Government of Canada Gouvernement du Canada

CENTRE for SECURITY SCIENCE

An Architecture Approach to Refining Requirements for an Interoperable CBRN Incident Scene Support IT Tool

Simona Verga
DRDC- Centre for Security Science

Defence R&D Canada –

DRDC Centre for Security Science N 2007-003

Canada

Principal Author

Simona Verga

DRDC Centre for Security Science Operational Research

Approved by

Dr. Paul Chouinard

DRDC Centre for Security Science Operational Research

Approved for release by

Dr. Andrew Vallerand

DRDC Centre for Security Science

Chair Document Review Panel

Abstract

This document explores the potential of using an architecture model to capture the need for interoperability and communications, in support of a potential project to build an integrated and interoperable crime scene support tool for managing CBRNE events. The model considered is the US Department of Defence Architecture Framework (DoDAF). Such a framework could provide a structured hierarchy where data collection and analysis can be carried out independently at different levels, allowing each contributing system/organization meet its internal needs, but in a way that is consistent with and respectful of the requirements of other organizations involved. The work outlines how DoDAF concepts and methodology may be applied for this purpose.

Résumé

Ce document explore la possibilité d'utiliser un modèle d'architecture pour saisir la nécessité de l'interopérabilité et de la communication, à l'appui d'un éventuel projet de construction d'un système intégré et interopérable de criminalistique appui outil pour la gestion CBRNE événements. Le modèle considéré est « US Department of Defence Architecture Framework » (DoDAF). Un tel cadre pourrait constituer une hiérarchie structurée, où la collecte et l'analyse des données peut être réalisée de manière indépendante, à différents niveaux, ce qui permet à chaque système de contingents ou de l'organisation face à ses besoins internes, mais d'une manière qui soit compatible avec et respectueux des exigences des autres organisations concernées. Le travail décrit comment DoDAF concepts et les méthodes peuvent être appliquées à cette fin.

This page intentionally left blank.

Table of contents

List of figures and tables

This page intentionally left blank.

The Chemical, Biological, Radiological/Nuclear and Explosives (CBRNE) Research and Technology Initiative (CRTI) has added a targeted funding category to its program, to address critical gaps in CBRNE response capabilities not addressed by any of the projects that have been submitted and approved through CRTI's five previous calls for proposals. The Forensic Portfolio Manager is considering one potential project that aims to build an integrated and interoperable crime scene support tool for managing CBRNE events. The project will combine commercial software with CRTI developed software products to create a portable, integrated and expandable CBRNE crime scene support tool for Police, EMS and HAZMAT personnel. The finished tool will provide responders with critical CBRNE information sources, standardized incident reporting forms and procedures, mass causality triage management and evidence tagging using Radio Frequency Identification (RFID), and will assist in managing the crime scene providing interoperability and data exchange between the various responding personnel and mobile command control centers as well as providing long-term crime scene data and information for use in potential on-going criminal investigations.

The Forensic Portfolio Manager requested OR assistance to articulate, or refine requirements for the crime scene support tool. This note explores the potential of using an architecture model to do this and capture the need for interoperability and communications, and summarizes the assessment for the Forensic Portfolio Manager. The US Department of Defence Architecture Framework (DoDAF) has found broad applicability across the private, public and voluntary sectors and it is especially suited to large systems with complex integration and interoperability challenges. Such a framework could provide a structured hierarchy where data collection and analysis can be carried out independently at different levels, allowing each contributing system/organization meet its internal needs, but in a way that is consistent with and respectful of the requirements of other organizations involved. The work outlines how DoDAF concepts and methodology may be applied to this project.

1 Background

The Chemical, Biological, Radiological/Nuclear and Explosives (CBRNE) Research and Technology Initiative (CRTI) has added a targeted funding category to its program, to address critical gaps in CBRNE response capabilities not addressed by any of the projects that have been submitted and approved through CRTI's five previous calls for proposals. The Forensic Portfolio Manager is considering one potential project that aims to build an integrated and interoperable crime scene support tool for managing CBRNE events. The project will combine commercial software with CRTI developed software products to create a portable, integrated and expandable CBRNE crime scene support tool for Police, EMS and HAZMAT personnel. The finished tool will provide responders with critical CBRNE information sources, standardized incident reporting forms and procedures, mass causality triage management and evidence tagging using Radio Frequency Identification (RFID), and will assist in managing the crime scene providing interoperability and data exchange between the various responding personnel and mobile command control centers as well as providing long-term crime scene data and information for use in potential on-going criminal investigations.

The Forensic Portfolio Manager requested OR assistance to articulate, or refine requirements for the crime scene support tool. This note explores the potential of using an architecture model to do this and capture the need for interoperability and communications, and summarizes the assessment for the Forensic Portfolio Manager. The US Department of Defence Architecture Framework (DoDAF) has found broad applicability across the private, public and voluntary sectors and it is especially suited to large systems with complex integration and interoperability challenges. Such a framework could provide a structured hierarchy where data collection and analysis can be carried out independently at different levels, allowing each contributing system/organization meet its internal needs, but in a way that is consistent with and respectful of the requirements of other organizations involved. The work outlines how DoDAF concepts and methodology may be applied to this project.

2 The proposed architecture development model

Enterprise IT architectures provide decision makers with information, common terms and concepts, procedures, models, and presentation products that can support operational or planning requirements. Here we follow a methodology used to develop enterprise IT architectures in compliance with the DoDAF Version 1.0. By using a six-step methodology, as seen in Figure 1, Operational, Systems, and Technical Standards Views can be developed to provide enterprise-wide analysis of IT and support various processes, such as capability needs determination.

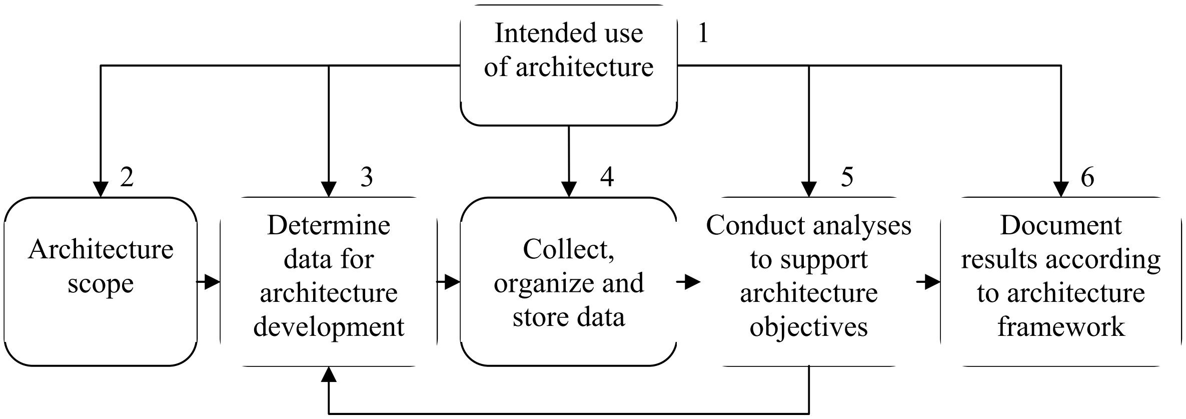

Intended use of architecture
1
2
3
4
5
6
Architecture scope
Determine data for architecture development
Collect, organize and store data
Conduct analyses to support architecture objectives
Document results according to architecture framework

Figure 1: Six step architecture development process

The six general steps are briefly outlined below:

- **Step 1***: Intended use of the architecture*. At this step, the purpose of the architecture should be unambiguously stated. The purpose explains why the architecture is being developed, what the architecture will accomplish and how it may affect organizations or system development. Critical issues, target objectives, key tradeoffs and probable analysis methods may also be clarified at this step.
- **Step 2***: Architecture scope*. The scope defines the boundaries that establish the depth and breadth of the architecture; it bounds the problem set and helps define its context. Other elements of the context that bound the architecture are the environment and the organization's mission and vision. The architecture's scope includes:
  - *Subject Area* - describes the applicable capability, organizational area, or domain to which the architecture applies
  - *Timeframe* - describes the point in time to which the architecture is applicable. Examples of words used to express time frame are current (As-Is or baseline), programmed (budgeted or planned), and objective (To-Be or future).
  - *Intended Users and Uses* - identifies the audience the architecture is intended to serve and how it is expected to use the architecture.

  - *Dimensionality* - helps identify the boundaries of the breadth and level of detail at which the architecture is to be developed; directly related to the purpose and perspective of the architecture.

- **Step 3***: Data required to support architecture development*. During this step, the data entities and attributes (such as activities, organizations, information elements, and other architecture components) are selected. Also selected is the level of detail to which these entities and attributes need to be identified to meet the objectives of the architecture.

- **Step 4***: Collect, Organize, Correlate, and Store Architecture Data*. Following data collection, cataloguing, organizing, and entering the data into automated repositories permit subsequent analysis and reuse. As data is captured and stored, it should be defined and tagged with source information. For reuse purposes, architecture data should be entered into a database. The contents of the database should be stored in terms of models. The database will include the scope, operational concept model, information process model, node connectivity model, behavioural model, and nodal-related data for the architecture.

- **Step 5***: Conduct Analyses to Support Architecture Objectives.* During analysis, the architect selects, compares, assesses, and transforms contextual and architectural inputs based upon the operational concept. The environment is then assessed and defined in terms of a set of assumptions and constraints regarding operational, functional, economic, technological and other factors. These are examined against mandates, missions, various conditions, and perceived needs. Typically, one or more scenarios are used to aid the analyses.

- **Step 6**: *Document Results in Accordance with the Architecture Framework.* The final step in the process involves building architecture products. DoDAF templates enable architecture products to be captured in reusable and shareable form. Architecture developers will build only those products necessary to meet the intended use of the architecture (Step 1).

3 Interoperable CBRN Incident Scene Support IT Tool - The architecture development process

Step 1: Intended use of the architecture

Support the development of an IT system to assist first responders across Canada with incident management and analytical tools, including portable knowledge about CBRNE hazards, calculators, data collection and management (evidence collection, RFID tagging and tracking: procedures, standards, storage) and collaborative information exchange
The architecture is developed as an analytical tool, to ensure a sound basis for the project in order to secure funding. It is intended to underline the capability needs and requirements; the architecture may not need to have the level of detail required for the development of the actual IT system

Step 2: Determine the architecture scope

The scope bounds the architecture's problem set and helps define its context. Elements of the context are the organization(s) involved and the environment. This step involves describing operational, functional, and technological limits of the architecture; determining time frame(s); and recognizing available resources and schedule constraints.

Subject area: CBRNE hazard/crime incident scene management and analytical support

Timeframe: objective – the architecture is applicable to a future system: "to-be" (but most building blocks exist)
Stakeholders (intended users and uses for the architecture):

CRTI – to make the case for allocation of funds for the project;
Department of Public Safety – to make the case for funding the acquisition of the developed product for first responders across Canada, trough JEPP
Police, EMS, Firefighters, HAZMAT, (ER-Hospital) in Canada – to make the case for adopting the product

Intended uses for the system:

- destination of CRTI research generated knowledge
- operational field support: information and operating procedures that are standardized and thus understandable and interoperable across organizations
  - portable knowledge for first responders (recognition guides, CBRNE agent databases and calculators)
  - incident scene management tool: procedures for evidence collection
  - interoperable data collection/processing: RF ID tagging and tracking, integrated triage system
  - interoperable metrics
  - integrated incident record/report

Breadth/depth:

- operational view across multiple first responder organizations (need for interoperability and standards)
- intended to underline the capability need and requirements; the architecture may not need to have the level of detail required for the development of the actual IT system

(**Note**: to avoid getting tangled into cross-jurisdictional issues and data formats, and to keep the analysis at a high level, only “generic” first responder organizations are considered here, and they are thought of in terms of characteristic functions they need to perform. This is the perspective adopted in what follows.)

Step 3: Data required to support architecture development

- Rules that govern how activities should perform
- Guidance for mapping activities to organizational elements and nodes
- Information needed to accomplish activities
- Relationships, task lists, required information about organizational elements and nodes
- Standard data dictionaries
- Rules on distribution and environment
- Guidance for developing linkages among activities
- Results from specific activities
- Known likely external interfaces with other organizations (joint or coalition)
- Linkages to higher-level activities

Step 4: Collect, Organize, Correlate, and Store Architecture Data

Data determined at **Step 3** needs to be collected, organized and stored in a way that permits subsequent analysis and reuse. Included in this step is the correlation of data in terms of activity, data, organizational, and dynamic models.

Step 5: Conduct Analyses to Support Architecture Objectives

The types of analyses that are typically performed are:

- Determination of shortfalls between requirements and capabilities
- Assessments of processing and communications capacities
- Assessments of interoperability
- Analysis of alternatives to determine investment tradeoffs

The analytical process provides insights into issues and concerns that were not readily apparent at the outset, and, as a result, Step 5 includes the identification of additional data collection requirements.

Step 6: Document Results in Accordance with the Architecture Framework

The final step in the process involves building architecture products in accordance with templates established in the DoDAF. A number of architecture tools are available to support this step. The tool should be selected based on the intended use of the architecture (Step 1).

4 How to develop the architecture views – proposed sequence

The proposed sequence starts with an overview and a dictionary; both need to be updated throughout the development of the architecture.

Architecture Project Overview and Summary Information → All-View (AV) – 1

- Define purpose, scope, context, and tools
- First view to be produced, it must be updated throughout;
- Provides a reference; development of this view facilitates shared understanding of what the architecture will provide
- Essential to document the assumptions, constraints and limitations that may affect decision processes related to the architecture;

1. Title of the architecture project	
Tablet/PC/PDA tool for first responders for CBRNE incident management	
2. Stakeholders	
3. Project dates	
4. Purpose of the architecture project	
Purpose:	• Support developing an IT system to assist first responders across Canada with incident management and analytical tools, including portable knowledge about CBRNE hazards, data collection and management (procedures, standards, storage) and collaborative information exchange • The architecture is developed as an analytical tool, to ensure a sound base for the project in order to secure funding. It is intended to underline the capability needs and requirements.
Objectives:	• operational field support for first responders (portable knowledge) • destination of CRTI research generated knowledge
Expected benefits:	
Guidance documents:	
5. Scope of the architecture project:	
Capabilities included in the architecture:	
Products developed in the architecture:	
Organizations involved:	
Assumptions:	
Constraints:	

6. Context of the architecture project:	
Mission associated with the architecture:	
Links to other architectures (?)	
7. Tools and file formats employed:	
Tools:	
File formats:	
8. Findings:	
Results:	
Recommendations:	
Reports:	

Integrated Dictionary (AV-2)

Define terms; should be started at the beginning of the architecture development process and updated continually.

Developing the Operational View (OV)

First, develop an **operational architecture** – top-down articulation of operational activities

1. Describe WHAT must get done, and the connectivity required to make it work
2. Level decomposed until the main concern is HOW it gets done

This way, the operational view sets the goals for the system development.

Obtain or build an Operational Concept → **High-Level Operational Concept Graphic (OV-1)**
High-level structured cartoon, shows a general picture describing the problem that the architecture is supposed to address. It orients the reader to the problem-at-hand.

Document the process → **Operational Activity Model (OV-5)**
The high-level concept is analyzed and an **activity model** is constructed detailing the operational concept in the form of a set of inter-related processes (operational activities).

- When possible, use activities from accepted standard tasks lists. Showing linkage between activities created for a given architecture and the activities in the standard lists provide a basis for architecture integration.
- Determine the information flow associated with the activity set. Identify inputs, controls, outputs, and mechanisms (ICOMs) associated with the activities, along with who (role/organization) performs them.
- To a very large extent, **OV-5** provides the foundation for the remaining OV products. Therefore, one must develop a reasonable version of **OV-5** before the other products are started.

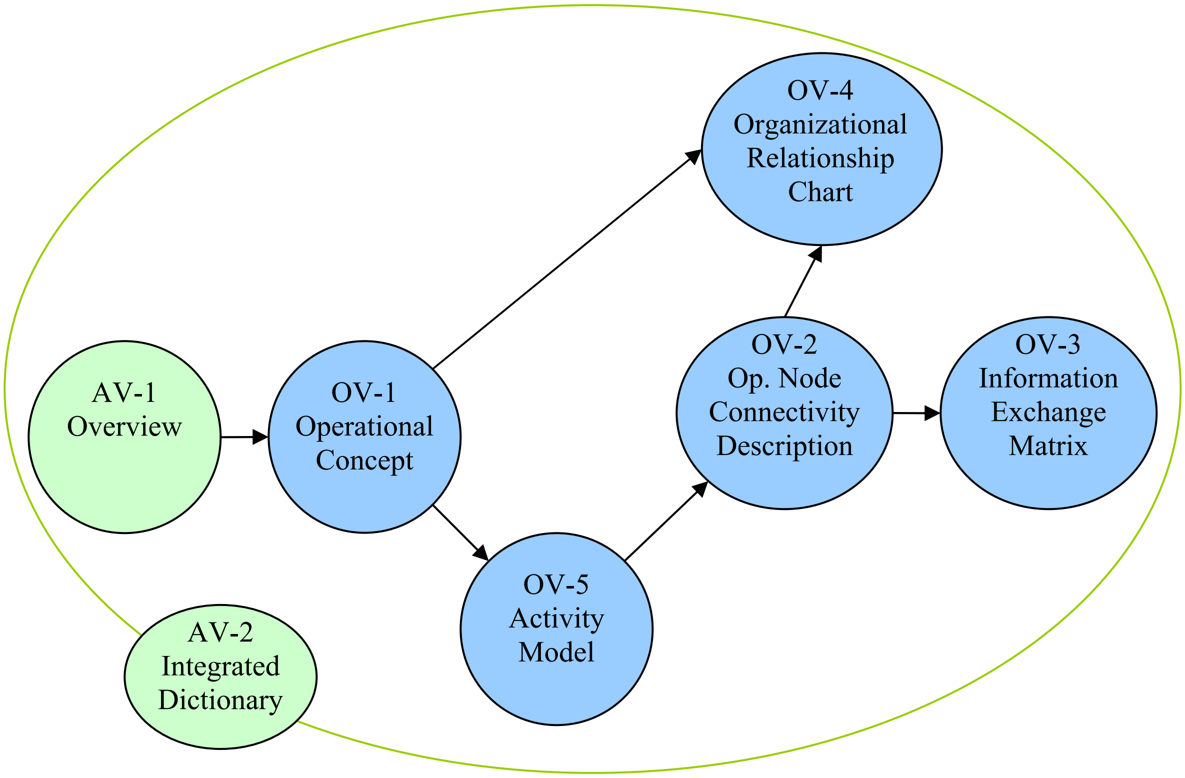
Based on ***OV-5:***
Aggregate activities into operational nodes → **Operational Node Connectivity**

Description (OV-2)
Organize activities into sets that will be logically collocated. Operational nodes are groupings of like activities that are performed together to carry out the operational concept. Nodes inherit the ICOMs associated with the activities performed at the nodes.
OV-5 provides the information flows among the activities performed at the various nodes. The information flows between two operational nodes are bundled into needlines. A needline represents an aggregation of information flows between two operational nodes, where the aggregated information exchanges are of a similar information type or share some characteristic.

*Based on **OV-5** and **OV-2:***
Determine information exchange requirements → **Operational Information Exchange Matrix (OV-3)**
OV-5 and **OV-2** provide the producing and consuming activities, the operational nodes at which they originate and to which they flow, and the information elements that they exchange. Relevant attributes of the information exchange are added to complete the matrix. This will help generate the information exchange requirements (IER) matrix. IERs are documented in **OV-3**.

*Based on **OV-1** and **OV-2:***
Identify organization types that will perform the activities associated with the operational nodes → **Organizational Relationships Chart (OV-4)**
Organizations identified for the given operational concept are assembled into a common structure for conducting a designated operation. A key element of this structure is the relationship that must exist among the organizations that it comprises. This captures the data required to produce the **OV-4**.

Assign organizations and physical locations to operational nodes and activities → **OV-4** is overlaid on **OV-2**.
Principal and secondary organizations are assigned to each operational node, resulting in a new construct with both functional and physical characteristics called the operational facility (OpFac). The organizations assigned to an OpNode represent real (either type or specific) entities that will perform assigned activities at the node. Identify actual organizations to perform the activities and tasks delineated in earlier steps; update **OV-3** with the organizations associated with each information exchange. This captures the requirements of the individual organizations for systems and communications equipment to be satisfied by the Systems View.

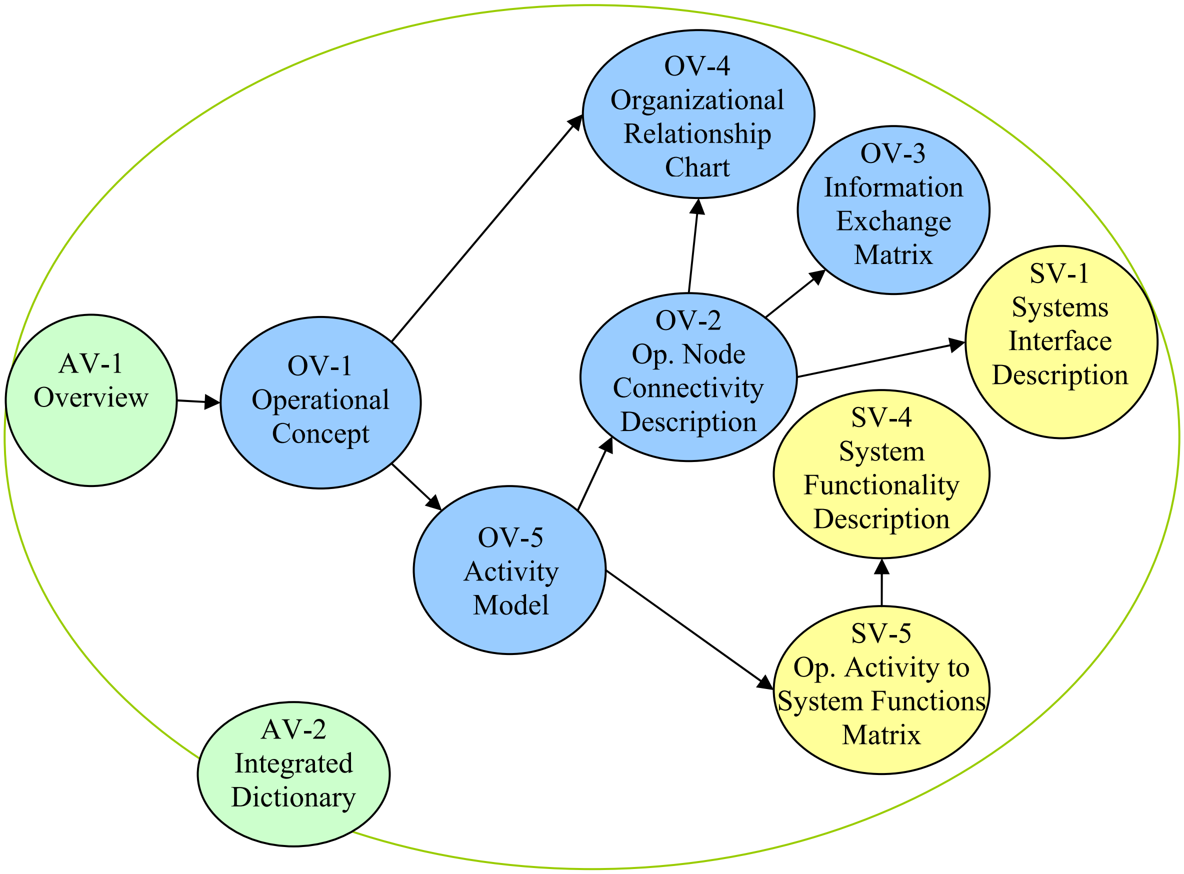


Developing the Systems View (SV)

Once the **Operational View** of the architecture is completed, the **Systems View** can be developed. Since the architecture is not intended to have the level of detail required for the development of the actual IT system, only a few relevant systems view products are illustrated here.

Based on operational activities, determine the required system functions → **Operational Activity to Systems Functions Traceability Matrix (SV-5)**
For the activities identified in **OV-5**, identify desired system functions to support each activity. The **SV-5** provides the primary bridge between the Operational View and the Systems View.

Define the relationship among system functions → **Systems Functionality Description (SV-4)**
Given the system functions identified in the **SV-5**, develop a decomposition of those functions by identifying and organizing associated subfunctions. This provides the functional decomposition version of the **SV-4**.



OV-4 Organizational Relationship Chart
OV-3 Information Exchange Matrix
SV-1 Systems Interface Description
AV-1 Overview
OV-1 Operational Concept
OV-2 Op. Node Connectivity Description
SV-4 System Functionality Description
OV-5 Activity Model
SV-5 Op. Activity to System Functions Matrix
AV-2 Integrated Dictionary

Based on ***SV-4*** *and* ***SV-5:***
<u>Assign systems and their interfaces to the Operational Facilities</u> → **Systems Interface Description (SV-1)**
Referring to **OV-2** to which organizations and physical nodes have been attached, each organization assigned to an Operational Facility brings with it a set of systems identified within the organization's authorization documents. Once the relevant systems at each OpFac are identified (i.e., those systems providing the functions associated with activities performed at the node), develop the **SV-1**.

Additional views may be developed as needed.

5 Summary

The present note considers the potential of using an architecture model to refine capability requirements and capture the need for interoperability and communications. It explores how DoDAF concepts and methodologies can be applied in support of a project to build an integrated and interoperable crime scene support tool for managing CBRNE events; this tool will provide responders with critical CBRNE information sources, standardized incident reporting forms and procedures, mass causality triage management and evidence tagging using Radio Frequency Identification (RFID), and will assist in managing the crime scene providing interoperability and data exchange between the various responding personnel and mobile command control centers as well as providing long-term crime scene data and information for use in potential on-going criminal investigations.

The work outlines how DoDAF could provide a structured hierarchy where data collection and analysis can be carried out independently at different levels, allowing each contributing system/organization meet its internal needs, but in a way that is consistent with and respectful of the requirements of other organizations involved. A six-step architecture development process is presented, including discussions on how each step applies to the specific project considered. The development of essential architecture views – which can be of three types: All-Views (AV, show project overview and summary information), Operational Views (OR) and Systems Views – is discussed. The note ends by proposing a particular sequence for the development of architecture views; the proposed sequence starts with an overview and a dictionary, both of which should be updated throughout the development of the architecture, followed by developing the operational view and finally the system view. Discussions of architecture views that are considered essential to the project in each category are included, together with graphical representations of functional relationships between different views.

The advantage of using the DoDAF approach as an analytical tool is that the analyst may choose the level of detail depending on the objectives of the architecture. In the present case, the focus has been on characteristic functions that generic first response organizations need to perform, and the analysis was performed at a higher level that what might be needed to aide the development of the real IT system. The templates established in the DoDAF allow the analyst to develop only the necessary architecture products, but if the level of the analysis needs to be refined, it can be done consistently, since any new products will fit nicely with the old ones in the whole of the architecture. The drawback is that DoDAF may be too elaborate a tool for analyzing simpler systems, and the effort to develop the DoDAF architecture products may not be commensurate with the scope of the required analysis. For simpler systems, establishing common reference views first and adopting a structured approach still apply, but only as principles for organizing the analysis, not necessarily involving the development of distinct products.

6 List of symbols/abbreviations/acronyms/initialisms

DND	Department of National Defence
CBRNE	Chemical, Biological, Radiological/Nuclear and Explosives
CRTI	CBRNE Research and Technology Initiative
R&D	Research & Development
EMS	Emergency Medical Services
HAZMAT	Hazardous Materials
RFID	Radio Frequency Identification
OR	Operational Research
DoDAF	Department of Defence Architecture Framework
IT	Information Technology
JEPP	Joint Emergency Preparedness Program
ER	Emergency Room
AV	All-View
OV	Operational View
SV	Systems View
PC	Personal Computer
PDA	Personal Digital Assistant
ICOM	Inputs, Controls, Outputs, and Mechanism
IER	Information Exchange Requirements
OpNode	Operational Node
OpFac	Operational Facility

This page intentionally left blank.

Distribution list

Document No.: DRDC Centre for Security Science N 2007-003

LIST PART 1: Internal Distribution by Centre:
ADM (S&T), DND/CEO DRDC - Dr. Robert Walker
DRDC Centre for Security Science

0 TOTAL LIST PART 1

LIST PART 2: External Distribution by DRDKIM

0 TOTAL LIST PART 2

0 TOTAL COPIES REQUIRED

This page intentionally left blank.

DOCUMENT CONTROL DATA

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 Security Science
344 Wellington St.
Ottawa ON

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

UNCLASSIFIED/UNLIMITED

3. TITLE

An Architecture Approach to Refining Requirements for an Interoperable CBRN Incident Scene Support IT Tool

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

Verga, Simona

5. DATE OF PUBLICATION
November 2007

6a. NO. OF PAGES
18

6b. NO. OF REFS
(Total cited in document.)

7. DESCRIPTIVE NOTES Note

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

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.)

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.)
DRDC Centre for Security Science N 2007-003

10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

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

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 This document explores the potential of using an architecture model to capture the need for interoperability and communications, in support of a potential project to build an integrated and interoperable crime scene support tool for managing CBRNE events. The model considered is the US Department of Defence Architecture Framework (DoDAF). Such a framework could provide a structured hierarchy where data collection and analysis can be carried out independently at different levels, allowing each contributing system/organization meet its internal needs, but in a way that is consistent with and respectful of the requirements of other organizations involved. The work outlines how DoDAF concepts and methodology may be applied for this purpose.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS
Interoperability; CBRNE, Incident Command; Defence Architecture Framework