure et la corrosion de la structure d'un navire. L'équipement de sauvetage et de navigation ont obtenu les troisième et quatrième pourcentages d'anomalies, soit 11,1% et 10,1%, respectivement (Sûreté maritime-contrôle des navires par l'État du port, rapport annuel 2002).

Ces quatre catégories d'anomalies indiquent des lacunes graves dans l'entretien de l'équipement et des structures essentielles à la sûreté de tout voyage mais il est inquiétant de constater qu'elles demeurent au sommet de la liste des problèmes, une fois de plus, en 2002. Les lacunes liées à l'élément humain ont augmenté de trois pour cent (3%) depuis 2001; cela pourrait être le résultat direct de l'entrée en vigueur du Code STCW 95 (Sûreté maritime-contrôle des navires par l'État du port, rapport annuel 2002).

1.2.7. Initiatives du G8

Dans le Rapport général du Secrétaire général des Nations Unies de 2003, le Canada s'est exprimé sur la question des mesures visant à empêcher les terroristes d'acquérir des

armes de destruction massive. 'Dans le cadre du Partenariat mondial contre la prolifération des armes de destruction massive et des matières connexes, lancé lors du Sommet du G-8 à Kananaskis (Canada) en 2002, le Canada s'est engagé à collaborer avec ses partenaires du G-8 pour éliminer la menace que représentent les dizaines de milliers d'armes chimiques et nucléaires existantes, ainsi que les matières connexes, que le régime soviétique avait laissé derrière lui. Dans tous ces projets, le Canada révèle sa ferme détermination et sa participation active à la lutte contre le terrorisme et contre la prolifération d'armes de destruction massive et des matières connexes. Le Canada a dirigé l'élaboration des six principes qui ont été adoptés au Sommet du G-8 de 2002 de Kananaskis, qui visent à empêcher les terroristes et ceux qui les abritent d'acquérir ou de mettre au point des armes nucléaires, chimiques, radiologiques et biologiques, des missiles et les matières, les équipements et la technologie qui y sont rattachés.

1.3 La chaîne logistique internationale

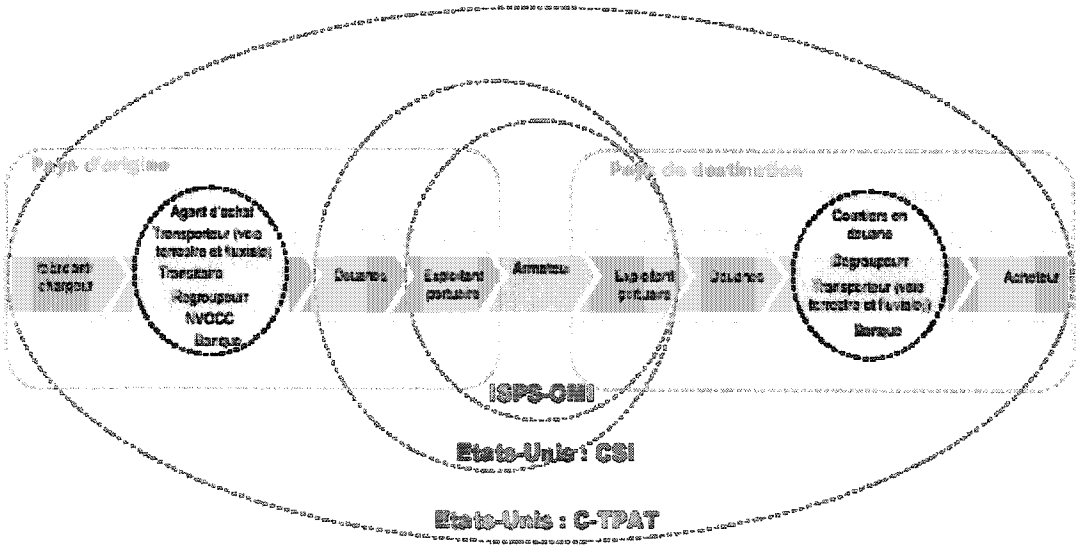
Nous avons vu à travers ce chapitre les différences et les similitudes entre le transport maritime américain et canadien. Nous avons abordé les différents programmes mis sur pied dans le cadre d'amélioration de la sûreté maritime qui ont été développé à la base par les É.U. dans l'objectif de sécuriser leur territoire national.

En conclusion, bien que la majeure partie du commerce mondial emprunte la voie maritime, le transport maritime n'est qu'une portion d'une chaîne plus complexe. L'acheminement porte à porte d'un conteneur maritime suppose l'intervention d'environ 25 acteurs différents, l'établissement de 30 à 40 documents, l'utilisation de 2 à 3 modes différents de transport et la manutention du conteneur dans 12 à 15 sites différents (OCDE, 2003). Ce réseau complexe peut être divisé en trois grands flux :

- Déplacement de marchandises d'un lieu vers un autre

- Transfert de la responsabilité de la garde des marchandises d'une personne à une autre
- Transfert des informations concernant la cargaison

La figure 1.1, présente de manière simplifiée les points saillants de vulnérabilité de la chaîne logistique et repasse en revue l'imbrication des différents programmes et de leur impact sur la chaîne logistique.



Tiré de Rapport de l'OCDE, 2003

Figure 1.1. : Évaluation de la vulnérabilité de la chaîne logistique internationale pour les conteneurs

Tel que l'on observe à partir de ce graphique, le programme C-TPAT englobe la totalité de la chaîne logistique et recoupe les exigences des programmes CSI et OMI.

Tel que le mentionne Mr. Don Young et Frank A. LoBiondo, députés de la chambre des représentants, 'It is important to keep in mind that total security cannot be bought no matter how much is spent on it. It is difficult if not impossible to successfully anticipate

and thwart all types of potential terrorist threats that highly motivated, well skilled, and adequately funded terrorist groups could devise.'

Par conséquent, en matière de sûreté portuaire, rien ne doit être laissé au hasard et toute opportunité d'exploitation des failles, doit faire l'objet d'une analyse poussée afin de pallier aux lacunes et d'éviter le pire. Le prochain chapitre examine les solutions actuelles en terme de sûreté.

CHAPITRE 2
RISQUES, SOLUTIONS ACTUELLES EN TERME DE SÛRETÉ PORTUAIRE, ET TECHNOLOGIES

' La moitié d'un port est occupée par des navires qui ne font rien ; la moitié d'un réseau par des wagons qui attendent ; la moitié d'une usine par des marchandises immobiles. Quel bénéfice, si tous les navires travaillaient, si tous les wagon roulaient, si toutes les marchandises circulaient! La vitesse de circulation de la monnaie est à la base de l'aisance financière, la vitesse de circulation des choses à la base de la prospérité économique.'

Auguste Detoeuf, Propos d'O. L. Barenton, confiseur, *Paris, 1938*

Ce chapitre se propose de regarder de près les méthodes et les moyens utilisés pour combattre le plus efficacement possible le terrorisme en matière de transport maritime. D'une part, une vue globale des technologies les plus avant-gardistes employées sera passée en revue. D'autre part, la technologie du RFID sera présentée comme une solution potentielle et intéressante permettant l'amélioration de la sûreté dans les ports.
L'économie de marché est fondée sur le principe de libre entreprise et nécessite un système d'échange et de mise en marché rapide et efficace. C'est dans ce but qu'une nouvelle approche de gestion manufacturière s'est développée permettant de raccourcir les délais, l'inventaire, et les coûts: le Juste-à-Temps (Just-in-Time). Cette nouvelle vision de la fabrication repose sur un concept clé, celui de l'efficience, afin de réduire les obstacles au flux régulier des marchandises. Dans la foulée de cette nouvelle approche, des processus de production et de nouveaux outils ont été développés pour atteindre une efficience des opérations. À l'aube de ce nouveau siècle, des intérêts divergents menacent de faire basculer la stabilité des marchés et de remettre en cause les infrastructures ayant été conçues pour soutenir le dynamisme des échanges et la libre

circulation des marchandises. Le terrorisme risque de devenir une pierre d'achoppement difficile à ignorer, transformant les mentalités et les approches des infrastructures industrialisées dont le système de transport n'est pas exclu.

Initialement, le système de transport maritime a été conçu pour être efficace et rapide mais pas nécessairement sécuritaire. Cependant, les réalités de notre monde ont changé la donne pour privilégier dorénavant la sûreté au détriment de l'efficience et la rapidité. En effet, dans le contexte actuel des attaques terroristes survenues récemment dans le secteur de l'aviation suites aux événements du World Trade Center et celui ferroviaire en septembre 2003 à Madrid, les gouvernements, les agences et les experts en matières de sûreté ont du changer leur approche pour se conformer aux impératifs des temps présents. Des changements s'imposent pour préserver l'économie des pays qui voient leurs intérêts menacés par des groupes d'extrémistes; le transport maritime qui soutient à 95% les échanges mondiaux est devenu le point de mire d'intérêts divergents. Pour ne regarder que quelques statistiques, en 2000, l'industrie du transport maritime a transigé un total de 230 millions de conteneurs dont 31 millions ont traversé les ports de l'Amérique du Nord (Richardson, 2002).

Dans des conditions normales, le système maritime international dépend de son habilité à maintenir le flux du trafic de conteneurs à travers les ports majeurs du monde. Dans la recherche de solutions innovatrices et sécuritaires pour transformer le système maritime actuel, il est important que le choix puisse garantir la vigueur de l'économie, et, de son réseau et par extension, le système global de commerce. C'est ainsi qu'en étudiant les menaces relatives au terrorisme, il est important à prime abord de considérer et d'évaluer quelles en sont les faiblesses exploitables et de connaître quelles sont les capacités organisationnelles des groupes menaçant les infrastructures car un dérangement dans le flux régulier du transport maritime de marchandises aurait des conséquences néfaste

2.1. L'évolution de la logistique des transports

Grâce aux effets de la mondialisation, à la logistique intégrée et au développement des technologies de l'information et des communications, le commerce mondial et les flux commerciaux matériels subissent des transformations qui ont pour résultat la croissance économique, plus de choix pour le consommateur et une concurrence accrue. Afin de demeurer compétitives dans ce contexte, les entreprises doivent répondre avec efficacité à la demande du marché et s'organiser grâce à une logistique mondiale ou une gestion de la chaîne d'approvisionnement devenue le nerf de la force de compétition. L'expansion du commerce mondial étant devenu plus complexe, il a crée une croissance du transport de marchandises et une amplification des réseaux de transport.

De plus en plus les industriels cherchent à concentrer leur production et leur capacité de stockage afin d'optimiser les économies d'échelle tout en minimisant les coûts de transport. Par ailleurs, les entreprises réalignent leurs chaîne d'approvisionnement en se concentrant sur leurs métiers essentiels et sous-traitent les activités qui n'apportent pas de valeur ajoutée ce qui a pour effet que le transport international renforce sa concentration sur un plus petit nombre de ports et aéroports de transit afin de profiter d'économies d'échelle (OCDE, 2002). Afin de demeurer compétitif sur le marché étranger, les temps de livraison sont raccourcis, ce qui permet aux entreprises de réduire les coûts d'inventaires, de répondre plus rapidement à des cycles de vie des produits plus courts et d'augmenter la fiabilité de la livraison. Un aspect clé de la gestion des inventaires, est l'utilisation des TIC dans la gestion des transports et de l'entreposage, car dans le but d'améliorer la visibilité de la chaîne mondiale des approvisionnements, plusieurs entreprises de transport ont investi massivement dans des systèmes de traçage pour localiser à tout moment leur envoi. Le service des Douanes américains s'est aussi doté d'un système automatisé de localisation de cargo et de passagers de 314 M$ afin de sécuriser d'avantage leur commerce et leurs frontières. Les sociétés dont les activités de

logistiques sont efficaces, ont une véritable valeur ajoutée. En effet, la mondialisation accentue le rôle d'importance de la distribution et des transports qui donne plus de valeur aux produits et maintient l'avantage compétitif d'une firme. C'est ainsi, qu'à la lumière des paragraphes précédents, l'on saisit mieux l'importance de la sécurisation des modes de transport afin de maintenir le flux normal et efficace des marchandises qui dépend d'un fonctionnement sans entrave, ni contraintes majeures.

Finalement, mentionnons que la nécessité de gérer efficacement les livraisons de porte à porte à l'échelle mondiale a contribué à l'expansion des réseaux d'information dans les entreprises. C'est effectivement grâce à l'avancée de la technologie de l'information que les opérations de logistique ont été intégrées dans la chaîne d'approvisionnement. Ainsi, l'application des TIC aux transports a crée l'émergence de systèmes de transports intelligents (STI) qui permettent un transport efficace et sûr. En effet, il est maintenant possible d'identifier, de tracer et de planifier les cargaisons presque partout dans le monde.

2.2. Les facteurs de risque

La sûreté des navires et des facilités est essentiellement une question de gestion de risque (Emerson, Nadeau, 2003), il importe donc de bien comprendre ce qu'est la gestion de risque afin d'offrir une perspective systémique qui permettrait de présenter des solutions et d'extrapoler sur les tendances dans le domaine de la sûreté. Cette section se propose de présenter la raison d'être des décisions de gestion en matière de risque et d'examiner les méthodes et la structure adoptée pour maximiser la sûreté portuaire. Le risque est toute circonstance créant une menace à l'entreprise, les gens ou les ressources (Kipp, Loflin, 1996). Ce qui importe dans la mitigation de risque c'est de faire les bons choix car indéniablement des décisions devront être prises qui dépendront de la revue et de l'analyse des informations disponibles et de leur qualité. Ipso facto, ces décisions auront des impacts sur l'environnement en question, c'est pourquoi il dépend des

responsables de bien comprendre les facteurs entrant en jeu, leurs conséquences, et comment atteindre l'équilibre entre les deux. Par ailleurs, la gestion est un processus dynamique qu'il est nécessaire de revoir périodiquement afin d'évaluer la pertinence des décisions ayant été prises. Enfin, des buts et des objectifs doivent être clairement définis qui permettront une meilleure prise de conscience de la direction à suivre.

Le principal facteur de risque associé au transport maritime est sans doute le volume et la quantité de marchandises acheminées par voie maritime. La conférence des Nations Unies sur le Commerce et le Développement (CNUCED) estime à 5.8 G de tonnes soit plus de 80% du commerce mondial, le volume de marchandises acheminées en 2001, pour l'essentiel à bord de plus de 46 000 navires desservant presque 4 000 ports dans le monde entier. Les experts s'accordent pour dire que prochainement le commerce maritime mondial ne sera pas à la baisse, d'autant que les négociations internationales visent expressément à faciliter et accélérer le commerce mondial plutôt qu'à le ralentir. Outre sa taille, le secteur maritime est par nature un réseau de transport complexe, international et ouvert qui pose un problème de taille, celui de la multiplicité des facteurs de risque terroriste. En effet, les navires de haute mer peuvent être les outils ou les cibles d'attentats. Ils peuvent également servir à faciliter d'autres attentats et/ou collecter des fonds pour des organisations terroristes. D'autre part, les principaux facteurs de risque liés aux transports maritimes, cargaisons, navires, personnel et sources de financement, sont aussi liés à des risques plus vastes : perturbations importantes du commerce mondial et accroissement des coûts économiques découlant du renforcement de la sûreté. Nous verrons en détails ces quelques facteurs de risques dans la prochaine section. Tel que le mentionne l'OCDE (2003) dans son rapport, 'Il est important que les gouvernements s'emploient à faire face à ces risques en recourant à tout un arsenal car il pourrait être à la fois coûteux et inefficace de se limiter à réagir au coup par coup aux diverses menaces.'

2.2.1. Le risque nucléaire

Depuis le 11 septembre 2001, les experts s'accordent pour souligner que le risque nucléaire est le plus probable de tous les risques à prendre en compte lorsque l'on considère les menaces possibles vis-à-vis des ports et des infrastructures maritimes. Il existe trois types d'actes terroristes envisageables en ce qui concerne le nucléaire. Tout d'abord des attentats terroristes contre des cibles civiles nucléaires, l'utilisation d'une arme nucléaire par des terroristes et l'emploi d'une bombe sale qui répandrait de la radioactivité sans pour autant provoquer d'explosion nucléaire (dirty bomb). De ces trois scénarios, celui que l'on retient comme étant le plus probable dans le cas d'une attaque d'un port est le dernier, d'où les moyens qui sont entrepris pour en éliminer le risque. En effet, une évaluation détaillée des risques permet de conclure qu'après avoir alloué les ressources dans les endroits les plus pressants de vulnérabilité en matière de sûreté, il est nécessaire d'attaquer le problème à sa source. Ceci implique donc l'utilisation de services d'intelligence pour recueillir des informations sur les groupes cherchant à se procurer des armes.

En 2002, le Bureau international des conteneurs (BIC) estimait à environ 15 000 000 le nombre de conteneurs en circulation et d'après les données de Conteneurs Online, 232 millions de conteneurs ont transité par les ports de conteneurs en 2001. Le volume considérable de mouvements de conteneurs, leur taux de rotation élevé dans le système commercial international et leur uniformité sont autant de défis pour la sûreté. L'on redoute de fait, l'utilisation de conteneurs pour y cacher et livrer des armes de destruction massive relativement rudimentaire, les 'bombes sales' dont il sera question dans cette section. Dans le scénario le plus pessimiste, une organisation terroriste pourrait placer une arme de destruction massive, muni d'un système de positionnement mondial par satellite, dans un conteneur maritime, l'introduire dans le réseau de transport international par le biais de chargeurs, d'intermédiaires et de transporteurs

légitimes puis actionner à distance le détonateur de l'arme au moment de son arrivée au cœur d'une importante zone habitée (OCDE, 2003). Les gouvernements craignent qu'une telle possibilité se produise car seulement 2% des conteneurs sont effectivement examinés. Les sous-sections suivantes se proposent de regarder de plus près comment une organisation terroriste pourrait facilement se procurer le matériel radioactif nécessaire pour introduire une bombe rudimentaire dans l'un de ces conteneurs.

2.2.2. Une attaque contre des cibles civiles

'Tout pays possédant des centrales nucléaires donne à ses adversaires une quasi-capacité nucléaire de les utiliser contre lui' (Labbé, 2003). Cette vulnérabilité des centrales nucléaires a été étudiée par maints chercheurs qui ont mis en évidence plusieurs lacunes dans les installations nucléaires, notamment, dans le cadre d'une étude menée sur la prévention du terrorisme nucléaire. En effet, certains spécialistes américains avaient remarqué la vulnérabilité des salles de contrôle, des turbines et des enceintes de confinement. Après les événements du 11 septembre, les pays industrialisés ont réalisé que les sites nucléaires pourraient devenir des cibles potentielles et que la protection de ces derniers deviendrait un impératif pour lequel tous les scénarios possibles devraient être envisagés. Une étude réalisée pour la direction générale de la Recherche de l'Union européenne par Wise-Paris soulignait qu'un accident majeur touchant les piscines de refroidissement de La Hague pourrait entraîner, du fait de l'échauffement des matériaux et de la rupture des gaines entourant des combustibles, un relâchement allant à 100% du Césium 137 contenu, soit une catastrophe de l'ordre de plus de 66 fois celle de Tchernobyl (Le Monde, 16-17 septembre 2001).

2.2.3. L'utilisation d'une arme nucléaire

Les armes de destruction massive peuvent provoquer des dégâts considérables. En effet, une seule arme nucléaire pourrait facilement tuer plus de 100 000 personnes dans une

zone donnée, auquel s'ensuivrait des dommages économiques, une panique généralisée, etc. Selon certains spécialistes, les terroristes de ce siècle nouveau auraient pour but la destruction du plus grand nombre de personnes, et pour atteindre ces objectifs ils se seraient dotés de spécialistes formés en la confection d'armes chimiques et biologiques et auraient développé des réseaux d'achat de matières dangereuses. En 1990, des agents d'Al-Qaeda ont essayé d'acheter de l'uranium hautement enrichi en Afrique, Europe et en Russie. Les matières fissiles disponibles à travers le monde, c'est-à-dire la matière nécessaire pour provoquer une réaction en chaîne de fission et donc de radiation, seraient d'environ 3 000 tonnes d'uranium hautement enrichi et de plutonium dans le monde (Labbé, 2003). Deux problématiques essentielles sont soulevées face à ces matières dangereuses hautement répandues, premièrement la sûreté autour des réacteurs de recherche est plus médiocre que celle des centrales nucléaires et la Russie possède une quantité non-répertoriée de plutonium militaire et d'uranium hautement enrichi qui n'est pas parfaitement sécurisée. Face au problème spécifique que pose la Russie, des accords signés entre 1991 et 1993 entre les É.U. et la Russie prévoyaient l'élimination d'uranium enrichi et de matières nucléaires d'usage militaire dont seulement une faible part des stocks ont été rendus inutilisables pour des armes à ce jour. Cependant, pour les stocks restants, les experts se montrent craintifs vis-à-vis des conditions de démantèlement de certains centres qui se font dans des conditions de sûreté inférieures aux normes occidentales.

2.2.4. La 'bombe sale'

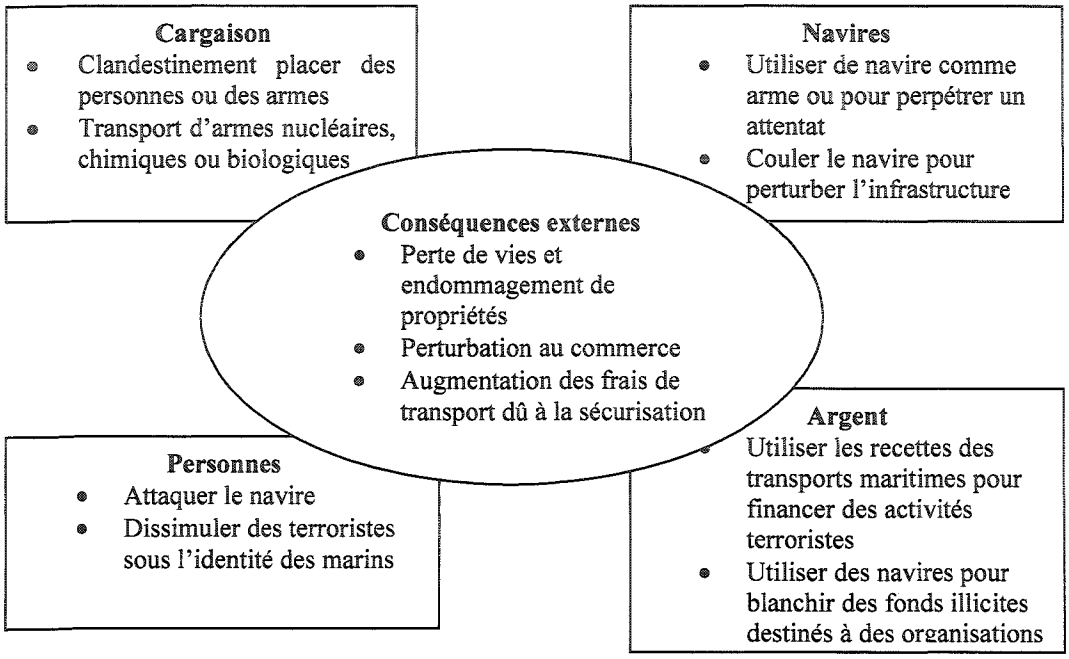
L'arme radiologique est une arme de destruction massive facile à produire qui a un effet psychologique dévastateur sur la population. À la base, cette arme contient des substances radioactives auxquelles on ajoute un explosif conventionnel pour en déclencher la dispersion. Ces matières peuvent être volées soit de centres nucléaires, de centres médicaux ou de sites industriels. En cas d'explosion, les personnes les plus

proches seront tuées, le désordre s'ensuivra et la décontamination sera difficile et onéreuse.

À la lumière de ces différentes menaces, un élément clé dans une stratégie de gestion du risque en matière d'actes terroristes nucléaires serait de sécuriser les entrepôts d'armes nucléaires en Russie et d'éliminer complètement le commerce illégal de matières radioactives. Puisqu'un des moyens par lequel les matières nucléaires se déplacent se fait par le trafic de conteneurs, il devient important pour les ports et les opérateurs de se doter de technologies leur permettant de détecter le transport illégal de matière radioactive. C'est ainsi qu'à Portsmouth et à Dover aux É.U., de l'équipement de détection et d'imagerie radioactive ont été installés et les douanes se sont dotés de 4 000 pagettes pouvant capter l'émission d'ondes de radiation nucléaire et n'ont pas hésité de se munir de systèmes de détection gamma et rayon-X (Seeking Safe Harbor, 2002). Pour que les solutions adoptées soient efficaces, il faut s'assurer d'avoir de l'équipement approprié pour les matières radioactives et les taux d'échec d'inspection doivent se conformer aux critères mis de l'avant en matière de sûreté, car un seul échec de détection pourrait engendrer des catastrophes. Lorsque l'on comprend que 25% de tous les conteneurs manipulés passent par les 5 ports les plus achalandés, la détection de substances nucléaires illégales dans ces superports revêt une importance non-négligeable. Présentement, il n'existe aucune technologie qui puisse parfaitement à elle seule détecter les matières radioactives avec une précision parfaite, c'est pourquoi pour aborder l'inspection de conteneur par une structure de défense par couches (layered defense) (Stanford Study Group, 2003). Ce sujet de la gestion du risque par une solution de sûreté par couches, sera abordé dans la prochaine section.

2.2.5. Facteurs de risque

En résumé, voici présenté sous forme de graphique les facteurs de risques découlant des transports maritimes :



Adapté du rapport de l'OCDE, 2003

Figure 2.1. : Typologie des risques en matière de sûreté portuaire

Facteurs de risque: la cargaison

Depuis longtemps, les autorités douanières mènent un combat d'arrière-garde contre l'utilisation abusive des conteneurs par les trafiquants de drogue, les mafiosi et les contrebandiers. En effet, entre 1996-1998, les autorités américaines ont fait 950 saisies de drogues totalisant 223 502 kilos qui ont été trouvées à bord de navires marchands d'armement, dissimulées dans des conteneurs (OCDE, 2003). Outre cet aspect, les conteneurs sont aussi la cible des tentatives de voleurs décidés à s'approprier rapidement et facilement des cargaisons de grande valeur. Les pertes dues au vol sont estimées entre 30 et 50 milliards de dollars par an et la plupart de ces vols touchent des camions (OCDE, 2003). Toutefois, les ports maritimes et les zones de rassemblement de conteneurs sont aussi exposés au vol de cargaisons conteneurisées car les voleurs bénéficient souvent de complicités internes parmi le personnel travaillant dans les ports ou le secteur des transports. Ainsi, grâce à ces complicités les voleurs peuvent identifier

et cibler les conteneurs transportant des marchandises de grande valeur. Par ailleurs, un autre risque identifiable demeure celui du transport de cargaisons de matières dangereuses. En effet, plusieurs cas de conteneurs mal étiquetés par des chargeurs sans scrupules cherchant à éviter les contraintes de coûts et des délais relatifs aux importations de substances de matières dangereuses, et la négligence possible de transporteurs qui dissimulent la nature véritable de ce type de cargaison, met en évidence certaines failles de la sûreté portuaire.

Facteurs de risque: les navires

Chaque année, des cargos, des navires à passagers et des bateaux de pêche sont attaqués par des pirates en quête de profit qui s'emparent de la cargaison pour la vendre et/ou rançonnent l'équipage. Alors que dans la plupart des cas, les attaques et les vols sont perpétrés sur des navires à l'ancre ou dans les ports, un nombre appréciable d'entre eux sont le fait de gangs de pirates relativement organisés et lourdement armés qui agissent en haute mer (OCDE, 2003). Le 'Piracy Reporting Centre' (centre de notification des actes de pirateries) de la Chambre de commerce internationale a enregistré pour la période 1999-2001 un nombre record d'attaques contre pratiquement tous les types de navires. La plupart de ces attaques concernaient plusieurs zones géographiques parmi lesquelles, le détroit de Malacca, les eaux indonésiennes et malaises, les côtes du Bangladesh et de l'Inde, la mer Rouge/la Corne de l'Afrique et la côte ouest de l'Afrique (OCDE, 2003). La piraterie peut être une activité très lucrative en raison du grand nombre de navires qui transportent des sommes importantes pour payer les taxes portuaires et les salaires de l'équipage. Cependant, parfois les pirates s'emparent de la totalité du navire et vendent la cargaison avec un bénéfice considérable (jusqu'à 1 000 000 $ dans le cas d'un pétrolier) (OCDE, 2003). En outre, un navire détourné peut devenir une source régulière de revenus par l'insouciance de chargeurs qui ne vérifieront pas forcément les papiers du navire et passeront des contrats dans le cadre de

transactions commerciales normales. Mais ensuite, le navire est dérouté, la cargaison vendue et le cycle recommence dans un autre port.

Facteurs de risque : les personnes

Les matelots sont souvent la cible d'acte de pirateries et/ou souffrent indirectement d'attentats visant les navires. Toutefois, l'un des risques que l'on craint à cause des droits de déplacements relativement généreux offerts aux marins grâce à l'octroi de visas de non immigrants, est que ceux-ci soient en fait des complices ou des membres de groupes terroristes. Malheureusement, il a été découvert qu'il est relativement facile d'acheter au marché noir des documents falsifiés ou contrefaits. Enfin, les navires exploités ou affrétés par des terroristes peuvent également faire entrer des agents dans des pays où il serait difficile de pénétrer par d'autres voies. Bien souvent, les agences de renseignements ont constaté, avec inquiétude, que des navires marchands avaient illégalement débarqué des membres d'équipage et/ou des passagers pendant qu'ils étaient à quai (OCDE, 2003).

Facteurs de risque : soutien financier/logistique

Il est de notoriété publique que des groupes terroristes peuvent exploiter des navires ou des flottes entières pour se procurer des fonds et soutenir leurs opérations logistiques. De plus le transport maritime peut également permettre de blanchir des fonds illicites (graphiques 2.1). Le cas des activités commerciales d'un groupe en particulier est très bien documenté.

2.3. La sûreté par couche

Depuis le 11 septembre des investissements substantiels ont été apportés afin d'étudier les procédures analytiques qui permettraient de définir le risque en ce qui à trait à la sûreté. Les outils qui seront utilisés seront la portée, la caractérisation des installations en terme de dangers et conséquences, l'identification et les caractéristiques des menaces, l'analyse des vulnérabilités, les contre-mesures, et le rapport et la communication qui s'ensuit. Pratiquement toutes les procédures analytiques peuvent se résumer en trois étapes qui sont de déterminer les dangers des matières présentes et calculer les conséquences d'une brèche dans l'un des conteneurs, puis énumérer l'ensemble des acteurs avec les capacités pour causer cette brèche et enfin évaluer comment les mécanismes en place peuvent empêcher une telle menace (Emerson, Nadeau, 2003).

La méthode conventionnelle pour créer un système de sûreté efficace est d'installer des obstacles à plusieurs niveaux, à l'exemple de couches, qui devront être franchis avant d'atteindre les installations les plus critiques. Afin d'intercepter et de neutraliser une menace, il faut pouvoir la détecter grâce à des caméras et des senseurs, créer un délai par des clôtures et des barrières fermées qui repousseront les intrus, y répondre en formant du personnel préparé pour répondre à des cas d'urgence, et enfin répondre adéquatement à la nature de la menace et en neutraliser son impact.

Les ports étant des installations ouvertes et exposées à la côte, ils ont été conçus pour promouvoir le flux du commerce et sont donc régis aux É.U. par une combinaison d'intervenants au niveau fédéral, étatique et des membres du gouvernement local du port. Tout comme la garde côtière canadienne a le mandat de protéger les eaux territoriales et les ports du pays, il en va de même aux É.U. avec la garde côtière américaine qui doit protéger quatre zones bien distinctes soit les ports étrangers, les eaux internationales (offshore zone), les côtes, et les quais. Ce concept de couches est encore ici repris pour être adapté aux ports, dans le but ultime de protéger efficacement les infrastructures en place.

1ère couche- les ports étrangers

Depuis le 11 septembre, la manière d'aborder la sûreté a changé pour devenir des mesures de prévention dès le port d'embarcation étranger lors du chargement de la marchandise dans les conteneurs. Ainsi, puisque cette marchandise doit aboutir aux É.U., des ententes ont été conclues entre le Département des Douanes afin que ces agents puissent dès les ports étrangers, inspecter la marchandise douteuse avant qu'elle n'atteigne sa destination. Ces ententes de partenariat ont été facilitées grâce à l'OMI (International Maritime Organisation), division des Nations Unies, qui a entériné auprès des 162 pays membres, des mesures de sûreté maritime et de prévention de la pollution. Ainsi, par la mise sur pied du code ISPS, des standards internationaux ont été développés pour les ports, les facilités et la sûreté des navires pour gérer les risques inhérents à ce domaine et faciliter les échanges entre gouvernements, compagnies, facilités et navires. Ce code impose aux nations de publier les niveaux de sûreté en vigueur et d'en transmettre l'information aux navires et aux ports. Afin d'établir un standard commun, trois niveaux de sûreté décrivent le risque associé aux menaces en cours contre un bateau ou une facilité portuaire ; le niveau 1 requiert une sûreté minimale qui doit être en vigueur en tout temps, le niveau 2 correspond à un risque plus élevé et le 3ième niveau est déclenché lorsqu'un incident est probable ou imminent. Par ailleurs, régulièrement une étude des vulnérabilités doit être entrepris pour décrire les menaces, et les failles des équipements et des infrastructures afin de s'assurer de satisfaire en tout temps aux exigences de sûreté. De plus, si un gouvernement le juge nécessaire, un navire étranger peut être empêcher de pénétrer les eaux d'un pays ou d'une côte si celui-ci considère qu'il y a suffisamment de raisons pour croire que celui-ci n'est pas conforme aux règlements.

2ième couche- zone des eaux internationales (offshore zone)

Cette zone correspond aux eaux à l'intérieur des 200 miles de la zone exclusive économique (EEZ) mais au-delà de 12 miles des eaux territoriales. Dans cette zone les navires doivent signaler leur intention de pénétrer au port, 96 hr à l'avance. Cette notice

doit identifier clairement la nature de sa cargaison et offrir des informations détaillées sur la provenance du navire et de son équipage. À nouveau, si le navire présente des anomalies, la garde côtière américain a l'autorité d'embarquer sur celui-ci et de le fouiller avant qu'il n'obtienne la permission d'amarrer. Pour améliorer la précision de l'information sur les navires en mer et les membres de l'équipage, la garde côtière cherche à se doter d'équipements de Systèmes d'Identification Automatique (AIS) qui permettraient d'obtenir de l'information plus précise et pertinente.

3ième couche- zone côtière

Dépendamment de la cargaison du navire, de l'infrastructure et de l'environnement du port, à l'intérieur de la zone de 12 miles des eaux portuaires, certains navires se verront escorter par la garde côtière pour empêcher que ces navires soient utilisés comme des armes de destruction massive, c'est-à-dire que ceux-ci soient pris en otage et bifurqués de leur trajectoire pour foncer dans des installations dangereuses tel une installation chimique à même le voisinage du port. Ainsi, afin d'éviter le pire, depuis le 11 septembre, les eaux entourant les ports américains ont été strictement réglementées, et ne permettent pas l'accès à tout type de navire et la surveillance s'est accrue.

4ième couche- zone portuaire

Bien que l'aspect sûreté des ports est couvert par l'OMI, le gouvernement américain s'est doté de lois requérant des évaluations sur la vulnérabilité des ports (Port Vulnerability Assessments, PVA). Ces évaluations seront effectuées sur les ports à haut risque et devra faire état des facilités disponibles sur les lieux afin de diminuer le risque inhérent à des attaques terroristes. Ces évaluations seront entreprises de façon systématique et régulière, et leurs résultats seront étudiés pour déterminer quels sont les ports les plus à risque et où les mesures de sûreté sont insuffisantes. Dans le respect de ses engagements en matière de sûreté maritime, le gouvernement américain a mis de l'avant des programmes d'aide et d'amélioration de la sûreté dont le montant disponible à chaque année est de 75 M$ (Emerson, Nadeau, 2003) et des comités d'étude

rassemblant des intervenants de différents milieux pour se pencher sur les questions de l'heure.

2.4. Les solutions de sûreté

Nous examinons de plus près deux autres types de solutions, soit les systèmes de suivi (section 2.3.0) et les systèmes d'inspection des cargos (section 2.3.2).
L'agence des douanes et de la protection de la frontière (Customs and Border Protection, CBP), branche du département de sûreté nationale (Department of Homeland Security, DHS), a pour mission d'assurer que les marchandises et les personnes entrantes et sortantes des É.U. respectent les lois et régulations américaines. De plus, le CBP a la responsabilité de contrôler la frontière contre les intrus, l'entrée de terroristes, la drogue et la contrebande. Pour ce faire, une inspection physique du cargo, de la marchandise et des personnes est essentielle.

2.4.1. Les systèmes de suivi (ACS, ACE et AMS)

Ce qui est devenu d'une grande importance est le grand nombre de cargos entrant dans le pays à chaque jour. Tel que M. Henry Bonner, commissaire du CBP le décrivait récemment: 'Because of the sheer volume of sea conteneur traffic and the opportunities it presents for terrorists, conteneurized shipping is uniquely vulnerable to terrorist attack. Many national security experts believe that a terrorist attack using a conteneur as a weapon or as means to smuggle a terrorist weapon, possibly a weapon of mass destruction, is likely. These experts have pointed out that if terrorists use a conteneur to conceal a weapon of mass destruction and detonate it on arrival at a port, the impact on global trade and the global economy would be immediate and potentially devastating- the economies of all nations could be adversely affected.'

'Given this vulnerable system, we realized the need to develop and implement a program that would enable us to better secure conteneurized shipping- the most important means of global commerce- against the terrorist threat. That program which Customs proposed in January 2002, is the Conteneur Security Initiative (CSI).'[1]

Les douanes américaines utilisent des techniques de gestion de risque à plusieurs couches leur permettant de cibler des conteneurs à des fins d'inspection. Le système utilisé pour suivre, contrôler et intercepter les marchandises importées aux É.U., est le ACS (Automated Commercial System) qui sera remplacé par un nouveau système permettant de traiter les échanges et de suivre le mouvement des marchandises, le ACE (Automated Commercial Environment). L'AMS est un autre progiciel qui transmet l'information sur le contenu des conteneurs entrant au pays et qui permet aux douaniers d'effectuer des inspections plus ciblées. Cependant, les informations transmises par les agences d'intelligence tel que le CIA sont tout aussi importantes, mais plus souvent qu'autrement, les décisions d'inspection sont basées largement sur les expériences acquises à travers les années par une démarche empirique d'observations et de tendances (Lewis, 2003). C'est ainsi, par exemple, qu'au port de New York et New Jersey, les douaniers ont vu tant de tuiles provenant du Brésil qu'ils peuvent reconnaître facilement une cargaison ayant été trafiquée. Par ailleurs, si un conteneur de 40 000 lbs de café est déclaré, il sera inspecté car le poids typique d'un conteneur de café est de l'ordre de 60 000 lbs. Par expérience aussi, on sait que sous les rayons-X, la densité des bananes est la même que celle de la cocaïne dont on aurait modifiée la forme et la couleur afin de leur donner l'apparence de bananes (Seeking Safe Harbour, 2002). Bien que l'inspection manuelle soit une méthode amplement utilisée, les douanes ont développé des outils de prises de décision pour déterminer les cargaisons à très haut risque, tel des cargaisons de drogues. Le système ATS (Automated Targeting System) utilise les déclarations de cargaisons provenant du système ACS, et par un système de critères pondérés, une note est attribuée et un profile est crée lorsque l'évaluation recèle une note trop grande.

Ainsi dans le but de détecter les anomalies auprès du cargo, de nouvelles technologies sont mises au point afin d'assurer au maximum la marchandise circulant dans les conteneurs. L'une de celle-ci permet l'inspection d'équipement de manière non-intrusive (Non-Intrusive Inspection, NII) basée sur les technologies de basse énergie rayon-X ou de radiation gamma afin de voir à travers les conteneurs, et d'identifier toute possibilité de contrebande. L'efficacité de cette méthode d'examen permettra à l'agence des douanes et de la protection de la frontière de se concentrer sur les personnes qui contreviennent aux lois et donc d'améliorer leurs méthodes de détection. En plaçant ces systèmes aux ports d'entrée (Ports of Entry, POE), cela permettra de créer une barrière efficace le long de la frontière, ce qui forcera les contrebandiers à prendre de plus grands risques. La figure 2.2 présente les différentes étapes nécessaires pour cibler un conteneur potentiellement problématique :

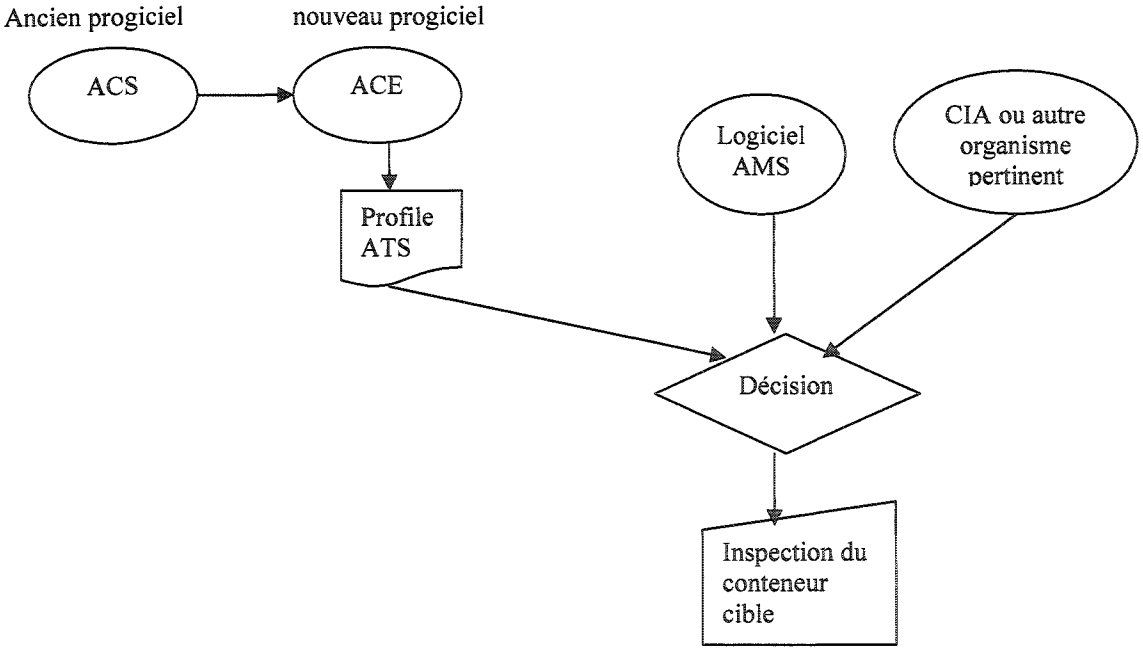


Figure 2.2.: Processus pour cibler un conteneur

2.4.2. Système d'Inspection Cargo et des Véhicules (VACIS)

Dans l'objectif de combattre la contrebande et la drogue, le Système d'Inspection Cargo et des Véhicules (Vehicule and Cargo Inspection System, VACIS) répond aux exigences établies en matière d'inspection. En effet, grâce à cette nouvelle technologie, l'efficacité et l'efficience des mises en application sont améliorées. La qualité, la quantité et la portée des activités des agents de la douane sont multipliées et la quantité d'inspections par jour est appelée à augmenter de l'ordre de 615% (Investment Review Board, High Technology Sub-Group – Immaging and Re-locatable Inspection System; USCS; 29 January 1999; page 8).

Le système d'inspection cargo et des véhicules (VACIS) est une famille de systèmes d'imagerie gamma développée par SAIC, Inc., qui offre des capacités non-intrusives de détection au CBP et de limiter la contrebande aux É.U. Le CBP planifie de déployer quatre configurations VACIS :

- une version semi-permanente conçue pour l'inspection de véhicules motorisés et de conteneurs cargo aux points d'entrée (VACIS II)
- une version portable pour les camions conçue pour l'inspection de véhicules motorisés et de conteneurs cargo (Mobile VACIS)
- une version fixe conçue spécialement pour l'inspection de wagons de chemin de fer (Rail VACIS)
- une version palette (Palette VACIS) conçue pour l'inspection d'items à l'intérieur de palettes, de boîtes ou de caisses.

Chaque configuration utilise un détecteur d'iodure de sodium. Le cargo est placé entre la source et le détecteur. En émettant la radiation gamma, celle-ci pénètre le cargo et traverse les matériaux différemment selon la densité des objets contenus. Les images sont transmises en temps réel à l'inspecteur des douanes qui, grâce à son expérience,

évalue la densité, la localisation et la forme des objets afin de détecter toute contrebande possible, tel la drogue, les armes ou tout item illégal importé.

VACIS incorpore une source de radiation gamma à faible énergie dans un enclos fermé avec une source de Césium-137 (^{137}Cs) ou de Cobalt-60 (^{60}Co) avec une activité entre 0.5 et 2.0 curies. Chaque configuration VACIS utilise une quantité différente de matériel source basée principalement sur la vitesse à laquelle le cargo à être scanné passe à travers les radiations gamma. Plus le niveau de curie est élevé, plus le cargo peut passer rapidement à travers le scanner. De plus, le fait d'augmenter le degré de curies permet une meilleure pénétration de la radiation. Par ailleurs, la source ^{137}Cs a une durée de vie de 15 ans tandis que le ^{60}Co a une durée de vie de 5 ans (U.S. Customs and Border Protection, 2004).

Basé sur les caractéristiques de source de radiation mentionnées, le VACIS II emploiera 1.0 curie de ^{137}Cs parce qu'il est principalement utilisé pour scanner des camions à vitesse lente et des conteneurs intermodaux dont l'épaisseur de métal est mince. Le Rail VACIS en contrepartie, sera utilisé pour scanner des wagons de train dont la vitesse est de 0.5 à 5.0 miles par heure et qui sont fait de métal plus épais. Ainsi, le VACIS Rail emploiera une source de 2.0 curie de source ^{137}Cs. Le Mobile VACIS a essentiellement une source de radiation intermédiaire lui permettant de scanner le cargo de camions, conteneurs intermodaux et certains wagons, à une vitesse qui ne sera pas aussi contrôlée et lente que le VACIS II mais pas aussi variable et rapide que le Rail VACIS. C'est pourquoi le Mobile VACIS emploiera 1.0 curie de ^{137}Cs. Le cargo qui est normalement scanner par des palettes VACIS, souvent contient une marchandise de fruits et de légumes riche en eau. Il a été démontré que la source de Césium n'est pas suffisamment consistante et fut remplacée par 0.5 curie de Cobalt (la forme la plus minime des 4 variantes de VACIS). La table 2.1, introduit le nombre de curies utilisés pour chaque variante :

Table 2.1: Configuration des différents types de VACIS

Configuration VACIS	Source Isotope	Source d'Activité (curie)
VACIS II	Cesium-137	1.0
	Cobalt-60	0.75
Mobile VACIS	Cesium-137	1.0
	Cobalt-60	0.75
Rail VACIS	Cesium-137	2.0
	Cobalt-60	1.0
Palette VACIS	Cesium-137	0.5
	Cobalt-60	0.25

(*Source*: SAIC Safety & Security Products; 2004)

Les zones d'exclusion sécuritaires pour la radiation ont été déterminées grâce à des mesures qui ont été prises par un physicien certifié dans la santé.
Dans les prochaines sections qui suivent, les différentes variantes sont présentées avec leurs caractéristiques fonctionnelles.

VACIS II

VACIS II consiste en deux rails de 90 pieds qui sont placés en parallèle à 30 pieds de distance. Sur le premier rail, se trouve la source de radiation (1.0 curie de ^{137}Cs ou 0.75 curie de ^{60}Co) et sur le rail opposé une tour de 21 pieds est placée contenant le détecteur d'iodure de sodium. Durant l'opération, le véhicule motorisé se stationne entre les deux rails et le conducteur sort du véhicule et est escorté dans une aire d'attente sécuritaire. La source de radiation et la tour de détection se mettent à bouger de manière synchronisée le long des rails, pendant que la séquence de détection débute par l'opérateur du VACIS II. Les rayons gamma sont émis par la source qui passe à travers le véhicule et sont récupérés par la tour de détection. L'image scannée est analysée par l'opérateur de la station VACIS II et affichée sur l'écran afin d'identifier les cargos de densités anormales qui seraient une indication d'une contrebande suspecte. Ces images

sont stockées dans des bases de données et peuvent servir à incriminer tout individu impliqué dans des activités illicites. L'équipement VACIS II requiert deux 120 VCA, 20A et un circuit de 60 Hz.

VACIS II incorpore deux sources radioactives, communément appelées source primaire et secondaire, qui sont physiquement alignées afin que l'obturateur secondaire soit aligné avec l'obturateur primaire. Chaque obturateur peut, par lui-même, bloquer la source de radiation et les deux observateurs sont redondants pour une meilleure sûreté. Durant l'opération, l'obturateur primaire est ouvert et demeure ainsi, tandis que le deuxième obturateur est ouvert pour scanner et sera par la suite fermé lorsque l'opération sera terminée. La vitesse du scanner VACIS II est de 1 pied par seconde et une moyenne d'inspection de 2 à 3 minutes par véhicule. Il est possible de scanner des objets de 8.5 pieds de large et de 72 pieds de largeur, avec une hauteur maximale de 14 pieds. Les parties externes de VACIS II sont construites d'acier, résistantes à la pluie, à l'humidité et à des vents modérés. Ce système peut opérer dans des températures allant de 0 à 120^0 F. Dans les régions présentant des variations de température très grandes, l'installation complète de VACIS II peut être localisée dans un bâtiment.

Afin de respecter les exigences de sûreté, chaque VACIS devra être installé dans une zone de 110 pieds x 65 pieds indépendante et doit comporter plusieurs éléments permettant de prévenir les accidents. Ceux-ci consistent en des lumières clignotantes, une alarme audible indiquant lorsque la radiation est émise, des interrupteurs et des absorbeurs de chocs pour empêcher le wagon de trop avancer, et des boutons d'arrêt d'urgence. Le deuxième obturateur ferme automatiquement lorsque la source ou la tour de détection atteint la fin de son parcours. L'opérateur peut également fermer l'obturateur manuellement de sa station. Ces obturateurs primaires et secondaires sont conçus afin qu'en cas de panne électrique, ils se ferment automatiquement (U.S. Customs and Border Protection, 2004).

Mobile VACIS

Mobile VACIS est similaire à VACIS II à l'exception que celui-ci est installé sur le plateau d'un camion. La source de radiation (semblable à celle du VACIS II) est localisée sur un bras mécanique éloigné du camion, et le détecteur d'iodure de sodium sur une tour installée sur le camion. Le Mobile VACIS possède un obturateur et le système fonctionne sur une prise électrique interne, requiert deux 120 VCA, 20 A, 60 Hz qui sont alimentés par un générateur interne au camion et dont les batteries sont rechargeables. La station de l'opérateur est localisée à l'intérieur du camion du Mobile VACIS. Afin de remplir les exigences de sûreté, chaque Mobile VACIS devra être installé dans une zone de 50 pieds x 50 pieds et à une hauteur de 17 pieds. Pour des raisons d'entreposage, une zone de 26 pieds de long par 8 pieds de largeur est requise, de même qu'un plafond haut d'au moins 10 pieds 4 pouces.

Mobile VACIS est capable de scanner une rangée à la fois de conteneurs cargo de même que des tracteurs à des vitesses de 88 pouces par seconde (5 mile par heure). Le système est équipé avec des lumières pour lui permettre d'opérer de nuit et dans toutes conditions météorologiques. Mobile VACIS peut scanner des véhicules motorisés et des conteneurs cargos en utilisant deux modes opérationnels : scanner fixe et scanner en mouvement. Lorsque l'équipement est en mode scanner fixe, le Mobile VACIS stationne en un endroit pendant que le véhicule motorisé à être scanner passe sous le bras mécanique entre la source de radiation et le détecteur et s'arrête au commencement de la cargaison. L'équipement VACIS est par la suite allumé, et le conducteur du véhicule avance le véhicule jusqu'à ce qu'il soit entièrement passé à travers le scanner. Une fois le processus terminé, le scanner est éteint.

Lorsqu'il s'agit de scanner en mouvement, le Mobile VACIS est positionné afin que le véhicule motorisé ou le cargo à être scanner soit aligné sous le bras mécanique, entre la source de radiation et le détecteur. Le Mobile VACIS est ensuite conduit près du

véhicule ou du conteneur cargo à être scanné, tandis que l'équipement VACIS est opérationnel. Lorsque le Mobile VACIS atteint la fin du véhicule ou du conteneur cargo se faisant scanner, l'équipement scanner est éteint. Dans les deux modes d'opération, les images scanner sont envoyées sur un écran localisé à l'intérieur du camion où se trouve l'opérateur. Celui-ci visualise les images pour en identifier des anomalies qui devraient faire l'objet d'une évaluation plus poussée. Ces images sont stockées dans des bases de données et peuvent servir à incriminer tout individu impliqué dans des activités illicites. Dans les régions présentant des variations de température très grandes, l'installation complète de Mobile VACIS peut être localisée dans un bâtiment.

Afin de respecter les exigences de sûreté, plusieurs éléments permettant de prévenir les accidents ont été rajoutés. Ceux-ci consistent en des lumières clignotantes, une alarme audible indiquant lorsque la radiation est émise, des interrupteurs et des absorbeurs de chocs pour empêcher le wagon de trop avancer, et des boutons d'arrêt d'urgence. L'obturateur ferme automatiquement lorsque la source ou la tour de détection atteint la fin de son parcours. L'opérateur peut également fermer l'obturateur manuellement de sa station. Cet obturateur est conçu afin qu'en cas de panne électrique, il se ferme automatiquement (U.S. Customs and Border Protection, 2004).

Rail VACIS

La source de radiation du Rail VACIS (2.0 curies de ^{137}Cs ou de 1.0 curie de ^{60}Co) est localisée dans un cabinet sur le côté des rails, et le détecteur d'iodure de sodium est installé sur une tour de 32 pieds du côté opposé de la source de radiation. Les installations comportent des senseurs de vitesse qui sont utilisés afin de s'assurer de la bonne vitesse de passage des wagons. Lorsque le train approche, une lumière du Rail VACIS est activée d'un côté des rails et un détecteur de l'autre côté détecte le faisceau lumineux. En passant, les wagons brisent le faisceau lumineux et l'équipement du Rail VACIS utilise cette information pour identifier chaque wagon faisant l'objet de la

détection en cours. Afin d'aider les opérateurs VACIS à identifier quel wagon se fait scanner, un lecteur radio fréquence est utilisé pour lire le code d'identification placé sur le côté des wagons.

Le système inclut une caméra vidéo afin d'enregistrer chaque wagon se faisant scanner, de même qu'une caméra TV en circuit fermé pour la sûreté et la surveillance. La station de l'opérateur qui abrite le système de contrôle et les postes des opérateurs, peut être localisée dans un bâtiment fixe, ou un véhicule mobile, dépendamment des exigences du site. L'équipement Rail VACIS fonctionne sur une prise électrique interne, requiert deux 120 VCA, 20 A et 60 Hz. L'endroit idéal pour installer l'équipement dépend du site, cependant il requiert une zone de 20 pieds x 50 pieds (U.S. Customs and Border Protection, 2004).

Palette VACIS

Chaque Palette VACIS contient 8 composantes majeures: un centre de commande, un mécanisme pour soulever, une étagère pour la source, une étagère pour le détecteur, le cabinet, le contrôleur logique programmable, le panneau d'électricité, le convoyeur et le senseur. Le centre de commande est placé dans une position qui lui permet d'avoir une bonne visibilité de l'équipement Palette VACIS. Dans le centre de commande se trouvera l'opérateur, un ordinateur personnel, des télévisions moniteurs et un système de control. Le mécanisme de lift contient 25 gallons d'huile de pétrole 32 AW(fluide hydraulique). La présence du fluide hydraulique peut nécessiter qu'un enclos soit construit autour ce qui permettra d'éviter des renversements (Programmatic Environmental Assessment for Gamma Imaging Inspection Systems, U.S. Customs and Border Protection, 2004). De plus, une source de puissance non-interrompue est installée dans l'éventualité d'une panne d'électricité. Un générateur de gazoline peut également être utilisé comme source de puissance en cas d'urgence.

Afin de respecter les exigences de sûreté, plusieurs éléments permettant de prévenir les blessures ont été rajoutés. Ceux-ci consistent en des lumières clignotantes, une alarme audible indiquant lorsque la radiation est émise, des interrupteurs et des absorbeurs de chocs pour empêcher le wagon de trop avancer, et des boutons d'arrêt d'urgence. L'obturateur ferme automatiquement lorsque la source ou la tour de détection atteint la fin de son parcours. L'opérateur peut également fermer l'obturateur manuellement de sa station. Cet obturateur est conçu afin qu'en cas de panne électrique, il se ferme automatiquement (U.S. Customs and Border Protection, 2004).

2.4.3. L'exemple du Port de Montréal

Dans la lignée des mesures de sûreté qui ont été adoptées par les autorités gouvernementales et institutionnelles suite aux événements du 11 septembre, le Port de Montréal s'est assuré de renforcer ses installations en matière de sûreté afin d'en interdire l'accès au grand publique, et de contrôler l'environnement de façon stricte. Tel que l'indiquait le directeur de la sûreté et de la prévention des incendies au Port de Montréal, 'Le contrôle de l'accès au port est une étape importante de l'identification des personnes qui s'y trouvent et améliorer en général la sûreté en vue de se rendre conforme aux normes du code ISPS.'

C'est ainsi que dans la foulée des nouvelles exigences de sûreté, de septembre 2001 à décembre 2002, des gardes de sûreté ont été ajoutés de même que de l'équipement d'inspection de bagages. Un périmètre a été tracé autour du terminal de passagers et l'accès publique a été défendu afin de limiter le nombre d'entrées au port et en restreindre l'accès aux individus travaillant dans le port en leur fournissant des cartes d'identité. Par ailleurs, le territoire du port est surveillé en tout temps par 50 caméras vidéo qui transmettent les images recueillies en temps réel au centre de contrôle du quai qui est ouvert 24 heures par jour, 7 jour sur 7. Les coordonnateurs du centre peuvent visualiser ces images sur des écrans plasma de 42 pouces et des écrans de projection de 84 pouces. L'angle des caméras peut être dirigé à distance pou obtenir une plus grande

précision des images captées. Chaque image reçue au centre de contrôle sera transmise automatiquement à la garde côtière canadienne et enregistrée. Dans certains cas, ces images peuvent être transférées à la police pour des fins de vérifications criminelles. Les améliorations effectuées ont coûté 1.2 M$ (66th annual joint conference canadian shipowners association, 2003).

Une patrouille contrôle les va-et-vient à raison de 24 heures par jour, 7 jours sur 7 et des gardes de sûreté ont été placés à chaque terminal en plus des postes de contrôle et de la surveillance caméra. Chaque périmètre et chaque terminal sont clôturés et bien éclairés, et les bâtiments se sont dotés de systèmes d'alarme et de sûreté. En ce qui a trait au personnel de sûreté, le port engage une force de sûreté permanente à qui elle assigne la patrouille à raison de 3 fois le matin et l'après-midi, et 2 fois dans la nuit et en fin de semaine. De plus, afin d'avoir sur place des experts en matières dangereuses, 7 inspecteurs en prévention des incendies font partie de l'équipe de sûreté. Au moins un coordonnateur est en fonction pour couvrir 24 heures, 7 jours sur 7. Bien que la garde côtière canadienne et Transport Canada assurent la sûreté sur les eaux, les forces de l'ordre tel la police et la RCMP ont accès en tout temps au port de Montréal.

Depuis le début de l'année 2004, le port de Montréal s'est assuré d'être conforme aux règlements de l'OMI concernant les nouveaux codes de sûreté maritime le ISPS tandis que la garde côtière canadienne s'est équipée de système d'identification automatique (AIS). Par ailleurs, sur les prémices, la douane canadienne inspecte 25 conteneurs par jour, grâce notamment à des machines rayons gamma et des chiens spécialisés dans le domaine. Depuis janvier 2003, les douanes canadiennes au port de Montréal ont 2 camions équipés avec des scanners VACIS qui permettront d'augmenter le nombre de conteneurs inspectés à 50 par jour. Ces conteneurs peuvent être inspectés aléatoirement ou choisis en utilisant une technologie sophistiquée. Il est à noter que par rapport au problème des passagers clandestins, chaque fois que l'on en retrouve sur un des navires,

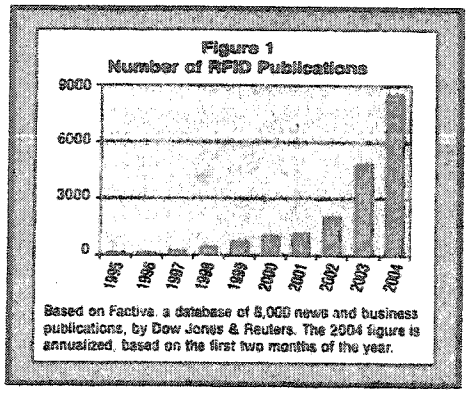
une caution de 15 000 $ doit être déboursée de la part de la compagnie de transport maritime.

Ainsi depuis 1998 et dans la foulée du mouvement de sécurisation de la chaîne d'approvisionnement, le Port de Montréal a investi 4.2 M$ en des mises à jour pour des infrastructures de sûreté, tandis que 3 M$ ont servi pour de nouveaux réseaux de fibres optiques, la création du centre de contrôle et l'installation de 40 caméras vidéo (66th annual joint conference canadian shipowners association, 2003).

Il est à souligner que Transport Canada définit les lignes directrices pour l'élaboration des plans de sûreté des navires auxquels les propriétaires et les exploitants des compagnies maritimes doivent se conformer. Ces plans visent la protection du navire, de ses marchandises, de son équipage et de ses passagers ainsi que du système de transport en général. Le mandat est d'inspecter les navires canadiens et étrangers amerrissant aux ports canadiens, d'inspecter les installations portuaires et d'émettre des certificats à l'intention des ports.

2.5. La technologie RFID

RFID fait la une des journaux mais est-ce un phénomène de mode ou retrouve-t-on de vrais bénéfices comparés aux technologies existantes? Pour tous les acteurs de la chaîne d'approvisionnement, est-ce une évolution ou une révolution dans la manière de conduire leur processus? Beaucoup d'articles sont écrits sur cette technologie promettant de révolutionner la chaîne d'approvisionnement et de modifier radicalement notre quotidien. Cependant ce qui surprend le lecteur est l'engouement récent porté sur une technologie déjà vieille de 40 ans. Tel que le montre la figure 2.3, le nombre de publications sur le sujet s'accroît de façon exponentielle et un bien bel avenir lui est encore réservé.



Tiré de Sheffi, 2004

Figure 2.3 : Nombre de publications RFID

Les débuts de la technologie RFID datent depuis la seconde guerre mondiale. Au départ, la Grande-Bretagne utilisait les ondes radio dans le but de détecter en soirée, les navires ennemis. Les applications militaires ont été nombreuses, car les pertes humaines représentaient des préoccupations plus importantes que les coûts d'utiliser cette technologie. Au fil des ans, ces applications se sont tournées vers le secteur privé pour une utilisation dans des réseaux internes d'entreprise. Dans les années 80, Compaq fit usage des étiquettes intelligentes pour suivre leurs composantes à travers leur processus de production. Aujourd'hui, grâce à l'évolution de la technologie et des applications, ces réseaux se sont tournés vers l'externe afin de permettre une observation plus poussée des flux de marchandises. Par exemple, lors de la guerre du Golf, on utilisa des étiquettes intelligentes afin de fournir des informations sur le contenu des conteneurs. Dans chaque cas, les avantages d'utilisation de cette technologie ont permis de compenser les coûts potentiels de perte, du vol ou de matériel déplacé. Plusieurs ont utilisé les applications du RFID sans pour autant savoir qu'il s'agissait de la technologie RFID. En effet, les cartes bancaires munies de puces intelligentes sont un autre exemple d'applications, mais la liste d'utilisations possible ne se limite pas à ces quelques exemples.

Ce changement s'est appuyé sur trois phases distinctes permettant le suivi des stocks, l'optimisation des inventaires, et la traçabilité de la marchandise :

- La définition d'un nouveau standard EPC global cohérent avec les standards déjà existant (GTIN, normes EAN/UCC)
- La standardisation des protocoles de communication
- Une lecture plus fiable et une diminution des coûts

2.5.1. La technologie RFID et les technologies de l'AIDC

La technologie du RIFD fait partie des technologies de l'identification automatique et de la capture de données (AIDC) permettant l'identification et la collecte de données directes dans un ordinateur. La raison d'être de ces technologies est d'une part l'identification et la collecte de données, et d'autre part la diminution du temps de traitement de ces données. Grâce à l'AIDC, il est possible de connaître le contenu d'une boîte sans l'ouvrir, parler à une machine pour ouvrir une porte ou lire une étiquette codée avec des barres pour en obtenir la description du contenu d'une cargaison.

Ces technologies de l'AIDC se sont répandues rapidement à travers le monde car elles permettent de réduire les erreurs, le temps de processus et de livraison ce qui par conséquent permet de faire des économies importantes tout en utilisant des outils efficaces et conviviaux. Il existe six technologies faisant partie de la famille des AIDC, l'une sur laquelle je vais prêter plus attention, le RFID. Les codes barres, la reconnaissance de caractères, les bandes magnétiques et la reconnaissance de la parole sont tous une partie intégrante de cette famille, mais possèdent des caractéristiques et des applications qui les rendent plus intéressantes vis-à-vis de telle solution plutôt qu'une autre. Cependant, le point commun entre elles est l'élimination d'erreurs dans la collecte de données qui se faisait auparavant manuellement et la réduction dans le temps de traitement. La figure 2.4 présente les différentes technologies de l'AIDC.

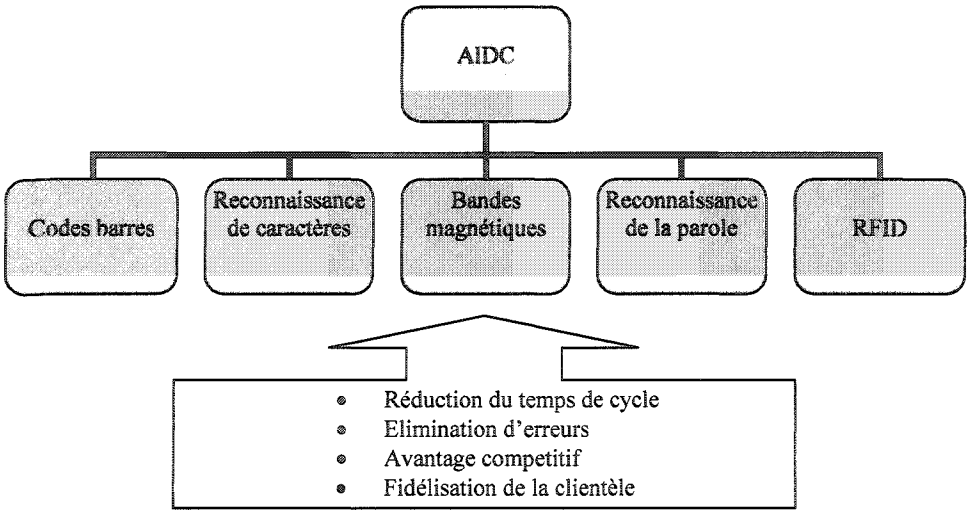


Figure 2.4 : Les technologies de l'AIDC

De plus en plus les entreprises sont appelées à réduire leur temps de cycle, éliminer les erreurs afin de réduire leurs coûts, obtenir un avantage compétitif face à leurs concurrents et fidéliser leur clientèle. C'est pourquoi les entreprises se sont massivement tournées vers l'AIDC afin d'obtenir plus de détails, optimiser leur processus et devenir plus compétitives. 'L'AIDC propose ainsi une façon rapide, efficace et économique pour entrer et collecter des données'' (Al-Bizri, 2004).

Les codes barres

Tel que nous l'avons mentionné plus haut, le code barres est une des sous-familles des technologies de l'AIDC (Identification Automatique et Collection de Données). Elle fit son apparition dans les années 70 grâce aux UPC (Code Universel de Produits) qui ont été d'abord utilisés dans les supermarchés. Grâce à l'impression mobile, sans-fil, le code barre est devenue une technologie répandue pour la collecte et le traitement de données.

Le code barres est une étiquette de barres et d'espaces de longueur et de largeur variable qui représentent une chaîne de 10 à 20 caractères numériques ou alphanumériques

permettant d'automatiser certaines opérations de lecture. Ces caractères servent de référence ou de pointeur à une base de données distante possédant l'information sur le prix, la date de fabrication, le numéro de lot et toute autre information pertinente sur le produit. Présent partout, ce code est devenu un standard global. La figure 2.5 présente un exemple de code barres linéaire :

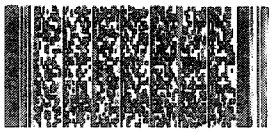
(UQAM, 1996)

Figure 2.5 Le code barres

Les entreprises nécessitent le traitement d'un volume plus élevé d'informations ce qui a crée un nouveau type de code barres, les codes barres bidimensionnels ou codes 2D. Les codes 2D ont les mêmes caractéristiques que les codes linéaires en terme de fiabilité, simplicité et rapidité de lecture, mais la capacité d'encodage a été augmentée jusqu'à 27 000 caractères dans un espace très réduit. En effet, 10 caractères peuvent être encodés sur 4 mm^2 alors qu'il faut une étiquette de format A4 pour contenir les 50 caractères d'un code barres linéaire (Chambre Régionale de Commerce et d'Industrie Champagne-Ardenne, 2003). On peut donc insérer un fichier complet de données à un coût faible.
Il existe deux types de code barres 2D: les codes empilés et les codes matriciels.

Codes empilés

Ces codes se caractérisent par un empilement de plusieurs lignes à codage linéaire, et stockent les informations en hauteur et en largeur. La figure 2.6 présente un exemple de code empilé.



(Zebra Technologies Corporation, 2003)

Figure 2.6 Le code empilé

Codes matriciels

L'encodage est différent, et les informations sont mémorisées dans des polygones à l'intérieur d'une grille fixe à raison de 3 750 caractères. La figure 2.7 présente un exemple de code matriciel.

(The technical knowledge base for you, 2004)

Figure 2.7 Le code matriciel

Le code barre est rapide, facile d'utilisation et précis dans sa collecte de données. Une fois les données collectées à travers un lecteur, les articles peuvent être retracés plus efficacement et rapidement qu'avec un traitement manuel et l'échange de données est instantané et en temps-réel. Le code barres est précis, en effet, des études montrent que le taux d'erreur de lecture est de l'ordre de une erreur par million de caractères versus une erreur par 300 caractères pour l'entrée manuelle de données (Zebra Technologies Corporation, 2003). Ainsi, il permet aux entreprises de suivre l'information sur leurs articles et activités au fur et à mesure qu'elle se produit, et donc permet une prise de décision sur des données concrètes, valables et précises.

Selon Frost & Sullivan, le marché mondial des équipements de codes à barres (principalement codes linéaires) devrait actuellement se situer autour de 8,5 G$.

2.5.2. L'historique de la technologie du RFID

Dans un pas vers une évolution dans l'utilisation répandue du code UPC (code universel de produits) et des codes barres pour l'identification automatique (Auto-ID), de nouvelles technologies se développent qui vont permettre d'étendre les capacités des entreprises à capter l'information adéquate à propos de la localisation et des statuts de marchandises à travers la chaîne de valeur. Dans plusieurs industries, les entreprises étudient le potentiel des EPC (code électronique de produit) et des technologies de l'identification radio fréquence (RFID)- les technologies Auto-ID du futur – afin de créer de nouveaux bénéfices pour leurs opérations et leurs activités à l'égard de la chaîne de valeur.

Des codes barres aux cartes à puce, les technologies de l'identification automatique (Auto-ID) sont maintenant utilisées dans presque toutes les industries. Leurs applications varient de l'accès et des systèmes de sûreté de dépistage d'items, à la gestion d'inventaire et de facilité de paiement aux détaillants. L'Auto-ID est à l'origine du développement des lecteurs de codes barres (1952), codes barres (1966) et le code universel de produit, UPC (1973). En effet, l'ubiquité des UPC et des codes barres a fait un impact dramatique sur l'industrie des biens de consommation. Celles-ci ont eu un effet de levier dans l'industrie de l'épicerie qui a su réaliser des économies de l'ordre de 2.76% à 2.89%. En 1997, l'industrie estima que ces économies approximèrent 17 milliards $ U.S. annuels sur les différentes parties de la chaîne de valeur (Kambil & Brooks 2002).

Aujourd'hui le développement des technologies de l'Auto-ID, en particulier le code produit électronique (EPC) et les étiquettes radio fréquence (RFID), offriront des économies substantielles. Ces technologies améliorent l'identification des objets, et permettent une plus grande précision des données. Cette information de plus grande qualité permettra aux entreprises de suivre la progression de la marchandise à travers la

chaîne de valeur, et leur permettra de répondre de façon plus appropriée aux changements des besoins du marché.

En gravant physiquement des objets avec une puce intelligente permettant de communiquer avec un lecteur, les technologies de l'Auto-ID pourraient révolutionner la façon de fabriquer, de vendre et d'acheter des produits. Ce faisant, les technologies de l'Auto-ID offriront des milliards de dollars en économies tout en permettant de pourvoir aux besoins du consommateur efficacement et rapidement (Kambil & Brooks 2002).

2.5.3. Le fonctionnement de la technologie RFID

Le RFID comporte 2 parties. Le transpondeur, également appelé étiquette RF, qui contient l'information du système. La deuxième composante est le lecteur qui récolte l'information du transpondeur.

Le transpondeur

Lorsque le transpondeur reçoit un signal du lecteur, il émet une réponse en envoyant des données. Ces données seront des informations spécifiques sur l'item mais peuvent aussi êtres des données sur une situation particulière.
Il existe deux types de transpondeur : les transpondeurs passifs et actifs. Les étiquettes passives ne possèdent pas leur propre source de puissance et donc dérive leur puissance par le champ électro-magnétique généré par le lecteur. Elles ont une durée de vie infinie. Les étiquettes actives, à l'opposé, possèdent une source de puissance ce qui explique leur durée de vie beaucoup plus courte de l'ordre de 10 ans mais une portée plus grande, un taux de transmission plus élevé à haute fréquence et une meilleure immunité contre le bruit. Les étiquettes peuvent être de type ROM, WROM ou RAM ou une combinaison des trois en fonction de leur utilité. Leur taille varie en fonction de leur utilisation etpeut être de la grosseur d'une mine de crayon jusqu'à des dimensions plus grandes pour

identifier des conteneurs. Les étiquettes ayant une mémoire de type ROM sont préprogrammées et on ne peut par la suite écrire par-dessus. Les étiquettes de type WROM ou RAM sont, en revanche, programmables et des informations peuvent être stockées dans leur mémoire.

Le lecteur RFID

Le lecteur est responsable pour activer l'étiquette en lui envoyant un signal. Lorsque l'étiquette transmet une réponse au lecteur, celui-ci doit pouvoir lire, décoder et emmagasiner les données afin de pouvoir les transmettre par la suite. Lorsque plusieurs étiquettes sont dans une zone, un algorithme détermine si les signaux émis par les étiquettes sont des signaux répétitifs et si oui, obligent celles-ci d'arrêter de transmettre autrement. Le lecteur peut également utiliser une autre méthode qui lui permet de lire chaque étiquette une à une jusqu'à ce qu'elles soient toutes lues.

Leur portée varie grandement, et va de la proximité de l'objet à 20m de distance de celui-ci et dépend surtout de leur besoin d'énergie et des fréquences qu'elles utilisent. Plus la portée est grande, plus elle requiert d'énergie et plus complexe est leur circuit.

Il n'existe pas de standard pour les fréquences mais plutôt une plage de fréquences communément utilisées. Les étiquettes fonctionnant dans la zone de 13,56 MHz et des fréquences inférieures à 135kHz sont passives et en lecture. Elles ont l'avantage d'avoir un signal peu absorbable par l'eau ou les tissus humains et ainsi sont idéales dans les environnements ou il pourrait y avoir un blocage par ceux-ci entre le lecteur et l'étiquette. En contre-partie, ces étiquettes demeurent plus sensibles aux composantes métalliques dans la zone d'opération. Dans la zone de 400-100 MHz UHF et 2 450 MHz, les étiquettes fonctionnent dans une plage de fréquence UHF et micro-onde, et sont donc moins sensibles au bruit électrique. L'antenne directionnelle est plus petite ce qui permet de la pointer dans une direction particulière. Le lecteur est donc d'avantage immunisé contre une interférence possible de d'autres lecteurs et sources de

transmission. Finalement, un système d'information pour sauvegarder l'information est également nécessaire.

Les caractéristiques techniques des étiquettes passives et actives du RFID

Dans la littérature les étiquettes actives et passives sont souvent confondues, cependant ce sont des technologies totalement différentes. Bien qu'elles utilisent toutes les deux une énergie radio fréquence pour communiquer entre l'étiquette et le lecteur, la façon que l'énergie leurs sont fournies est foncièrement différente. L'étiquette active RFID emploie une source interne de puissance, une batterie intégrée, pour l'alimenter. L'étiquette passive, en revanche, reçoit son énergie par le lecteur qui émet un rayonnement. En effet, les étiquettes passives soit réfléchissent l'énergie du lecteur ou en absorbe une petite quantité du signal du lecteur afin de générer sa réponse. Dans l'un ou l'autre des cas, les opérations RFID passives nécessitent un signal puissant du lecteur, et la puissance du signal que l'étiquette retournera, sera en contrepartie faible. Par opposition, les étiquettes actives peuvent capter un signal faible de la part du lecteur et grâce à leurs sources internes, elles sont en mesure de générer un signal fort qui sera reçu par le lecteur. Par conséquent, une étiquette active émet constamment un signal, quel soit dans le champs d'un lecteur ou non. Dans le tableau 2.2, les différences entre les étiquettes passives et actives sont énumérées,

Tableau 2.2 Les différences techniques entre les étiquettes passives et actives RFID

	RFID Active	RFID Passive
Source de puissance	Interne à l'étiquette	Énergie transférée par le lecteur par les ondes RF
Besoin de piles	Oui	Non
Disponibilité de la puissance de l'étiquette	Toujours en fonction	Seulement dans le champ de vision du lecteur
Puissance du signal du lecteur à l'étiquette	Faible	Fort (doit pouvoir alimenter l'étiquette)
Puissance du signal du lecteur au lecteur	Fort	Faible

Tiré de Hallberg, Nilsson, 2002

Les fonctionnalités des étiquettes passives et actives RFID

Avant de choisir une technologie pour une application quelconque, il est important de bien saisir les différences entre chaque.

Portée de la communication : Pour les étiquettes passives RFID, la portée de la communication est limitée par deux facteurs, la nécessité pour celles-ci de recevoir un signal puissant afin d'être activé et la quantité d'énergie disponible à l'étiquette pour répondre au lecteur, ce qui limite la portée de l'étiquette au lecteur à moins de 3 mètres. En revanche, les étiquettes passives n'ont aucune restriction de puissance et peuvent communiquer à des distances de 100 mètres ou plus.

Collecte de plusieurs étiquettes : À cause de la portée limitée des étiquettes passives RFID, la collecte de plusieurs étiquettes à la fois est difficile et souvent peu fiable. Un scénario typique serait celui d'une palette comportant plusieurs items étiquetés. L'identification de plusieurs étiquettes en même temps requiert une communication importante entre le lecteur et celles-ci. Chaque interaction individuelle prend un temps considérable et la possibilité d'interférences augmente avec le nombre d'étiquettes, ce

qui prolonge la durée de la communication. Ainsi, par exemple, pour identifier 20 étiquettes il faut plus de 3 secondes ce qui ramène la durée de la vitesse à moins de 3 miles par heure. Par opposition, des milliers d'étiquettes actives RFID, grâce à leur portée de 100 mètres ou plus, peuvent être lues simultanément par un seul lecteur. La vitesse de lecture est de l'ordre de 100 miles par heure et les données recueillies sont précises et fiables.

Capacité du senseur : Dans diverses applications, il est souvent nécessaire de surveiller de près la température de l'environnement, l'humidité, les chocs, la sécurité et la falsification. Puisque les étiquettes passives ne sont alimentées que dans le champ de vision d'un lecteur, celles-ci ne sont pas adéquates pour une surveillance continue d'un senseur. Étant en tout temps fonctionnelles, les étiquettes actives sont souvent employées pour mesurer la température et le statut des sceaux placés sur les conteneurs. Par ailleurs, les étiquettes actives enregistrent des informations précises tel l'heure et la date.

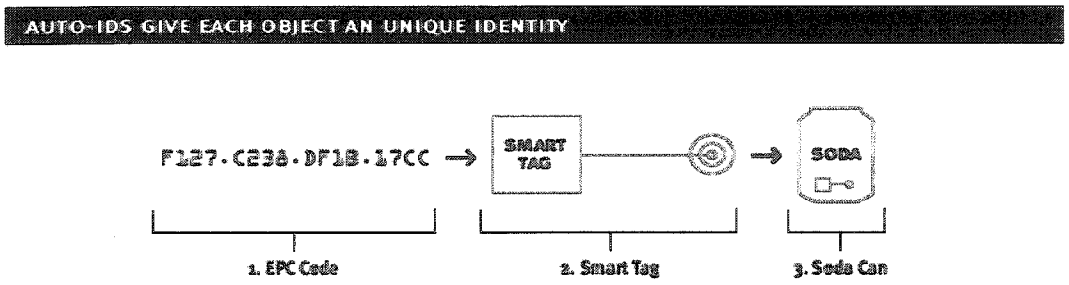
Entreposage des données : L'une ou l'autre des technologies peut emmagasiner des données. Cependant, les étiquettes passives ont une capacité de l'ordre de 128 bytes ou moins, et l'on ne peut les manipuler facilement à cause de leur durée très courte en mode actif. Les étiquettes actives, par opposition, offrent une plus grande flexibilité de manipulation et emmagasinent des données de l'ordre de 128K bytes en mode lecture/écriture.

Bien qu'elles soient différentes, les étiquettes actives et passives se complètes et couvrent des aspects différents de la chaîne d'approvisionnement. Les étiquettes passives sont idéales lorsque le déplacement des items étiquetés est constant et contrôlé, il y a peu de surveillance nécessaire et les données à enregistrer sont minimes. Les étiquettes actives sont préférables lorsque les processus d'affaire sont dynamiques et sans contraintes, la vitesse de lecture est variable, la surveillance est obligatoire et l'écriture de données est essentielle. Une considération importante dans le choix

d'utilisation du RFID est son impact sur les processus d'affaire. En effet, l'objectif est de limiter ces impacts, cependant il est difficile de tous les enrayer. En règle générale, l'utilisation d'étiquettes actives RFID ne demandent pas une réorganisation des processus d'affaire contrairement aux étiquettes passives. Par conséquent, les coûts associés à la ré-ingénierie doivent être pris en compte au même titre que les autres coûts. En conclusion, l'un des avantages majeurs des étiquettes passives est leur coût très bas, c'est pourquoi elles sont souvent employées lorsque les exigences sont minimales et les processus d'affaire sont bien contrôlés.

Le fonctionnement des technologies de l'Auto-ID

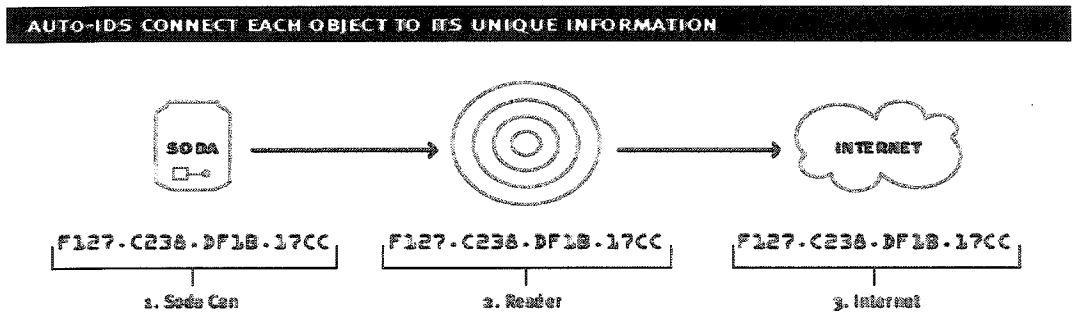
Les objets physiques individuels sont identifiés avec un code électronique de produit (EPC) à 96 bits emmagasinés dans une mémoire à puce, une étiquette intelligente. L'EPC peut identifier de façon unique plusieurs centaines de millions de fabricants et de produits, tout en ayant une capacité pour étiqueter tous les produits à fabriquer dans le futur. Ces étiquettes intelligentes sont attachées ou gravées dans le produit et possèdent une antenne leur permettant de communiquer à travers des ondes Radio Fréquence avec d'autres objets. La figure 2.8 présente l'insertion d'une étiquette intelligente sur un produit pour lui donner une identité propre.



(Schéma tiré de Kambil & Brooks 2002)

Figure 2.8 L'identité unique

Des lecteurs radio-fréquence vont lire le signal émis par les étiquettes et transmettre le contenu de la réponse obtenue vers l'Internet qui emmagasinera dans une base de données l'information produite afin qu'elle soit disponible aux fabricants, détaillants et fournisseurs. La figure 2.9 présente la communication entre l'étiquette intelligente et le lecteur.



(Schéma tiré de Kambil & Brooks 2002)

Figure 2.9 L'information unique

Sur Internet, le code produit EPC fonctionne avec le serveur ONS (object naming device) et le langage PML (Product Markup Language). L'ONS indique à l'ordinateur où trouver l'information sur n'importe quel objet ayant un code EPC, et localise les données pour chacun des objets. Le PML, en contrepartie, est un nouveau langage permettant la description d'objets qui dicte au navigateur comment afficher les pages web.

Une des technologies Auto-ID souvent utilisée est le RFID, l'identification radio-fréquence. Cette technologie utilise soit des étiquettes radio fréquence passives bon marché ou des étiquettes actives dispendieuses.

Ainsi, les technologies de l'Auto-ID fusionnent des bits et des atomes pour créer un réseau d'objets qui communiquent en temps réel et de manière intelligente avec des gens et des entreprises. (Kambil & Brooks 2002)

2.5.4. Comparaison entre code barres et la technologie RFID

La technologie RFID est une des technologies de l'AIDC ayant la plus forte croissance. Les experts de l'industrie considèrent la technologie RFID comme un complément au code barres plutôt qu'un remplacement car en effet, dans plusieurs cas tel que le suivi des palettes, des cartons et des caisses dans un entrepôt, les deux technologies sont employées. Les avantages principaux du RFID versus le code barres sont qu'il n'est pas nécessaire d'être dans la ligne de mire de l'objet étiqueté et que l'on peut changer les données sur l'étiquette qui sont en mode lecture/écriture. Bien que la vente d'étiquettes intelligentes est appelée à croître à plusieurs milliards en 2007, le RFID ne remplacera pas totalement le code barres. Selon Zebra Technologies (2004), la croissance du RFID sera alimentée par l'émergence de la technologie des étiquettes intelligentes dans la chaîne d'approvisionnement logistique qui combine les coûts bas des codes barres avec les fonctionnalités du RFID. De nouvelles imprimantes permettent maintenant d'imprimer sur la surface d'étiquettes intelligentes (smart label) tout en encodant de l'information sur une puce RFID insérée dans l'étiquette.

Les étiquettes intelligentes sont des étiquettes dans lesquelles on a incrusté une tag RFID. Ces tags sont disponibles dans trois gammes de fréquences majeurs soit le 13.56 MHz, 860 à 930 MHz et le 2.45 GHz. Ces étiquettes sont appelées intelligentes à cause de la flexibilité offerte par les tags RFID qui peuvent être programmées et/ou mises à jour sans contact ce qui permet de réutiliser l'étiquette. De plus, ce mode lecture/écriture peut se faire à travers divers matériaux, à des vitesses de passage pouvant atteindre 1m/s et les échanges d'information peuvent se faire via Internet. Ainsi, l'étiquette n'est plus statique tel le code barres, mais devient dynamique lorsque munie du tag RFID.

Si l'on étudie les étiquettes passives du RFID, on se rend compte qu'elles n'ont pas plusieurs des limitations des codes barres en ce que, entre autre, l'on obtient une transmission sans fil qui est sans erreur et qui ne nécessite pas de batteries ou un entretien. Le tableau suivant se propose d'étudier de plus près ces caractéristiques du RFID et du code barres qui les distinguent l'une de l'autre.

Tableau 2.3 Le codes barres vs RFID

Paramètres du système	Code barres	Système RFID
Quantité de données (bytes)	1-100	1-100
Densité des données	Basse	Basse
Qualité de lecture machine	Bonne	Bonne
Qualité de lecture humaine	Limité	Impossible
Influence saleté/humidité	Importante	Aucune
Influence d'une couverture partielle	Échec	Aucune
Influence direction et position	Minimale	Aucune
Dégradation	Limité	Aucune
Achat coût/lecture électronique	Bas	Médium
Coûts opération	Bas	Aucun
Contrefaçon	Légère	Impossible
Rapidité lecture	Bas (env. 4s)	Très rapide (env. 0.5s)
Distance maximale entre lecteur/étiquette	0-50 cm	0-5 m

(Adapté de Finkenzeller, 2003, p. 8)

La technologie RFID complémente effectivement le code barres par sa disponibilité sous différents formats, son intégration dans le produit dès le stade de fabrication et la quantité et diversité d'informations qu'elle peut supporter allant de l'information sur le produit à des codes cryptés d'anti-contrefaçon. Également, toute lecture ou reproduction non autorisée peut être interdite.

Les gains les plus importants au niveau de la technologie sont dans l'optimisation de la chaîne logistique où par exemple il sera possible d'éliminer les inventaires physiques ou encore d'alimenter automatiquement les rayons grâce à un signal qui sera émis lorsque le nombre de produits descend en dessous d'un certain seuil.

La technologie du RFID a plusieurs point en commun avec les codes barres, cependant le RFID apporte une plus value en créant un système d'identification sans fil. En effet, dans certains domaines cette technologie pourrait remplacer les codes barres, toutefois elle pourrait jouer un rôle dans un éventail d'applications beaucoup plus larges. Voici pourquoi :

- La technologie plus sophistiquée permet aux étiquettes d'être gravées et lues à distance.
- La lecture n'est pas obligée de se faire dans le champ de vision restreint du lecteur.
- Les étiquettes peuvent être lues à travers des matériaux tels le bois, le plastique et le carton et peuvent inclure des capteurs de température ou de choc mécanique.
- Les étiquettes sont facilement programmables et fonctionnent aisément dans des environnements variés.
- Les étiquettes RFID comportent 96 bits d'information versus seulement 19 bits pour le code barre.
- Les lecteurs peuvent lire plusieurs étiquettes à la fois en captant cette information à distance grâce à des algorithmes anti-collision.
- Une intervention humaine dans le processus de la lecture de l'étiquette n'est pas nécessaire.
- La technologie entraîne une amélioration de la logistique, du traitement des stocks, du suivi, et des garanties et une diminution de la fraude grâce à la possibilité d'éliminer la contrefaçon, le vol et le clonage grâce au cryptage des données.
- La technologie RFID permet la traçabilité de la température permettant d'assurer un suivi des conditions propres à certains produits. (Adapté de Morgenroth, Hales, Fobes 2004)

L'infrastructure Auto-ID est conçue pour pouvoir synchroniser les informations EPC et RFID dans les systèmes ERP tel :

- Le numéro EPC
- La localisation des biens
- Le statut
- L'endroit de la dernière lecture
- Le numéro de l'unité
- Des informations pertinentes au statut d'emballage du produit (i.e. item, item-caisse, caisse-pallette)

Ses données sont par la suite redirigées au système ERP en faisant l'association nécessaire avec l'unité de transport utilisée (Handling units). L'en-tête de l'unité de transport inclus des informations tel son numéro, le poids, le volume et les dimensions. Cependant, l'information qui est envoyé contient toutes les données importantes sur la marchandise et sa provenance à savoir, le numéro du matériel utilisé, la quantité, l'unité de mesure, le numéro de lot, le numéro de l'usine et sa localisation, la catégorie d'inventaire, de même que le numéro de série et les données d'inspection de lot. Ces unités de transport sont alors associées avec les numéros EPC et sont intégrées dans la transaction appropriée pour les processus de commandes tel la production, le transfert, les ventes, la livraison et la réception, l'emballage, et l'inventaire. Dans le but d'être versatile avec les différents systèmes d'ERP, l'infrastructure Auto-ID supporte plusieurs interfaces de communication (http, SOAP, WSDL, SOCKET/TCPIP), de même que les interfaces mobiles tel le PocketPC 2003 et le Mobile Linux. De plus, elle marche avec Windows (XP, 2000, NT), Unix, et Linux, et supporte Oracle, SAP DB, DB2 et le serveur Microsoft SQL.

2.5.5. Coûts, standards et viabilité de l'Auto-ID

Le consortium du centre Auto-ID crée par le MIT et d'autres universités à travers le monde, se penche sur les codes EPC et RFID comme technologies d'avenir des systèmes d'identification automatique qui permettront des économies et génèreront des revenus à travers la chaîne de valeur. Cette nouvelle technologie fait suite aux progrès imminents qui ont été faits depuis plusieurs années face à la traçabilité des marchandises. En utilisant les étiquettes RFID, les entreprises seront capables d'obtenir de l'information en temps réel sur chaque objet, depuis l'usine de production jusqu'à sa fin de vie.
Il existe présentement deux obstacles majeurs dans l'adoption de la technologie de l'Auto-ID : le coût des étiquettes et la création d'un standard unique. Aujourd'hui les étiquettes RFID sont disponibles auprès de plusieurs vendeurs mais demeurent dispendieuses et propriétaires. En effet, pour s'assurer d'une adoption massive le prix des étiquettes doit être au plus de 5 cents tandis qu'à ce jour le coût demeure autour de 40 cents. En contrepartie, les codes barres, beaucoup plus abordables, se vendent 1 cent et les lecteurs se vendent pour aussi peu que 120$. Le centre Auto-ID travaille avec des promoteurs pour rendre la technologie de l'Auto-ID une alternative bon marché aux codes barres en développant des étiquettes RFID de 5 cents ou moins pour de gros volume d'achat. Présentement, les technologies Auto-ID sont incompatibles entre elles ce qui est un obstacle dans l'utilisation massive des lecteurs et des étiquettes. Bien qu'il existe des groupes de vendeurs offrant des produits compatibles, afin d'en assurer le succès, cette technologie devra avoir un standard ouvert, but que s'est donné le consortium Auto-ID.

En résumé, le tableau suivant illustre certains des obstacles à l'implantation du RFID :

Tableau 2.4 Les obstacles à l'implantation du RFID

Les problèmes	Les faits	À résoudre
Prix des étiquettes trop élevé	Pour de gros volumes, les prix demeurent de l'ordre de 0.25- 0.35 $. Pour de petites quantités, les prix sont de 0.50- 0.70 $.	Pour la majorité des produits de consommation, ces prix demeurent trop élevés pour être absorbable dans le coût de l'article.
Problème de performance des étiquettes	10-12 % étiquettes sont inefficaces à leur arrivée, celles qui passent l'inspection sont lisibles à 80- 90%.	À l'extérieur des laboratoires, crainte de la performance des étiquettes qui subissent le transport turbulent dans les camions.
Lois de la physique	Les ondes radio-fréquence ne passent pas facilement à travers le métal ou le liquide.	Des difficultés persistent malgré l'engouement de certains joueurs tel Wal-Mart qui poussent de l'avant cette technologie
Absence de standards	2 organisations de standards, ePC et ISO travaillent sur un standard global. Aucun standard unique n'est disponible pour l'instant.	La plupart des compagnies utilisent le standard ePC de base en espérant que les mises à jour ne seront pas trop onéreuses.
Absence de réseaux	VeriSign a été choisit pour être l'opérateur du directoire de ePC.	Bien que VeriSign ait été choisi, l'industrie n'a pas forcément adopté ce réseau
Vie privée	Le Sénat Californien a passé une loi prohibant aux entreprises et aux librairies l'utilisation du RFID pour identifier une personne. L'information collectée ne peut inclure ce que les clients	Le RFID est déployé presque exclusivement au niveau des caisses et des palettes. Lorsque les items sont taggés, l'étiquette peut être enlevé à travers l'emballage.

	avaient voulu prendre mais se sont désistés, ce qu'ils portent, ou ce que contient leur porte-monnaie.	
Pas de ROI pour les fournisseurs (L'exemple de Wal-Mart)	Plusieurs fournisseurs cherchent à justifier les coûts d'investissement de 13 à 23 M$ nécessaire pour satisfaire aux exigences de Wal-Mart.	Chaque plan d'affaire est différent dépendamment des compagnies.

(D'après AMR Research, 2004)

L'engouement pour le RFID a principalement été mené par Wal-Mart, détaillant géant américain, qui par son pouvoir d'achat énorme dicte le comment et le quand de l'adoption de cette technologie par les fournisseurs. Tout comme les débuts des codes barres, Wal-Mart mène le bal en forçant la conformité de ses fournisseurs à la technologie RFID pour janvier 2005, et profite de ce que la majorité des entreprises possèdent déjà leur propre système d'information (ERP), gestion de chaîne d'approvisionnement (SCM) et système de logistique et de distribution qui leur permettront de capter et de traiter l'information. La standardisation des protocoles et du contenu de même que la conformité du matériel permettra une utilisation à grande échelle. De plus, la convergence des réseaux, le perfectionnement de la technologie, le déclin des coûts et l'uniformisation des standards sont tous des éléments à l'avantage de Wal-Mart qui a donné un élan à cette technologie vouée à une adoption précoce.

Pour Wal-Mart et d'autres détaillants, les bénéfices immédiats sont une efficacité accrue et une réduction des erreurs à la réception. Effectivement, il sera possible de vérifier si la marchandise reçue correspond bien aux détails envoyés sur le reçu d'expédition et ainsi diriger la marchandise au bon endroit. Les étagères munies d'un système de détection RFID enverront un signal pour un réapprovisionnement lorsque nécessaire ce qui permettra d'évaluer les tendances auprès des consommateurs et prévoir juste les bonnes quantités d'articles nécessaires. Il ne sera plus nécessaire de chercher dans l'entrepôt une

marchandise perdue, puisqu'elle sera facilement retrouvable et le vol à l'étalage sera grandement réduit. Dans une étude de 'Grocery Manufacturers of America', A.T. Kearney Inc. estime que détaillants et manufacturiers perdent annuellement 2 millions $ pour chaque 1 milliard $ de ventes dû à de mauvaises informations. Ils estiment ainsi que l'élimination de ce problème pourrait faire économiser 10 milliards $ par année.
Ainsi, tel que le souligne RedPrairie (2003), grâce à la transparence de la chaîne d'approvisionnement qu'offre le RFID, fournisseurs et distributeurs vont pouvoir mieux s'ajuster à la demande et les manufacturiers réduiront leur temps mort. Voici les informations clés que Wal-Mart transmettra à ses fournisseurs :

- Réception de la marchandise au centre de distribution
- Départ du centre de distribution
- Réception au magasin
- Départ de l'entrepôt du magasin (arrivée sur les étagères)
- Caisse ou étiquette détruite

Une autre application utile des étiquettes intelligentes est dans la contrefaçon afin d'identifier le vrai produit du faux ce qui permettra de sauver des millions de dollars annuellement. Finalement, Wal-Mart mise sur la réduction de leurs coûts, un meilleur service à la clientèle, une augmentation des profits et de la loyauté de leurs clients.

2.5.6. L'évolution prévue de la technologie RFID

Toute entreprise s'intéresse à gérer ses activités sur la chaîne d'approvisionnement afin de surveiller chaque item, établir des prévisions, et obtenir des indications sur les tendances du marché. Toutefois, grâce à cette technologie, il est possible non seulement de surveiller ces items mais de faire des paiements électroniques, ou faire du marketing interne. Les bénéfices offerts sont l'efficience, la sûreté et le marketing. Tel que cela s'est produit avec l'introduction des codes barres, l'industrie des produits de

consommation CPG (consumer packaged goods) et des distributeurs mènent le développement et l'adoption des technologies de l'Auto-ID. C'est d'ailleurs dans le secteur de la grande distribution tel Wal-Mart et Carrefour en France, que les projets pilotes sont les plus nombreux. Ces acteurs misent sur cette technologie en espérant pouvoir générer des gains rapides grâce à la diminution des ruptures de stock, mais aussi en améliorant l'efficacité de leur chaîne d'approvisionnement et la visibilité de l'inventaire. Dans les années à venir, le marché de la technologie RFID est appelé à croître rapidement car en effet, plusieurs organisations chercheront à intégrer cette technologie afin d'en tirer les bénéfices qu'elle apporte. Des initiatives de la part d'industries telles Wal-Mart et le Département de Défense Américaine aideront la croissance et l'adoption du marché global de RFID de 3 milliards $ d'ici 2007 (Morgenroth, Hales, Fobes 2004).

Voici présenté dans au tableau 2.5, quelques prévisions de vente d'étiquettes intelligentes:

Tableau 2.5 Évolution attendue à l'horizon 2006

	2003	2004	2005	2006
Ventes d'étiquettes (millions d'unités)	500	1200	3 500	15 000
Prix unitaires pour les utilisateurs des plus grands volumes (en $)	0.25	0.15	0.10	0.05
Ventes de lecteurs (en millions d'unités)	0.3	0.6	1	2

(Source AMR Research, 2004)

Bien qu'elle ait été de l'ordre de 8-10% au début des années 2000, on observe une forte croissance de la technologie RFID qui progresse actuellement de 20-30% par an et devrait se maintenir d'ici 2008. Selon la Chambre Régionale de Commerce et

d'Industrie Champagne-Ardenne, les parts de marché mondiales sont réparties entre les USA et le Canada qui représentent un peu moins de 50% du marché, l'Europe qui se situe autour de 35% et le reste par l'Asie-Pacifique. Pour la campagne en Irak, l'armée américaine a voulu tracer tous ses colis et a dépensé 90 millions $ dans cette technologie. Le tableau 2.6 présente les prévisions de déploiement des étiquettes intelligentes de 2004-2008.

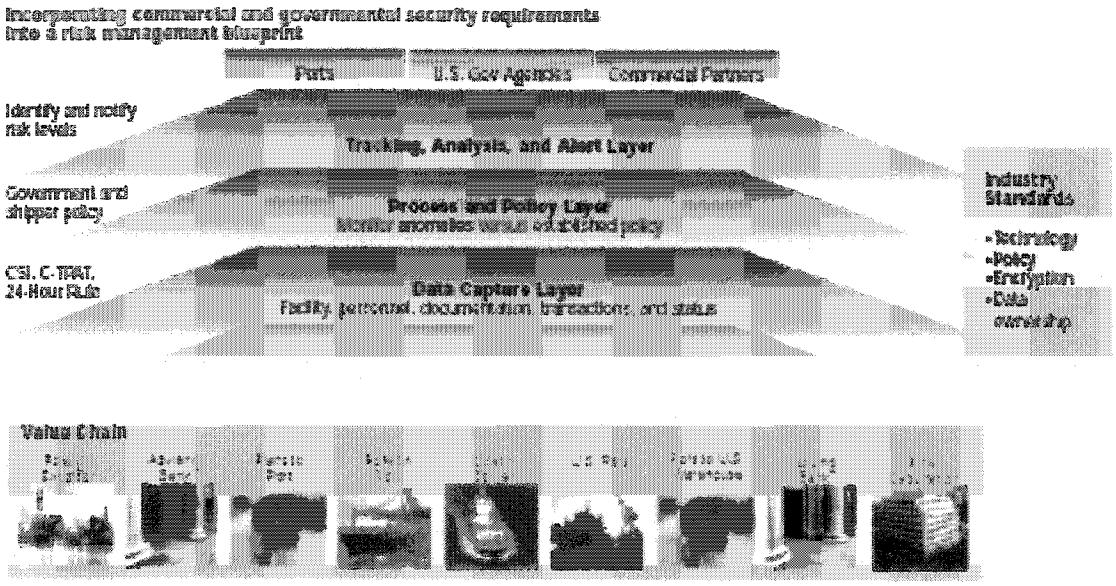
Tableau 2.6 Prévisions de déploiement des étiquettes RFID dans la distribution

	2004	2005	2006	2007	2008
Textile		palette	carton/article		
Alimentaire	palette	palette	carton		article
Électronique	palette	carton/article	article		
Hygiène/Beauté	palette	carton	article		
Pharmacie		carton/article			

(D'après ePC forum, 2002)

Sommaire

À travers ce chapitre, nous avons regardé les différents risques attachés à la sûreté maritime ainsi que les couches qui forment l'approche de base des plans de sûreté mis sur pied par les grands ports. La figure 2.10 présente en résumé les différentes couches qui forment la sûreté maritime et leur mise en applications à tous les niveaux de la chaîne de valeur. Nous observons ainsi que la sûreté doit être un effort concerté entre les ports, les instances gouvernementales et les entreprises car chacun de ces acteurs doit intervenir activement au niveau de la chaîne logistique qui lui est propre pour s'assurer de l'intégrité des biens ayant transité sur son passage.



Tiré de Unisys, 2004

Figure 2.10 Chaîne de valeur de la sûreté portuaire

Par ailleurs, nous avons regardé de près les grandes technologies qui forment le tissu technologique sur lequel se base l'information duquel les décisions en matière de sûreté portuaire émanent. La figure 2.11 récapitule les technologies utilisées et leur imbrication dans le modèle de prise de décision.

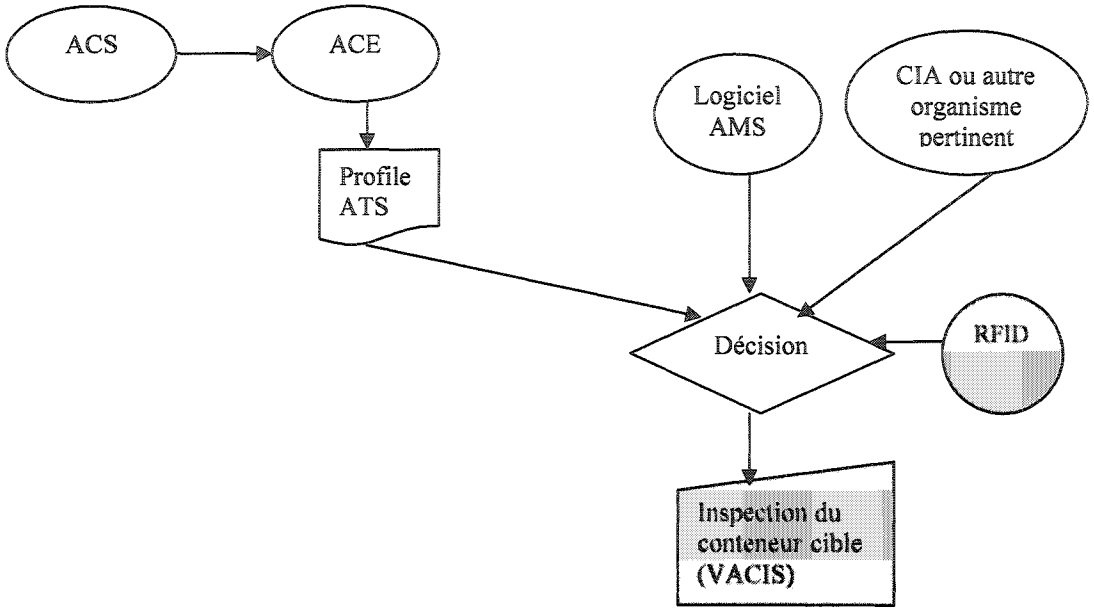


Figure 2.11 Les solutions de sûreté

Toutefois, d'autres technologies sont utilisées et souvent empruntées à la sûreté aéroportuaire. En effet, depuis déjà plusieurs décennies les aéroports et le transport aérien ayant été les premières victimes d'attaques terroristes, les solutions technologiques ont d'abord pris naissance dans ce domaine, ce qui explique bien souvent que leur savoir-faire est appliqué et modifié pour renforcer la sûreté maritime. De fait, des détecteurs d'explosifs sophistiqués sont employés pour valider la présence ou l'absence de ces substances dangereuses, de même que des portiques de détection sont en application dans la sûreté maritime, cependant uniquement dans le cas des bateaux de croisière où la sécurité des passagers ne peut être laisser pour compte. Parmi toutes les mesures de sécurité mises en place par les autorités dans le transport maritime, il est à noter que les bateaux de croisière possèdent les règlements les plus stricts, dans le but de protéger les passagers d'une attaque terroriste d'une quelconque nature. De plus, tel que nous avons vus grâce à la technologie du VACIS, des rayons –X sont utilisés pour la détection de métaux, de matière organique et inorganique afin de déterminer sur un écran toute masse suspecte grâce à une codification de couleur qui assigne une couleur particulière aux explosifs de types organiques et inorganique. L'on fait également usage

de détecteurs manuels d'objets métalliques pour la détection d'armes métalliques de tout genre.

De ce chapitre, nous retenons que plusieurs solutions en matière de sûreté des infrastructures portuaires existent et que la technologie RFID pourrait éventuellement y jouer un rôle important. Le prochain chapitre explore le potentiel de cette technologie à partir des résultats d'une étude menée sur le terrain.

CHAPITRE 3
ÉTUDE SUR LE TERRAIN

3.1 Approche théorique privilégiée

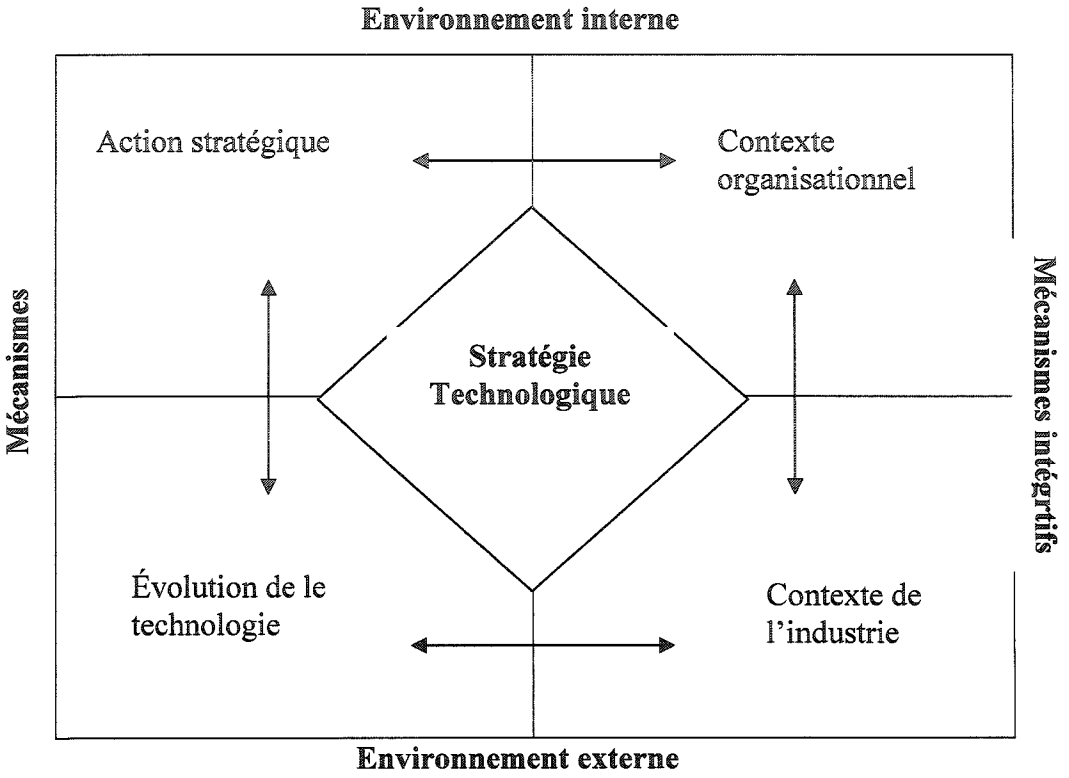
Dans le but de bien comprendre le contexte de la sûreté maritime et portuaire, une recherche des documents relatifs au domaine des enjeux du secteur a été effectuée. Afin de recueillir des données sur le terrain permettant de mieux s'aligner avec la réalité, des entrevues avec des intervenants du secteur privé oeuvrant dans l'offre de solutions intégrées ainsi que des entretiens avec des membres du gouvernement responsables de la mise en application des mesures de sûreté ont été entreprises. Dans le but de bien saisir l'implication de tous ces intervenants dans le tableau global et complexe du secteur maritime, un cadre de recherche qui permet d'analyser la nature du contexte des stratégies en matière de technologie a été utilisé, celui du cadre de Burgelman. En effet, grâce à ce cadre conceptuel, il est possible de saisir les motivations ayant aiguillées l'usage de telle technologie versus une autre, et de comprendre les forces et les faiblesses de chaque entreprise étudiée face à ses compétences fondamentales, actuelles et futures, dans le but de survivre ou de croître dans un marché hautement compétitif. La finalité de ce chapitre est de proposer des pistes d'actions aux entreprises rencontrées dans le cadre de ce mémoire en s'inspirant du modèle de Burgelman, outil méthodologique de recherche qui sera présenté dans les sections suivantes.

Afin de bien saisir l'évolution des entreprises ayant fait l'objet de cette étude, il est primordial d'exposer le modèle d'étude ayant été utilisé et la théorie qui sous-tend ce modèle. La théorie évolutionniste appliquée aux systèmes organisationnels se concentre sur des mécanismes de variation-sélection-rétention pour expliquer des comportements dynamiques sur une période de temps (Campbell 1969; Aldrich 1979; Weick 1979 ; Burgelman 1991 ; Van de Ven and Garud 1989). Celle-ci reconnaît l'importance de

l'histoire, de l'irréversibilité, et de l'inertie pour expliquer le comportement d'organisations mais elle considère aussi les effets des processus d'apprentissage (Burgelman 1986). L'étude de développements technologiques semble compatible avec la structure de cette théorie évolutionniste tel que le souligne certains auteurs (Rosenberg 1982; Kelly et Krantzberg 1978; Abernathy 1978; Clark 1985; Henderson et Clark 1990 ; Burgelman 1994). Dans la recherche d'une meilleure compréhension des facteurs qui façonnent l'élaboration d'une stratégie technologique, nous examinerons brièvement chacun des éléments du cadre conceptuel présenté à la figure 3.1.

3.1.1. Évolution de la technologie

La stratégie technologique est bien sûr directement influencée par l'évolution des technologies. Dans la littérature, cette évolution de la technologie a été abordée de différentes manières: 1) l'étude des trajectoires en forme de courbe en S (Twiss 1980 ; Dosi 1982) ; 2) les interactions entre le développement de produits et de processus technologiques (Abernathy 1978) ; 3) l'émergence de nouvelles technologies (Foster 1986) ; 4) les conséquences de nouvelles technologies qui accroîssent les compétences ou les détruisent (Astley 1985 ; Abernathy, Clark, et Kantrow 1983 ; Tushman et Anderson 1986) ; 5) le renouvellement de l'innovation technologique (Abernathy, Clark, et Kantrow 1983) ; ou 6) les déterminants organisationnels du changement technologique (Tushman et Rosenkopf 1992). À travers cette étude, nous tenterons d'évaluer l'évolution de la technologie RFID et de son impact au sein des deux entreprises ayant été rencontrées.



Tiré de *Burgelman, Maidique, Wheelwright, 1996*

Figure 3.1: Le cadre méthodologique de Burgelman

3.1.2. Le contexte industriel

Les aspects importants du contexte industriel sont 1) la structure de l'industrie qui est représentée par cinq forces majeures (Porter 1980) modulées de façon importante par la technologie (Porter 1983) et qui détermine les compétences technologiques qui seront la base d'un avantage compétitif (Burgelman 1994); 2) l'appropriation d'une innovation technologique (Teece 1986); 3) les atouts complémentaires nécessaires pour commercialiser une nouvelle technologie (Teece 1986); 4) l'émergence d'un design dominant (Utterback et Abernathy 1975; Abernathy 1978); 5) le retour sur investissements de l'adoption pour des technologies particulières (Arthur 1988; David

1985); 6) l'émergence de standards dans l'industrie (Farrell et Saloner 1987; Metcalfe et Gibbons 1989); ou 7) les aspects du système social du développement de l'industrie (van de Ven et Garud 1989). Ces différents facteurs mentionnés affectent la distribution des profits générés par une innovation technologique et les choix stratégiques des organisations.

3.1.3. L'action stratégique

La stratégie d'une entreprise se bâtit à partir des connaissances acquises par ses succès passés et présents (Burgelman 1991; Donaldson et Lorsch 1983; Weick 1979). Cooper et Schendel (1976) ont remarqué que lorsque des entreprises établies de longue date sont confrontées par la menace de nouvelles technologies radicales, elles ont plutôt tendance à miser sur leur technologie existante plutôt que d'adopter une nouvelle technologie, même si celle en utilisation est vétuste. Par ailleurs ces entreprises, lorsqu'elles font face à des innovations architecturales, ont souvent de la difficulté à adapter les efforts déployés pour le développement de produits (Henderson et Clark 1990). Burgelman (1994) remarqua que les compétences actuelles d'une entreprise peuvent représenter des forces d'inertie qui bloquent l'adaptation au changement. Cependant, les compagnies peuvent privilégier certaines actions stratégiques qui leur permettent de pénétrer dans de nouvelles sphères d'affaires (Penrose 1968; Burgelman 1991).

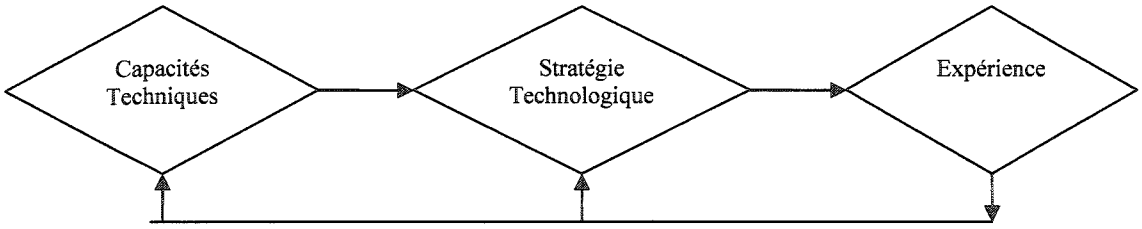
3.1.4. Le contexte organisationnel

Le contexte organisationnel représentes essentiellement les caractéristiques de l'environnement interne d'une organisation: structure, cultures, mécanismes et directives, produits et gammes de produits, représentent quelques caractéristiques organisationnelles. De plus l'habileté pour exploiter des opportunités associées à sa stratégie, l'aptitude à miser sur des opportunités qui émergent et la facilité pour faire face à divers défis (Burgelman et Sayles 1986) affectent la stratégie technologique.

3.1.5. L'application du cadre théorique

À la lumière du cadre théorique de Burgelman, nous nous proposons d'offrir une stratégie technologique qui miserait sur le potentiel de la technologie RFID pour deux entreprises qui offrent des services en matière de sûreté portuaire.

Notons que l'élaboration d'une stratégie technologique n'est pas un procédé statique mais bien un procédé dynamique qui évolue dans le temps, et est directement influencée par les compétences techniques, c'est-à-dire les capacités de l'entreprise et l'expérience. L'expérience qui découle de la stratégie technologique sert de fondement aux capacités techniques qui vont s'ajuster à leur tour et permettre le développement d'une nouvelle stratégie technologique. La figure 3.2 présente l'interaction entre l'apprentissage et la stratégie technologique.



Tiré de Burgelman, Maidique, Wheelwright, 1996

Figure 3.2: Apprentissage et stratégie technologique

Avec le temps, les entreprises développent des capacités techniques qui leur permettent de faire face aux exigences de leur environnement (Selznick, 1957). Associés aux capacités techniques, plusieurs concepts sont soulevés: connaissances organisationnelles (McKelvey et Aldrich, 1983), routines (Nelson et Winter, 1982), pièges de compétences (Levitt et March, 1988), rigidités fondamentales (Leonard-Barton, 1992) et forces inertielles (Burgelman, 1994). À partir de la définition de Selznick et Andrews, Prahalad et Hamel ont apporté une nouvelle définition pour les compétences clés : 'the collective learning in the organization, especially how to coordinate diverse production skills and

integrate multiple streams of technologies'. Selon ces auteurs, une compétence clé devrait pouvoir 1) permettre potentiellement l'accès à une grande variété de marchés différents, 2) contribuer de façon significative à la valeur perçue par le client 3) être difficile à imiter. Ainsi les compétences techniques et les capacités sont des concepts complémentaires.

La substance de la technologie stratégique

L'entreprise doit définir le rôle que la technologie devrait jouer pour se différencier et/ou réduire le coût de ses produits ou services (Porter, 1983, 1985). En effet, la technologie peut être utilisée défensivement pour acquérir un avantage concurrentiel en matière de différentiation ou de coûts, ou offensivement pour créer de nouvelles gammes de produits ou pour développer de nouveaux produits et marchés. Ainsi, les entreprises qui ont du succès sur de longues périodes, ont développé des compétences technologiques et des capacités qui sont distinctes de celles de leurs compétiteurs, et que l'on ne peut facilement répliquer. Ce leadership technologique ne peut être ni facilement acheté, ni être rapidement déployé dans une organisation.

3.2. Approche méthodologique privilégiée

Les étapes sur le terrain permettent d'observer des phénomènes ou des évènements dans leur contexte. Elles aboutissent généralement à des données qualitatives voir à des observations que l'on ne peut ramener forcément à des nombres. Bien que la recherche sur le terrain puisse être utilisée pour obtenir des données quantitatives, typiquement la recherche est qualitative.

La recherche sur le terrain est une méthode pour étudier des évènements qui se produisent dans un endroit spécifique et pendant une période précise et d'examiner de plus près des communications subtiles et des évènements qui ne pourraient autrement être anticipés ou mesurés.

3.2.1. Considérations spéciales pour la recherche sur le terrain

Il y a plusieurs aspects à prendre en considération pour chaque méthode de recherche, et la recherche qualitative de terrain n'est pas une exception. Dans ce domaine, l'on est confronté au rôle que l'on joue comme observateur et de notre relation avec les gens observés. De fait, dans la recherche de terrain, l'observateur peut jouer plusieurs rôles y compris être participant dans ce qu'il cherche à observer. Tel que Marshall et Grossman (1995) le soulignent, 'The researcher may plan a role that entails varying degrees of participantness- that is the degree of actual participation in daily life. At one extreme is the full participant, who goes about ordinary life in a role or set of roles constructed in the setting. At the other extreme is the complete observer, who engages not at all in social interaction and may even shun involvement in the world being studied. And, of course, all possible complementary mixes along the continuum are available to the researcher.' Il existe cependant un cas d'observateur que l'on nomme l'observateur complet, car il observe un processus organisationnel sans pour autant en prendre part. Bien que plus objectif dans ses observations, le chercheur n'aura pas une entière appréciation de ce qui est étudié, par conséquent ces observations seront plutôt transitoires et sommaires. Ultimement, l'observateur doit choisir le rôle qui est convenable pour chaque situation car il n'existe aucune règle précise à suivre si ce n'est de suivre les considérations méthodologiques et éthiques. Dans le cadre de cette étude, nous n'avons fait qu'être un observateur complet, car le but de ce mémoire était d'abord et avant tout une recherche sur le domaine de la sûreté portuaire et par la suite une évaluation de la technologie RFID comme apport possible à ce secteur.

3.2.2. Conduire des recherches sur le terrain

La première phase à entreprendre lorsque l'on entame une étude quelconque, et d'effectuer des recherches sur la littérature pertinente au domaine afin de se faire une idée des observations et des opinions d'autres auteurs. Par la suite, l'on peut vouloir

discuter avec d'autres chercheurs ayant également étudier le même sujet ou tout simplement se familiariser avec le sujet en se créant des liens avec des gens qui pourraient être un apport précieux pour l'étude. C'est d'ailleurs pourquoi, l'on souligne souvent l'importance de forger de bonnes relations dès le départ afin de faciliter le processus de l'étude et d'avoir des résultats qui ne soient pas biaisés.

Pour faire une recherche sur le terrain, il est possible d'être simplement là où trouve l'action et simplement regarder et écouter. Souvent, il est approprié de poser des questions à des gens et d'enregistrer leurs réponses, c'est pourquoi les entrevues sont préférablement menées avec plus de flexibilité. Tel que l'expriment Herbert et Rubin (1995) 'Qualitative interviewing design is flexible, iterative, and continuous, rather than prepared in advance and locked in stone.' Une recherche qualitative sur le terrain peut être essentiellement une conversation dirigée par l'interviewer qui guide l'entrevue afin de parcourir les sujets d'importance. Kvale (1996) fait l'analogie avec l'interviewer et le mineur qui connaît le terrain et doit creuser pour trouver de la matière de valeur et le voyageur qui parcourt, sans trop de connaître l'endroit où il se trouve, et pose des questions aux gens de la place. De fait, les questions en soi ont leur importance et peuvent venir influencer les sujets, c'est l'une des raisons pour laquelle l'interviewer doit être flexible et doit savoir écouter son interlocuteur pour poser les bonnes questions, interpréter les réponses et diriger l'entrevue dans la bonne voie. Il y a donc une part de spontanéité à avoir; le tout n'est pas simplement de préparer des questions d'avance. C'est pourquoi faire de bonnes entrevues est un art qui demande une bonne capacité d'écoute, savoir poser les questions pertinentes et s'intéresser aux autres plutôt que de chercher à être intéressant. Herbert et Rubin renchérissent sur l'importance de savoir diriger une entrevue et mettre l'emphase sur la nécessité de manier l'art de passer d'un sujet à un autre sans pour autant couper court la conversation afin de ne pas laisser paraître un désintéressement de la part de l'interviewer. Ainsi l'interviewer doit démontrer son intérêt en sachant écouter plus que de vouloir parler. Les auteurs Lofland (1995) suggèrent de jouer le rôle 'd'incompétent socialement acceptable' qui veut apprendre tout en ne sachant rien, tel un étudiant; 'A naturalistic investigator, almost by

definition, is one who does not understand. She or he is ignorant and needs to be taught.' Kvale (1996) propose en revanche 7 étapes pour compléter une entrevue, 1) thématiser 2) faire le design du processus d'entrevue 3) passer les entrevues 4) transcrire ses notes 5) analyser les données 6) vérifier la validité et la fiabilité de ce que l'on a trouvé et 7) présenter les résultats.

Dans le cadre de cette étude nous avons pris contact avec divers intervenants dans les secteurs privés, public et académique afin d'obtenir un portrait le plus juste et réaliste possible. Les entrevues, par conséquent, ont été menées avec une grande flexibilité afin de permettre à chaque intervenant d'exprimer son point de vue, toutefois en cherchant à récolter un maximum d'information afin de bâtir le portrait d'un domaine d'activité complexe et sensible de nature.

L'essentiel lors de l'observation est de prendre des notes qui incluront des observations empiriques (les faits) et des interprétations (ce que l'on comprend). Comme le chercheur ne peut tout capter, ses observations représenteront un échantillon et ses notes en seront la base sur lesquelles celles-ci auront été fondées. Certaines observations peuvent être anticipées d'avance, tandis que d'autres seront plus apparentes au fur et à mesure. Finalement, l'observateur se rendra compte qu'il existe une grande quantité d'informations que l'on peut enregistrer et qu'un choix s'impose pour trier le plus pertinent.

3.2.3. Les étapes

Tel qu'il a été mentionné, traditionnellement les auteurs ont développé des théories à partir d'observations de la littérature, du bon sens et de l'expérience. Cependant les liens avec les données sont souvent minces (Perrow, 1986; Pfeffer, 1982) et c'est la relation avec la réalité empirique qui permet le développement d'une théorie, valide, pertinente et que l'on peut tester Glaser et Strauss (1967). Il existe encore beaucoup de confusion

entre les données qualitatives, la logique inductive et la recherche d'étude de cas. Eisendhardt (1988) propose une approche par étapes pour accomplir une étude de cas, voici sous forme de tableau les étapes que nous avons suivies:

Tableau 3.1. Les étapes suivies pour la recherche sur le terrain

Étape	Activité	Raison
Se préparer	Définir la question de recherche : la RFID représente-t-elle une valeur ajoutée pour la sûreté maritime et portuaire?	Permet de concentrer nos efforts sur le sujet d'intérêt
Choisir les cas	Le choix de 2 entreprises, Entreprise X1 et Entreprise X2 oeuvrant dans le secteur sont retenues comme les cas d'étude.	Deux entreprises permettent une validité plus élevée
Développer instruments et protocoles	Multiples méthodes de collecte de données et des entrevues avec plusieurs experts dans le domaine: une revue de la littérature traitant du domaine de la sûreté portuaire a été effectuée et 16 experts du secteur privé et public ont été interviewés.	Permet la triangulation de l'évidence et une synergie des points de vue
Effectuer l'étude sur le terrain	Le contexte d'entrevues semi-structurées auprès de 16 experts a été la méthode privilégiée qui a permis d'obtenir l'opinion d'intervenants à divers niveau.	Révèle différentes perspectives.
Analyser les données	Les entrevues semi-dirigées ont permis de mieux caractériser chacun des éléments du cadre conceptuel retenu. L'analyse des données s'est effectuée selon chacun des éléments de ce cadre.	Permet une meilleure interprétation des données et de mieux structurer cette interprétation.
Formuler des recommandations	Les recommandations se sont basées sur les données recueillies.	Termine le processus tout en proposant des améliorations à la situation actuelle

Adapté de Yin, 1989

Bien que dans le cadre de cette recherche, le but n'a pas été de bâtir une théorie à partir de l'étude de cas, des conclusions ont été tirées afin d'enrichir le mode de fonctionnement des deux entreprises qui ont été rencontrées et de proposer une nouvelle stratégie technologique sur un sujet brûlant d'actualité, celui de la sûreté maritime.

3.3. Résultats et interprétations

Le choix de la stratégie méthodologique a été influencé par deux éléments. D'une part, les informations relatives au RFID sont émergentes, complexes et en évolution. De plus, bien que plusieurs universités et instances gouvernementales investissent des sommes incroyables pour développer des applications viables dans le contexte de la sûreté, ces informations sont rarement disponibles et ouvertes, de part leur nature sensible et confidentielle, ce qui rend l'analyse difficile à entreprendre. En effet, maintes fois en discutant de technologies appliquées à la sûreté avec des intervenants dans l'industrie et auprès de membres du gouvernement, je me suis confrontée à des discours fermés. Toutefois, malgré cette embûche reliée à mon domaine de recherche, le croisement des données primaires (celles obtenues des entrevues) et des données secondaires (celles obtenues de documents existants) permet quand même de tirer certaines conclusions. D'autre part, la question de recherche de ce mémoire est de nature exploratoire. En effet, le but premier est de valider ce qui, à prime abord est une proposition, et d'organiser une réflexion stratégique en fonction d'informations pertinentes à la sûreté maritime, sujet brûlant d'actualité mais de nature également sensible. La démarche méthodologique adoptée doit donc prendre en considération cet impératif de validation et doit pouvoir amener le chercheur à tirer des conclusions raisonnables. Compte tenu de ces facteurs, l'étude de cas s'est présentée comme la stratégie de recherche la plus adéquate. En effet, ce type d'étude s'effectue dans un contexte réel et favorise l'utilisation de multiples sources d'évidences afin que le chercheur puisse développer une compréhension holistique d'une situation (Yin, 1994). Dans ce contexte, bien que conscients de la difficulté d'obtenir certaines données, nous avons répondu à la question de recherche en

effectuant des entrevues dans le secteur privé de la sûreté maritime et portuaire, ainsi que dans le secteur public en particulier auprès de l'entité régissant les lois et ordonnances en matière de transport dans ce pays, Transport Canada. Par ailleurs, une revue de la littérature qui a été réalisée préalablement à la phase de terrain mais s'est également poursuivie tout au long, au fur et à mesure que de nouvelles informations se sont présentées.

Le tableau ci-dessous ventile les différentes entrevues menées dans le cadre de ce projet de recherche :

Tableau 3.2 Liste des répondants

Nom et niveau hiérarchique de la personne	**Organisme/Entreprise**	**Années de service au sein de l'entreprise**	**Nombre de rencontres**
Directeur de l'ingénierie	Entreprise X2	En fonction dans l'entreprise X2 depuis moins d'un an, mais possède une expérience solide de plus de 10 ans en ingénierie.	3 rencontres de septembre à octobre. Plusieurs échanges courriels et 3 appels téléphoniques.
Directeur du développement des affaires à l'étranger	Entreprise X2	Depuis moins d'un an dans l'entreprise X2 mais est en charge des marchés africains	1 appel conférence
Chef de projet	Entreprise X1	Œuvre depuis 17 ans auprès de l'entreprise X1 et depuis 4 ans dans la division de sûreté maritime	1 rencontre et 4 appels téléphoniques. Quelques échanges par courriel.
Ingénieur de projet	Entreprise X1	Travaille depuis 6 ans	1 rencontre et 2 appels

		dans l'entreprise X1 et depuis 4 ans dans la division de sûreté maritime	téléphoniques
Directeur Général	Transport Canada	Œuvre depuis 2 ans dans ce ministère et depuis plusieurs années dans le domaine	1 rencontre dans le cadre d'un colloque sur la sûreté maritime
Directeur	Transport Canada	Œuvre dans le domaine depuis 30 ans.	1 rencontre
Conseiller principal	Transport Canada		1 rencontre
Inspecteur régional	Transport Canada	Travaille depuis 9 ans dans le domaine	1 rencontre
Spécialiste de la technologie de la sûreté	Transport Canada	Travaille depuis 29 ans dans le domaine	1 rencontre
Vice-Président	International Longshoremen's Asociation		1 rencontre dans le cadre d'un colloque sur la sûreté maritime
Expert	Professeur dans un des établissements universitaires à Montréal	Groupe de recherche sur l'industrie militaire et la sécurité et groupe de recherche sur la reconversion industrielle	1 appel téléphonique
Expert	Professeur invité dans un des établissements universitaires à	Service de l'enseignement des affaires internationales	1 appel téléphonique

	Montréal		
Expert	Chercheur dans un des établissements universitaires à Montréal	Œuvre depuis 12 ans dans le secteur militaire canadien	1 appel téléphonique et 2 échanges courriels
Expert	Professeur dans un des établissements universitaires à Montréal	Centre d'expertise en commerce électronique	Rencontres multiples
Consultant	North River Consulting	Membre du Strategic Council for Security Technology. Spécialiste de la sécurisation de la chaîne d'approvisionnement, la productivité et la technologie. Conférencier au U.S. Maritime Security Expo	1 appel téléphonique
Associate editor	KPMG	Participant à la conférence du U.S. Maritime Security Expo	1 appel téléphonique

En résumé, 6 répondants proviennent du secteur privé, 6 répondants proviennent des différents ministères ou associations, et 4 répondants oeuvrent dans le milieu universitaire (figure 3.3). Ces différents répondants ont permis d'obtenir des informations sur chacun des éléments de notre cadre théorique.

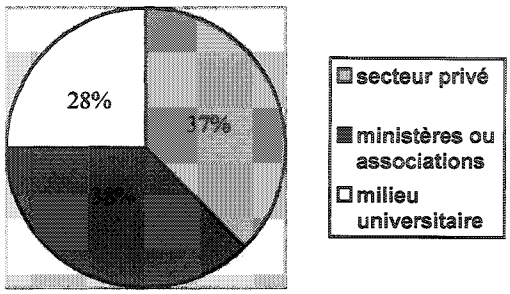
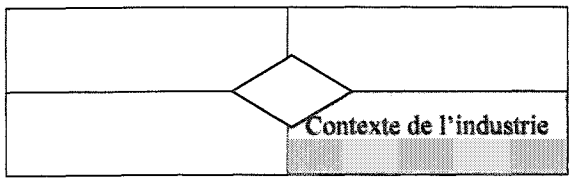


Figure 3.3: Proportions des répondants par secteur d'activité

3.3.1. Le contexte de l'industrie: le secteur de la sûreté



Suite aux différentes entrevues ayant été menées auprès des entreprises X1 et X2, les répondants sont demeurés évasifs sur leurs compétiteurs ne sachant pas précisément ni leur identité, ni leur provenance. En effet, au plus trois noms d'entreprises ont pu être obtenu. L'interlocuteur auprès de l'entreprise X2 a manifesté l'intérêt d'avoir plus d'informations sur leurs compétiteurs et s'est montré très coopératif tout au long des entretiens. Chez l'entreprise X1, le gestionnaire de projet, bien que relativement ouvert au début de la rencontre est devenu plus craintif à fournir des informations suite à une mésentente entre les entreprises X1 et X2 sur l'exclusivité des informations à fournir. Pour l'entreprise X2, il semble difficile de croire que celle-ci ne soit pas au courant de ses compétiteurs, par conséquent nous en déduisons encore une volonté de leur part de ne pas trop dévoiler d'informations ce qui n'est pas étonnant vue le caractère stratégique des informations demandées. Par conséquent, étant donné la pénurie d'informations disponibles sur les concurrents des entreprises ayant été rencontrées et dans le but de compléter les données sur le contexte de l'industrie, le recour à une étude globale

effectuée par le gouvernement du Québec sur le marché de la sûreté aux É.U. pour les entreprises souhaitant offrir leurs services dans le créneau en pleine expansion a été consultée.

Les États-Unis sont une plaque tournante majeure sur les plans économiques, touristiques et de l'immigration. Pays vaste et populeux, la protection du territoire nécessite un nombre important d'intervenants de plusieurs organismes gouvernementaux et du secteur privé. Depuis le 11 septembre, les sommes dépensées à cet effet par le gouvernement fédéral américain prennent des proportions toujours grandissantes et la tendance ne fait que s'accélérer. Plus de 234 G$ sont accordés annuellement par le gouvernement fédéral américain. Au-delà de 156 G$ (66%) vont à la défense uniquement, 60 G$ sont dépensés pour des technologie de l'information (TI) et la sûreté intérieure représente un budget de plus de 23 G$. Le ministère des Transports américain a accordé le plus grand nombre de contrats en 2001, pour une valeur de 24 G$ (Développement économique et régional et Recherche Québec, 2003).

La garde côtière reste l'agence dont le budget consacré à la sûreté est le plus élevé. Afin de moderniser sa flotte, ses avions de reconnaissance et ses équipements, des contrats de l'ordre de 17 G$ ont été accordés à Lockheed Martin et Northrop Gumman, les deux plus importants fournisseurs du gouvernement. D'après une étude de Deloitte Consulting et Aviation Week, les budgets consacrés à la sûreté en 2003 par les secteurs publics et privés devaient se situer entre 93 G$ et 138 G$ répartis selon le mode suivant :

Tableau 3.3 Budget consacré à la sûreté

Gouvernement Fédéral	Gouvernements des États	Gouvernements locaux	Grandes entreprises du secteur privé
32.6 G$	5.1 G$ - 10.2 G$	9.5 G$ - 19 G$	45.9 G$ - 76.5 G$
	Plus de 50% des budgets sont alloués à la gestion de la santé, à la gestion de la réponse, à l'information stratégique et au contrôle.	Plus de 50% des budgets sont alloués à la gestion de la réponse, à la sûreté et à la protection, et ainsi qu'à l'éducation et à la sensibilisation.	Près de 50% des budgets sont alloués à la sûreté et à la protection, à l'information stratégique, au contrôle, ainsi qu'à une meilleure intégration des systèmes.

Tiré de Développement économique et régional et Recherche Québec, 2003

Le budget consacré à la sûreté met l'emphase sur des mesures défensives d'amélioration de la sûreté aux frontières, dans les ports et dans les transports, et vise surtout à améliorer l'étanchéité des postes frontaliers. Une bonne part du budget cherche à développer des capacités de défense de chaque agence, à rajeunir la flotte de la garde côtière et à intégrer de nouvelles technologies dans les agences jouant des rôles importants. De 2003 à 2005 le marché évoluera en quatre phases :

Tableau 3.4 Évolution prévue du marché

2003	Caractère immédiat	Répondre aux besoins les plus pressants en infrastructures, équipements, ressources humaines et communications
2004	Mise à niveau	Compléter la mise en place des solutions et se tourner vers l'intégration et la maintenance
2005	Structuration, consolidation et standardisation	Les systèmes arriveront à maturité et seront exploités de façon maximale
Au-delà de 2005	Convergence des systèmes, efficacité accrue et réduction des coûts	Les dépenses connaîtront une nouvelle hausse avec le remplacement progressif des solutions mises en place en 2003

Adapté de *Deloitte Consulting/Aviation Week 2003*

Dépendamment qu'il s'agisse du secteur public ou du secteur privé, les menaces identifiées et les interventions privilégiées ne seront pas les mêmes. En effet, tandis que le gouvernement se concentre sur des lacunes que les terroristes pourraient exploiter pour maximiser l'impact de leurs attaques, le secteur privé en revanche, cherche à prévenir et atténuer les effets négatifs de possibles attaques sur des opérations. Le tableau 3.5 résume les enjeux par secteur:

Tableau 3.5 Enjeux par secteur

Secteur public	Secteur privé
Menaces identifiées : - Utilisation d'armes de destruction massive - Menaces à la santé publique - Attaques contre les infrastructures physiques	Menaces identifiées : - Utilisation d'armes de destruction massive - Transport - TI/communications
Interventions privilégiées : L'accent est placé sur la sûreté publique et la nécessité de mieux répondre, mieux communiquer et mieux éduquer.	Interventions privilégiées : Assurer de façon sécuritaire le déplacement des employés et le maintien de l'approvisionnement et de la distribution.

Adapté de *Deloitte Consulting/Aviation Week 2003*

Depuis 2001-2002, le budget pour le *Department of Homeland Security (DHS)* ne fait qu'augmenter pour atteindre en 2003-2004 la somme gigantesque de 36.2 G$. Si l'on en juge les récentes décisions de l'administration Bush, cette tendance n'est pas pour ralentir, mais les États-Unis sont encore très préoccupés de l'intégrité de leur territoire national qui serait le point de mire des terroristes. Le tableau ci-dessous ventile de façon détaillée le budget pour l'exercice financier de 2003-2004 :

Tableau 3.6 Budget du DHS par secteurs d'intervention en (M$ US)

Sûreté des frontières et des systèmes de transport	18 100
Sûreté des ports et des voies navigables	6 800
Préparation et réponse aux urgences nationales	6 000
Amélioration des services d'immigration	1 800
Avancement de la science et exploitation des nouvelles technologies	800
Amélioration de l'analyse de l'information stratégique et protection des infrastructures	800
Autres activités du DHS	1 900
Total	***36 200***

Tiré *de Développement économique et régional et Recherche Québec, 2003*

Il est à souligner que malgré les sommes importantes allouées à la sécurisation du territoire, certains experts craignent que ces montants soient insuffisants pour améliorer de façon significative la sûreté du pays étant donné la nature de la menace du terrorisme. De plus, le DHS étant un département jeune dans sa création, l'on craint qu'il n'ait quelques difficultés à gérer ses 22 agences et ses 180 000 employés surtout que les secteurs publics et privés s'appuient sur le gouvernement fédéral pour lutter efficacement contre le terrorisme.

Les concurrents

Les contrats ayant été accordés par le DHS en 2001, étaient de l'ordre de 215 G$ de toutes les entreprises qui se sont vues récolter une part de gâteau, il n'y a que quelques grands fournisseurs du gouvernement américain qui ont reçu une part importante des budgets de défense et de sûreté. Ci-dessous au tableau 3.7 sont énumérés les 20 entreprises américaines offrant le meilleur potentiel de sous-traitance pour les PME, d'après la Chambre de commerce des États-Unis :

Tableau 3.7 Sociétés Contrats en 2001 ($ US)

Lockheed Martin Corporation	17 951 303 000
The Boeing Company	14 362 243 000
Raytheon Company	6 123 605 000
Newport News Shipbuilding & Dredging	5 689 359 000
Northrop Grumman Corporation	5 636 124 000
General Dynamics Corporation	4 928 238 000
United Technologies corporation	3 500 465 000
Bechtel Group Inc.	3 075 316 000
TRW inc.	2 499 816 000
General Electric Company Inc.	1 808 984 000
Computer Sciences Corporation	1 648 495 000
Honeywell International Inc.	1 422 018 000
DynCorp	1 364 004 000
ITT Industries Inc.	879 772 000
Alliant Techsystems Inc.	862 269 000
Booz Allen & Hamilton Inc.	808 907 000
Oshkosh Truck Corporation	566 511 000
Motorola Inc.	522 520 000
Unisys Corporation	549 905 000
Boeing Sikorsky Comanche Team	527 657 000

Tiré de *Développement économique et régional et Recherche Québec, 2003*

D'après cette liste, nous remarquons que les contrats offerts par le DHS sont énormes et lucratifs pour ceux pouvant en décrocher. Selon des observations, afin d'être plus alléchantes aux yeux des instances gouvernementales américaines, plusieurs entreprises nomment les départements directement visés par ce marché par le titre de 'Homeland Security Division' tel l'exemple de l'entreprise X1. En effet, les enjeux étant de taille, une stratégie marketing est mise de l'avant pour faciliter et valider la légitimité des acteurs dans le domaine. Après avoir analysé sommairement la liste des produits offerts en matière de sûreté maritime et portuaire, il semblerait raisonnable de déclarer que ces entreprises listées dans le tableau 3.7, pourraient être une menace en terme de

compétition pour nos entreprises canadiennes. Cependant, le directeur de l'entreprise X2 a assuré que ces entreprises ne sont pas prêtes à se lancer dans certains marchés à cause de toutes les implications dans ces contextes particuliers. De plus, le gestionnaire de projet de l'entreprise X1 confirme que ces grandes entreprises sous-traitent avec de plus petites entreprises pour utiliser les compétences clés développées par d'autres et les intégrer dans leurs gammes de produits de sûreté, allant de flottes navales à des systèmes satellites. Par conséquent, nos entreprises canadiennes, bien que n'ayant pas les capitaux des multinationales américaines, peuvent malgré tout offrir leurs services en matière de sûreté portuaire en se démarquant au niveau des produits offerts par une spécialisation dans des produits qui ne font pas partie des investissement en R&D de celles-ci, et en cherchant des créneaux particuliers et des marchés spécifiques. En contrepartie, pour certains de ces marchés bien qu'il existe une volonté de vouloir rehausser les mesures de sûreté de leurs ports, parfois les moyens financiers ne sont pas suffisants. Pour citer l'intervenant auprès de l'entreprise X1, 'pour faire affaire en Chine, il faut passer par 2 ou 3 intermédiaires ... ils n'ont pas de budget... L'Afrique n'a pas de budget et l'Amérique Centrale n'a pas de budget.' Malgré ce constat peu optimiste, les pays en voie de développement n'ayant pas le choix de se conformer au code ISPS afin de continuer de faire de l'import-export de marchandises choisiront un jour ou l'autre d'améliorer leurs infrastructures portuaires afin de s'assurer que les pays développés puissent continuer de transiger avec eux.

Pour compléter cette section, notons que le contexte industriel peut être aussi caractérisé par certains impératifs. Lors des entretiens avec les intervenants de Transport Canada, l'un d'entre eux a fait mention qu'un conteneur est le plus vulnérable lorsqu'il est stationnaire, et plus le délai en mode stationnaire est grand plus les risques que l'intégrité du conteneurs soit modifiée sont grands. Par conséquent, les lieux d'entrepôt, des centres de groupage/dégroupage, les plates-formes intermodales et les infrastructures de transport sont les endroits de prédilection où l'on craint le plus l'intervention d'intrus. Lors d'une participation à un colloque sur la sûreté maritime, l'une des interventions

ayant été faite proposait justement de renforcer la sûreté des conteneurs dans des entrepôts en donnant les moyens au propriétaire de se doter de mesures supplémentaires pour sécuriser les marchandises en leur possession. Bien que d'accord avec cette proposition, il va sans dire que si tout au long de la chaîne logistique le personnel n'est pas fiable dans ces fonctions, un investissement supplémentaire au niveau de la sûreté ne peut avoir un impact appréciable. Ce problème des ressources humaines sera abordé dans le chapitre suivant. Par ailleurs, l'un des problèmes que l'on note également est la fraude documentaire observée dans les cas de vol de cargaisons. Ce risque est aggravé du fait que la majeure partie du flux d'informations relatives aux transactions du commerce international est consignée sur papier ce qui est coûteux et inefficace. Bien que les erreurs puissent être involontaires, certaines erreurs peuvent être effectuées pour avantager un certains groupes d'individus et contrevenir aux règlements établies. Bien que l'inspection manuelle de tous les conteneurs soit une tâche impossible, il est important de vérifier le plus grand nombre de conteneurs par des inspecteurs, et par conséquent d'investir dans la formation de cette main-d'œuvre cruciale, pour laquelle de toute évidence les antécédents judiciaires auront été vérifiés.

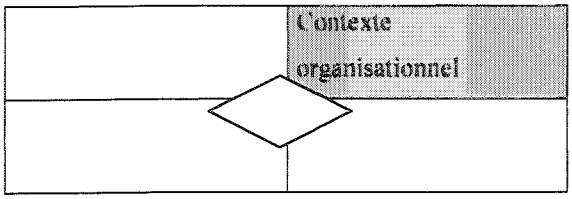
Certains petits ports moins nantis, bien qu'ayant la volonté d'augmenter leur niveau de sûreté pour se prémunir de l'avantage compétitif qu'offre l'adhésion à ces programmes, peuvent néanmoins demeurer compétitifs grâce au programme qu'offre le gouvernement fédéral pour aider financièrement les ports dans la transformation et la sécurisation de leurs effectifs par une subvention. Une des remarques recueillie lors d'un entretien avec un inspecteur de Transport Canada était, qu'un des aspects négatifs de ces subventions est que souvent au lieu de prendre le devant pour investir dans le rehaussement de la sécurisation des ports, certains propriétaires de petits ports vont se contenter d'investissements minimaux tel mettre des barrières supplémentaires autour de la propriété du port et attendre la subvention pour vraiment faire les travaux qui se doivent pour se conformer au programme. La réalité de ce commerce est que les grands ports sont ceux qui ont l'argent et qui peuvent se permettre d'investir dans la sûreté, car ces

coûts ils peuvent les récupérer plus facilement que les petits exploitants notamment en haussant les taxes portuaires, en chargeant des montants plus chers au navires voulant accoster et en appliquant au programme de subvention fédéral. Les petits ports ayant des marges de profit plus minces n'ont pas toute cette marge de manœuvre qu'ont leurs plus gros compétiteurs et peuvent, en effet, se retrouver en marge de ce marché malgré leurs prix plus bas parce qu'ils n'ont pas la certification des programmes OMI, CSI et C-TPAT. Le tableau 3.8 résume le contexte industriel de la sûreté.

Tableau 3.8: Le contexte industriel de la sûreté

- De nature très sensible
- Marché en pleine expansion qui recoupe les efforts des pays pour assurer la défense et l'intégrité de leur territoire.
  ex : É.U. $36.2 G mis de côté pour le Department Homeland Security (DHS)
- Compétition importante pour décrocher des contrats de sûreté car les compétiteurs sont multiples et les marchés sont très lucratifs
  ex : É.U. budget de $234 G alloué à la défense
- Evolution future vers la convergence des systèmes, une plus grande efficacité et la réduction des coûts

3.3.2. Contexte organisationnel



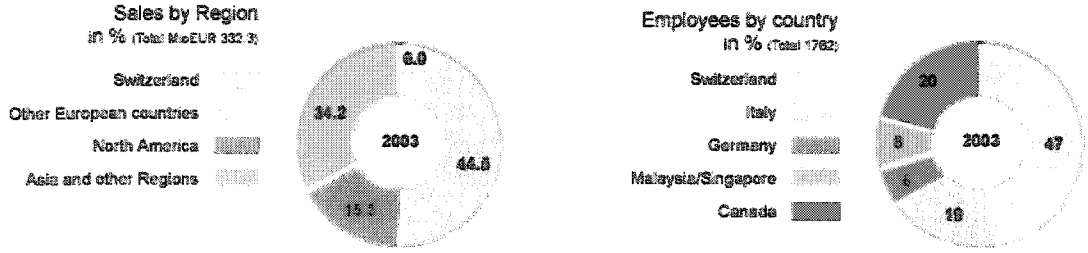
Dans cette section, nous regarderons de près le contexte organisationnel des entreprises X1 et X2 d'après le modèle proposé de Burgelman. Cette section est basée sur des informations recueillies suite à différentes entrevues menées auprès de répondants durant le mois de septembre, mais surtout en ce qui concerne le contexte organisationnel, à partir des documents m'ayant été remis. À nouveau, durant les entrevues il y a toujours eu cette crainte de donner l'information, mais grâce à la taille de l'entreprise X1 certaines informations sont de nature publique. Pour ce qui est de l'entreprise X2, un maximum de document a été transmis, surtout de nature marketing. En dépit de leur bonne volonté, peu de données ont pu être récoltée sur cette deuxième entreprise, et ce malgré leur inscription dans le CRIQ. Par conséquent, l'explication de celle-ci demeure abrégée.

Le contexte organisationnel de l'entreprise X 1

L'une des entreprises oeuvrant dans la sûreté portuaire et ayant un pied d'attache dans la province de Québec, est la compagnie X1. Cette entreprise est en fait une division de la multinationale allemande à exploitation diversifiée, entreprise mère dont les ventes annuelles se chiffrent à 4.6 G€ et le nombre d'employés est de 26 000 de par le monde. La compagnie mère possède trois divisions, dont l'une est spécialisée dans l'industrie automobile, l'autre en électronique, et celle qui nous intéresse dans le cadre des solutions offertes en sûreté portuaire, en défense. Les compétences de chaque division de l'entreprise mère sont organisées selon quatre axes stratégiques chacun de ces derniers établi comme centre de profit responsable pour leur segment de marché

respectif, soit les systèmes terrestres, les systèmes de défense aériens, les armes et la munition et l'électronique de défense. Cette structure permet ainsi de mettre à profit les forces et les avantages compétitifs du groupe et grâce à l'interaction des systèmes et des composantes clés orientées clients, les produits de l'entreprise mère couvre la chaîne fonctionnelle requise pour la performance de tâches militaires, et des troupes d'infanterie. De plus, l'entreprise X1 est un des fabricants de premier plan de systèmes d'armement complexe pour la défense aérienne dont les compétences clés comprennent non seulement le développement et la fabrication de système de défense aérienne mais aussi des simulateurs et des systèmes d'entraînement. Tous les produits sont soumis à des tests et des essais rigoureux par un personnel qualifié, compétent et efficace.

L'entreprise X1, division qui nous intéresse dans le cadre de cette étude, est une sous-division de l'entreprise mère dont les ventes annuelles sont de 1.7 G€ et le nombre d'employés à plus de 8 800. La figure 3.4 présente la répartition des ventes et du nombre d'employés de l'entreprise X1.



Source : Rapport annuel de l'entreprise mère, 2004

Figure 3.4: Répartition des ventes et du nombre d'employés de l'entreprise X1

Établie au Canada depuis juin 1986, l'entreprise X1 fait partie du groupe de l'entreprise mère depuis janvier 2000, et est active dans les secteurs des pièces automobiles, des systèmes électroniques et des systèmes de défense. Située sur la rive Sud de Montréal, son volume de ventes annuelles s'élève à 52 M$ canadiens et le nombre de ses employés

se chiffre à plus de 300 personnes. Offrant des solutions novatrices pour les systèmes complexes de logiciels, de communication et de défense, l'entreprise X1 est une firme d'intégration de systèmes reconnue à l'international, spécialisée dans la conception, l'assemblage, l'intégration, les essais et la livraison de solutions de systèmes complets. En mettant à profit leur expérience et les technologies acquises par le biais de l'intégration de leur système de missiles, leur gamme de produits et de services s'est élargi pour comprendre des systèmes logiciels, des systèmes de communication, des systèmes d'armes et de détection, et depuis 2001, des technologies du transport. Par le biais de commandes importantes de 1999 à 2003, l'entreprise X1 a connu une croissance de son chiffre d'affaire et du nombre de ses employés, et c'est ainsi que des alliances stratégiques ont pu être établies avec des corporations majeures, un nouveau portfolio de produits high-tech a été mis sur pied, et le nombre de ses clients est à la hausse.

Fournisseur de produits et de services mondialement reconnus, la vision de l'entreprise est de développer et de fournir des solutions innovatrices d'avant-garde et de haute performance ce qui lui a valu le titre de chef de file dans les systèmes de défense et l'ingénierie de soutien pour la durée de vie du matériel. D'autre part, leurs systèmes en temps réel avec logiciel intégré se placent parmi les trois meilleurs produits offerts sur le marché, tandis que, pour les systèmes de communications et d'intégration de systèmes, des partenariats ont été signés. Dans le cadre de solutions offertes de systèmes maritimes, ce partenariat se fait avec une entreprise française. Les facteurs clés du succès de l'entreprise X1 résident dans ses compétences de coopération mondiale dans la fourniture des produits et services de très grande qualité au niveau de la performance, de la fiabilité et de la sûreté, ainsi que dans le respect des échéanciers établis. L'entreprise X1 effectue autant de la veille technologique, que de l'ingénierie de production et offre un service après-vente de haute qualité.

En matière de sûreté maritime, les solutions offertes par la division de Homeland Security, se basent sur deux produits de communication complémentaires, soit le AIS

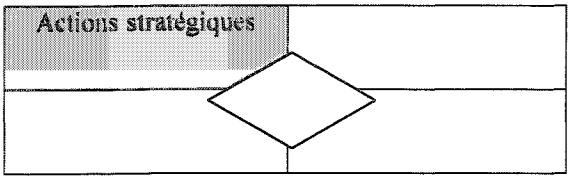
(Automatic Identification of Ship) qui permet la localisation et la visualisation à l'écran des navires, ainsi que sur le GMDSS (Global Maritime Distress and Safety System) qui est un système maritime mondial de sûreté et de secours en cas de détresse par appel sélectif numérique. Bien que la technologie du RFID ne soit pas utilisée, l'un des ingénieurs de projet chez l'entreprise X1, offre le commentaire suivant, 'ce n'est pas pour dire que dans le futur nous n'utiliserons pas cette technologie' et laisse donc entendre une migration possible de leurs produits vers les RFID.

Le contexte organisationnel de l'entreprise X2

En existence depuis février 1986, l'entreprise X2 est un distributeur et intégrateur des télécommunications fournissant des systèmes clés en main. PME de 25 personnes, la longévité et l'expansion de cette entreprise reposent sur le professionnalisme de son équipe ayant développé une expertise dans le domaine de la radiocommunication, la sûreté, les communications sans fils et la vidéo conférence. Forte de son expérience acquise au fil des ans, l'entreprise X2 a développé des compétences dans un marché de niche, celui des systèmes de sûreté maritimes et exécute des projets directement liés à la sûreté nationale et militaire grâce à des partenariats avec plusieurs entreprises. Un des partenariats s'effectue avec l'entreprise X1. Par son appui technique innovateur et qualifié, la base de clients de cette entreprise s'est élargie pour inclure aujourd'hui des entreprises de services publiques, des agences publiques de sûreté, des compagnies de transport, des gouvernements, des aéroports, des ports maritimes et autres clients industriels.

Bien que peu d'information soit disponible sur cette PME, sa taille explique en grande partie un contexte peu formalisé, l'absence de rapport annuel et une structure administrative toujours en évolution.

3.3.3. Actions stratégiques



Les actions stratégiques dont il est question dans cette section ont été élaborées à partir d'une discussion avec un expert qui détient une chaire universitaire responsable de sujets d'intérêts sur l'industrie militaire et la sécurité ainsi qu'une autre chaire sur la reconversion militaire. Ainsi, des articles qu'il a publié sur la reconversion militaire ont été une source d'information utile et de même qu'un entretien téléphonique ayant eu lieu au courant du mois d'octobre. D'autre part, un mémoire de maîtrise sur la reconversion militaire de l'entreprise X1, est venu enrichir cette étude et a permis d'obtenir les informations non disponibles qui n'auraient pu être autrement détenu. Par ailleurs, une discussion avec un autre expert a aidé à comprendre les enjeux ayant mené à la reconversion de l'industrie militaire française. Sur les raisons de cette reconversion au Canada et l'essor et/ou la dégénérescence de l'industrie militaire en Amérique du Nord, l'interlocuteur est demeuré prudent. De plus, pour les conclusions vis-à-vis de l'entreprise X2, elles ont été établies à partir d'entretiens et de documents qui m'ont été remis et d'ouvrages consultés.

Les actions stratégiques dans un contexte de reconversion des entreprises militaires

Depuis la fin du Pacte de Varsovie, de nouvelles puissances militaires ont fait leur apparition sur la scène internationale qui n'avaient auparavant pas accès à ces marchés, ce qui a eu pour conséquence de réduire la taille du marché du militaire et d'augmenter la concurrence. C'est ainsi qu'afin de demeurer concurrentielles et d'assurer leur survie,

les firmes militaires de l'OTAN ont dû s'adapter au changement en diversifiant leurs activités sur des marchés civils et en redéployant leurs compétences fondamentales. La compétence fondamentale s'impose alors comme la pierre angulaire du devenir de la firme militaire confrontée à un monde en perpétuelle redéfinition au sein duquel l'avantage concurrentiel d'hier ne sera plus d'aucune utilité demain, voire obsolète aujourd'hui même (Cimon, 2000).

Dans le but de faire faces aux nouvelles contraintes imposées par le marché, les entreprises du militaire n'ont pas le choix que d'embrasser le changement en investissant dans de nouveaux créneaux. Tel que le mentionne Hamel et Prahalad (1994b):

> 'The nature of rapid industry transformations is creating a need for managers not only to manage existing competencies in a firm, but to rapidly acquire new ones. Sometimes, firms have to discard competencies to enable them to adapt. For example, how does a defense contractor acquire the competence to create and manage consumer business?' (Hamel et Prahalad, 1994b :5-16)

Tableau 3.9 Actions Stratégiques en faveur de la reconversion des entreprises militaires

la reconversion permet: • De maintenir la base industrielle de défense • De réduire la dépendance au marché militaire • D'améliorer la productivité • De protéger les parts de marchés et suivre la compétition • De développer de nouveaux axes de recherche et développement D'offrir de nouveaux débouchés et de nouveaux marchés

Adapté de Bélanger, 1997

Ainsi, la stratégie de redéploiement des compétences fondamentales recouvre des enjeux liés à la revitalisation technologique, à la compétitivité des entreprises et à l'expansion du commerce (Tableau 3.9).

Le contexte du marché militaire n'ayant pas été favorable dans les années ayant précédé le 11 septembre 2001, un puissant mouvement de consolidation visant à préserver la viabilité des bases industrielles de défense en s'appuyant notamment sur les fusions, la reconversion et la diversification des entreprises jugées les plus stratégiques a émergé (Bélanger, 1997). Dans l'industrie de la défense, plusieurs firmes possèdent des compétences fondamentales et un fort pourcentage de leur production destiné aux marchés militaires, dont le seul client est l'État. Dans le cas de certains pays, notamment le Canada, l'État a réduit depuis plusieurs années les dépenses militaires, les entreprises dans le domaine se sont vues dans l'obligation de réduire leurs effectifs ou de se reconvertir en utilisant les compétences acquises, vers d'autres marchés, notamment vers le marché du civil plus stable et prometteur.

Les actions stratégiques de l'entreprise X1

À ses débuts, l'entreprise X1 était un fabricant suisse d'artillerie antiaérien qui est devenu célèbre lors de la deuxième guerre mondiale pour ses cannons de 20 mm. Depuis qu'elle a été fondée en 1986, l'entreprise X1 a su mettre à profit ses compétences-clés comme fabricant de systèmes intégrés de défense antiaérienne pour diversifier sa gamme de produits et exploiter de nouveaux créneaux technologiques et devenir ainsi l'une des principales entreprises d'intégration de systèmes. Cependant vu la décroissance du marché militaire et la fluctuation des marchés selon le cycle des conflits armés, comme plusieurs autres dans le secteur miliaire, l'entreprise a du entreprendre des démarches de reconversion et de diversification pour aller chercher de nouveaux marchés. Afin de capitaliser sur ses compétences techniques acquises grâce à ses systèmes anti-tank de défense et par extension d'intégration de systèmes, et ses compétences de marketing

personnes à personnes reconnues sur le marché de la défense, l'entreprise X1 s'est lancée sur le marché des systèmes de communication pour le marché civil et notamment du marché qui nous intéresse, celui de la sûreté maritime et portuaire afin d'élargir ses possibilités d'affaires dans le secteur commercial. Ainsi sur le plan technologique, les compétences de l'entreprise X1 résident dans l'intégration de systèmes qui requièrent une habileté à développer des systèmes complexes avec des assemblages de technologies variées. Par ailleurs, la force en marketing de celle-ci réside en ses capacités à bâtir la confiance auprès de ses clients. Par conséquent, sa stratégie adoptée pour faire face aux nouveaux impératifs du marché a été de diversifier son portefeuille de produits en se lançant dans le marché civil, plus particulièrement celui de la sûreté portuaire, malgré le fait que les nouvelles règles du jeu diffèrent d'un client gouvernemental versus un client du secteur privé telles par exemple, des délais plus courts, des marges de profits moins importantes et un contrôle de coûts plus strict. L'entreprise X1 favorise une niche commerciale et, par une nouvelle combinaison d'éléments technologiques existants, elle a privilégié une adéquation à un marché en émergence, celui de la sûreté maritime: c'est dans cette dernière phase que l'entreprise X1 se retrouvait il y a 4 ans, avant la création de son département de sûreté maritime. Plutôt que de provoquer une 'rupture', en recherchant une technologie radicalement nouvelle qui aurait demandé un investissement considérable en R&D et qui serait entrée en concurrence directe avec de gros joueurs dans l'industrie, l'entreprise X1 a choisi plutôt de capitaliser sur la technologie maîtrisée en remaniant ses compétences sous une autre forme et en se positionnant sur un marché stratégique en pleine effervescence. Le tableau 3.10 présente un sommaire des stratégies et des éléments structuraux de l'entreprise X1.

Tableau 3.10 Sommaire des stratégies et des éléments structuraux de l'entreprise X1

Actions Stratégiques		
Reconversion	**Diversification**	**Partenariats/alliances**
• Convertir ses compétences fondamentales pour des applications civiles	• Élargir sa gamme de produits pour atteindre de nouveaux marchés	• Favoriser la fusion avec le groupe allemand (entreprise mère)
• Développer des systèmes complexes	• Se tourner vers des systèmes de sûreté maritimes	• Favoriser l'accès à de nouveaux marchés et rechercher de nouveaux partenariats

Les actions stratégiques de l'entreprise X2

Distributeur autorisé de Motorola, l'entreprise X2 est un intégrateur de technologies ayant réalisé plusieurs projets sur la scène internationale, notamment en Amérique du Sud et récemment en Afrique, pour un port autonome important. En effet, grâce à ce contrat de 10 M$, plusieurs systèmes de sûreté ont été mis en application soit des systèmes de contrôle d'accès, de la vidéosurveillance et des systèmes radars VTS et d'identification automatique AIS. Une plate-forme sans fil Motorola a été installée pour supporter toutes les communications et le transfert de données tandis que les systèmes de sûreté ayant été mis en application l'ont été afin d'être conformes au code international ISPS.

L'entreprise X2 étant une PME, le contexte organisationnel est moins formalisé que celui d'une grande entreprise: bien qu'aucune stratégie marketing majeure ne soit articulée, il est possible de déduire certaines actions stratégiques. Tel qu'énoncé plus

haut, l'offre de solutions intégrées clés en main représente un élément important de différentiation au sein d'un marché qui cherche la qualité, la fiabilité et un bon rapport qualité/prix. L'entreprise X2 adopte donc, à l'égard de cette activité, une stratégie de concentration et sait adapter son produit et son offre afin d'offrir une plus grande flexibilité à ses clients. La stratégie de concentration signifie que l'intégrateur-produit, l'entreprise X2, accomplit lui-même les actions stratégiques et qu'il possède l'ensemble des compétences requises pour leur réalisation. L'action la plus stratégique pour cette entreprise consiste à offrir un produit de haute qualité, fiable, offrant des fonctionnalités intéressantes et parfois essentielles pour le client, et un contrat d'entretien et une formation incluse dans le prix de ses services.

Par ailleurs, une autre stratégie se dessine, celle de la stratégie de collaboration car l'intégrateur-produit s'associe à des partenaires d'affaires pour réaliser une activité. En effet, à l'exemple de leur partenariat avec l'entreprise X1, les éléments structuraux sont ainsi conjointement maîtrisés ; d'une part l'entreprise X1 offre son expertise en matière de systèmes de sûreté maritime, et d'autre part l'entreprise X2 complémente la solution par son expertise en matière de sûreté portuaire. Ainsi, les compétences des partenaires d'affaires sont complémentaires.

Propre au contexte de la PME, la stratégie d'opportunisme prévaut en matière de recherche de clients. En effet, l'obtention du contrat en Afrique s'est faite grâce à un contexte favorable pour l'entreprise qui a su se positionner sur ce marché et exploiter l'opportunité qui s'ouvrait devant elle. Tel que l'exprime l'un de ses hauts dirigeants, il s'agissait d'être 'Au bon endroit, au bon moment, et avec la bonne technologie'. Bien que son marché de prédilection soit celui du marché de la sûreté portuaire, et, notamment plus récemment le contexte africain, l'entreprise X2 évolue également sur la scène locale en offrant la location d'équipements de sûreté pour des événements spéciaux, ce qui lui permet de diversifier ses sources de revenus. En ce qui concerne le marché africain, l'entreprise X2 a un avantage stratégique par rapport à d'autres gros

joueurs tel Motorola, en ce que le contexte du continent africain se porte bien à la flexibilité que peut se permettre une PME. En effet, certains hauts dirigeants ne fonctionnant pas selon les normes d'un marché de libre concurrence ou des processus législatifs et administratifs établis d'avance, plusieurs grandes entreprises choisissent de ne pas se lancer dans des marchés incertains, ce qui est donc une barrière à l'entrée pour les grandes entreprises et une source d'opportunité pour d'autres. Par ailleurs, les sources de financement étant fragiles auprès des pays en voie de développement, le nerf de la guerre demeure le moment auquel l'entreprise ayant gagné l'offre de service se fera payer. Conséquemment, l'entreprise X2 bien qu'ayant un potentiel intéressant pour décrocher d'autres contrats prometteurs, se voit freiner dans ses habiletés par son manque de ressources et de disponibilité, problèmes propres aux PME. Ainsi, l'entreprise X2 a su obtenir un avantage compétitif en proposant un ensemble de solutions technologiques variées et flexibles offerts en fonction des besoins et des moyens financiers de leurs clients. Leurs offres sont caractérisées par des solutions à haute valeur ajoutée, combinées à des contrats de service après-vente. De plus, l'entreprise a choisi d'investir dans des technologies performantes, innovantes mais dispendieuses tel les scanners à rayon–X VACIS, et d'offrir, grâce à des alliances stratégiques, une gamme de produit très large. Enfin, à l'affût de nouveaux marchés, l'entreprise a su se diversifier pour offrir des produits et des solutions dans un créneau prometteur en pleine expansion, celui de la sûreté portuaire. De plus, en ce qui a trait au type d'innovation privilégiée par cette entreprise, il ne s'agit pas de produire de nouveaux produits mais plutôt de cibler les produits qu'elle veut offrir, en rendant ceux-ci compétitifs en matière de prix. En effet, elle cherche à pérenniser ses relations avec sa clientèle et le marché, et à garder un avantage concurrentiel afin de survivre dans un marché hautement compétitif. Le tableau 3.11 présente un sommaire des stratégies et des éléments structuraux de l'entreprise X2.

Tableau 3.11 Sommaire des stratégies et des éléments structuraux de l'entreprise X2

Actions Stratégiques		
Concentration	**Collaboration**	**Opportunisme**
• Offrir une solution clés en main de haute qualité à bon prix	• Créer des partenariats	• Chercher des marchés en nécessité de conformation au code ISPS
• Équipe compétente et utilisation d'équipements de haute qualité	• Sûreté portuaire	• Utilisation de contacts

3.3.4. Les actions stratégiques découlant du partenariat des entreprises X1 et X2

Le choix des entreprises X1 et X2 s'est fait grâce à l'accessibilité de ces entreprises établies à Montréal qui œuvre dans la sûreté maritime et portuaire, leur expertise et leur savoir-faire. En effet, les candidats potentiels ayant une expérience dans l'élaboration de sûreté maritime et portuaire dans ce pays n'étant pas abondant, leur proximité a permis de rencontrer aisément ces interlocuteurs qui ont accepté de participer et d'enrichir cette étude. Grâce à cette collaboration, l'évaluation de l'impact et de la pertinence de la technologie RFID appliquée au domaine maritime et portuaire s'est faite plus aisément et les besoins des clients en matière de sûreté ont pu être mieux cerné.

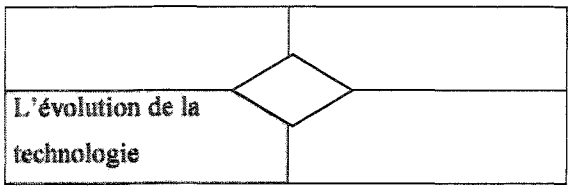
Fort de ses capacités de vente et de la panoplies de produits et services qu'elle offre, l'entreprise X2 ayant signé un contrat de plusieurs millions de dollars pour la sécurisation d'un port en Afrique de l'Ouest, elle n'avait pas toutes les ressources nécessaire pour mener à bien le projet de sûreté maritime et portuaire et a fait appel à l'entreprise X1 pour assurer le volet maritime de ce contrat. Ce contrat devait se conformer aux exigences de l'OMI et de son code ISPS. Leur collaboration fructueuse a

débouché dans l'établissement d'un partenariat pour la soumission de d'autres projets à venir.

Plusieurs entrevues ont été menées auprès des entreprises X1 et X2 afin de ratisser les informations suffisantes et pertinentes pour obtenir la description de la solution finale ayant été développée. De plus, des documents ayant été élaborés conjointement par les deux entreprises et le site Internet du port en question sont venus enrichir cette étude. Selon des entretiens avec différents intervenants auprès du port en question, celui-ci possédait déjà au préalable de l'équipement de sûreté haut de gamme, mais en quantité insuffisante et parfois non-fonctionnel. Afin de palier à ces lacunes, plusieurs caméras ont été ajoutées pour accroître la visibilité des opérateurs sur les installations du port, et les accès aux quais ont été sécurisés davantage tandis que les opérateurs ont été outillés avec des technologies adéquates . En revanche, certains quais possédaient déjà des accès contrôlés tel le port de pêche et des statistiques étaient disponibles sur la quantité des entrées/sorties journalières, cependant ces équipements étaient mal exploités faute de formation du personnel qui n'utilisait pas toujours efficacement la technologie. Ces technologies quoique intéressantes doivent pouvoir être supportées par un personnel qualifié et formé, nécessité absolue pour répondre à l'évolution des besoins et des équipements mis à leur disposition. De plus, le contexte culturel de cet environnement colore le milieu du port qui se voit aux prises avec un problème de sûreté flagrant, car des itinérants habitent sur les lieux du port malgré qu'ils soient chassés de façon intermittente. Bien que deux radars avaient été installés, des problèmes de maintenance n'étaient pas toujours résolus et un de ceux-ci était non-fonctionnel. De plus, l'entreprise française qui devait normalement en assurer la maintenance avait certains litiges avec les autorités portuaires. C'est ainsi, que les deux entreprises X1 et X2 ont saisi l'occasion pour offrir un forfait de formation des techniciens, de soutien après-vente et d'assistance dépannage en cas de problèmes majeurs pour les équipements existants et les équipements achetés nouvellement. Par ailleurs, le vol et le piratage régulier des bateaux reste une situation préoccupante: le vol de navires et la revente qui se fait sur le marché

noir ne sont pas inconnus des autorités qui jugent ne pas avoir les moyens ou l'autorité suffisante pour remédier définitivement à ce trafic illégal, malgré l'existence d'une police maritime, de l'armée de mer sénégalaise et française ainsi que des douanes. De plus, afin d'échapper aux douanes, il existe un trafic halieutique où les grands navires de pêche transbordent le poisson vers des pirogues qui le revendent sur le marché ou aux entreprises de transformation. Finalement, bien que les autorités soient sensibilisées aux risques inhérents à des environnements malsains, tel celui au quai des conteneurs de soufre, les travailleurs manquent de formation au niveau de la prévention de la santé et la sûreté au travail qui se traduit par des précautions simples tel celui de porter des masques ou de mettre des souliers de sûreté. Cependant, ces outils que l'on prend pour acquis dans nos pays industrialisés, représentent une fortune pour un salarié dans ce pays et ne sont pas fournis par l'entreprise. Enfin, bien que la solution portuaire et maritime développée dans ce port soit à l'avant-garde technologique des autres ports africains, un pays ayant un budget limité tel un pays en voie de développement, doit se questionner sur la redondance des équipements et, faute d'instances administratives et de zones grises dans l'attribution des responsabilités des unités en place, n'a pas tous les moyens adéquats pour répondre adéquatement aux appels d'urgence d'un navire en détresse si celui-ci se fait aborder par des pirates. C'est ainsi, que les pays en voie de développement pourront, par l'entremise d'instances financières tel la Banque Mondiale ou leur gouvernement propre, se munir de moyens plus importants pour tout d'abord se conformer, au code ISPS puis se doter d'une structure en place et de procédures mises à jour qui répondront aux besoins pressants de sûreté. Tel que le souligne l'OCDE, des dispositifs de financement innovateurs comme des partenariats entre secteurs publics et privés sont certainement une option envisageable dans le contexte de la sûreté portuaire.

3.3.5. L'évolution de la technologie



Les solutions technologiques qui sous-tendent la sûreté portuaire ont été examinées dans la section 2.3 tandis que la technologie RFID a été analysée dans la section 2.4 Cette section 3.3.4. traite spécifiquement de l'évolution de la technologie dans le contexte de la sûreté portuaire et résume ce que l'étude sur le terrain a permis d'établir à ce sujet.
Grâce aux entretiens avec divers intervenants auprès de Transport Canada, il a été possible de prendre connaissance d'un projet d'étude de la technologie du RFID impliquant le Port de Montréal. Malgré la nature sensible et confidentielle des informations concernant la sûreté portuaire, quelques renseignements ont pu être obtenus. De plus, des documents rendus publics sur le site de Transport Canada ont toutefois été acheminés. Par la suite, afin d'approfondir le contexte de cette étude en cours, un entretien téléphonique avec un intervenant du Port de Montréal, a permis de ratisser quelques données supplémentaires mais cependant sans rentrer dans le spécifique.

Dans le cadre du projet américain 'Safe Commerce', le Port de Montréal s'est joint avec le Port de Halifax et plusieurs états américains du Nord-Est pour étudier les nouvelles technologies pouvant rendre plus sécuritaires le transport de conteneurs. Ainsi, une étude de traçabilité d'un conteneur en partance de l'Europe de l'Est transigeant par le Port de Montréal et en destination du New Hampshire, a été menée. Un système multiple utilisant la technologie du RFID couplée avec du GPS, et des communications satellite et cellulaire, a été regardée de près. Selon mon interlocuteur 'le RFID marchait bien... Sur le bateau, ça marchait bien, mais on a eu quelques problèmes de lecture de la puce.' En effet, quelques problèmes ont été rencontrés en ce qui concerne la lecture/écriture des

puces et leur capacité, car l'information qui est incluse est à caractère confidentielle, et certaines des informations doivent n'être lisibles qu'au département et intervenant à qui elles sont assignées. Par conséquent, cette information est codifiée différemment selon les personnes à qui elles sont réservées et doivent n'être accessibles qu'à ces personnes.

L'industrie du transport intermodal recherche les moyens les plus efficaces lui permettant de mieux suivre les conteneurs en transit et d'améliorer ainsi la manutention et la capacité de traitement des marchandises, de relever la sécurité des contenus et d'utiliser les technologies de l'échange de données informatisées (EDI). L'utilisation d'étiquettes radiofréquences (RFID) ou de sceaux électroniques n'étant pas généralisée dans l'industrie du transport par conteneurs, l'automatisation de la reconnaissance doit encore passer par l'identification de numéros marqués sur le conteneur même. Le Port de Montréal étant à l'avant garde des moyens lui permettant de rehausser la compétitivité et la productivité de ses installations, s'est lancé dans un projet conjoint avec le Centre de développement des transports de Transport Canada (CDT) pour rendre l'exploitation des conteneurs plus efficace de façon à préserver sa position de leader en tant que terminal de conteneurs. L'objectif est un meilleur suivi des conteneurs, une diminution des retards et une réduction des coûts associés à la manutention, au transit et à la facturation.

Le système utilisé intègre l'identification automatique d'équipement (IAE) à un moteur de reconnaissance optique des caractères (ROC) pour l'identification automatique des wagons et des conteneurs. Ce système est conçu pour identifier en temps réel tous les conteneurs entrant dans la zone ferroviaire du Port de Montréal ou en ressortant. Au moment où le train s'engage dans le terminal et lorsqu'il en sort, le système saisit, archive les numéros des conteneurs et enregistre l'heure d'arrivée ou de départ du train. Équipé de caméras à balayage linéaire ultra-rapides et à haute résolution, celui-ci reconnaît l'image vidéo de chaque numéro d'identification inscrit sur les conteneurs et transmet ces numéros à un ordinateur central. Ces données sont mises en rapport avec

les numéros d'identification des wagons, qui sont 'lus' par un système IAE, ce qui permet de générer instantanément une liste de décompositions du train. (Transport Canada, 2004)

Les critères retenus pour évaluer la performance du système IAE/ROC avaient trait à la précision et au temps de traitement des données. Ce système a été conçu pour reconnaître les codes conformes à la norme ISO sur les conteneurs isolés ou gerbés sur les wagons. La précision minimale exigée était de 80 p. 100 dans toutes les conditions climatiques. En ce qui a trait au temps de traitement des données, l'objectif visé était de 20 minutes après le passage d'un 'train de référence', défini comme un train à deux niveaux de 6 000 pieds chargés à capacité, soit l'équivalent de 120 plates-formes portant chacune un maximum de trois conteneurs. L'étalon était un fonctionnement convenable pour un train roulant à des vitesses de 10 à 20 mi/h (15 à 30 km/h). Ce système a été conçu et mis au point par l'Institut national d'optique (INO) en sous-traitance avec le CDT.

Durant les essais préliminaires de réception menés en 1998 et 1999, le système avait atteint le niveau de performance d'au moins 80 p. cent pour l'identification de conteneurs tandis qu'en 2003, cette performance s'est accrue à 91.31 p. 100 avec 3 359 conteneurs valides. Les changements apportés se sont traduits par une diminution appréciable du temps de transfert de données entre les ordinateurs et par une augmentation de la vitesse de traitement. Des passages de trains sur une distance de 1 309 à 9 821 pieds ont été observés durant les essais de réception. Le délai de traitement du fichier EDI après le passage du train était seulement de 3 minutes versus les 20 minutes préalablement établi.

3.3.6. Évolution de la technologie RFID dans le contexte de la sûreté portuaire

La technologie du RFID ayant un avenir prometteur comme technologie incontournable pour offrir la sûreté de la marchandise, cette section se propose de regarder de plus près son évolution dans le contexte de la sûreté et servira d'élément de réponse dans l'élaboration d'une nouvelle stratégie technologique pour les entreprises X1 et X2.

À travers différents entretiens avec des consultants dans l'industrie, de l'information sur les développements de la technologie du RFID et de son application à la sûreté portuaire a pu être obtenu. En effet, suite à un entretien avec un consultant spécialiste dans la sûreté portuaire, celui-ci a transmis des articles qu'il avait publiés sur les différentes technologies utilisées dans le domaine. En effet, suite à de nombreuses discussions et à des recherches, l'on se rend rapidement compte que l'industrie cherche à développer un nouveau produit à valeur ajoutée, celui du conteneur intelligent. Lors de la conférence de United States Maritime Security Conference à New York en Septembre 2004, 4 entreprises travaillant ensemble ont développé des fonctionnalités sur le conteneur de base pour le rendre plus 'intelligent' et efficace dans le but de décourager et documenter les intrusions possibles. N'ayant pu assister à cette conférence, un résumé des entretiens et une compilation de la documentation récoltée sur les applications du RFID et du conteneur intelligent sont présentés.

Les cargaisons de marchandises voyageant par avion, mer ou terre sont vulnérables au vol, vandalisme et terrorisme. Le FBI estime que le vol de conteneurs se chiffre à plus de 18 G$ par année tandis que le Département de Transport américain évalue les coûts administratifs associés à ces pertes de l'ordre de 20 G$ à 60 G$ (KPMG Technology insider, 2004).

Afin de protéger les envois et réduire les coûts, les compagnies de technologie font la promotion de conteneurs intelligents qui pourraient sécuriser la chaîne d'approvisionnement. En effet, ce nouveau conteneur, en combinant plusieurs technologies telles les ultrasons et l'identification radio-fréquence RFID, est suffisamment sophistiqué pour détecter l'ouverture de portes, et le changement de luminosité à l'intérieur du contenant, de température, vibration ou de volume. De plus, en ajoutant la technologie du GPS, ces conteneurs intelligents peuvent être repérés à travers le monde, et permettent ainsi aux entreprises une meilleure visibilité de la marchandise, l'efficience des opérations et une amélioration du service à la clientèle. Deux études indépendantes évaluent les économies potentielles entre 200 $ et 400 $ par cargo par conteneur pour une amélioration de la sécurisation des conteneurs. Le conteneur intelligent représente un conteneur qui utilise un sceau de haute sécurité dans un endroit autre que la poignée de porte et qui contient un senseur électrique, capable de déterminer les intrusions (P& O Nedlloyd, 2003). Lors de la conférence sur la sûreté maritime ayant eu lieu à New York, E J Brooks, RAE Systems, Savi Technology et Matrics ont dévoilé un nouveau conteneur, celui-ci également intelligent, qui en plus de pouvoir détecter les intrusions, peut également détecter les matières dangereuses et communiquer par ondes radio fréquence sa localisation en temps réel. En effet, ce conteneur ayant été présenté durant cette conférence comportait un sceau de porte senseur par Brooks, un senseur radioactif de RAE Systems, un transpondeur de Savi et des étiquettes passives de Matrics.

La technologie RFID est une composante clé des conteneurs intelligents, qui permet de transmettre l'information à tous les endroits stratégiques d'un port, et offre non seulement le statut de ceux-ci mais aussi garantit l'intégrité de la marchandise. Cependant, le seul inconvénient demeure sa portée limitée. Présentement plusieurs manufacturiers utilisent des cadenas mécaniques de moins de un dollar et des sceaux électroniques variant de 25 $ à 50 $ pour connaître les conditions internes du conteneur (KPMG Technology insider, 2004). En revanche, les conteneurs intelligents avec un prix

maximal par utilisation de 50 $ (RFID Journal, 2004), permettent de faire le suivi en temps réel. Ce qui freine pour l'instant l'utilisation généralisée de cette technologie est son coût, la standardisation non-existente et le souci de piratage possible des étiquettes RFID. Ainsi, une étude récente menée par le groupe Research and Market conclut que l'économie américaine pourrait bénéficier d'économies de l'ordre de 10 G$ par année et de certains avantages tels la réduction des délais et de marchandises égarées, l'amélioration de la fiabilité juste-à-temps, la diminution des inventaires, la diminution des vols et des coûts d'assurance et une moins grande vulnérabilité aux attaques terroristes

Tel que le mentionnait l'un des intervenants auprès de Transport Canada, d'après les tests préliminaires, cette technologie est très prometteuse mais afin d'être efficace sur toute la chaîne d'approvisionnement mondiale, il est nécessaire de pouvoir convaincre les pays d'adopter cette nouvelle technologie et par conséquent de promouvoir une culture internationale de la sûreté.

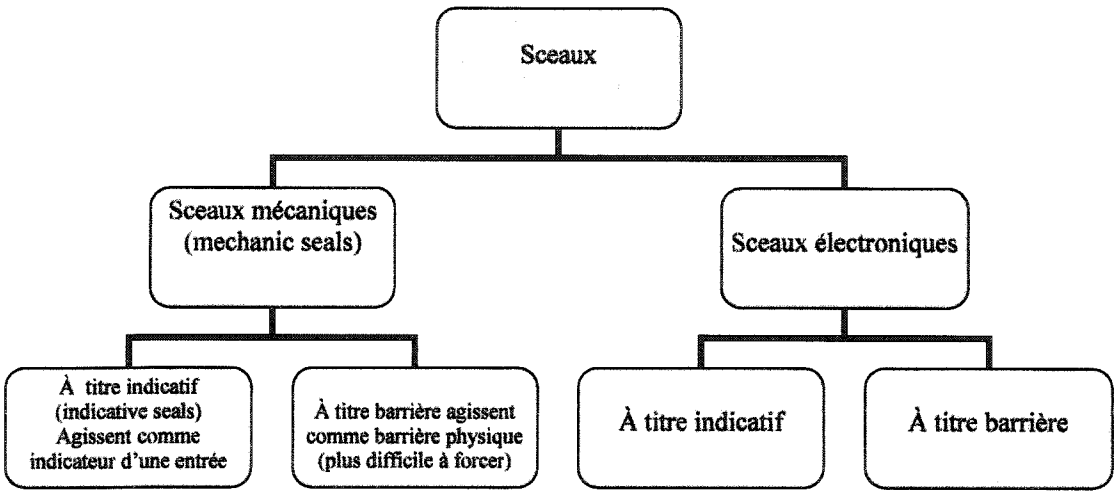
Bien que le conteneur intelligent offre plusieurs fonctionnalités à valeur ajoutée, il est toutefois nécessaire de passer en revue les différentes technologies présentement en utilisation. Les sceaux apposés sur les conteneurs étant un aspect important de la sécurisation de la marchandise contenue dans le conteneur, nous regarderons de plus près les différents sceaux (tableau 3.11). Les sceaux mécaniques sont de trois types, indicatifs, barrière et électronique. Les sceaux indicatifs permettent de déterminer si ceux-ci ont été trafiqués tandis que les sceaux barrières offrent une sécurité physique. Cependant, dans un cas comme dans l'autre les sceaux indiquent s'ils ont été manipulés. En contrepartie, les sceaux électroniques sont des sceaux mécaniques auxquels ont été rajoutées des composantes électroniques et qui peuvent être combinés soit avec une technologie GPS ou une technologie cellulaire. Le tableau ci-dessous présente une liste des avantages et inconvénients de ces différents sceaux tandis que la figure 3.5 présente les différents sceaux sur le marché.

Tableau 3.12 : Type de sceaux mécaniques

	Sceaux indicatifs	Sceaux barrières	Sceaux électroniques hybrides (identification et barrière)
Caractéristiques	• Fabriqués en plastic ou en métal • Peu dispendieux et mécanisme simple • Numéro d'identification unique • Ne doivent pas être utilisés pour créer une barrière physique	• Fabriqués en acier, câble ou un matériel résistant • Plus dispendieux • Permettent bonne barrière à l'entrée	• Sceaux mécaniques associés avec une technologie RF, IF ou fibre optique • Numéro d'identification unique • Possèdent une capacité de mémoire • Souvent associés au GPS
Technologie associée	• Aucune car trop peu chers	• Peuvent être intégrés à un sceau électronique pour obtenir un sceau hybride	• Intégrés avec RF, IF, fibre optique, téléphone cellulaire ou autre technologie pour obtenir un sceau hybride
Intégration et gestion de l'information	• Aucune car trop peu chers	• Peuvent être intégrés à un sceau électronique pour obtenir un sceau hybride	• Permet de répondre aux questions suivantes: qui ? comment ? et où ? • Lecture à distance des données, avant même l'arrivée du conteneur
Approvisionnement et prix	• Prix de quelques sous à quelques	• Prix de 50¢ à quelques	• Prix de 5 $ à 1 000 $ et plus, prix

	dollars • Fabriqués en gros dans les pays du Sud-Est asiatique	dollars • Souvent fabriqués en gros dans les pays du Sud-Est asiatique	élevé donc hésitation du client • Encore à l'état de tests

Adapté de Wolfe, 2002



Adapté de Wolfe, 2002

Figure 3.5 : Les différents sceaux sur le marché

Ainsi, nous observons clairement que les sceaux électroniques offrent différentes possibilités qui rendent leur utilisation intéressante. Cependant, ce qui peut freiner une utilisation massive serait leur prix élevé. Toutefois, pour le transport de marchandises de grande valeur, le coût de ces sceaux devient secondaire face à la visibilité et la sécurisation qu'offrent ces sceaux. Le tableau 3.13 présente la matrice de fonctionnalité des sceaux.

Tableau 3.13: Matrice de fonctionnalité des sceaux

Type de sceau	Indique l'intégrité du conteneur ?	Difficile à percer ?	Peut être contrefait ?	Permet suivi de marchandises ?	Compatible avec d'autres technologies ?
Identification	Oui	Non	Oui	Non	Non
Barrière	Oui	Oui	Oui	Non	Non
Électronique identification	Oui	Non	Possiblement	Oui	Oui
Électronique barrière	Oui	Oui	Possiblement	Oui	Oui

Adapté de Wolfe, 2002

À nouveau, nous remarquons que les sceaux électroniques ont une valeur ajoutée vis-à-vis des autres technologies. Il existe plusieurs types de sceaux électroniques que nous regarderons de plus près à travers le tableau qui suit. Dans le cas de ce mémoire, les sceaux RFID sont les sceaux qui nous sont d'intérêt. Le tableau 3.14 présente les types de sceaux électronique.

Tableau 3.14: Type de sceau électronique

Comparaison des sceaux électroniques		
	Forces	Faiblesses
RFID	• Grandes capacités • En mode passif peu être bon marché • Grande capacité en mode actif et coûts modérés • Pas besoin d'une inspection manuelle	• manque de standards • manque de fréquence globale surtout pour le RFID actif
Infrarouge (IF)	• très efficace pour des portées courtes	• manque de clarté sur les forces et faiblesse-information contradictoire
Contact et près du contact	• certains sont très efficaces même dans des conditions climatiques dificiles • nécessite une intervention humaine pour l'inspection des sceaux	• nécessite intervention humaine • clés de contacts peuvent être perdues ou utilisées abusivement
Éloigné	• Potentiel immédiat pour une identification de problèmes • Potentiel pour couverture globale	• Coût élevé • Nécessite généralement une source de puissance importante
Tous	• Potentiel d'amélioration de l'efficience et de la sûreté	• Risque d'augmentation de la complexité et d'un sentiment de fausse sécurité • Evaluations indépendantes nécessaires

		• Nécessité d'évaluer les impacts opérationnels et la performance technique • Nécessité de pouvoir gérer le flux de données

Adapté de Wolfe, 2002

Ce qui caractérise les sceaux RFID des autres sceaux sont leur grande capacité, la flexibilité qu'ils offrent, et surtout l'absence d'inspection humaine. Cependant, leur lacune demeure le manque de standardisation de cette technologie émergente et l'absence d'une fréquence unique utilisable par tous les continents. Le tableau suivant fait état des fréquences en utilisation de par le monde.

Tableau 3.15: Fréquence des sceaux RF

Sceau RFID et fréquence du transpondeur		
Fréquence (MHz)	**Lieu d'adoption**	**'Promoteurs'**
315	Majorité de l'Asie	Offert comme options par e-Logicity et Hi-G-Tek
433	Europe et Amérique du Nord; certaines régions d'Asie	e-Logicity, Encrypta, and Savi. Utilisé en Europe par Hi-G-Tek et SecuReSeal
915	Amérique du Nord et du Sud	Utilisé aux É.U. par Hi-G-Tek et SecuReSeal Uilisation passive par TransCore
862-928	Recherche une acceptation globale pour des applications de logistiques en mode passif	Uniform Code Council at EAN International
2 450	Japon	Entreprises japonaises et Alien

Adapté de Wolfe, 2002

En analysant ce tableau, nous saisissons mieux l'importance de standardiser cette technologie et d'avoir une fréquence qui puisse être disponible pour une utilisation à l'échelle globale. En effet, le but des sceaux RFID couplés avec le GPS étant d'offrir une plus grande visibilité de la marchandise à l'échelle mondiale, il est important que d'un pays à un autre les standards soient identiques afin que l'information puisse transiger d'un continent à un autre sans entrave technologique. Le tableau 3.16 présente les différents sceaux disponibles sur le marché et leurs fonctionnalités.

Tableau 3.16: Caractéristiques des sceaux RF

Nom du sceau	**eSeal**	**DataSeal**	**ST-605-SL1 SmartSeal**	**AllSeal**	**Navalock+ MacSema**
Vendeur	e-Logicity	Hi-G-Tek	Savi	All Set tracking	CGM
Fréquence RF	433.92 MHz	916 MHZ	433.92 MHz & 123 kHz	2.44 GHz	n/a
Protection conteneur	barrière	indicatif	barrière	indicatif	Anneau ou barreau
Réutilisable?	Non	Oui	Oui	Oui	Non
Input Méthodes et modulation	RS232	RF, 125kHz ou 916 MHz	132 kHz RF	2.44 GHz DSSS, ASK	contact
Output Méthodes et modulations	Actif, toujours allumé, 315 ou 433 MHz	RF, 125 kHz ou 916 MHz	433 MHz, FSK	2.44 GHz DSSS, ASK	contact
Portée	13.3 dB à 21 m	30-80 m (916 MHz)	8 m (132 kHz) 100-300m (433 MHz)	30 m à 80 m	n/a
Protocole de communication	broadcast	query	Query, broadcast	Bluetooth	n/a
Transmission de données	Actif RF	Actif RF	Actif RF	Actif RF	Mémoire contact
Enregsitrement des données	Identification du sceau	Tout	Tout	Tout	Tout

Espace de stockage	Un peu pour l'identification du conteneur	2 kB	32 kB	5 kB	
Mécanisme de sécurité	Non	Encryption 3DES	Mot de passe pour l'identification du lecteur	Authentification de la réponse	
Durée de batterie	3 mois	+4 ans et 50 lectures/jour	5 ans	10 ans	

Adapté de Science Applications International Corporation, 2003

Ainsi, à travers ce parcours des différentes technologies disponibles, nous pouvons affirmer que le RFID pourrait offrir une valeur ajoutée pour la sûreté portuaire qui prendra de l'ampleur avec les efforts de standardisations d'intervenants qui cherchent à mettre de l'avant cette nouvelle technologie.

3.3.7. Pistes d'actions

Stratégie générale

Pour les deux entreprises, le choix de s'être lancées dans un marché de niche celui de la sûreté portuaire a été une bonne chose, car depuis sept. 2001, une attention particulière a été placée sur la sûreté des grands ports du monde entier. En effet, avant cet événement tragique, les autorités gouvernementales avaient déjà souligné plusieurs lacunes auxquels il fallait pallier, et suite au 11 septembre, un intérêt plus marqué et une pression plus importante furent apportés pour solutionner les problèmes auxquels faisaient face les ports. D'autre part, les opportunités ne cessent d'abonder dans le domaine de la sûreté et ne feront que s'accroître dans les années à venir; par exemple aux É.U. en 2003, 36.2 G$ a été réservé pour le Department of Homeland Security (DHS) et une augmentation de 9% du budget a été alloué par le

DHS en 2004 pour la marine américaine (U.S. Coast Guard) qui assure la sûreté des ports et des voies navigables.

Stratégie de différentiation

Étant donné que les joueurs dans ce domaine sont de grandes multinationales qui offrent une gamme complète de produits (ex : Lockheed Martin, Northrop Grumman, Groupe Bechtel etc.), les entreprises X1 et X2 devront se différencier par des solutions innovatrices mais raisonnables en matière de coût, afin d'éviter de se retrouver dans des créneaux dans lesquels ces grandes multinationales sont déjà bien implantées. Il demeure donc important de réaliser des activités de veille stratégique et de surveiller l'évolution des concurrents, dans le but de suivre les tendances du marché mais aussi s'assurer de pouvoir se distinguer en offrant des produits distincts des autres concurrents qui se démarquent par leur contenu à haute valeur ajoutée. Par conséquent, il serait intéressant pour X1 et X2 de participer à des colloques sur la sûreté maritime, tel celui du U.S. Maritime Security Expo ayant lieu à New York en septembre 2005, qui leur permettraient de faire de la veille technologique active, de suivre l'évolution solutions technologiques telles que les sceaux RFID et leurs applications au domaine maritime. Cette exposition serait également un moment privilégié pour les deux entreprises d'établir des contacts clés dans la sûreté maritime.

De plus, les entreprises X1 et X2 devront être flexibles quant à la nature des produits qu'elles offrent et devraient capter précisément les besoins de leurs clientèles. Il s'agit de savoir se différencier par rapport à leurs concurrents en offrant une solution intégrée qui leur permettrait de choisir à travers une gamme complète de produits de prix variés, laissant ainsi le choix au client de choisir la solution intégrée qui lui convient le mieux au prix le plus compétitif. D'après l'étude menée par le gouvernement québécois sur le marché militaire, l'entreprise X2 ayant développé des

compétences par rapport à ses composantes formant le système DATS, peut espérer vendre son savoir-faire auprès des géants militaires américains, ce qui est une porte pour un marché potentiellement intéressant.

Stratégie sur les marchés étrangers

Les marchés des pays en voie d'industrialisation étant en pleine expansion, les entreprises X1 et X2 ont choisi un créneau prometteur avec des initiatives en Afrique. Toutefois la contrepartie demeure les moyens limités et un processus de financement long qui doit se faire auprès des instances bancaires internationales (Banque Mondiale, Fond Monétaire Internationale, Banque Africaine de Développement, Banque Ouest africaine de Développement lorsque applicables et autres Banques de Développement propres aux pays en voie de développement). Afin d'éviter le piège d'être dans le processus fort long de négociation sur le continent africain et de se limiter uniquement à ce marché particulier, l'entreprise X1 qui n'est qu'une PME, devra s'assurer de poursuivre de petits contrats plus sûrs sur des marchés de moindre risque afin de garantir une entrée d'argent continue. Dans le même ordre d'idée, je recommanderais aux entreprises X1 et X2 de diversifier leurs marchés en Europe, en Asie ou au Moyen-Orient pour des ports de moindre importance où ils auront plus de chance d'être retenus. Grâce à l'envergure du projet dans le pays d'Afrique de l'Ouest, un précédent a été établi qui renforce la crédibilité des entreprises X1 et X2 à offrir des solutions en matière de sûreté maritime et portuaire. Le momentum étant favorable, il faut profiter de l'ouverture des marchés face à la sûreté du transport maritime et capitaliser sur leur succès récent.

Stratégie technologique

En ciblant leurs clients et en misant sur le service et en offrant des solutions technologiquement avant-gardiste et de qualité, les entreprises X1 et X2 devraient pourvoir percer.

Les partenariats et alliances que les entreprises X1 et X2 se sont forgés, leur permettent de se concentrer sur leurs compétences clés et d'assurer des solutions complètes et sur mesure à leurs clients. Toutefois, d'autres partenariats devraient être établis avec les entreprises qui oeuvrent dans l'offre de produits de sûreté, afin qu'une gamme complète de produits puisse être offerte aux clients. Pour l'entreprise X1, la technologie RFID représenterait un cheminement normal dans lequel l'entreprise devrait se lancer. De plus, elle bénéficierait d'introduire certaines solutions apportées par des entreprises développant des sceaux électroniques qui utilisent la technologie des puces RFID (e-Logicity, Hi-G-Tek, Savi, All Set tracking, CGM) afin de pouvoir offrir une nouvelle gamme de produits à ses clients présents et futurs. Pour l'entreprise X2, puisqu'elle a choisi d'être d'abord et avant tout un intégrateur de services, elle gagnerait à établir des alliances avec ces mêmes entreprises oeuvrant dans l'application des puces RFID au domaine portuaire (e-Logicity, Hi-G-Tek, Savi, All Set tracking, CGM) afin de réaliser des sites béta et projets pilotes qui permettraient de développer des applications plus bénéfiques et appropriées pour les marchés des pays en voie de développement. Cependant, dans la connaissance des besoins de marchés spécifiques, les entreprises X1 et X 2 en possédant des compétences dans un marché particulier soit celui de l'Afrique, pourraient devenir des intermédiaires entre les entreprises qui développent les sceaux et les clients africains. Étant donné que les sceaux seront bientôt une norme dans l'industrie du transport maritime et de la sûreté, les entreprises X1 et X2 devront tôt ou tard offrir à leurs clients ces solutions.

CONCLUSION

Pour sécuriser la chaîne d'approvisionnement mondiale, les autorités gouvernementales se doivent d'avoir une approche intermodale plus globale. Par ailleurs, la sûreté doit être abordée par une stratégie intégrée qui permettrait de retracer les conteneurs et d'assurer un historique de ces contenus afin de garder le pedigree de toutes marchandises transigeant d'un port à un autre. Puisque les fouilles systématiques sont impossibles, vu le nombre trop important de conteneurs, celles-ci doivent être conduites de manière stratégique en misant sur les services des douaniers, des armateurs de navires et des agences d'intelligence ainsi que sur les nouvelles solutions technologiques telles que les sceaux électroniques et la technologie RFID. Le défi est de taille puisque les cargaisons effectuent plusieurs escales sur maints ports. Il est donc essentiel de bien comprendre le système dans son ensemble pour saisir les nuances et les enjeux de ce contexte parallèle. Tel que le mentionne un des directeurs chez Transport Canada, 'La technologie du RFID a définitivement sa place, cependant il faut étudier la technologie dans son ensemble pour pouvoir maximiser son utilisation'. Une technologie sans comprendre l'environnement dans laquelle celle-ci doit évoluer, serait en effet un investissement substantiel pour un rendement minime. Les É.U. investissent des milliards en R&D pour trouver des solutions technologiques en matière de sûreté, le Canada en revanche y participe de façon plus modeste n'ayant pas les moyens de son voisin. Cependant, le gouvernement canadien, a choisi une approche plus intégrée en regardant au-delà des balises, en travaillant avec d'autres organismes et en faisant des audits auprès des pays en voie de développement nécessitant de l'aide dans l'élaboration de leur programme de sûreté portuaire. Ainsi, le Canada se veut plus visionnaire, en tendant la main dans les domaines politiques et socio-économiques à ses voisins moins nantis.

Les pays en voie de développements ont certains problèmes de gouvernance, qui rendent difficile l'élaboration d'un cadre adéquat favorisant la sûreté. De fait, les ressources manquant, la sûreté n'est pas réellement une priorité pour ces pays. C'est pourquoi il

devient important pour les pays développés d'offrir un soutien continu sur plusieurs années et montrer les bénéfices rattachés à la conformité des normes internationales établies. Les entreprises X1 et X2 peuvent s'inscrire dans cette démarche.

La technologie, bien qu'importante et utile, ne peut à elle seule résoudre le problème de la sûreté dans les ports. Cependant, nous avons démontré dans le cadre de cette étude, que les systèmes de suivi (ACS, ACE et AMS), les systèmes d'inspection (VACIS), la technologie RFID et les sceaux électroniques permettront d'améliorer assurément la sûreté portuaire.

Enfin, comme avenue future de recherche, il serait intéressant de poursuivre l'évolution des entreprises X1 et X2 dans leur adoption du RFID et récolter le taux d'adoption des pays en voie de développement face à cette technologie prometteuse mais encore dispendieuse. De plus, un tableau de comparaison des ports se munissant de cette technologie pourrait être établie, avec le temps d'adoption et les facteurs influençant cette adoption. Toutefois, cette recherche n'ayant pas traité à fond le cas d'un port utilisant présentement le RFID, une prochaine étude pourrait valider l'intérêt réel de cette technologie dans le cadre d'un port en phase d'essais et d'adoption de la technologie.

Ainsi, le but de cette étude étant de déterminer la pertinence du RFID en matière de sûreté maritime et portuaire, nous avons démontré à travers cette étude que le RFID permet en effet une meilleur traçabilité de la marchandise et par conséquent un accroissement de la sûreté, toutefois, nous concluons en insistant que cette technologie doit s'intégrer à d'autres technologies et méthodes existantes et ne peut présenter à elle seule une panacée pour les problème de sécurisation de la marchandise ou des infrastructures portuaire.

BIBLIOGRAPHIE

ABERNATHY, W. J. *The productivity dilemma : roadblock to innovation in the automobile industry.* Baltimore : Johns Hopkins University Press. 267 p.

ABERNATHY, W. J., UTTERBACK, J. (1978). '*Patterns of industrial innovation.*' Technology Review (80) 7. 40-47 p

ABERNATHY, W. J., CLARK, K. , KANTROW, A. M. (1983). *Industrial Renaissance.* New York: Basic Books. 194 p.

ACDI. (2004). *Évaluation de l'Impact Social Prévisionnel dû à l'Introduction d'Outils et de Mesures de Sûreté dans le Port Autonome de Dakar.*

AÎT-EL-HADJ, S. (1989). *L'entreprise face à la mutation technologique.* Paris: Éditions d'organisation. 258 p.

ALDRICH, H. E. (1979). *Organizations and Environments.* Englewood Cliffs, NJ: Prentice Hall. 384 p.

ARTHUR, W. B. (1988). 'Competing Technologies: An Overview'. In G. Dosi et al (eds). *Technical Change and Economic.* Pinter, London. 590-607 p.

ASTLEY, W. G. (1985). ,The Two Ecologies: Population and Community Perspectives on Organizational Evolution.' *Administrative Science Quarterly 30.* 224 –241 p.

ALLIED BUSINESS INTELLIGENCE. *RFID white paper.* (2002). Oyster Bay, NY. 14 p. [Ën ligne].www.alliedworld.com

ASSOCIATION OF CANADIAN PORT AUTHORITIES. (2004). *Charting A Course for Tomorrow – Today*. [En ligne]. www.acpa-ports.net/

ASSOCIATION OF CANADIAN PORT AUTHORITIES. (2004). *Submission to Transport Canada On Proposed Marine Transportation Security Regulations*. In site Association of Canadian Port Authorities. [Ën ligne]. www.acpa-ports.net/psecure/coalition_committee04.pdf

ASSOCIATION FOR AUTOMATIC IDENTIFICATION AND MOBILITY. RFID bootcamp. Standards. Warrendale, PA. [En ligne]. http://www.aimglobal.org/standards/

Barcodes (2004) [Ën ligne]. http://www.tkb-4u.com/code/barcode/aztec.php

BÉLANGER, Y. (1997). *La Reconversion des Entreprises Militaires: Quel Rôle pour l'État et Comment le Canada Peut-il Aborder la Question ?* p 687-709. Revue Canadienne de Science Politique, 30.

BERGER, D. L. *Industrial security*. 1st ed. (1979). Los Angeles : Security World Pub. Co. 361 p.

BURGELMAN, R. A. (1983). 'Corporate Entrepreneurship and Strategic Management: Insights from a Process Study'. *Management Science 29, 1349-1364 p.*

BURGELMAN, R. A. (1986). 'Strategy Making and Evolutionary Theory: Towards a Capabilities-Based Perspective.' In M. Tsuchiya (ed.). *Technological Innovation and Business Strategy*. Tokyo: Nihon Keizai Shinbunsha.

BURGELMAN, R. A. (1988). 'Strategy-Making as a social Learning Process: The Case of Internal Corporate Venturing.' *Interfaces* 18, no.3 (May-June), 74-85 p.

BURGELMAN, R. A.(1991). 'Intraorganizational Ecology of Strategy Making and Organizational Adaptation: Theory and Field Research.' *Organization Science* 2, 239-262 p.

BURGELMAN, R. A. (1994). 'Fading Memories: A process Theory of Strategic Business Exit in Dynamic Environments.' *Administrative Science Quarterly* 39.

BURGELMAN, R. A., Sayles L.R.(1986). *Inside Corporate Innovation.* New York: Free Press.

BURGELMAN, R. A., Rosenbloom, R. S. (1989). 'Technology Strategy: An Evolutionary Process Perspective.' In R.S. Rosenbloom and R.A. Burgelman (eds.), *Research on Technological Innovation, Management, and Policy*, vol. 4. 1-23 p. Greenwich, CT, JAI Press.

BURGELMAN, R. A, MAIDIQUE, M. A., WHEELWRIGHT, S. C. *Strategic Management of Technology and Innovation.* 2nd edition. Irwin. p 923

CAMPBELL, D.T. (1969). 'Variation and Selective Retention in Sociocultural Evolution.' *General Systems.* 14, 69-85 p.

CLARK, K.B. (1985). 'The Interaction of Design Hierarchies and Market Concepts in Technological Evolution.' *Research Policy.* 14, 235-251 p.

CLARK, K.B. (1987). 'Managing Technology in International Competition: The Case of Product Development in Response to Foreign Entry.' In M. Spence and H. Hazard (eds.), *International Competitiveness*, 27-74 p. Cambridge, MA: Ballinger.

COOPER, A.C., and SCHENDEL, D. (1976). 'Strategic Responses to Technological Threats.' *Business Horizons* (February), 61-63 p.

CANADIAN SHIPOWNERS ASSOCIATION. (2003). *Proud of the Past: Focused on the Future, Safety and security Panel.* 66th Annual Joint Conference.

CANADIAN SHIPOWNERS ASSOCIATION. (2004). *Managing Change and Moving On, Panel: the New Security Regime.* 67th Annual Joint Conference.

CARD TECHNOLOGY TODAY. *Another link in the chain.* April (2004).

CHAMBRE REGIONALE DE COMERCE ET D'INDUSTRIE CHAMPAGNE-ARDENNE. Décembre (2003). *Dossier technique: les étiquettes communicantes.* Version 2. 21 p. [En ligne]. www.champagne-ardenne.cci.fr

CIMON, Y. (2000). *Stratégies de Diversification des Entreprises Militaires.* P 187. École des Hautes Études Commerciales Montréal.

CHIN, L-P, WU, C-L. (2004). *The role of Electronic Container Seal (E-Seal) with RFID Technology in the Container Security Initiatives.* IEEE Computer Society.

DAVIS, B. M. *La France nucléaire: matières et sites.* (2001). WISE-Paris. [En ligne]. http://www.francenuc.org/index.html

DAVIS, P.A. (1985). 'Clio and the Economics of QWERTY.' American *Economic Review.* 75, no. 2 (MAY), 332-337 p.

DÉVELOPPEMENT ÉCONOMIQUE ET RÉGIONAL ET RECHERCHE. (2004). *La Sûreté Intérieure aux États-Unis.* [En ligne]. www.mderr.gouv.qc.ca

DENZIN, N. K., LINCOLN, Y. S., 2nd ed. (2000). *Handbook of Quantitative Research.* Oaks, CA: Sage Publications. 1143 p.

Dictionnaire des arts médiatiques (1996)
Groupe de recherché en arts médiatiques –UQAM. [En ligne]. http://www.comm.uqam.ca/~GRAM/C/MT/inf/inft47.html

DONALDSON, G., LORSCH, J.W. (1983). *Decision Making at the Top.* New York: Bani Books.

DOSI, G. (1982). 'Technological Paradigms and Technological Trajectories: A suggested Interpretation of the Determinants and Directions of Technical Change.' *Research Policy.* 11, 147-162 p.

EISENHARDT, K., BOURGEOIS, L. J. (1998). *Politics of Strategic decision making in high velocity environments: Toward a mid-range theory.* Academy of Management Journal, 31, 737-770 p.

EMERSON, S. D., NADEAU, J. (2003). *A Coastal Perspective on Security.* p 1-13. Journal of Hazardous Materials, Volume 104, Issues 1-3.

EMERSON, R. M., 2nd ed. (2001). *Contemporary Field Research: Perspective and Formulations* . Boston: Waveland Press. 433 p.

ENTREPRISE MÈRE. (2004). *Annual Report 2003.* In site Entreprise mère.

ENTREPRISE X1. (2003). *Études Préliminaire des Besoins du PAD.*

ENTREPRISE X2. (2004). *Présentation aux Autorités du Port Autonome de Dakar.*

ENTREPRISE X2.(2004). *Systèmes de Sûreté Maritimes.*

EVANS, F. (2004). *Maritime and Port Security. Securing the Nation: Issues in American National Security since 11 septembre* . Philadelphia: Chelsea House. 112 p.

FARRELL, F., SALONER, G. (1987). 'Competition, Compatibility, and Standards: The Economics of Horses, Penguins, and Lemmings.' In G. Landis (ed.), *Product Standardization and Competitive Strategy.* New York: Elsevier. 1-21 p.

FINKENZELLER, K. (2003). *RFID handbook : fundamentals and applications in contactless smart cards and identification.* 2nd ed. Chichester, England ; Hoboken, N.J. : Wiley. 427 p.

FRITELLI, J. F., LEE, M. R., MEDALIA, J., O'ROURKE, D., PERL, R. (2003). *Port and Maritime Security (Background and Issues).* New York: Novinka. 96 p.

GLASER, B., STAUSS, A. (1967). *The discovery of grounded theory: Strategies of qualitative research.* Aldine. 271 p.

GUBRIUM, J. F., HOLSTEIN, J. A. (1997). *The New Language of Qualitative Method.* New York: Oxford University Press. 256 p.

HADDOW, G. D., BULLOCK, J. A. *Introduction to emergency management.* (2003). Amsterdam : Butterworth-Heinemann. 275 p.

HALLBERG, J., NILSSON, M. (2002). *Positioning with Bluetooth, IrDA and RFID.* 58 p. Master of Science Programme, Lulea University of Technology, Department of computer science and electrical engineering.

HENDERSON, R. M., CLARK, K.B. (1990). 'Architectural Innovation: The Reconfiguration of Existing Product Technologies and the Failure of Established Firms.' *Administrative Science Quarterly.* 35, 9-30 p.

INTERNATIONAL MARITIME ORGANIZATION. (2003). *ISPS Code*. p 141. IMO publication. London, UK.

KAMBIL, A., BROOKS, J. D. June (2002). *Auto-ID across the value chain: from dramatic potential to greater efficiency & profit*. Cambridge , MA: Auto-ID center, Accenture. 22 p.

KELLY, P., KRANZBERG, M. (1978). *Technological Innovation: A Critical Review of Current Knowledge*. San Francisco Press.

KING, J. (2004). *The Security of Merchant Shipping.* Cardiff University, UK. Marine Policy, Corrected Proof, In Press.

KINSELLA, B. March (2004). *RFID – it's more than tags and standards.* Sapient. 4 p. [En ligne]. www.usingrfid.com

KIPP, J. D., LOFLIN, M. E. (1996). *Emergency incident risk management : a safety & health perspective.* New York ; Toronto : Wiley. 303 p.

KPMG. (2004). *Securing the Supply Chain with Smart Containers.* KPMG Technology Insider. [En ligne]. www.kpmginsiders.com

KVALE, S. (1996). *Interviews: An Introduction to Qualitative Research Interviewing.* Thousand Oaks, CA: Sage Publications. 344 p.

LABBÉ, H. (2003). *Le risque nucléaire.* [Paris] : Presses de sciences po. 135 p.

LÉGER, P. M. (1999). *De la réflexion stratégique au sein de le nouvelle économie: principes structurant l'analyse d'une chaîne de valeur famille-produit.* École Polytechnique de Montréal. 115 p.

LEONARD-BARTON, D. (1992). 'Core Capabilities and Core Rigidities: A Paradox in New Product Development.'*Strategic Management Journal* 13 (Special Issue, Summer). 111-126 p.

LEVITT, B., MARCH, J. G. (1988). 'Organizational Learning.' *Annual Review of Sociology 14.*

LEWIS, B. (2002). *Port Security: Container Targeting and Inspection Procedures of the United States and Singapore.* The Logistics Institute, Georgia Tech and The Logistics Institute, Asia Pacific, National University of Singapore.

LOJKINE, J. (2002). *Les Sociologies critiques du capitalisme.* 1re éd. Paris : Presses universitaires de France. 236 p.

MARX, B. (1979). *L'économie capitaliste.* Paris : Editions Sociales. 281 p.

MCKELVEY, B., ALDRICH, H.E. (1983).'Populations, Oganizations, and Applied Organizational Science.' *Administrative Science Quarterly* 28, 101-128 p.

METCALF, J.S., GIBBONS, M. (1989). 'Technology, Variety, and Organization: A Systemic Perspective on the Competitive Process.' In R.S. Rosenbloom and R.A. Burgelman (EDS.), *Research in Technological Innovation, Management and Policy*, vol.4, 153-194 p. Greenwich, CT: JAI Press.

MODERN BULK TRANSPORTER. (2004). *Three Companies Unveil Smart Intermodal Container.* [En ligne]. www.findarticles.com

NATIONS UNIES. (2003). *Mesures Visant à Empêcher les Terroristes d'Acquérir des Armes de Destruction Massive, Rapport du Secrétaire Général.* In site Nations Unies. [En ligne]. www.un.org

NATIONS UNIES. (2003). *Étude sur les Transports Maritimes 2003.* Conférence des Nations Unies sur le Commerce et le Développement. In site Nations Unies. [En ligne]. www.un.org

NELSON, R.R., WINTER, S.G. (1982). *An evolutionary Theory of Economic Change*. Cambridge: Harvard University Press.

NIEMEYER, A., PAK, M. H., RAMASWAMY, S. E. (2003). *Smart tags for your supply chain.* Number 4. The McKinsey Quarterly. 3 p.

OCDE. (2002). *Logistique des Transports, Défis et Solutions.* [En ligne]. www.ocde.org

OCDE. (2001). *Transport et Développement Économique, Table ronde.* [En ligne]. www.ocde.org

P&O Nedloyd. (2003). *The Smart Container in Us Trades*. News Archive. [En ligne]. http://www.ponl.com/topic/home_page/language_en/newsroom/news/latest_news?action=item&usetemplate=archive_news_item&resourceitem_no=10516

PENBROSE, E.T. (1995). *The Theory of the Growth of the Firm*. Oxford University Press. 3 rd edition. 272 p.

PERROW, C. (1986). *Complex organizations: A critical essay.* 3rd edition. McGraw-Hill Humanities. 3rd edition. 307 p.

PFEFFER, J. (1982). *Organizations and organization theory.* Marshfield, MA: Pitman.

PORT DE MONTREAL. (2004). *Statistiques*. [En ligne]. http://www.port-montreal.com/site/index.jsp?lang=fr

PORTER, M. E. (1980). *Competitive Strategy.* New York : Free Press. 396 p.

PORTER, M. E. (1983). 'The Technological Dimension of Competitive Strategy.' In R.S. Rosenbloom (ed.), *Research on Technological Innovation, Management and Policy*, vol.1, pp. 1-33

PORTER, M. E. (1985). *Competitive Advantage*. New York: Free Press.

RAYNAUT, J. (2001). *Sûreté Maritime et Concurrence Portuaire: les Enjeux pour l'Europe.* p 127. Faculté de Droit et de Science Politique d'Aix-Marseille III. Université d'Aix-Marseille III.

RED HERRING. (2004). *Harboring Destruction.* [Ën ligne]. www.redherring.com

REDPRAIRIE. December (2003). *RFID: just the facts.* 16 p. [Ën ligne]. www.RedPrairie.com

RESEARCH AND MARKETS. (2004). *2004-2012 – Maritime Smart Container Market/Technology Forecast Report.* In site Research and Markets.
www. researchandmarkets.com

Research article
DIEGEL, O., BRIGHT, G., POTGIETER, J.
<<Bluetooth ubiquitous networks: seamlessly integrating humans and machines>>
Assembly Automation Volume 24. Number 2. (2004) pp.168-176

RFID JOURNAL. (2003). *Building a Smarter Container.* [En ligne]. www.rfidjournal.com

ROACH, J. A. (2004). *Initiatives to Enhance Maritime Security at Sea.* p 41-66. Marine Policy, Volume 28, Issue 1.

SAP INSIDER. (2004). *The path to the RFID-Enabled supply chain for immediate compliance and rapid ROI.* July-August 2004.
SAVI TECHNOLOGY. (2002). *Industry Launches Port, Shipping Security Initiative-Smart and Secure Tradelanes.* [En ligne]. www.acpa-ports.net/psecure/tradelns.pdf

SCIENCE APPLICATIONS INTERNATIONAL CORPORATION. (2003). *Container Seal Technologies and Processes Phase 1.* U.S. Department of Transportation Maritime Administration

SELZNICK, P. (1957). *Leadership in Administration.* New York: Harper and Row.

SHAFFIR, W. B., STEBBINS, R. A. (1991). *Experiencing Fieldwork: An Inside View of Qualitative Research.* Newbury Park, CA: Sage Publications. 288 p.

SHEFFI, Y. (2004). *RFID and the Innovation Cycle.* The International Journal of Logistics Management. Volume 15, Number 1. pp. 1-10.

SILVERMAN, D. (1999). *Doing Qualitative Research: A Practical Handbook.* Thousand Oaks, CA: Sage Publications. 336 p.

STANDING SENATE COMMITTEE ON NATIONAL SECURITY AND DEFENSE. (2004). *National Emergencies: Canada's Fragile Front Lines, Volume 1.* Standing Senate Committee on National Security and Defense.

STANFORD STUDY GROUP. (2003). *Container Security Report.* p 39.

STATISTIQUE CANADA. (2003). *Les futurs rivalités entre les ports pour conteneurs du Canada et des États-Unis.* [Ën ligne]. www.statcan.ca

TEECE, D. I. (1986). 'Profiting from Technological Innovation: Implications for Integration, Collaboration, Licensing and Public Policy.' *Research Policy 15*, pp. 285-305.

TEECE, D. I., PISANO, G. SHUEN, A. (1990). 'Firm Capabilities, Resources, and the Concept of Strategy.' Working Paper #90-9, University of California at Berkeley, Center for Research in Management.

The University of Reading (2004)

Disponible en ligne:
http://www.rdg.ac.uk/AcaDepts/kc/CMandE/IT_in_construction/Autoid.htm

TRANSPORTATION RESEARCH BOARD OF THE NATIONAL ACADEMIES. (2002). *Deterrence, Protection and Preparation.* Special report 270. [En ligne]. www.trb.org

TRANSPORTATION RESEARCH BOARD OF THE NATIONAL ACADEMIES. (2004). *The Marine Transportation System and the Federal Role, Measuring Performance, Targeting Improvement.* In site of Transportation Research Board. [En ligne]. www.trb.org

TRANSPORT CANADAOPÉRATIONS DE LA SURETE MARITIME. (2004). *Directives Opérationnelles de Sûreté Maritime*. In site Gouvernement du Canada.

TRANSPORT CANADA.(2004). *Canada's Approach to Marine Security*. [En ligne]. www.tc.gc.ca

TRANSPORT CANADA. (2004). *New Marine Security Initiatives*. [En ligne]. www.tc.gc.ca

TRANSPORT CANADA. (2004). *Canada's Marine Transportation System*. [En ligne]. www.tc.gc.ca

TRANSPORT CANADA. (2004). *AEI/OCR system verification (TP 14143E).* [En ligne]. www.tc.gc.ca

TRANSPORT CANADA. (2004). *Automated container ID recognition (TP 13295E).* [En ligne]. www.tc.gc.ca

TRANSPORT CANADA. (2004). *AEI/OCR system integration (TP 13880E).* [En ligne]. www.tc.gc.ca

TRANSPORT CANADA. (2004). *Système intégré d'identification automatique d'équipements et de reconnaissance optique de caractères (IAE/ROC).* [En ligne]. www.tc.gc.ca

TRANSPORT Canada. (2003). *Sûreté Maritime, Contrôle des Navires par l'État du Port. Rapport Annuel 2002.* [En ligne]. www.tc.gc.ca

TUSHMAN, M. L., ANDERSON, P. (1986). 'Technological and Organizational Environments.' *Administrative Science Quarterly* 31, pp. 439-465

TUSHMAN, M. L., ROSENKOPF, L. (1992). ,Organizational Determinants of technological Change.' In B. Staw and L. Cummings (eds.), *Research in Organizational Behavior*, vol. 14, pp. 311-325. Greenwich, CT: JAI Press.

TWISS, B. (1980). Managing Technological Innovation. London: Longman.

U.S. CUSTOMS AND BORDER PROTECTION. (2004). *Programmatic Environmental Assessment for Gamma Imaging Inspection Systems.* U.S. Department of Homeland Security.

U.S. DEPARTMENT OF TRANSPORTATION. (2004). Industry Survey Series: Mainstream Container Services 2003.

U.S. TREASURY ADVISORY COMMITTEE ON COMMERCIAL OPERATIONS OF THE UNITED STATES CUSTOMS SERVICE (coac). (2002). *Report on Seal*

Technologies. Subcommittee on U.S. Border Security Technical Advisory Group. Volume 7.

UNISYS. *A secure supply chain blueprint.* (2004). In site Unisys.

UNITED STATES GENERAL ACCOUNTING OFFICE. (2003). *Customs Service Modernization. Automated Commercial Environment Progressing, but Further Acquisition Management Improvements Needed.* In site United States General Accounting Office.

UNITED STATES GENERAL ACCOUNTING OFFICE. (2004). *Substantial Work Remains to Translate New Planning Requirements into Effective Port Security.* In site United States General Accounting Office.

UNITED STATES EMBASSY, TOKYO, JAPAN. (2003). *Container Security Initiative Now Operational in Singapore.* In United States Embassy. [En ligne]. http://japan.usembassy.gov/e/p/tp-20030319a4.html.

UTTERBACK, J., ABERNATHY, W. J. (1975). , A Dynamic Model of Product and Process Innovation.' *Omega 3*, no 6, pp. 639-656.

VAN DE VEN, A. H., GARUD, R. (1989). 'A Framework for Understanding the Emergence of New Industries.' In R. S. Rosenbloom and R. A. Burgelman (eds.), *Research on Technological Innovation, Management, and Policy*, vol. 4, pp. 195-226. Greenwich, CT: JAI.

WEICK , K. (1979). *The Social Psychology of Organizing.* Reading, MA: Addison-Wesley.

WHITE HOUSE OFFICE OF COMMUNICATIONS. (2004). *Protecting America's Seaports and Securing Cargo Shipments*. [En ligne]. http://www.aapa-ports.org/govrelations/Port%20Security%20Fact%20Sheet%202-04.pdf

WHITE HOUSE OFFICE OF COMMUNICATIONS. (2004). *Protecting America's Seaports and Securing Cargo Shipments*. In site White House Office of Communications.

WOLFE, M. (2003). *Automating Cargo Security: Do Electronic Seals Make Sense?* [Ën ligne]. http://www.eyefortransport.com/index.asp?news=34832

WOLFE, M. (2002). E*lectronic Cargo Seals: Context, Technologies, and Marketplace.* http://ops.fhwa.dot.gov/freight/publications/eseal_wp_final_july12/eseal_wp_final_01.htm

WORLD TRADE ORGANIZATION. (2003). *International Trade Statistics*. [En ligne]. www.wto.org

YIN, R. (1981). *The case study crisis: Some answers.*Administrative Science Quaterly, 26. 58-65 p.

YIN, R. (2002). *Case study research.* Beverly Hills, CA: Sage publications. 3rd ed. 300 p.

ZEBRA TECHNOLOGIES. *RFID: the next generation AIDC*. Application white paper. 2004. 8 p.

ZEBRA TECHNOLOGIES. *The basics of barcoding*. Application white paper. 2004. p 19.