Future Utilization of RFID Technology in the DND Supply and Distribution System

Albert Lam
CANOSCOM Operational Research

Patricia Moorhead
CANOSCOM Operational Research

DRDC CORA TM 2007–68
December 2007

Defence R&D Canada
Centre for Operational Research and Analysis

CANOSCOM Operational Research Team
Canadian Operational Support Command

National Defence Défense nationale

Canada

Future Utilization of RFID Technology in the DND Supply and Distribution System

Albert Lam
CANOSCOM Operational Research

Patricia Moorhead
CANOSCOM Operational Research

DRDC – Centre for Operational Research and Analysis

Technical Memorandum
DRDC CORA TM 2007-68
December 2007

Author

Albert Lam Patricia Moorhead

Approved by

R.M.H. Burton
Acting Section Head, Joint and Common Operational Research

Approved for release by

D. Haslip
Acting Chief Scientist

The information contained herein has been derived and determined through best practice and adherence to the highest levels of ethical, scientific and engineering investigative principles. The reported results, their interpretation, and any opinions expressed therein, remain those of the authors and do not represent, or otherwise reflect, any official opinion or position of DND or the Government of Canada.

Abstract

This report presents recommendations for future utilization of Radio Frequency Identification (RFID) technology in the Department of National Defence (DND) supply and distribution systems. The recommendations are based on the lessons learned from the recent RFID project and an analysis of some of the choices the department has for different aspects of the technology.

Based on the analysis performed, the best plan of action for the utilization of RFID in the DND supply and distribution system includes using barcodes for item level tracking and active RFID tags for consignment tracking, and transitioning to a solely Canadian based information technology infrastructure.

The Canadian Forces global in-transit visibility (GITV) strategy is still under development; hence this report was produced without departmental strategic guidance. It is imperative for DND to clearly state a GITV strategy before any automated identification technology system is implemented on a large scale.

Résumé

Le présent rapport présente des recommandations pour l'utilisation future de la technologie d'identification par radio-fréquence (RFID) dans les systèmes d'approvisionnement et de distribution du ministère de la Défense nationale (MDN). Les recommandations sont basées sur les leçons tirées du récent projet RFID et sur une analyse de certaines des options qui s'offrent au ministère quant à différents aspects de la technologie.

Selon l'analyse effectuée, la meilleure stratégie d'utilisation de la technologie RFID dans les systèmes d'approvisionnement et de distribution du MDN inclut l'utilisation de codes à barres pour le suivi au niveau des articles et l'utilisation d'étiquettes RFID actives pour le suivi des livraisons, ainsi que la transition vers une infrastructure de technologie de l'information entièrement canadienne.

La stratégie globale de visibilité en cours de transfert (GITV) des Forces canadiennes est encore en cours d'élaboration ; par conséquent, le présent rapport a été produit sans orientation stratégique ministérielle. Il est impératif que le MDN établisse clairement une stratégie pour la technologie GITV avant qu'un système de technologie d'identification automatisé soit implanté à grande échelle.

This page intentionally left blank.

Executive summary

Introduction

The purpose of this report is to present recommendations for future utilization of Radio Frequency Identification (RFID) technology in the Department of National Defence (DND) supply and distribution systems. By drawing from lessons learned during the recent RFID project, and analysing some of the choices the department has for different aspects of the technology, this report aims to produce a series of recommendations for the way ahead.

It is imperative for DND to clearly state a Global In-Transit Visibility (GITV) strategy before any Automated Identification Technology (AIT) system is implemented on a large scale. The strategy will provide a direction for AIT technologies in general, providing requirements and constraints for their use. This report is produced without a Canadian Forces (CF) GITV strategy for guidance, and therefore only aims to maximize the benefits of the technology while balancing security and integration of RFID with the barcode system currently in use.

IT Infrastructure Options for the Way Ahead

Three options for an RFID Information Technology (IT) infrastructure within DND were considered and compared. These three options were as follows.

Option #1:

- Make the procedural and operational changes recommended in the RFID Project Lessons Learned (LL) process.
- Continue using the United States (US) server to store RFID In-Transit Visibility (ITV) information.
- Procure additional tags and readers to expand visibility to more consignments.

Option #2: The same three recommendations as Option #1, plus

- Enhance functionality and resilience of the IT system by developing a secure and reliable connection between the US server and the CF National Movement and Distribution System.
- Develop an interface that allows information from all consignment related systems to be displayed at the same time.

Option #3:

- Make the procedural and operational changes recommended in the RFID Project LL process.

- Migrate away from the use of the US server to a Canadian server for storing RFID ITV information.
- Procure additional tags and readers to expand visibility to more consignments.
- Integrate the RFID ITV information on the Canadian server with other Canadian consignment information systems and decision-making tools.
- Develop an interface that allows information from all consignment related systems to be displayed at the same time.
- Maintain interoperability with allies, ensuring Canadian RFID tag information can be routed securely and reliably to the Canadian server.

Evaluation Criteria and Assumptions

Through general research in the area, basic requirements for an AIT system were determined. As well, a vision from an operational perspective for the future of the distribution IT system (a network of servers that provide consignment and tracking information, allowing users to order materiel when needed) was examined. Based on this background research, the following criteria were developed for evaluating the above three proposals for the way ahead with regards to potential IT infrastructure options. The recommended plan of action should:

a. minimize costs;

b. be programmed and operational in the shortest amount of time possible;

c. be reliable under a maximum number of conditions and circumstances;

d. allow for rapid transition into new systems given short notice and be robust against any changes/adjustments that may need to be made;

e. minimize the need for manpower for its operation and maintenance; and

f. should be secure and not expose personnel and equipment/materiel to an increased risk of discovery and targeting, and the consignment information should be made available on a need to know basis only.

Each criteria was weighted low, medium or high, based on the amount of influence each has in determining how favourable a particular option is. Quantitative values were then assigned to these weightings.

The evaluation of the proposed plans for the way ahead was based on the following assumptions.

- Current hardware is fully interoperable with North Atlantic Treaty Organisation (NATO) and its allies.

- Any implemented AIT IT system can be designed to meet the Memorandum of Understanding (MOU) for consignment information sharing between NATO and its allies.
- Any ITV capability can be integrated into other Canadian information systems and related decision making tools.

Results

A computational decision making method was used to analyse the options proposed and it was determined that Option #3 is the best option. Within the evaluation, it was rated as the best choice for reliability, scalability and security, all three of which are the key advantages to having a Canadian owned RFID ITV information server. Eliminating the need for correspondence with the US for Canadian RFID tag information gives DND more control over the system and minimizes reaction time to any changes that need to be made. The main issue with this option is that it requires development time and money that the other options do not require.

Option #3 describes a slightly more mature RFID system within DND that allows greater flexibility and security. Option #2 can be implemented on a much shorter time frame allowing a more rapid improvement to the functionality of the system, and could serve as an intermediate step towards Option #3.

Recommendations

DND should have a Canadian hosted server for RFID data, and it must be integrated with the rest of the consignment related systems in the department. Also, a user interface must be developed that allows RFID data and consignment contents to be viewed simultaneously.

Individual items should continue to be tagged with barcodes for the time being; transition to passive RFID tags may occur when the volume of items increases enough to make this a viable option. Consignments should be tagged with active RFID tags.

Consignment content information, as well as handling and safety instructions should be stored directly on the active RFID tags. Precautions to maximize information security, such as encryption and blocking radio signals while in transit and storage, must be taken. It is assumed that the necessary level of interoperability with NATO and allies will be maintained in terms of hardware (readers and tags) and information sharing.

A highly customized and homogenous training program that puts an emphasis on troubleshooting and general operation must be developed. Also, retaining at least one person experienced in using the RFID technology in the CF context at each RFID enabled location at any given time is important.

Support and maintenance tasks should be contracted out, however management responsibilities for the RFID capability must be retained within DND.

Conclusion

RFID ITV technology will inevitably play a part in DND supply and distribution systems. Based on the analysis performed herein, the best plan of action for the utilization of RFID in the DND supply and distribution system includes: using barcodes for item level tracking; using active RFID tags for consignment tracking; and transitioning to a solely Canadian based IT infrastructure.

Two key requirements for any AIT/ITV capability within DND are: interoperability with NATO and Canadian allies; and ease of integration into the existing DND distribution processes and related information systems. It was assumed throughout the analysis that any AIT/ITV capability adopted by DND will be structured to meet these requirements, through appropriate choices of hardware and software products.

Albert Lam, Patricia Moorhead; 2007; Future Utilization of RFID Technology in the DND Supply and Distribution System; DRDC CORA TM 2007–68; DRDC – Centre for Operational Research and Analysis.

Sommaire

Introduction

L'objectif du présent rapport est de formuler des recommandations au sujet de l'utilisation future de la technologie d'identification par radiofréquence (RFID) au sein des services d'approvisionnement et de distribution du ministère de la Défense nationale. Ce rapport se fonde sur les leçons retenues au cours du récent projet de RFID et sur des choix qui s'offrent au ministère dans certains domaines d'application de cette technologie pour formuler une série de recommandations pour l'avenir.

Il est impératif que le MDN énonce clairement une stratégie de visibilité en transit mondial (GITV) avant que l'on ne mette en place tout système de technologie d'identification automatisée (AIT) à grande échelle. Cette stratégie définirait l'orientation générale des technologies d'identification automatisée, énonçant les besoins et les contraintes s'appliquant à leur usage. Le présent rapport est rédigé sans s'appuyer sur une telle stratégie de GITV des Forces Canadiennes, et il vise alors à maximiser les avantages de cette technologie, mais en préservant un équilibre avec la sécurité et l'intégration des technologies RFID au système de codes à barres en usage.

Options d'infrastructure de TI pour le chemin à suivre

Trois options d'infrastructure de technologie de l'information (TI) RFID au sein du MDN ont été envisagées et comparées. Ces trois options sont les suivantes :

Option 1 :

- Apporter les modifications procédurales et opérationnelles recommandées au cours du processus de leçons retenues du projet RFID.
- Continuer d'utiliser le serveur des États-Unis pour stocker l'information RFID de visibilité en transit (VIT).
- Se procurer des étiquettes et des lecteurs additionnels afin d'appliquer la visibilité à un plus grand nombre de chargements.

Option 2 Mêmes recommandations que l'option 1, mais en plus :

- Améliorer la fonctionnalité et la résilience du système de TI en établissant une liaison sécurisée et fiable entre le serveur américain et le Système national de distribution du matériel (SNDM) des FC.
- Développer une interface qui permettrait l'affichage simultané de toute l'information provenant de tous les systèmes liés à un chargement.

Option 3

- Apporter les modifications procédurales et opérationnelles recommandées au cours du processus de leçons retenues du projet RFID.

- Migrer de l'utilisation du serveur des É.-U. et passer à un serveur canadien pour le stockage information RFID de visibilité en transit.
- Se procurer des étiquettes et des lecteurs additionnels afin d'appliquer la visibilité à un plus grand nombre de chargements.
- Intégrer l'information RFID de visibilité en transit sur le serveur canadien avec d'autres systèmes d'information sur les chargements et systèmes de prise de décision.
- Développer une interface qui permettrait l'affichage simultané de toute l'information provenant de tous les systèmes liés à un chargement.
- Assurer l'interopérabilité avec nos alliés, assurant ainsi que l'information d'étiquettes RFID canadiennes puisse être acheminée en sécurité et avec fiabilité jusqu'au serveur canadien.

Critères d'évaluation et hypothèses de départ

Des recherches générales sur le sujet des systèmes d'identification automatisée ont permis de déterminer les besoins de base en la matière. De plus, nous avons examiné une vision de l'avenir considérant sur le plan opérationnel le futur du système informatisé de distribution (un réseau de serveurs fournissant de l'information sur le contenu des chargements et sur leur suivi, permettant aux utilisateurs de commander du matériel lorsque c'est nécessaire). En se basant sur la recherche de fond, les critères suivants ont été élaborés en vue d'évaluer les trois propositions ci-dessus pour le chemin à suivre en tenant compte des options potentielles en infrastructure de la TI. Le plan d'action recommandé doit :

a. minimiser les coûts ;
b. être programmé et opérationnel dans les délais les plus courts ;
c. être fiable en présence du plus grand nombre de conditions et circonstances ;
d. permettre la transition aux nouveaux systèmes avec un court préavis et se prêter à tout changement ou ajustement requis ;
e. minimiser la main-d'œuvre requise pour son fonctionnement et sa maintenance ;
f. être sécuritaire. Le personnel et les équipements/le matériel ne doivent pas être exposés à la découverte ou au ciblage ; l'information sur les chargements doit être fournie seulement en respectant la règle du besoin de savoir.

Un poids fort, moyen ou léger a été attribué à chaque critère en fonction de la mesure dans laquelle il a une influence sur le degré d'intérêt de chaque option. Des valeurs quantitatives ont alors été assignées à ces pondérations.

L'évaluation de chaque plan proposé pour le chemin à suivre a été basée sur les hypothèses suivantes.

- Le matériel actuel est entièrement interopérable avec l'Organisation du Traité de l'Atlantique Nord (OTAN) et ses alliés.

- Tout système informatisé d'identification automatisée mis en oeuvre peut être conçu de manière à respecter le mémorandum d'entente sur le partage de l'information sur les chargements entre l'OTAN et ses alliés.
- Toute capacité de visibilité en transit peut être intégrée à d'autres systèmes d'information et outils de prise de décision connexes canadiens.

Résultats

Une méthode de prise de décision informatique a été mise en oeuvre afin d'analyser les options proposées et il a été déterminé que l'option 3 était la meilleure. Dans le cadre de l'évaluation, elle a été choisie comme meilleure solution sur les plans de la fiabilité, de l'extensibilité et de la sécurité, ces trois aspects représentant les avantages d'un serveur d'information de visibilité en transit RFID appartenant au Canada. L'élimination du besoin de correspondre avec les États-Unis afin d'obtenir de l'information des étiquettes RFID canadiennes donne au MDN un plus grand contrôle sur le système et cela minimise les temps de réactions requis pour effectuer tout changement. Le principal problème de cette option est qu'elle exige du temps de développement et du financement, ce que les autres options ne requièrent pas.

L'option 3 décrit un système RFID légèrement plus mûr au sein du MDN. Ce système offrirait plus de souplesse et de sécurité. L'option 2 peut être mise en oeuvre beaucoup plus rapidement, ce qui permettrait d'obtenir une amélioration plus rapide des fonctionnalités du système et constituerait une étape intermédiaire de réalisation de l'option 3.

Recommendations

Le MDN devrait posséder un serveur hébergé au Canada pour les données RFID et ce dernier devrait être intégré avec les autres systèmes liés aux chargements. De plus, une interface devrait être développée afin de pouvoir voir simultanément les données RFID et le contenu des chargements.

Les articles individuels devraient continuer d'être étiquetés avec des codes à barres ; la transition aux étiquettes RFID passives pourrait se faire lorsque le nombre d'articles augmentera suffisamment pour rendre cette option viable. Les chargements devraient être étiquetés avec des étiquettes RFID actives.

L'information sur le contenu des chargements ainsi que les instructions relatives à la manutention et à la sécurité devraient être stockées directement dans les étiquettes RFID actives. Des précautions à l'effet de maximiser la sécurité de l'information, comme le chiffrement et le blocage des signaux radio pendant le déplacement des chargements et leur stockage, doivent être prises. Il est supposé que le degré d'interopérabilité avec les membres de l'OTAN et ses alliés sera maintenu sur le plan du matériel (lecteurs et étiquettes) et du partage de l'information.

Un programme de formation très adapté et uniforme, mettant l'accent sur le dépannage et sur le fonctionnement général doit être élaboré. De plus, il est important de maintenir la présence d'au moins une personne ayant l'expérience de la technologie RFID dans le contexte des FC à chaque emplacement doté de la technologie RFID.

Les tâches de soutien et de maintenance devraient être assumées par des sous-traitants, mais les responsabilités en matière de gestion doivent être conservées au sein du MDN.

Conclusion

La technologie de visibilité RFID en transit jouera inévitablement un rôle au sein des systèmes d'approvisionnement et de distribution du MDN. Selon l'analyse présentée dans le présent document, le meilleur plan d'action portant sur l'utilisation de la RFID dans les systèmes d'approvisionnement et de distribution du MDN comprendrait les éléments suivants : utilisation de codes à barres pour le suivi des articles individuels, utilisation des étiquettes RFID actives pour le suivi des chargements et transition à une infrastructure de TI basée uniquement au Canada.

Deux exigences s'appliquent à toute capacité d'identification automatisée et de visibilité en transit au MDN. Ce sont l'interopérabilité avec l'OTAN et les alliés du Canada et la facilité d'intégration aux processus de distribution actuels du MDN et aux systèmes d'information connexes. Tout au long de l'analyse, il a été supposé que toute capacité d'identification automatisée et de visibilité en transit adoptée par le MDN serait structurée de matière à respecter ces exigences grâce à des choix conséquents de produits matériels et logiciels.

Albert Lam, Patricia Moorhead; 2007; Future Utilization of RFID Technology in the DND Supply and Distribution System; DRDC CORA TM 2007–68; RDDC – Centre pour la recherche et l'analyse opérationnelles.

Table of contents

Tables

This page intentionally left blank.

1 Introduction

The purpose of this report is to present recommendations for future utilization of Radio Frequency Identification (RFID) technology in the Department of National Defence (DND) supply and distribution systems. By drawing from lessons learned during the recent RFID project, and analysing some of the choices the department has for different aspects of the technology, this report aims to produce a series of recommendations for the way ahead.

It is imperative for DND to clearly state a Global In-Transit Visibility (GITV) strategy before any Automated Identification Technology (AIT) system is implemented on a large scale. The strategy will provide a direction for AIT technologies in general, providing requirements and constraints for their use. This report is produced without a Canadian Forces (CF) GITV strategy for guidance, and therefore only aims to maximize the benefits of the technology while balancing security and integration of RFID with the barcode system currently in use.

RFID is composed of three main components: the tags (active and passive types); the readers (also called interrogators); and the Information Technology (IT) systems required to store the Consignment Tracking (CT) information. It uses a unique radio frequency to identify consignments rather than an optical pattern as used in barcodes. As multiple tags can be read and recorded simultaneously, the magnitude of human error in the process is reduced. Since RFID tags are capable of storing more information within the tag than just a tracking number, a variety of useful information can be stored directly on the tag such as a list of the contents, special handling/storing instructions, maintenance history (if applicable), and travel history.

Readability of the tags relies on the type of tag, proximity of the reader to the tag and the ambient environmental conditions. Radio waves can be absorbed or reflected by various liquids or metals, hindering readability of the tags and what materials can be transported with RFID tags. It is also a potential hazard for certain types of ammunition that are sensitive to radio waves.

2 Basic Requirements of an AIT System

The following requirements for an AIT system are derived from general research on AIT and RFID. The requirements outline basic capabilities considered to be essential to the overall success of a distribution system.

a. The ability to identify consignments by some sort of automated means that allows stock and in-transit information to be collected.

b. Information on the contents of a consignment must be secure and resilient to unauthorized attempts to extract such information.

c. The ability to provide near real-time CT information at supply and distribution nodes along a Line of Communication (LOC).

d. The system must be able to operate under austere environments and be resistant to damage; the specific criteria to be satisfied would need to be clearly defined by DND in a statement of requirements.

e. Interoperability with allies and the North Atlantic Treaty Organisation (NATO) at all levels. This includes information sharing, hardware (reader/tag) interoperability, and compliance with signed Memorandum of Understanding (MOU).

f. The system must be manageable and supportable by current organizations and systems in DND (no new ones need to be created).

g. The decision maker(s) in the theatre of operations must have access to the following information:
   - the inventory of current supplies on hand; and
   - supplies ordered, where they are, and approximately when they will arrive.

3 Operational Perspective on the Future of the Distribution IT System

The following is a vision for the future of the distribution IT system (a network of servers that provide consignment and tracking information, allowing users to order materiel when needed) based on operational and user perspectives. By looking at how the system would work from the perspective of the user, it is easier to direct the items that are key to reaching the desired end state.

1. Orders are made by selecting items in a database that draws data from servers containing the necessary information, and entering the day by which the supplies are required to arrive. A middleware program then takes that information and determines the optimal location the items can be drawn from and when they should be sent out to provide just-in-time delivery.

2. Individual items are branded with AIT and scanned; the scanned information is automatically entered into the distribution IT system as the consignment is being created. The consignment is also branded with AIT and the details of the contents are associated with the identifier attached. The consignment information data is stored in a secure Canadian server and is also available directly on the consignment in the form of a physical waybill or as part of the AIT.

3. The consignment AIT identifier provides In-Transit Visibility (ITV) at key transport nodes and information is collected to improve transit time estimations in future improvements to the middleware that determines these estimates. Global Positioning System (GPS) information can be relayed to the AIT system if vehicles with the necessary capabilities are transporting the consignment.

4. Along with monitoring the movement of materiel ordered, the distribution IT system allows changes to the route, destination or required arrival date to be made as needed by personnel with the appropriate level(s) of authority. All redirection information and history is retained.

5. The consignment arrives in the theatre of operation and the consignment contents can be identified using a handheld reader or a physical waybill. This process does not require a network connection to receive the consignment information, as the AIT label and/or the waybill contains the relevant data. The information is resynchronized with the Canadian distribution IT network as soon as network connectivity is re-established.

6. Reusable AIT identifiers are returned though the LOC along with regular shipments of mail and other items. By using a process that is already in place, little to no additional burden is added to the regular operational routine.

It is desirable that sensitive and high value consignments are tracked with GPS. Theft can be detected by conductive seals that, when broken, cause the GPS/AIT tag to signal theft. Consignments that need to be kept under certain environmental conditions can have monitors on them that record environmental data; this information can be read and/or transmitted to the Canadian consignment information storage servers when they are received at transport nodes.

4 Barcodes vs. RFID Tags

Barcodes are the AIT of choice in DND at the moment and provide unique advantages over other AITs, although RFID also offers certain advantages. There are key differences between the two technologies that make them optimal choices for different aspects of the process involved in supply and distribution.

It is clear that a combination of barcodes and RFID active tags provides a system that meets the basic requirements of a DND AIT System. It is advantageous to leverage both technologies for their benefits in order to improve different aspects of the department's processes.

Barcodes must be manually read one at a time and the barcode must be accessible, visible and clear. Suppliers apply the same barcode for each type of item (called a Universal Product Code) while consignments are tagged with unique barcodes generated by DND. The unique barcodes are linked with information hosted on a Canadian server such as consignment contents, travel route and history, handling instructions and other notes. Visibility of the consignment is maintained as the barcode information is read at key transport nodes; consignment information is obtained through a network connection to the data storage server. Since the barcode on its own is meaningless, hacking into the Canadian servers or intercepting the data transfer is the only way to obtain unauthorized access to consignment information; the security of the information is as secure as the Canadian servers and the network connection.

The shortfalls of the barcode AIT include:

- Barcodes become exceedingly tedious and inefficient when faced with a high flow of goods. They can be read only one at a time, and therefore bottlenecks can arise as the amount of goods flowing through the system is increased.
- Readability is highly dependant on the clarity of the barcode. This is less of a problem within warehouses and other controlled environments, however once in the field, environmental and operational conditions can rip or stain the barcode with dirt making it difficult for the reader to recognize the barcode.
- Access to full consignment information is completely dependant on a reliable network connection to the data storage servers, and/or a physical waybill attached to the consignment.
- It is easier for allies to apply their own barcode to Canadian consignments than to make the technologies interoperable in terms of hardware and information sharing.

Unlike barcodes, multiple RFID tags can be read simultaneously reducing the potential for bottlenecks in receiving and shipping. RFID tags are more resistant to damage and can be read under harsher environments while using a handheld interrogator than is the case for barcodes. Since information can be stored directly on the RFID tag, it is possible to obtain consignment information without a network connection. Therefore RFID is a more versatile

technology. Also RFID tags have been shown to be interoperable with allied interrogators as United Kingdom (UK) readers read Canadian tags during the RFID Project. With more formal testing and policy making, DND RFID technology can be made fully interoperable with our allies' systems.

In addition to filling some of the deficiencies of barcodes, RFID can also be used to eliminate in-house theft since any unauthorized removal of a consignment will be detected by the AIT system if items are moved out of range of the interrogators in the warehouse. Also, if a transport vehicle is equipped with a GPS transmitter along with an RFID interrogator, DND has the option of tracking consignments while in-transit in near real time. Both of these capabilities are not possible using a barcode system.

Unfortunately RFID is not without its own shortfalls such as:

- the cost of active RFID tags, which have varying prices within a large range ($5 to $100). For example, the average purchase price for an active RFID tag bought by the United States (US) Department of Defense from December 1997 to June 2005 was $99.79 US per tag [1];
- the potential security vulnerabilities involved with RFID technology such as enemy interrogators reading Canadian tags, tampering with the data on the tags themselves, and the potential for malicious code to be programmed into a tag;
- the sensitivity of the equipment to the environment it is set up in, affecting readability, range, and battery life of active tags;
- the safety hazards that may exist due to the sensitivity of some consignment contents, such as munitions, to radio waves; and
- the lack of an international standard for a range of frequencies to be dedicated to RFID use, complicating implementation and setup.

Comparing the capabilities of both AITs with the operational vision on the future of the supply and distribution system (Section 3), it is clear that the use of active RFID tags for consignment tracking and barcodes for item level tracking matches the vision at the most basic level. RFID offers many options and can be implemented in a variety of ways. DND must explore all of these options in order to ensure the technology is used to the fullest possible potential while adhering to departmental strategy.

Network connectivity to maintain up-to-date databases and for obtaining information is integral to both AITs, and therefore acts as a vulnerability for both systems. Maintaining local copies of databases that are regularly backed up, combined with storing information from barcode and RFID tag reads locally, provides a buffer in the event that network connectivity is compromised.

There are a few gaps in the process that cannot be addressed by barcodes or RFID tags, such as theft of in-transit consignments.

5 Discussion on Implementing RFID Technology

There are many aspects to RFID AIT, and there are many issues and concerns that must be considered. The following sections address some concerns and options within the areas of security, tagging, training, human resources, support and maintenance.

5.1 Security

The issue of concern is the security of information stored on the RFID tag. Security concerns regarding the IT infrastructure will be discussed in Section 6.

An advantage to storing information on the actual RFID tag is that it eliminates the need to have a network connection to get a list of the contents of the consignment without opening it. This is particularly useful for personnel who are in the theatre of operations and don't have a consistent IT network connection due to their location. Although the same information can also be kept on a server, having this information on the tag itself makes it more convenient and not susceptible to network problems. In the event that there are many consignments all in one location, such as the Olympics of 2010 or any theatre of operations, it is advantageous for workers to be able to identify contents of consignments quickly and effectively while under various operational pressures related to the organization of such a massive undertaking.

There are also several disadvantages to storing information directly on the active RFID tag. Since the selection of interrogators is limited, their designs are quite universal and can be replicated by third parties. This is a cause for concern, as favourable environmental conditions are known to significantly increase the read range of RFID interrogators. While DND can ensure that the Canadian servers are secure, RFID tags could be more susceptible to unauthorized access and corruption of data. The security risks associated with RFID tags can be reduced by encrypting the data on the tags and also by insulating consignments with metallic plating to prevent broadcasting of signals [2].

One recommendation, with regards to the type of information stored on the RFID tags, is to store all the consignment information on the tag such as contents, handling and safety instructions, and history of transit. The information should be encrypted for all consignments, and where possible appropriate insulation should be used to prevent signal leakage during transit.

Regarding theft, as long as it is possible to keep the items or consignments within range of an interrogator at all times, it is possible to detect theft as soon as a tag leaves the range of interrogation without authorization. While this is feasible in a static warehouse environment, theft detection by automated means in a theatre of operation is not likely to be possible.

With respect to barcodes, they do not have the same security issues as RFID tags since their only vulnerability is the network connection to the Canadian servers to obtain the

consignment information. Although information is more secure, barcodes are unable to track consignments to the level where they could detect theft or damage. Overall, barcodes provide more security to the consignment information than RFID tags, but lack several capabilities that could offset some operational risks.

5.2 Tagging

There are many options for tagging consignments and items: barcodes, passive RFID tags, active RFID tags, or some recently developed hybrid active tags that also act as mini interrogators. In general, passive RFID tags do not require a power source and send out a weak signal only when an interrogator scans them, which limits the readability range. Active tags continuously broadcast a signal, thus requiring a power source, and the signal strength is much stronger allowing for better read rates compared to passive tags. Although tagging everything with an active tag would ensure greater readability and visibility, it is not cost effective.

At the item level, barcodes are recommended. This is because the majority of suppliers are still using barcodes and DND already has the necessary capability and processes in place to make use of barcodes for item level tracking in a warehouse.

It is possible that the department may transition to passive RFID tags in the future for some additional benefits. Passive RFID tags improve warehouse management if the positioning of items within a warehouse can be optimized to save a fair amount of time and money. It is cost effective when there is a very high volume of goods that need to be tracked. Passive tags partnered with appropriate middleware applications can optimize the management of materiel within the warehouse, and ensure items are exactly where the system says they are. SmartCode Corp. supplies passive tags for $0.05 each [3].

In terms of readability, passive RFID tags are more appropriate for item level tracking than active RFID tags. The lower readability rate of passive tags (due to weaker signal strength) is not an issue in a warehouse environment; fixed interrogators have sufficient time to sweep the area for any passive RFID tags within range. Active RFID are designed for more dynamic environments in which tags must be read quickly while the items are in movement. This latter situation occurs frequently during the movement of collections of consignments.

At the consignment level, active tags are the best due to their high readability and the enhancements that can be made to them, such as temperature/humidity monitoring of the consignment and the storing of pertinent handling and safety instructions. Active tags are also more resistant to damage than passive tags.

5.3 Training and Human Resources

The Lessons Learned (LL) report [4], reveals some of the changes DND should make to the training program for RFID operation in order to improve its effectiveness. A summary of

the relevant lessons learned is located in Annex A.

Lessons learned ‘A1’ addresses the issue that current training programs are lacking in certain aspects of the use of the technology. DND needs to ensure future training programs are relevant and effective. This would require a short study on the needs of the operators and collaborations with Project Manager Joint-Automatic Identification Technology to come up with an appropriate training program. A customised program is to DND’s advantage since it will be designed specifically for the needs of DND (time constraints, location, etc.) and will put more emphasis on areas most beneficial to the department.

Lessons learned ‘A2’ is very important, since it outlines the lack of troubleshooting instruction and training that was received. Operators with a reliable ability to troubleshoot operational issues effectively reduce the amount of downtime with RFID kit. Having the ability to troubleshoot also means the operators have a firmer understanding of the system and can therefore use it more effectively. If DND focuses on an end goal of training operators with good troubleshooting skills, the operators will complete their training with much more confidence than if they only received training on how to use the system.

Lessons learned ‘A3’ addresses concerns around personnel rotation and knowledge/skill retention. One means of alleviating these concerns is to train at least one civilian at each warehouse or intermediate staging base if possible. If there is at least one permanent experienced person on staff who is familiar with the nuances of the particular system that is set up in that location, the department can reduce many operational issues that may arise with inexperienced operators. If hiring a civilian is not possible, then complete turnover of military staff should be avoided to ensure there will be personnel familiar with the RFID set-up in that location at all times.

Lessons learned ‘A4’ states that DND should keep the same trainer for consistency and have that person act as a point of contact for any questions. This ensures homogenous training across the CF so the skills that people develop would be equivalent among all operators. In addition, this LL plays an important role when posting people to different locations: common skill levels will help to ensure that movements of personnel do not hinder operational efficiency.

Maintaining sole use of barcodes will eliminate the need to develop new training programs, something that is necessary whenever a new technology is introduced into DND. Time and money spent on developing training programs can be saved if the department stays with using only barcodes, although RFID has benefits that are outside of the capabilities of a barcode.

At the moment, with only one Line of Operation (LOO) being conducted by the CF, the personnel resources needed to manage the current barcode AIT system are reasonable. However, when the CF starts to sustain more than one major LOO simultaneously, the advantages of RFID technology over barcodes will increase proportionally. With RFID, the manpower and time necessary for shipping and receiving will be much lower in comparison to just using barcodes due to the increased level of automation.

5.4 Support and Maintenance

The only alternative to contracting out support services is to have someone in-house. It has been shown that technical problems do not arise very frequently. To hire a full-time expert for that reason may not be cost effective. A part-time expert is not practical since the occurrence of technical failures is unpredictable. Therefore a support contract that provides a helpline and service within 24 hours would be ideal for the support of RFID kit. This applies to support for both personnel working in warehouses and personnel using the technology in the field.

The delegation of responsibilities for the equipment and care of the RFID system is discussed in the RFID Project LL report. RFID can be managed the same way barcodes are managed today since equivalents between the barcode kit and RFID kit can be made.

If the providers of support for barcode kit and RFID kit are different, the overhead costs for support will double assuming both providers charge a similar amount. This is not cost effective and DND should avoid such arrangements whenever possible.

6 IT Infrastructure Options for the Way Ahead

An evaluation and analysis of the first two phases of the RFID Project (materiel movement from the Port of Montreal to Kandahar Airfield and back) has revealed many operational and procedural issues that need to be addressed. There are also larger issues that are integral to the efficiency of the supply chain that are hampered by current infrastructure. Information flow, access and automation are aspects of the RFID Project that require collaborative effort for improvement to ensure the system in place is adequate enough to provide an interim ITV capability.

RFID should be a key component, in addition to barcodes, in any interim ITV capability for DND because it will most likely play a role in the future GITV strategy. It can provide pertinent information about shipments that barcodes cannot (such as environmental conditions and tampering) and it also increases interoperability with our main allies and NATO.

The RFID system currently in place provides DND with ITV information that is hosted on an American owned server. To acquire complete information on a consignment that is identified by a tracking number, data must be accessed from two separate interfaces that cannot be viewed simultaneously.

The future of RFID in DND relies heavily on the GITV strategy that has not yet been finished. In the meantime, the department should work to ensure requirements are met, with regards to interoperability and functionality, and to improve ITV capability through RFID as much as possible with minimal commitment, so it can be used effectively as part of an interim solution.

When deciding on the best plan for the way ahead, the decision making process must contain minimal bias and objectively form an opinion on different aspects of proposed plans before reaching a conclusion. In order to achieve this, criteria by which each plan for the way ahead will be evaluated must be generated, assumptions identified, and weights assigned to each evaluation criterion. With all this in place it is then possible to start judging each option against the criteria to determine the best plan in an unbiased and critical way.

6.1 Decision Criteria

The following criteria are used to evaluate proposals for the way ahead with regards to potential IT infrastructure options.

a. Cost: The recommended plan of action should have a minimized cost.

   Rationale: Until RFID is confirmed to be part of the GITV strategy, it is still a project and capital will not come easily. DND should aim to maximize the effect of what it already owns.

b. Scalability: The recommended plan of action should allow for rapid transition into new systems given short notice and be robust against any changes/adjustments that may need to be made.

Rationale: Once a GITV strategy has been decided on, it is to the department's advantage to phase in the new plans as quickly and seamlessly as possible to provide maximum service to the theatre of operations.

c. Manpower: The recommended plan of action should minimize the need for manpower for its operation and maintenance.

   Rationale: Decreased manpower requirements is one major factor that contributes to decreased overhead costs and increased efficiency.

d. Time: The recommended plan of action should be programmed and operational in the shortest amount of time possible.

   Rationale: DND should aim to maximize the effects of the new technology given the equipment and infrastructure it has, as soon as it can, to ensure the maximum amount of support can be provided to troops in the theatre of operations.

e. Reliability: The recommended plan of action should be reliable under a maximum number of conditions and circumstances.

   Rationale: Due to the nature of military operations and the importance of the supply chain, the solution should be functional under as many conditions (environmental/operational) as possible.

f. Security: The recommended plan of action should be secure and not expose personnel and equipment/materiel to an increased risk of discovery and targeting, and the consignment information should be made available on a need to know basis only.

   Rationale: Due to the vulnerability of supply chain assets and their high value to the enemy, the IT system must be designed to provide information security, systems security and personnel security, but impact as little as possible on the velocity and reach of the distribution and tracking requirements.

6.2 Assumptions

The evaluation of the proposed plans for the way ahead is based on the following assumptions.

- Current hardware is fully interoperable with NATO and its allies.
- Any implemented AIT IT system can be designed to meet the MOU for consignment information sharing between NATO and its allies.
- Any ITV capability can be integrated into other Canadian information systems and related decision making tools.

6.3 Weighting of Decision Criteria

Each criterion is weighted low, medium or high, based on the amount of influence each has in determining how favourable a particular option is. Quantitative values[1] are then associated to these weightings. The rationales behind the weightings shown in Table 1 are discussed below.

Table 1: *Weighting of the Decision Criteria*

Criteria	Qualitative	Quantitative
Cost	Low	9%
Time	Low	9%
Reliability	Medium	16%
Scalability	High	21%
Manpower	High	21%
Security	High	24%

6.3.1 Cost

Cost has been weighted as low compared to the other criteria because it is a secondary concern compared to the main purpose of the solution, which is to improve the supply chain. Capital may be difficult to collect, although with a solution that will improve current systems it will come with persistence.

6.3.2 Time

As with cost, time is weighted as a low criterion and for very similar reasons. The supply chain as it is now is functional at the very least, although operational support is sub-optimal. Additional time, to collect capital to cover costs and facilitate the development of technical improvements, is readily available and the process can be fast-tracked when needed.

6.3.3 Reliability

Reliability is a moderately important criterion because in addition to RFID tagging, consignments are also being labelled with barcodes. With a highly reliable back-up capability such as the barcode system, the proposed plan of action does not have to be as concerned with the reliability as much as other criteria. However, reliability still plays an important role.

6.3.4 Scalability

Ease of scalability is a central ability the proposed plan of action should possess. The level at which RFID is to be included in the DND-wide ITV strategy is unknown. The

[1]These values were decided upon by the primary author, and have not been validated by subject matter experts. In Section 6.6.3 a sensitivity analysis of these weightings is conducted.

implementation of an interim RFID capability should be set up so that it can be downsized or, a more likely scenario, upsized to meet new guidelines.

6.3.5 Manpower

Reduction of manpower is another key ability that must be maximized in the proposed plan of action. This is a main benefit that saves the supply chain time, money and potentially increases velocity and is something DND should aim to maximize.

6.3.6 Security

Security is always a concern within DND especially due to the critical nature of consignment information and its potential value to the enemy. Security is the most important criterion for the proposed plan of action.

6.4 Proposed Plans for the Way Ahead

Option #1

- Make the procedural and operational changes recommended in the LL process (summarized in Annex B).
- Continue using the US server to store RFID ITV information.
- Procure additional tags and readers to expand visibility to more consignments in this LOC.

Option #2

- Make the procedural and operational changes recommended in the LL process (summarized in Annex B).
- Continue using the US server to store RFID ITV information.
- Procure additional tags and readers to expand visibility to more consignments in this LOC.
- Enhance functionality and resilience of the IT system by developing a secure and reliable connection between the US server and the CF National Movement and Distribution System.
- Develop an interface that allows information from all consignment related systems to be displayed at the same time.

Option #3

- Make the procedural and operational changes recommended in the LL process (summarized in Annex B).

- Migrate away from the use of the US server to a Canadian server for storing RFID ITV information.
- Procure additional tags and readers to expand visibility to more consignments in this LOC.
- Integrate the RFID ITV information on the Canadian server with other Canadian consignment information systems and decision-making tools.
- Develop an interface that allows information from all consignment related systems to be displayed at the same time.
- Maintain interoperability with allies, ensuring Canadian RFID tag information can be routed securely and reliably to the Canadian server.

6.5 Options Analysis - Method I

With the weightings and options defined, we can now compare the results using a computational decision-making method ([5], Section 15.5.1).

The structure of Table 2 outlines the methodology used for computational decision-making. The rows of the table are the criteria on which the options are to be judged. The columns consist of criteria weights (w), option ratings (c), option scalings (p) and option scores (f).

Table 2: *Computational Decision Making Table*

		Option #1			Option #2			Option #3		
Criteria	$\mathbf{w_i}$ **(%)**	$\mathbf{c_{i1}}$	$\mathbf{p_{i1}}$	$\mathbf{f_{i1}}$	$\mathbf{c_{i2}}$	$\mathbf{p_{i2}}$	$\mathbf{f_{i2}}$	$\mathbf{c_{i3}}$	$\mathbf{p_{i3}}$	$\mathbf{f_{i3}}$
Cost	9.0	1	0.1	0.9	4	0.4	3.6	10	1.0	9.0
Time	9.0	1	0.14	1.26	6	0.86	7.74	7	1.0	9.0
Reliability	16.0	2	1.0	16.0	2	1.0	16.0	1	0.5	8.0
Scalability	21.0	10	1.0	21.0	8	0.8	16.8	1	0.1	2.1
Manpower	21.0	5	1.0	21.0	1	0.2	4.2	3	0.6	12.6
Security	24.0	8	1.0	24.0	8	1.0	24.0	1	0.125	3
Totals	**100.0**			**84.16**			**72.34**			**43.7**

The quantitative evaluation of each option is based on its relative fulfillment (to the other options) of each criterion.

The criterion of Cost will be used to demonstrate how Table 2 was completed. Recall that Cost has an overall weighting of 9% of the final score; this value is entered in the w_i column for Cost.

Next, each of the three options is rated from a cost perspective on a scale from one to ten, where one is the most favourable and ten is the least favourable; c_{ij} represents the rating of option j under criteria i.

Option #3 is the least favourable of all the options from a cost point of view since it requires the procurement of a lot of equipment, funding for developers of the new system and other costs related to implementation: it is ranked as 10 (the first entry in column c_{i3}). The most favourable option is the first, and it is giving a rating of one (the first entry in column c_{i1}). Option #2 is given an intermediate rating of four. The subjectivity in the ratings used is discussed in Annex C.

The ratings assigned to two or more options under the same criterion can be the same if there is no difference between the options (e.g. Options #1 and #2 under the Reliability criterion).

The next value calculated is p_{ij}, the scaling value that sets the rating of option j under criteria i relative to the worst rated option. For a given criteria (i) and option (j), p_{ij} is calculated by dividing c_{ij} by the highest option rating out of all the options in that row of the table.

For the criterion of Cost, the highest rating is ten (given to Option #3). Thus for Option #1, the option scaling is calculated as $1/10 = 0.1$, which is the p_{ij} value seen in Table 2 under Option #1 for Cost.

The last item calculated is the final relative score that is assigned to option j under criteria i, denoted by f_{ij}. This is done by multiplying p_{ij} by w_i. In the end all the scores are summed up together and the lowest score is associated with the most favourable option overall. "Most favourable overall" does not necessarily mean "best"; other options may have advantages that the most favourable option does not have.

Through the above method of computational decision-making, it is apparent that Option #3 is the preferred option. Within the evaluation, it was rated as the best choice for reliability, scalability and security, all three of which are the key advantages to having a Canadian owned RFID ITV information server. Eliminating the need for correspondence with the US for Canadian RFID tag information gives DND more control over the system and minimizes reaction time to effect any changes that need to be made. The main issue with this option is that it requires development time and money that the other options do not require.

Option #3 describes a slightly more mature RFID system within DND that allows for greater reliability, flexibility, and security. Option #2 can be implemented on a much shorter time frame allowing a more rapid improvement to the functionality of the system, and could serve as an intermediate step towards Option #3.

6.6 Options Analysis - Method II

At the recommendation of a reviewer of this paper, the option analysis conducted above was repeated using an alternate methodology. The Multicriteria Analysis and Ranking Concensus Unified System (MARCUS) [6] program was developed by the Central Operational Research Team within the Centre for Operational Research and Analysis (CORA), and has become a widely used decision support tool. Given multiple rankings for several options,

the goal of MARCUS is to find a single ranking or prioritization of the options that best reflects the consensus of the rankers.

For the analysis conducted here, there are three options for the way ahead, and six rankings (the six criteria) for each option. Each ranking is also given a weight, to indicate their importance relative to each other.

In order to assess the sensitivity of the results to the weightings and rankings, several scenarios were run in MARCUS. Each is described below.

6.6.1 Baseline Scenario

The baseline scenario is a replication of the options analysis conducted in Section 6.5. The weights shown in Table 3 are the same as those used above, and the rankings reflect the exact same ordering of the options as used in the previous analysis. The ties observed in Table 2, between Options 1 and 2 for Reliability and Security, are treated as weak ties in the baseline scenario. This means that for these two criteria there is indifference between the two options: they are not equally preferred, but rather we are deliberately not putting a preferred relative ordering between them. The coding of "-2" reflects this weak tie relationship.

Table 3: *Baseline Scenario Weights and Ranks Inputs to MARCUS*

Criteria	Weight	Option #1	Option #2	Option #3
Cost	9.0	1	2	3
Time	9.0	1	2	3
Reliability	16.0	-2	-2	1
Scalability	21.0	3	2	1
Manpower	21.0	3	2	1
Security	24.0	-2	-2	1

Only one consensus ranking solution was found for the baseline scenario. Option #3 is the preferred choice, followed by Option #2. Option #1 is the least preferred. These results are the same as those obtained in Section 6.5.

6.6.2 Sensitivity Analysis on Input Rankings

To investigate the sensitivity of the MARCUS results to the rankings given to each Option under the various criteria, certain rankings were changed.

In the baseline scenario, Options #1 and #2 are weakly tied on the criterion of Security. Since Option #2 involves creating a permanent connection between Canadian and American data servers, it may be argued that Option #2 is slightly less secure than Option #1 which does not require such a server connection. For this reason, we created a second scenario in which the Security rankings are changed so that Option #1 has a ranking of two and Option #2 a ranking of three, as shown in Table 4.

Table 4: *Scenario II Weights and Ranks Inputs to MARCUS*

Criteria	Weight	Option #1	Option #2	Option #3
Cost	9.0	1	2	3
Time	9.0	1	2	3
Reliability	16.0	-2	-2	1
Scalability	21.0	3	2	1
Manpower	21.0	3	2	1
Security	24.0	2	3	1

The resulting consensus ranking from MARCUS places Option #3 as the first choice, followed by Option #1 and then Option #2. Comparing these results to those for the baseline scenario, we see that the "best" option has not changed, only the ordering of the other two lesser preferred options differs.

Under the criterion of Time, Options #2 and #3 are given relative rankings very close together in Table 2 (values of six and seven). Some people may be of the opinion that these two options are in fact tied on this issue. For a third scenario run in MARCUS, the rankings of these two options under Time were changed from two and three to be "-2" for each, reflecting an indifferent weak tie. The changes made in the second scenario were also retained (see Table 5).

Table 5: *Scenario III Weights and Ranks Inputs to MARCUS*

Criteria	Weight	Option #1	Option #2	Option #3
Cost	9.0	1	2	3
Time	9.0	1	-2	-2
Reliability	16.0	-2	-2	1
Scalability	21.0	3	2	1
Manpower	21.0	3	2	1
Security	24.0	2	3	1

Once again, the consensus ranking determined by MARCUS placed Option #3 at the top of the list. The other two options end up being tied for second place.

The sensitivity analysis on the input rankings indicates that the consensus preference for Option #3 is not influenced by changes in the rankings of options that are tied or close to tied under one or more criteria.

6.6.3 Sensitivity Analysis on Input Weights

To investigate the sensitivity of the results to the input weights assigned to each criteria, scenarios were run in which each all six criteria were given equal weightings. The baseline scenario, plus scenarios II and III above were repeated, but this time with the weight for each criteria set to one in all instances.

For all three runs of MARCUS with equally weighted criteria, the consensus solutions had Option #3 as the preferred choice. The only differences observed were the orderings of the other two options. For the baseline scenario with equal weights, the consensus is to place Option #2 ahead of Option #1. For scenarios II and III with equal weights, Option #1 is preferred over Option #2 in the consensus solutions.

The sensitivity analysis on the input weights indicates that Option #3 is the consensus preference, regardless of the weights assigned to the criteria.

7 Recommendations

After doing analyses on different aspects of RFID technology and determining what may be the best plan for the way ahead for DND, the following is a summary of recommendations.

DND should have a Canadian hosted server for RFID data, and it must be integrated with the rest of the consignment related systems in the department. Also, a user interface must be developed that allows RFID data and consignment contents to be viewed simultaneously.

Individual items should continue to be tagged with barcodes in the interim; transition to passive RFID tags may occur when the volume of items increases enough to make this a viable option. Consignments should be tagged with active RFID tags.

Consignment content information, as well as handling and safety instructions, should be stored directly on the active RFID tags. Precautions to maximize information security, such as encryption and blocking radio signals while in transit and storage, must be taken. It is assumed that the necessary level of interoperability with NATO and allies will be maintained in terms of hardware (readers and tags) and information sharing.

A highly customized and homogenous training program that puts an emphasis on troubleshooting and general operation must be developed. Also, retaining at least one person experienced in using the RFID technology in the CF context at each RFID enabled location at any given time is important.

Support and maintenance tasks may be contracted out, however management responsibility for the RFID capability must be retained within DND.

8 Future Development

The use of RFID allows for more accurate capture and retrieval of data regarding transit times and the general dynamics of the distribution system. This allows for better forecasting models to be made to predict transit time and to determine the optimal amount of stock to keep, which will reduce operational costs associated with storing excess stock.

This technology could also give DND a clearer picture of how effectively supplies are being used and also how much of those supplies are stolen or lost.

9 Conclusion

RFID ITV technology will inevitably play a part in DND supply and distribution systems. The recommendations reached in this report can provide knowledge and insight into the technology to better utilize it when it becomes a larger part of the department's processes.

Capabilities of barcodes were compared with RFID active tags, outlining some of the advantages and disadvantages each technology offers. Next, basic requirements for an ideal AIT system within DND were outlined, along with an operational vision. This was followed by a discussion of various aspects of RFID technology, such as security, tagging, training and human resources, and support and maintenance. An options analysis was done to compare and rank options for the way ahead with respect to AIT/ITV IT infrastructure.

Based on the analysis performed, the best plan of action for the utilization of RFID in the DND supply and distribution system includes: using barcodes for item level tracking; using active RFID tags for consignment tracking; and transitioning to a solely Canadian based IT infrastructure.

Two key requirements for any AIT/ITV capability within DND are: interoperability with NATO and Canadian allies; and ease of integration into the existing DND distribution processes and related information systems. It was assumed throughout the analysis that any AIT/ITV capability adopted by DND will be structured to meet these requirements through appropriate choices of hardware and software products.

RFID technology is constantly evolving and changing. However, the basic principles behind the technology will remain the same, and the same concerns outlined in this report will still be applicable.

References

1. Government Accountability Office (GAO) (online), http://www.gao.gov/new.items/d06366r.pdf (Access Date: 26 April 2007).

2. So, Stuart C.K. (2006), Securing RFID Applications: Issues, Methods, and Controls, *Information Systems Security*, 15(4).

3. SmartCode Corp. (online), http://www.smartcodecorp.com/index.asp (Access Date: 12 April 2007).

4. CANOSCOM COST (2007), Radio Frequency Identification (RFID) Capability for Roto 2 Task Force Afghanistan (TFA) Lessons Learned (LL) Analysis Report. 3000-1 (COST) 19 March 2007.

5. G.C. Andrews, J.D. Aplevich, et. al. (2006), Introduction to Professional Engineering in Canada, 2nd ed, Pearson Education Canada.

6. Emond, E.J. (2006), Developments in the Analysis of Rankings in Operational Research, (Technical Report DRDC CORA TR 2006-37) Centre for Operational Research and Analysis, Ottawa, Canada.

Annex A
Training Related Lessons Learned Summary from "RFID Capability for Roto 2 TFA, LL Analysis Report"

LL A1: For the time being, there are two RFID courses, one for the static system (two days) and one for the mobile system (five days). The current mobile course did not initially contain a section on writing tags until staff insisted it be included; this section is still not a standard component of the course.

In the future, the course content must be analysed from the perspective of the end user. It must be ensured that all related equipment is given enough training time in the course for comfortable use. The training course should aim to have the user become fully autonomous in the operation of RFID AIT.

LL A2: Troubleshooting and self-diagnosis was not covered in sufficient depth in the training course. More time should be allocated to troubleshooting operational issues to ensure maximum up-time for the RFID kit.

LL A3: The people who are allowed to take these training courses need to be chosen carefully; personnel rotation and knowledge/skill retention issues must be kept in mind. A periodic refresher course for static and mobile systems may have to be designed to supplement the main training courses.

LL A4: Skill level varies depending on the person and trainer, resulting in inconsistent service level by different people. Keeping the same trainer for all training courses will ensure personnel that receive training will have a consistent skill level within DND. This trainer could also act as a point of contact for any questions.

Annex B
Operational and Procedural Lessons Learned Summary from "RFID Capability for Roto 2 TFA, LL Analysis Report"

LL B1: Ten percent of the batteries were defective, so quality control needs to be improved and alternate sources of batteries should be identified in the event a supplier encounters quality issues.

LL B2: Setup of mobile systems should be planned two days in advance to allow for testing and proper configuration prior to first use. This is due to an observation that the actual physical set up takes about an hour, but the network configurations may take longer depending on the connection.

LL B3: Software drivers for the readers, handheld interrogators and other software were not available on the RFID laptop, so equipment would have been rendered unserviceable in the event one of those files was corrupted during use. These backups must be kept on the laptop in the event the equipment does require reformatting.

LL B4: Due to inconsistent network connectivity, batching read events together before sending is more reliable than transmitting individual read events.

LL B5: Frequency clearance tasks need to be part of mission planning to ensure there are no radio wave conflicts within the host nation.

Annex C
Rationale Behind Option Ratings

Option #1 reflects the state of RFID technology within DND at the time this report was written. The second option suggests some changes to how information is routed and accessed. Option #3 goes one step further and suggests that DND set up its own in house information systems for RFID data, rather than use a US server for data hosting.

Cost Ratings: Option #1 is the cheapest since there is no change that needs to be made. The future cost for leasing space on the US server is still up for negotiation, and as such is not considered. Option #2 only requires development costs to redirect information in existing IT systems so it is rated as a four. The most expensive option is the third, with a rating of ten, since a new IT infrastructure would need to be designed to accommodate RFID within existing systems.

Time Ratings: Option #1 requires no additional time to implement so it is given a rating of one. Option #2 requires developers to coordinate with the US and reprogram parts of the systems DND uses to access information, which will take a moderate amount of time to accomplish, hence the rating of six. Option #3 is rated at seven, not ten, because preliminary designs have already been drawn up and about 60% of the work has already been done, so it will only take a little bit more time to implement a Canadian system.

Reliability Ratings: The main issue behind reliability is the dependence on the US server that both Option #1 and #2 require. The US server is reliable (US Forces use the same server for hosting their own data), meriting a rating of two for both options. Option #3 is given a rating of one, as a Canadian owned server is considered to be even more reliable.

Scalability Ratings: Both Option #1 and #2 recommend continued use of the US server, which limits the level of scalability available. Option #2 rates slightly better than Option #1 (rating of eight versus ten), because it includes some preparation for a Canadian based system (better user interface and information access). Option #3 is the best option since it is much easier to change things within Canadian owned systems than on the US system.

Manpower Ratings: Option #1 provides no additional improvement to efficiency of the distribution system and instead provides movers with extra work since the barcodes and RFID are still required to be used together. Option #2 lessens the extra work of searching for data, and doesn't require a lot of time to implement and develop, which in comparison to Options #1 and #3 decreases manpower requirements the most overall. Option #3 takes a longer time to develop and once implemented requires additional work by IT support to maintain the extra hardware and systems. The manpower ratings have been done on a one to five scale, due to the minute differences between options.

Security Ratings: The main concern here is the relative lack of security the US has for their consignment information. The US server that hosts RFID CT data is not a secure server. It is a separately managed network where their best interest lies with themselves and not

hosted nations such as Canada. We cannot make changes easily to their system if at all and are under the whim of how the US wants to organize Canadian data. Since this significant security issue is common to both Option #1 and #2, these two options have a rating of eight. Option #3, on the other hand, eliminates these security issues and brings the responsibility to Canada. This allows for greater internal flexibility, management, security and process transparency leading to a more secure system.

List of Acronyms

AIT	Automated Identification Technology
CANOSCOM	Canadian Operational Support Command
CF	Canadian Forces
CORA	Centre for Operational Research and Analysis
COST	Chief of Operational Support Transformation
CT	Consignment Tracking
DND	Department of National Defence
DRDC	Defence Research and Development Canada
GITV	Global In-Transit Visibility
GPS	Global Positioning System
IT	Information Technology
ITV	In-Transit Visibility
LL	Lessons Learned
LOC	Line of Communication
LOO	Line of Operation
MARCUS	Multicriteria Analysis and Ranking Concensus Unified System
MOU	Memorandum of Understanding
NATO	North Atlantic Treaty Organisation
RFID	Radio Frequency Identification
UK	United Kingdom
US	United States

Distribution letter

1630-1 (DMGOR)

January 2008

Distribution List

Future Utilization of RFID Technology in the DND Supply and Distribution System

Reference Albert Lam and Patricia Moorhead. *Future Utilization of RFID Technology in the DND Supply and Distribution System*, DRDC CORA TM 2007–68, December 2007 (enclosed).

1. This report presents recommendations for future utilization of Radio Frequency Identification (RFID) technology in the Department of National Defence (DND) supply and distribution systems. The recommendations are based upon lessons learned during the recent RFID project, and an analysis of some of the choices the department has for different aspects of the technology.

2. Based on the analysis performed, the best plan of action for the utilization of RFID in the DND supply and distribution system includes: using barcodes for item level tracking; using active RFID tags for consignment tracking; and transitioning to a solely Canadian based Information Technology (IT) infrastructure.

3. Two key requirements for any Automated Identification Technology (AIT) / In-Transit Visibility (ITV) capability within DND are: interoperability with North Atlantic Treaty Organisation (NATO) and Canadian allies; and ease of integration into the existing DND distribution processes and related information systems. It was assumed throughout the analysis, that any AIT/ITV capability adopted by DND will be structured to meet these requirements through appropriate choices of hardware and software products.

4. Questions or comments are welcome and should be addressed to Ms. P. Moorhead at (613) 944-9211 or by email at *moorhead.ph@forces.gc.ca*. Electronic copies of this report are also available upon request from *Repsys.R@forces.gc.ca*.

D. Haslip
Acting Chief Scientist
Enclosures: 1

Distribution List

D/COS ADM(Mat)
C Prog
DFPPC
CFD
CANOSCOM//COST/OS J5/JSG/JSR/CMSG
DMG Compt
DMPP
DMGSP
DDA
DSFC
DMIS
DSCO
DRDC CORA//DG CORA/DDG CORA/Chief Scientist/SH J&C (1 copy on circulation)
DFPPC 2
DFPPC 3
DFPPC 4
DFPPC 6
DDA 2
DMG Compt 5
DFPPC 6-2
DFPPC 6-3
DFPPC 6-6
ADM(S&T) / DGRDP / CANOSCOM LO - Maj. Karl Leclerc
DRDC Ottawa - Dr. Qinghan Xiao
Authors - P. Moorhead (2)
DRDC CORA Library (2)
DRDKIM (2)

Spares (2)

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

DRDC – Centre for Operational Research and Analysis
NDHQ, 101 Col By Drive, Ottawa ON K1A 0K2

2. SECURITY CLASSIFICATION (overall security classification of the document including special warning terms if applicable).

UNCLASSIFIED

3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C,R or U) in parentheses after the title).

Future Utilization of RFID Technology in the DND Supply and Distribution System

4. AUTHORS (Last name, first name, middle initial. If military, show rank, e.g. Doe, Maj. John E.)

Lam, Albert ; Moorhead, Patricia

5. DATE OF PUBLICATION (month and year of publication of document)	6a. NO. OF PAGES (total containing information. Include Annexes, Appendices, etc).	6b. NO. OF REFS (total cited in document)
December 2007	46	6

7. DESCRIPTIVE NOTES (the category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered).

Technical Memorandum

8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development. Include address).

DRDC – Centre for Operational Research and Analysis
NDHQ, 101 Col By Drive, Ottawa ON K1A 0K2

9a. PROJECT OR GRANT NO. (if appropriate, the applicable research and development project or grant number under which the document was written. Specify whether project or grant).	9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written).
N/A	

10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the originating activity. This number must be unique.)	10b. OTHER DOCUMENT NOs. (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC CORA TM 2007–68	

11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification)

(X) Unlimited distribution
( ) Defence departments and defence contractors; further distribution only as approved
( ) Defence departments and Canadian defence contractors; further distribution only as approved
( ) Government departments and agencies; further distribution only as approved
( ) Defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution beyond the audience specified in (11) is possible, a wider announcement audience may be selected).

13. ABSTRACT (a brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual).

This report presents recommendations for future utilization of Radio Frequency Identification (RFID) technology in the Department of National Defence (DND) supply and distribution systems. The recommendations are based on the lessons learned from the recent RFID project and an analysis of some of the choices the department has for different aspects of the technology.

Based on the analysis performed, the best plan of action for the utilization of RFID in the DND supply and distribution system includes using barcodes for item level tracking and active RFID tags for consignment tracking, and transitioning to a solely Canadian based information technology infrastructure.

The Canadian Forces global in-transit visibility (GITV) strategy is still under development; hence this report was produced without departmental strategic guidance. It is imperative for DND to clearly state a GITV strategy before any automated identification technology system is implemented on a large scale.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified. If it not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title).

Automated Identification Technology (AIT)
Barcodes
Global In-Transit Visibility (GITV)
Radio Frequency Identification (RFID)
Supply and Distribution System

DRDC CORA

www.drdc-rddc.gc.ca