Copy No. _____

Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

Thoughts on a Design Framework for System Integration

Anthony W. Isenor
Anna-Liesa S. Lapinski

Defence R&D Canada – Atlantic

Technical Memorandum
DRDC Atlantic TM 2006-143
November 2007

Canada

This page intentionally left blank.

Thoughts on a Design Framework for System Integration

Anthony W. Isenor and Anna-Liesa S. Lapinski

Defence R&D Canada – Atlantic

Technical Memorandum
DRDC Atlantic TM 2006-143
November 2007

Principal Authors

Original signed by Anthony Isenor and Anna-Liesa Lapinski

Anthony W. Isenor and Anna-Liesa S. Lapinski

Defence Scientists

Approved by

Original signed by David G. Hazen

David G. Hazen

Head, Technology Demonstration Section

Approved for release by

Original signed by James L. Kennedy

James L. Kennedy

DRP Chair

Abstract

The problem of integrating heterogeneous systems is discussed. Some keys to the success of multi-system integration are establishing a team environment among those performing the integration, ensuring data interoperability, and designing an integrated system that takes into account everything the new system must do. The interaction of personnel to build a collaborative and trusting environment for the integration process is discussed. The important issues related to data interoperability, such as data naming, structure and content, are described. The data and personnel elements are then considered within a design framework. The framework of Cormier is reposed as a series of questions that should be considered before the integration development. Regulative elements of system integration, such as the impact of the Canadian Privacy Act on personal information, are also considered.

Résumé

Le problème d'intégration de systèmes mixtes est abordé. Quelques clés de la réussite de l'intégration de multisystèmes consistent à établir un environnement d'équipe parmi ceux qui effectuent l'intégration, à assurer l'interopérabilité des données et à concevoir un système intégré capable de toutes les tâches qu'il doit accomplir. L'interaction du personnel qui bâtira un environnement de coopération et de confiance pour le processus d'intégration est étudiée. Les questions importantes liées à l'interopérabilité des données, telles que l'appellation, la structure et le contenu des données sont décrites. Les éléments données et personnel sont alors examinés dans un cadre de conception. Le cadre de Cormier est réétudié sous forme d'une série de questions qu'on devrait prendre en considération avant d'effectuer l'intégration. Les éléments normatifs de l'intégration des systèmes, comme les effets de la *Loi sur la protection des renseignements personnels* du Canada sur notamment les renseignements personnels sont également examinés.

This page intentionally left blank.

Executive summary

Thoughts on a Design Framework for System Integration:

Isenor, Anthony W.; Lapinski, Anna-Liesa S.; DRDC Atlantic TM 2006-143; Defence R&D Canada – Atlantic; November 2007.

Background

The integration of multiple heterogeneous systems is a current topic of interest. The people performing the integration obviously play an important role. However, data interoperability, or the ability to share and utilize the data across the systems is also important. The process of integrating systems also requires a design plan, or framework, which helps identify important characteristics of the integration process. A recent article in the Canadian Military Journal by Cormier outlined a design framework (termed an architecture by Cormier) for information management at the Office of the Judge Advocate General. Cormier identified nine key components to be considered during the design of an individual system. However, the design framework can also be considered from the perspective of system integration, where multiple autonomous systems are brought together or joined via a data interoperability strategy.

Principal results

The interaction of personnel to build a collaborative and trusting environment is identified as a key to the integration process. The important issues related to data interoperability are identified as the data naming, structure and content. The framework of Cormier is reposed as a series of questions that should be considered before the integration development. Regulative elements of system integration, such as the impact of the Canadian Privacy Act on personal information, are also considered.

Significance of results

The article assembles many of the critical issues faced by those attempting system integration. The paper would be of benefit to those about to begin or already involved in system integration. It is a general treatment of the topic that could be applied to any system integration tasking, especially those in a government, security or military environment.

Future work

Further efforts related to data interoperability issues are being addressed during the Networked Underwater Warfare Technology Demonstration Project, underway at DRDC Atlantic. These efforts are focused on sonar and environmental data related to antisubmarine warfare operations.

This page intentionally left blank.

Sommaire

Thoughts on a Design Framework for System Integration:

Isenor, Anthony W.; Lapinski, Anna-Liesa S.; DRDC Atlantic TM 2006-143; R & D pour la défense Canada – Atlantique; Novembre 2007.

Situation générale

L'intégration de systèmes multiples constitue un sujet d'intérêt courant. Il est évident que les personnes qui effectuent l'intégration jouent un rôle important. Toutefois, l'interopérabilité des données ou la capacité de partager et d'utiliser les données dans tous les systèmes est aussi importante. Le processus d'intégration de systèmes exige également un plan, ou cadre, de conception qui contribue à en déterminer les caractéristiques importantes. Un article récent de Cormier, publié dans la Revue militaire canadienne décrit un cadre de conception (appelé architecture de Cormier) pour la gestion de l'information au Cabinet du Juge-avocat général. Cormier a dégagé neuf éléments clés à étudier pendant la conception d'un système isolé. Cependant, le cadre de conception peut aussi être considéré du point de vue de l'intégration de systèmes où de nombreux systèmes autonomes sont réunis ou reliés par une stratégie d'interopérabilité des données.

Résultats

Une discussion sur l'interaction du personnel qui bâtira un environnement de coopération et de confiance pour le processus d'intégration est présentée. Les questions importantes liées à l'interopérabilité des données sont déterminées comme étant l'appellation, la structure et le contenu des données. Le cadre de Cormier est réétudié sous forme d'une série de questions qu'on devrait prendre en considération avant d'effectuer l'intégration. Les éléments normatifs de l'intégration des systèmes, comme les effets de la *Loi sur la protection des renseignements personnels* du Canada sur notamment les renseignements personnels sont également examinés.

Portée

L'article réunit un grand nombre des questions critiques auxquelles sont confrontées les personnes qui essayent d'intégrer des systèmes. Les personnes qui sont sur le point de commencer ou ont déjà commencé l'intégration de systèmes bénéficieraient du travail, qui traite le sujet de manière générale, permettant ainsi de l'appliquer à tout travail d'intégration de systèmes, notamment dans l'environnement gouvernemental, militaire ou de la sécurité

Recherches futures

Les futures recherches concernant les questions d'interopérabilité des données sont traitées dans le cadre du projet de démonstration de technologies de la guerre sous-marine en réseau, mis en œuvre par RDDC Atlantique. Les travaux se focalisent sur les données sonar et environnementales relatives aux opérations de guerre anti-sous-marine.

This page intentionally left blank.

Table of contents

List of figures

1 Introduction

Many things are taken for granted, for example, our ability to transfer ideas. Consider the words on this page, or the sounds from someone's voice. Both relay information because a receiver can read the words, or hear the sounds. If the two people involved – the writer and reader, or speaker and listener – share a common language, then it is likely that the two have made a successful transfer of information.

Information transfers also play an important role in computer networks. Relating the above people example to a computer network, it is realized that the two people have formed an integrated system. The system is constructed from four parts; namely: the people, the staging (e.g., two or more people who are able to speak and hear standing in proximity to each other, in an air filled room), the information being passed, and the dictionary and grammar rules of their language. Each person is analogous to an individual computer system; that is, a set of software applications that share a common goal. The staging is analogous to the structure or architecture implementation of the integrated system which enables the exchange of information. The verbal or written information being passed is analogous to electronically stored data transferred between systems. Finally, the dictionary and grammar correspond to the data structure.

In the computer networking world, the goal is easy to express – system integration. System integration, in both the human and networking case, is formed by the successful exchange and utilization of the data that exists in the individual systems. Simply, the requirement is to have individual systems communicate among each other as easily as when your friend tells you that it's going to rain.

The two main ingredients of system integration, which are illustrated in Figure 1, are data and people. The proportions of data and people will be unique for each integrated system, but both ingredients must always be present. However, in order for the integration to take place an architecture must be designed and implemented. It is proposed that for a successful system integration there are data, people and architecture design issues that must be addressed. Some keys to completing the goal would be (see Figure 1):

i. establishing collaboration and trust between the people involved,

ii. ensuring successful exchange and utilization of data; i.e., data interoperability, and

iii. designing an integrated system that takes into account everything the new system must do.

This paper attempts to highlight some system integration issues by addressing the above three points. First, consideration is given to the people involved in the process of system integration and how these people need to build a collaborative and trusting environment. Next, insights into the problems caused by the data themselves are discussed. Following that, a design framework for multi-system integration is reviewed, with the framework constructed largely from the work of others. The framework is intended to help the designers formalize the functionality of the integrated system. An example is described where the design framework is applied to a simplistic scenario involving two systems. The design framework is then placed in context with the DND

Architectural Framework. Finally, as an example of the regulative processes that can influence system integration, a particularly difficult type of information, personal information, is considered. Personal information (e.g., a persons name, sex, race, age, etc.) places additional constraints on the data exchange and sometimes makes the direct and explicit exchange between multiple government departments impossible. Without prejudicing the ongoing design process, the Canadian Marine Security Operations Centre (MSOC) approach to this problem is described as a method of dealing with personal information. The MSOC is attempting to bring together various government departments to collaborate on maritime security issues.

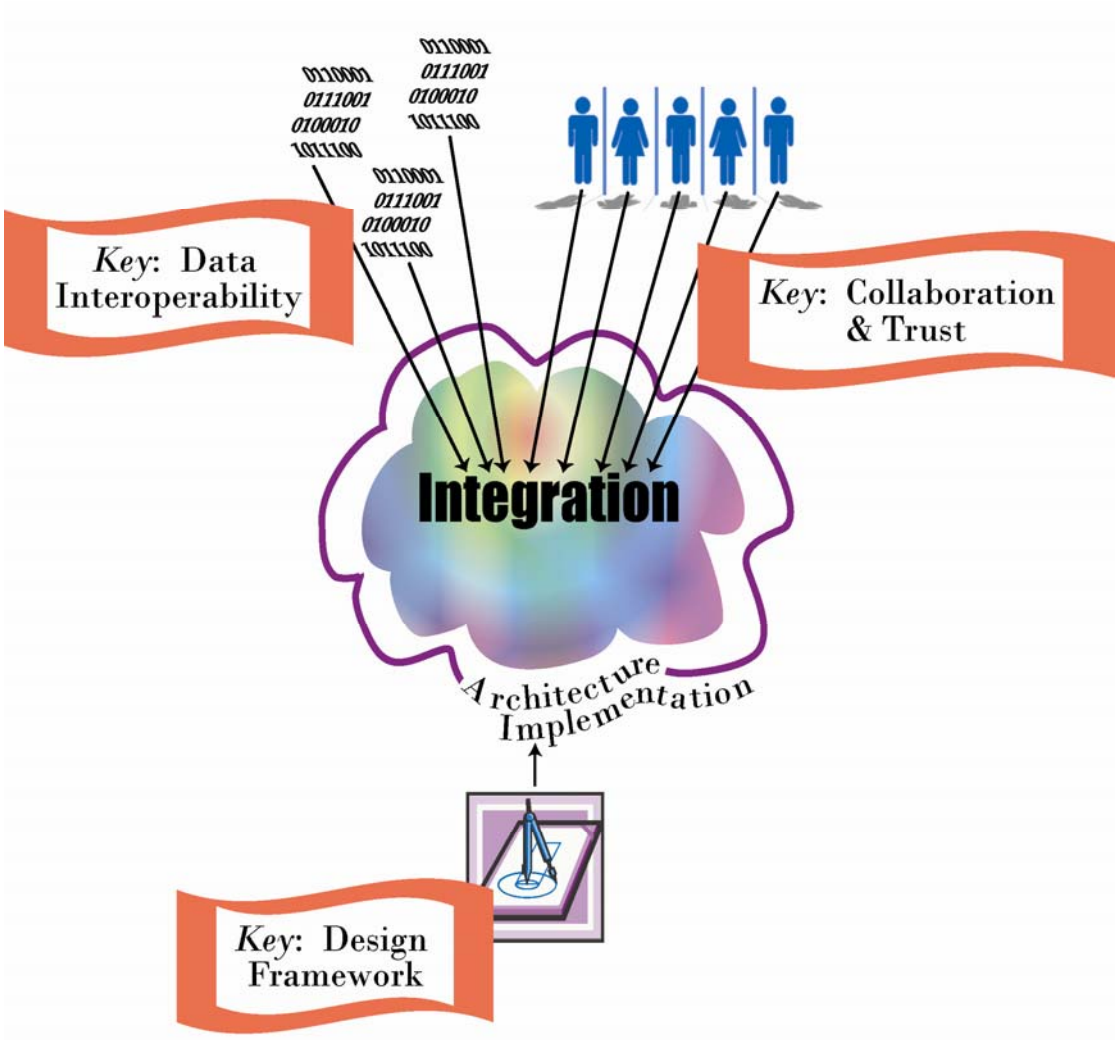

Figure 1: Two main ingredients of system integration are data and people. The mixture's exact ratio depends on the level and type of required integration. A third requirement is the architecture design that structures the architecture implementation. Three keys to successful system integration are (i) establishing trust and collaboration between the people involved, (ii) ensuring data interoperability, and (iii) designing an appropriate architecture by utilizing a design framework.

2 People: Collaboration & Trust

A system design approach must recognise people as the builders of the initial systems and also as the drivers for the integration. Therefore, the construction of any system involving multiple players must deal with the issue of personal interaction between representatives of the initial systems. The process has to start at the personal interaction level and only after personal interaction is established, can integration begin. In effect, this places people as the initial and most critical component in the integration process.

The follow-on from the initial personal interaction is the first requirement for the formation of a team – *collaboration*. Personal interaction is the act of meeting and talking, while collaboration is the act of working jointly on a task that hopefully furthers the functionality of the parties involved. Some degree or amount of collaborative work is required to take the participants to the next team requirement – *trust*.

Trust has many definitions, but here it is considered to be a state of mind. Trust is a faith or belief in something or someone. Trust is based on cumulative past experience, rather than on current evidence. Trust is often applied to the future. A person constructs a sense of trust toward someone else after interacting with them. Although systems can be constructed to assess past performance, reliability, and uncertainty in output, this is not really a measure of trust. Systems don't experience trust; people do.

Collaboration and trust are required to bring the integrated system into existence. People must work together to integrate systems and there must be trust between the people that they will do it correctly. However, collaboration and trust also play a role after integration. In fact, collaboration and trust are a critical factor throughout the integration and implementation. Take for example, the integration of systems between government departments. Upon the examination of requirements and availability, it may become clear that one department needs information that another department has access to but has previously not been storing or even collecting. Collaboration is required for one department to request that information from the collecting department. After this arrangement is set up, trust becomes an issue because the typical employee of the collecting department may not be privy to why the information is needed. Of course, there is advantage in having a collector possess an understanding of the benefits associated with the particular data. In that case, the collector is better able to prioritize their efforts in high tempo situations. When the collector does not understand why they are collecting the particular data, if trust has been established (and plausible reasoning can solidify the justification for collection), then the collector will likely proceed to feed the data into the system. The collector must also trust the receiving department to properly handle and safe-guard the collected data.

Another example of how collaboration and trust might influence integration involves two or more departments independently collecting identical information. An agreement could be established between departments, with one department being made responsible for collecting and distributing the information to the other departments. In this case, collaboration is represented by both the agreement and the completion of the data collection and distribution task, while trust is represented by the receiving department having faith in the competence of the data collection and distribution.

People are an important ingredient in system integration and establishing collaboration and trust between the key people is a necessary element of the system integration process. Given this perspective on some of the issues related to people, the next consideration is toward the more technical area of how data interoperability is important in the process of system integration.

3 Data Interoperability

Achieving data interoperability is important in establishing a useful integrated system. It can provide an assortment of positive outcomes in the government, security and military realms. For example, data fusion, which is the combining of data from multiple sources, can become enhanced by allowing new information to be discovered that was unrealizable from any one source. Also, the ability to visualize data sets from multiple sources has the potential to provide operators or analysts with capabilities only previously realized by examining multiple paper representations of information on a board room table.

Anyone who has attempted to design a system that contains and utilizes one or more data sources has a sense of the potential extent of the data interoperability problems. The issue really boils down to understanding the data within the constructed system. However, it is not good enough to understand some of the data characteristics. Those involved have to understand the details of the data, such as relationships between data, units associated with the data, how the data were processed, etc.

Data is often considered to be "closer to the sensor", as compared to information[1]. However, at the system level, data and information may both be represented as numbers or characters that are passed between systems. Thus, in terms of transfers between systems, both data and information may be considered data. This is the perspective taken in this paper.

Creating a single system that utilizes sensor data is a large problem. There are so many issues to consider, such as what the sensor is actually measuring as compared to the parameter required, or the complex algorithms that derive the required parameter. Of course, the single system perspective is only the initial phase. The focus on interoperability places a clear requirement on systems to allow the sharing and, more importantly, the utilization of data from multiple sources. Problems are amplified when considering system integration, especially non-similar, or heterogeneous, systems.

Consider for a moment two independently built systems that are related, but nevertheless, serve different purposes. The problem of linking, joining or integrating these heterogeneous systems is as complex as the initial development that created the systems. Here, the issue is not the physical merging of the systems into another individual system, but rather a joining that occurs at the data level between the existing individual systems. It is the development effort that allows one system to use data from another system that represents the main challenge.

Of course, this challenge has been evolving over the years. Initially, the challenge was one related to software; specifically, how the software could be modified to read system-dependent data formats produced from other software. Incompatible formats provide many parsing challenges, which meant it was a difficult and complicated task to write an application to read the data. More recent advances in formats have resulted in available parsers (e.g., eXtensible Markup Language parsers [3]) which greatly reduce this problem. This reduction in the parsing problem

[1] Data may be considered the processed measurements produced by a sensor. Information is constructed by combining data to form an understanding of the environment. For a description of data and information, see [2].

has shifted the focus of the problem towards the data itself; specifically, making a system understand what the data means. The receiving system cannot hope to utilize the data unless it understands the meaning of the data, as understood and used within the providing system.

To fully understand the data, one needs to consider and understand three key data-aspects: the name, structure and value associated with the data from the providing system. These aspects are related to both the data content and the data representation. Data content is essentially the data values, while representation deals with naming and structure associated with the data.

Consider further name and structure. The name is typically a label associated with the data. It may be a real label that is part of the stored data or it may be an assumed name. The name will often have certain connotations to the problem area for which the data was collected. Second, the data are often contained within a structure, like a hierarchy. Structures are important because they sometimes provide implicit relationships among data items. It is common that the data structure in one system does not exactly match the structure used in another system.

So what kind of problems could result from incompatibility in the three data-aspects? Well, terminology in one system (i.e., the label) could be identical to the terminology in another system, while referring to totally different types of data. Of course, the opposite is also true – different labels could refer to the same type of data. In terms of data structure, it may be that relationships formed in one system do not apply to the other system. In one particularly difficult case, the actual label may implicitly contain structured data. For example, a system may use data that has a label of *shipname*. The datum value associated with this label could be "CFAV QUEST". This implies the "CFAV QUEST" is a ship, because the label contains the ship information. Finally, one system may allow a particular content, which is not allowed in another. For example, a current system considering water vehicles allows for autonomous underwater vehicles. However, an older system that also considers water vehicles may not even recognize the existence of such a vehicle. Units of measure associated with the data are another common content issue.

Data, like people, are an important ingredient in system integration. Ensuring successful exchange and utilization of data is key to successful system integration. Understanding the three key data-aspects will help in the pursuit of data interoperability and, therefore, system integration. However, the data and people need a stage within which to work. The next section introduces this stage – or design framework – to help architect the integrated system.

4 Design Framework

At this point there should be an appreciation for the key data-aspects and personal interaction required to integrate systems. Next, components of a design framework are considered. A recent article by Cormier [1] discussed a system development architecture at the Office of the Judge-Advocate General. Although Cormier identifies this as an architecture, here it is identified as a design framework, thereby distinguishing it from a more computer-based architecture that describes system components.

The Cormier paper describes a design framework for the development of a single system. Although Cormier notes that this framework may not necessarily meet the requirements of the higher-level organization, many of the ideas expressed by Cormier can be applied to the higher-level integration. The relationship between the components of the Cormier framework and the integration process are presented here. As well, the Cormier components are expanded to encompass some additional issues important in system integration.

Cormier outlines a framework with nine components:

- business context;
- information requirements;
- information resources;
- information management activities;
- records management;
- human resources;
- standards, education and training;
- sustainable development; and
- information technology.

In the following, each of these components is considered from the perspective of system integration (the components are indicated using bold text). However, the components are first transformed into a set of questions. These questions are shown in Figure 2 and described in the sections that follow.

4.1 Why is the information needed?

The first of these components, the **business context**, must be understood during system integration. The business context helps in the understanding of why the information is needed (i.e., in what context with regards to the business taking place). As Cormier points out, knowing the business context helps in "later analysis [of the organizational processes] and to enable the optimization of information flows and holdings". While it is important to understand why the

information is needed in the individual systems, at the integration level it is also important to understand why one system requires certain information from another system. Understanding is an important first step to optimizing the architecture design of an integrated system. In addition, understanding why information is needed and explaining the need to the departments involved helps instil trust.

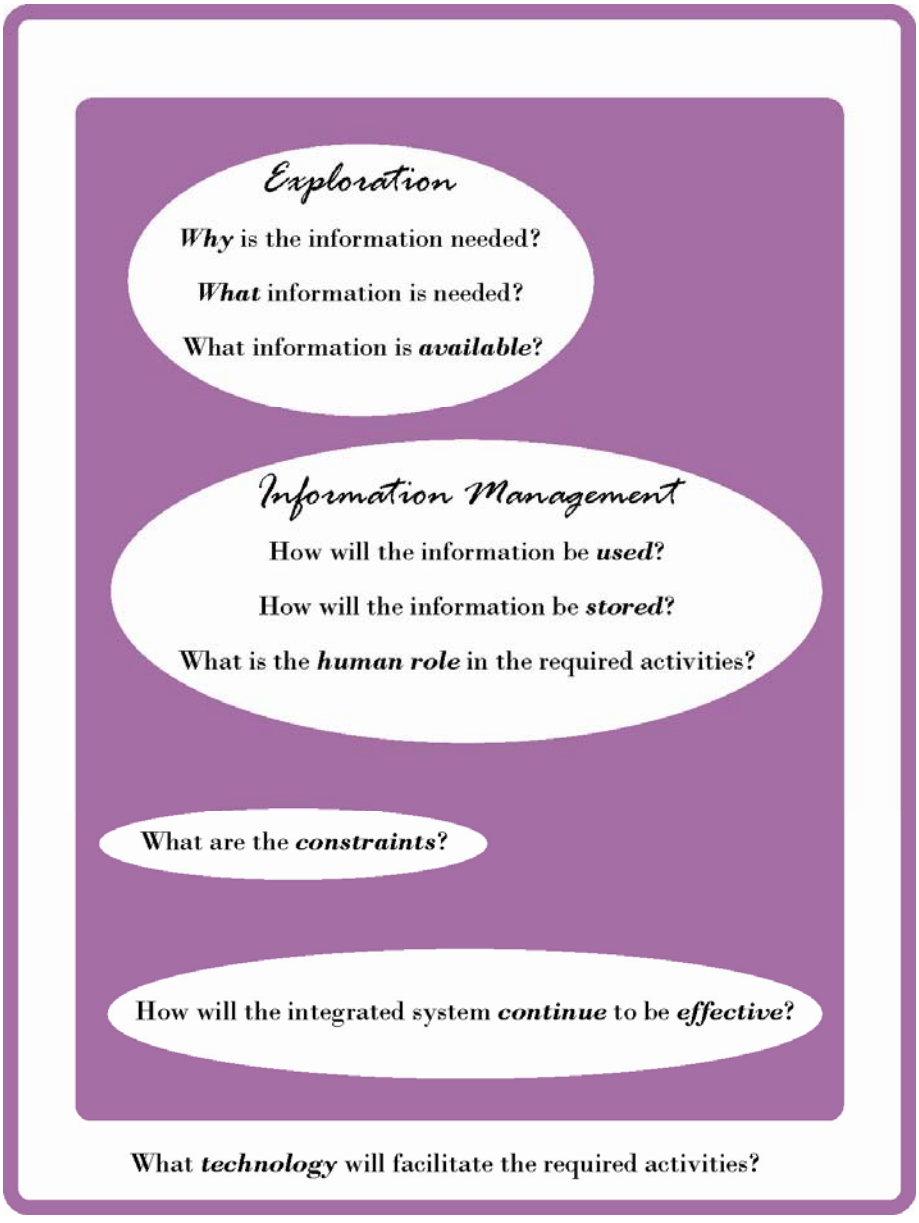

Figure 2: The design framework. A question-based interpretation of the Cormier [1] architecture.

4.2 What information is needed?

The business context is intertwined with the **information requirements**. The motivation for integrating systems in the first place is because the combined information requirements of the departments are not adequately satisfied by systems presently accessible by those departments. The information requirements of the collective departments can only be realized by the integration of the multiple systems. In order to design an effective architecture all individual information requirements must be documented so that when examining the information available for cross-over from one system to another, the information that is needed can be found in the information that is available.

4.3 What information is available?

As implied above, it is important to document the **information resources** that each system can contribute to the integrated system. Each individual system that is a component of the integration has numerous information resources. The individual system effectively combines these resources and presents the multiple resources as a single resource to the integrated system. Thus, it is likely that the available information resources decrease in number in the integrated system as compared to the set of individual systems. It should also be realized that as departments examine the information available from other departments, there will likely be modifications to the initial information requirements.

4.4 How will the information be used? How will the information be stored?

The Cormier components of **Information management activities** and **Records management** are encompassed by the above two questions. These components are related and are somewhat difficult to separate. For example, Cormier lists the information management activities as "find, create, receive, acquire, monitor, classify for records management, index for content management, safeguard, verify for accuracy, organize, store, access, use, collaborate, send, route, disseminate, publish, transfer, archive and dispose." However, some of those activities may be more rightly considered records management activities. That suggestion is elaborated upon below as the two questions are discussed.

In terms of how the information is used, consider Cormier's **information management activity** descriptors: collaborate, verify for accuracy, monitor, use, find, access, disseminate, publish, send, and route. Only slight modifications to these system level descriptors are required when considering the integration level. For example, verification for accuracy at the system level may become verification of consistency at the integration level. The responsibility for accuracy of

content will remain at the collection system level. The consistency issue will deal with the reconciliation of near-duplicate data, or worse the reconciliation of opposing data.

Next, the Cormier information management activities of archive, dispose, receive, organize, store, and safeguard are considered in terms of how the information is stored (i.e., similar to Cormier's **Records management**). All of these activities will also be required in the integrated system. The integrated system may also need additional activities; for example, a reaction strategy for changes in the source data. In this situation, the source data changes need to be identified and reassembled in the integrated system.

The remaining information management activities identified by Cormier include transfer, classify for records management, index for content management, acquire, and create. These activities may be related to usage, but perhaps more specifically are activities which enable usage.

4.5 What is the human role in the required activities?

With regard to the single system information design framework, Cormier states, "one must imagine what comprehensive information management would be like, state it in the form of a Concept of Operations (CONOPS), and project that CONOPS onto **human resources**". Human resources will continue to play a role at the integration level. The new information sources available in the integrated system will change the information set used to complete a particular tasking. The CONOPS for the integrated system will need to reflect these new information sources. Of course, this means the CONOPS related to each single system must be understood before the integrated system CONOPS can be developed.

4.6 What are the constraints?

Cormier points out that "people need **Standards, education and training** if they are to efficiently conduct information management activities." Standards, education and training will again play an important part in the integrated solution. While all three can apply to the human dimension (e.g., standard operating procedures, education and training in system use), the use of standards in terms of the technical solution also applies. Standardized structures for data transfer, standardized dictionaries of terms, thesauri, and gazetteers, will all be important to the successful integration of the systems. These types of things assist with both standardization of name, structure and content, as discussed earlier.

Taking it a step further, the authors propose that standards, education and training essentially fall into a larger category: constraints. These are constraints placed upon the people (e.g., an essential skill set) and the system (e.g., structures for data transfer). Under this larger umbrella of constraints are also things such as legislation, departmental statutes, policies and security regulations. All of these additional things restrict the transfer of data and the manner in which it is transferred. Some impacts of these non-technical constraints are described in the following section.

4.7 How will the integrated system continue to be effective?

Sustainable development at the integration level relates to the governance of the integrated system. Governance is critical, because without it there is no evolution of the integrated system. Governance provides a means for system stakeholders to influence and modify the system to better meet their needs, while not hindering or disrupting the needs of others. All of the planning layers for architecture maintenance noted by Cormier, those being "business strategy, information management strategy, architectural inputs, information architecture, guidance and direction, training, platforms, environments, security, and information," apply at the integration level as well.

4.8 What technology will facilitate the required activities?

Cormier describes **information technology** as a core enabler to information management. Information technology also remains a critical enabler at the integration level. The information technology is the computers, monitors, keyboards, cabling, software, internet connections, etc. The technology is obviously an important part, but business context and requirements must drive the technology choices, not the other way around.

***

The design framework described by Cormier provides us with a basis to conceptually describe other more general systems created through the integration of individual systems. It is proposed that by answering the questions posed in Figure 2 and following the framework as described above, system integration designers will better formalize the functionality of the new system. In the following section the framework is applied to help demonstrate this point.

5 Simplistic Application of the Framework

A brief and simplified example may illustrate the application of the design framework in an integration scenario.

Think about the case where two individual systems are being considered for integration into a single system. System A is an air-based system, flown in a patrol aircraft. This system collects information on suspicious vessels, for example instantaneous vessel position, course, speed, name and aerial photograph. System L is a land-based system. It is used to coordinate interception of sea-to-shore activities. This system requires location information, road atlas information and gradation information on potential shore landing areas.

In order to prepare for integration, the design framework is applied to typical scenarios for which integration will help the land and air sides achieve their individual goals. In this particular scenario, a vessel has been identified as a vessel of interest (VOI). During daylight, the aerial unit investigates from a distance while not drawing any suspicion from the vessel. The suspected landing time is during the night. The following considers the framework questions in relation to this scenario:

Why is the information needed? – The information is needed because System L needs to facilitate the tracking and identification of the VOI so that land activities can be coordinated. The land authorities need the location and characteristics of the vessel as it approaches the shoreline, prior to being in view from the shore. For example, the land-based identification typically takes place from the shore. Thus, visual characteristics of the vessel are needed to enable identification from a large distance and low elevation.

What information is needed? – Position, speed and heading information on the VOI and visual characteristics of the vessel, such as dominant vertical infrastructure on the vessel or dominant colors.

What information is available? – System A contains the information needed. The aerial surveillance has instantaneous position, course, speed, vessel name and photographic information available. All information is in digital form in System A, on the aircraft.

What are the constraints? – 1) Bandwidth limitations between air and land systems greatly limit the communication ability making transmission of photographic information impossible. 2) System A must allow for the electronic storage of text descriptions of the ship, which it currently does not do. 3) System L requires the information to be sent in plain text format using a set structure such that standard database technology can parse and store the information in System L.

Transfer data standards for map-based objects also allow the integrated System L to visually represent the predicted position of the VOI. Mapping between the naming conventions used within each System could present problems. 4) System L uses a secure, encrypted, network which includes a firewall. 5) Certain weather conditions can disrupt communication abilities between the systems.

Note that there is a difference between system integration constraints and constraints (or limitations) on the information's usefulness. For example, the following are constraints on the information from the surveillance aircraft being used to coordinate interception of sea-to-shore activities, but have little to do with the actual integration: 1) Prior to being in view from the shore, the position of the vessel is only well known when the aerial surveillance is taking place therefore the land authorities do not have a constant source of information, and the quality of past information degrades with time. 2) The surveillance aircraft only flies during the day and the ship is expected to make landfall at night.

What is the human role in the required activities? – CONOPS generally remain the same on both sides with the following exceptions: The land authorities require visual information that is useful from a large distance and low elevation. The air personnel do not typically collect this, as the photograph meets their immediate needs. In an integrated system that doesn't allow the passing of digital photographs, the air personnel will need to explicitly note this information in electronic form; thus an alteration in operating procedures is required. On the land side, there must be someone charged with the task of anticipating and monitoring the new information for their tracking and identification activities.

How will the information be used? Stored? – The instantaneous position, course and speed will be used to predict the vessel's position at the time corresponding to land searching. Some form of an error estimate will also be required to indicate the uncertainty in the prediction. The characteristic information will be used to help positively identify the ship from shore as it approaches. The aerial information will be collected and stored electronically in the basic file system already in use in System A. System L will store the information in a database.

What technology will facilitate the required activities? – 1) The form the integration of the systems can physically take will have to be based on feasibility and the needs requirements of the land and air communities, which should become clear after applying this design framework to all the scenarios (i.e., it can't be stated at this time). For this particular scenario, simple one-way integration could be achieved by emailing the information from System A to system L. 2) The transfer of position, speed, heading, etc. should be coordinated via standard database technology. 3) Technology that adheres to transfer data standards for map-based objects that allows the integrated System L to visually represent the predicted position of the VOI.

How will the integrated system continue to be effective? – Increased bandwidth between systems would facilitate transfer of photographic information. As well, standardisation of data transfer would allow a common map display between System A and L. This would allow both systems to access and display common information.

***

The above example is simplistic; however, it illustrates that the nine question framework can provide a basis from which to begin an assessment prior to integrating two or more systems. To construct a more detailed view of the system integration, the DND and Canadian Forces (CF) Architecture Framework (DNDAF) is a complementary option, as described in the next section.

6 DND and CF Architecture Framework

It is instructive to now consider the questions developed within this design framework, to other existing frameworks within DND - in particular the DNDAF [4].

The DNDAF is a guidance document that assists in the organization, analysis and communication of information relevant to the life-cycle of systems. Since it is a guide, the DNDAF provides numerous representations of information that could be relevant to a system. These representations, or views, are different perspectives on the system.

A similarity can be drawn between the views in the DNDAF and the process followed during the construction of a building. During the building design phase, blueprints would be created for the building. At some stage of the process, these blueprints would diverge into specialized perspectives, or views, of the building. For example, individual blueprints would deal with the electrical view of the building; the plumbing view; the concrete view; and the steel-work view. All of these views would pertain to the same building; yet all views would provide a slightly different perspective on the building. The views developed within the DNDAF are similar, where, instead of constructing a building, a system is constructed. The DNDAF views are also applicable to the construction of a system-of-systems.

The DNDAF provides guidance on the construction of six primary views, namely:

- Common view (CV; 2)
- Operational view (OV; 7)
- System view (SV; 11)
- Technical view (TV; 1)
- Information view (IV; 2)
- Security view (SecV; 2)

Each primary view is constructed from one or more subviews, with the number of subviews indicated in the parenthesis. In some cases, subviews are further divided into additional subgroupings.

As an example, the CV provides information that is general to all other views. The CV is composed of two subviews. CV-1 is an overview and summary of the system. This view can be used as a planning guide or information source for a executive-level audience. The summary information is intended to be consistent with CV-1 documents produced for other developments, thus providing a means to quickly compare architectures. CV-2 is a data dictionary for the entire development. The dictionary would specify the terminology used within the other views. CV-2 definitions should be built from CV-2 descriptions for other systems. In this way, there will be consistency across systems thus allowing comparisons among the systems.

The 25 subviews have been compared to the nine questions (Figure 3) in the present design framework. The subviews typically deal with multiple topics, and thus produce an overlap between the questions. This should be expected, as the questions often need context established

by other facts. For example, constraints in terms of information or constraints on human activities have implications for system design.

Figure 3 shows all 25 subviews and the placement of these subviews within the context of the nine questions. For most cases, the subviews relate naturally to the questions. For example, the security view is related to constraints on the use or distribution of information and thus falls within the overlap between available information and constraints. Similarly, operational views are clustered between the information that is required and available, and how it is used by the personnel and the system itself.

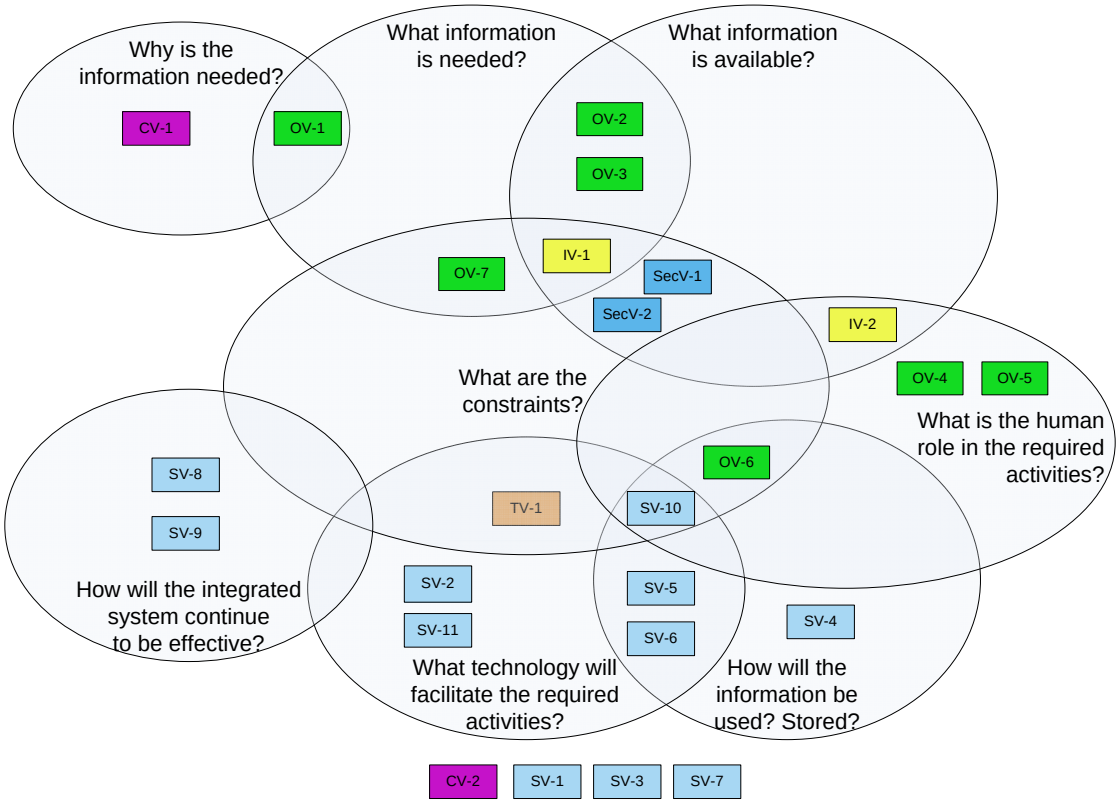

Figure 3: The design framework questions are shown as ovals. The DNDAF is represented as multiple boxes. Each box is labelled and coloured consistent with the DNDAF [4] .

Four subviews do not fit naturally within the nine question framework; these being CV-2, SV-1, SV-3 and SV-7. As noted previously, CV-2 is a data dictionary of terminology that establishes the language used in all other views. Thus, CV-2 doesn't provide a particular view to the system, but rather defines terminology used within the other views. SV-1 describes system distribution among all nodes being considered while SV-3 provides a system-system matrix of interface characteristics between the systems. The design framework presented here does not account for

physical distribution of systems. As well, the framework assumes none of the systems have been integrated and thus, that no interface exist between systems. SV-7 deals with system performance. None of the nine framework questions deal with the end functionality of the system. Although information usage and activities could be related to performance, they were not conceived with that intent.

The design framework as presented in the nine questions shows aspects of system integration in a very broad categorization. Effectively, the questions provide a non-technical basis from which system integration may be understood. For example, management, policy makers and to a large extent the users of the systems do not need to be concerned with the details of SV-4[2]. It may be sufficient for this audience to understand SV-4 as related to the usage of data and information. The design framework helps provide a high-level view of the integration issues.

[2] SV-4 contains clear descriptions of information input and output from each system. This helps ensure that a system's inputs are satisfied by outputs from other systems. In this way, the functional connectivity between the systems is accounted for.

7 Non-technical constraint

In identifying the framework constraints it may become evident that system integration is not possible. In this case, the difficulty may be a non-technical constraint that is common in the government, security and military realms.

7.1 Regulative elements – A Legal Example

This paper has attempted to highlight some key system integration issues. As a final point of discussion, consider the situation where system integration, for non-technical reasons, doesn't appear possible. What if it appears that system integration is not feasible due to constraints caused by legislation or policy, rather than technical problems? Here, the suggestion is that people and data still comprise the central ingredients of the solution. In terms of people, the design framework can be applied to the actual people-integration process. As well, a technical-based solution for sharing sensitive data is described.

As an example, consider the situation where government departments are brought together to share information for a common goal. They will immediately be faced with one critical issue: the data held by the individual departments were not collected with sharing in mind. Here, the primary issue is related to privacy and the collection of data for a particular purpose; thus the Canadian Privacy Act [5] becomes relevant. The Canadian Privacy Act, which took effect in 1983, is an important piece of legislation that protects Canadians from the potential abuse of our personal information. The Act outlines the restrictions on personal information collection, disclosure by government, and distribution to other government departments or institutions. Of course, there are mechanisms in place to release the information for official investigations. However, the use of personal information for data mining purposes (e.g., to identify possible relationships between information items) is prohibited.

Data mining is the process of examining (typically) large volumes of data for relationships or patterns, without particular regard to cause and effect. The data mining task is particularly interesting because it is often a reason for the integrated system to collect the data from the individual systems. However, if the information is personal, the actual exchange of the information likely violates the Privacy Act. In addition, many current practices of collecting information, such as passenger lists, are being questioned from the basis of the Canadian Charter of Rights and Freedoms [6]. The legal issues surrounding the collection and dissemination of information related to an individual becomes very complex, very quickly.

So, how should a security tasking be addressed when it is affected by the privacy issue? In the short term, consider the two initial elements of integration (Figure 1) - data and people - and build potential solutions around these elements.

If personnel are considered, then a conceptual model may be formed of people from multiple government departments working together in the same room, towards a common goal. The systems held by the contributing departments may not need any level of integration, because the

"integrated system" is in effect an integrated system of people. These people understand and respect the constraints of the Canadian legal system, and work to integrate the data from their respective departments while not violating Canadian law.

This is the type of model being followed by the Marine Security Operations Centres (MSOC). It is the goal that these centres will ultimately house personnel from various government departments to work together on various facets of marine security. The core members (Figure 4) will be from the Department of National Defence, Canadian Border Services Agency, Transport Canada, Royal Canadian Mounted Police and Canadian Coast Guard (including Fisheries and Oceans Conservation and Protection Branch). This model co-locates people from the various departments rather than attempting application-level integration.

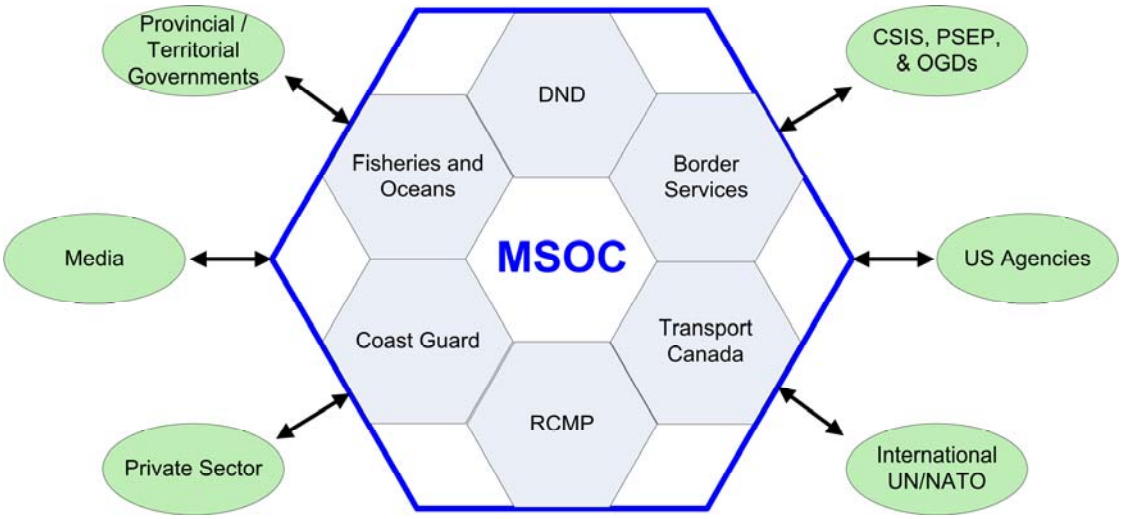

Figure 4: The MSOC co-locates people from multiple government departments and agencies. The MSOC provides an interface to external national and international groups on maritime security issues. Note that the logical entry point for these external groups would likely be specific departments. (CSIS – Canadian Security and Intelligence Service; PSEP – Public Safety and Emergence Preparedness; ODG – Other government departments; UN – United Nations; NATO - North Atlantic Treaty Organisation).

However, what's interesting to note is that the design framework outlined to integrate systems for information sharing (Figure 2), can also be applied to the integration of people – for example, at the MSOC. The person seeking information must understand why the information is needed (e.g., the questions being answered by the information) and what information is needed before they can ask for anything. They must then determine what information is available to them, given the constraints on sharing data. The person in need of the information and the person providing the information must then agree on the information management practices that will be applied to the information, again within the data sharing constraints. All the different types of constraints,

including skills, formats, standards, etc. must be identified. Communication between the two parties must be kept unbroken so that the "integrated system" can remain effective. There will also likely be agreed upon technology that will facilitate the exchange of the information. In effect, the MSOC personnel, who deal with information exchange on a case by case basis, will essentially revisit the questions in Figure 2 for each situation they encounter.

The short term solution of integrating people rather than systems is unlikely to satisfy the needs over the longer term. Two likely reasons will be response time and staffing costs. Fortunately, the data element of Figure 1 provides an avenue to a technical-based solution. A technical solution lies in our ability to share and compare representations of the original data, without sharing the original data. IBM ([7], [8]) is now marketing anonymous resolution software for this purpose – the sharing and comparing of private information. The software performs a one-way hash function[3] on input data, to produce a scrambled string of alphanumeric characters. This string of characters is analogous to a "fingerprint" for the input data. Individual sites (e.g., databases from two departments) run the same one-way hash function to produce their scrambled strings. Then, a search for commonality takes place. The strings are compared using specialized fuzzy matching software. If matches are identified in the scrambled strings, personnel at the analysis sites can make necessary arrangements (e.g., legal authorization) to obtain permission to view the actual data. In this way, strings are shared and compared while the original data remains at the individual sites.

In Canada, the Maritime Information Management and Data Exchange System ([9], [10]) (MIMDEX) is attempting inter-departmental sharing of maritime security information by implementing alerts. These alerts are defined by MIMDEX users, and notify the user when positive conditions are identified in the underlying data. However, legal constraints continue to delay implementation, to the point of threatening the project's future.

Automated systems will be both faster and less expensive to operate over the longer term and will thus be tempting additions to any operational system. In the longer term, government may explore a data and information policy that in some way allows exploitation of the information, while respecting the need for personal privacy. Of course, this will be a complicated balancing act and as such, will be a time consuming process.

[3] A one-way hash function is an algorithm that accepts variable length input strings or documents, and produces fixed length output strings. The one-way aspect means it is computationally infeasible to compute the input, given the output.

8 Summary

The movement towards system integration needs to recognize three keys to the success of the integration process. People are a key initial element, and of particular importance is the building of a collaborative and trusting team. Data interoperability is also widely recognized as a critical ingredient. However, for interoperability there needs to be recognition of the importance of true data understanding as a necessary prerequisite. System integration also needs to follow a clear design framework or methodology. Fortunately, existing frameworks such as that discussed by Cormier provide an important level of understanding to the integration process. The Cormier framework may also be represented as a set of questions which explore the nature of the system integration problem. The Cormier framework is a higher level framework than the DNDAF and therefore potentially more useful in the early stages of planning a system integration. As well, the Cormier inspired design framework questions apply not only to integration at a system level, but also to integration at a people level. This is of importance because the integration process may introduce regulative issues related to the exchange of information which can be dealt with on a case by case basis through the "integration" of people. These regulative issues may have social and legal implications, such as the sharing of personal information. Efforts are underway to balance the need for system integration with the social and legal issues.

9 References

[1] Cormier, Maj. Patrick, (2005), The Way Ahead for Information Management, Canadian Military Journal, Autumn 2005.

[2] Girard, Lieutenant-Colonel John, (2004), Defence Knowledge Management: A Passing Fad?, Canadian Military Journal, Summer 2004.

[3] See the World Wide Web Consortium for information on XML and parsers. http://www.w3.org/

[4] DND, D.E.A. (2006), Department of National Defence and Canadian Forces Architecture Framework (DNDAF), Department of National Defence (unpublished).

[5] Privacy Act (R.S., 1985, c. P-21), see http://laws.justice.gc.ca/

[6] The Privacy Commissioner of Canada (2002), Annual Report to Parliament 2001-2002, see http://www.privcom.gc.ca/information/ar/02_04_10_e.asp

[7] IBM Entity Analytic Solutions, (2005), IBM DB2 Anonymous Resolution: Knowledge discovery without knowledge disclosure, IBM DB2 Anonymous Resolution Whitepaper, May 2005, see www.ibm.com/db2/eas/

[8] SRD Introduces New ANNA Software for Anonymous Data Sharing, Releasing Beta Version, (2004), see http://www.in-q-tel.com/news/releases/10_27_04.html

[9] Standing Senate Committee on National Security and Defence, (2003), Canada's Coastlines: The Longest Under-Defended Borders in the World, , Vol. 1, Chapter 3, October 2003.

[10] Aikins, Greg, (2005), Network-Centric Operations and Interdepartmental Marine Security, Canadian Naval Review, Vol. 1, No. 3, Fall 2005.

List of symbols/abbreviations/acronyms/initialisms

CF	Canadian Forces
CONOPS	Concept of Operations
CSIS	Canadian Security and Intelligence Service
CV	Common View
DND	Department of National Defence
DNDAF	DND and Canadian Forces Architecture Framework
DRDC	Defence Research and Development Canada
DRP	Document Review Panel
IV	Information View
MIMDEX	Maritime Information Management and Data Exchange System
MSOC	Marine Security Operations Centre
NATO	North Atlantic Treaty Organisation
OGD	Other Government departments
OPI	Office of Primary Interest
OV	Operational View
PSEP	Public Safety and Emergence Preparedness
R&D	Research & Development
RCMP	Royal Canadian Mounted Police
SecV	Security View
SV	System View
TM	Technical Memorandum
TV	Technical View
UN	United Nations
VOI	vessel of interest

Distribution list

Document No.: DRDC Atlantic TM 2006-143

LIST PART 1: Internal Distribution by Centre:

2 DRDC ATLANTIC LIBRARY FILE COPIES
3 DRDC ATLANTIC LIBRARY (SPARES)
1 D. HAZEN
1 M. E. LEFRANÇOIS
1 W. A. ROGER
1 G. R. MELLEMA
1 J. S. KENNEDY
1 M. MCINTYRE
1 W. CAMPBELL
1 T. HAMMOND
1 D. CHAPMAN
1 S. WEBB
1 F. DESHARNAIS
1 B. MCARTHUR
1 A.-L. LAPINSKI
2 A. W. ISENOR (1 CD COPY, 1 HARD COPY)

20 TOTAL LIST PART 1

LIST PART 2: External Distribution by DRDKIM

1 NDHQ/DRDKIM 2-2-5

1 LCDR DAVID ANDERSON, DPDOIS OR
National Defence Head Quarters
101 Colonel By Drive
Woodline, 546
Ottawa

1 ANDREW BILLYARD, CFAWC OR
3701 Carling Ave
Ottawa, Ontario
K1A 0Z4

1 MAJOR PATRICK CORMIER
30, rue de l'Éboulis
Gatineau QC J8Z 2T9

1 ABE JESSION
National Defence Head Quarters
101 Colonel By Drive
Ottawa

1 J6
PO Box 99000
Stn Forces
Halifax, NS
B3K 5X5

1 J6
Maritime Pacific Headquarters
PO Box 17000
Stn Forces
Victoria BC
V9A 7N2

1 DAVID MASON, DASOR
National Defence Head Quarters
101 Colonel By Drive
Ottawa

1 MICHAEL ORMROD, LFORT 4
National Defence Head Quarters
101 Colonel By Drive
Ottawa

1 LAURA OZIMEK DSTM 5
DRDC Corporate
305 Rideau Street
Ottawa

1 JOCELYN TREMBLAY, CORA CSci
National Defence Head Quarters
101 Colonel By Drive
Ottawa

1 GREG WALKER, DSTM 3
DRDC Corporate
305 Rideau Street
Ottawa

1 DONNA WOOD, DST C4ISR 4
DRDC Corporate
305 Rideau Street
Ottawa

13 TOTAL LIST PART 2

33 TOTAL COPIES REQUIRED

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall 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.)

Defence R&D Canada – Atlantic
9 Grove Street
P.O. Box 1012
Dartmouth, Nova Scotia B2Y 3Z7

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.)

Thoughts on a Design Framework for System Integration:

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

Isenor, Anthony W.; Lapinski, Anna-Liesa S.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
November 2007	34	10

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.)

Defence R&D Canada – Atlantic
9 Grove Street
P.O. Box 1012
Dartmouth, Nova Scotia B2Y 3Z7

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
11cg01	

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC Atlantic TM 2006-143	

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.)

The problem of integrating heterogeneous systems is discussed. Some keys to the success of multi-system integration are establishing a team environment among those performing the integration, ensuring data interoperability, and designing an integrated system that takes into account everything the new system must do. The interaction of personnel to build a collaborative and trusting environment for the integration process is discussed. The important issues related to data interoperability, such as data naming, structure and content, are described. The data and personnel elements are then considered within a design framework. The framework of Cormier is reposed as a series of questions that should be considered before the integration development. Regulative elements of system integration, such as the impact of the Canadian Privacy Act on personal information, are also considered.

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 is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

system integration; data interoperability; information management; design framework, architecture framework; DNDAF; MSOC; collaboration; information sharing; data sharing

This page intentionally left blank.

Defence R&D Canada

Canada's leader in defence
and National Security
Science and Technology

R & D pour la défense Canada

Chef de file au Canada en matière
de science et de technologie pour
la défense et la sécurité nationale

www.drdc-rddc.gc.ca