Contractor Final Report

For the Technology Demonstration of the Joint Network Defence and Management System (JNDMS)

Prepared By:
MDA Systems Ltd.
Suite 60, 1000 Windmill Road
Dartmouth NS B3B 1L7
MDA Reference # DN1011
Contract Project Manager: Brett Trask, 902-481-3511
PWGSC Contract Number: PWGSC Contract Number: W7714-040875/001/SV
CSA: Marc Gregoire, JNDMS Project Manager, 613-998-2113

The scientific or technical validity of this Contract Report is entirely the responsibility of the Contractor and the contents do not necessarily have the approval or endorsement of Defence R&D Canada.

Contract Report
DRDC-RDDC-2014-C62
October 2013

Principal Author

Scott MacDonald

Project Engineer, JNDMS

Approved by

Approved for release by

Abstract

This document has been written to fulfill the deliverable DID-PM-007 for the Joint Network Defence and Management System (JNDMS) Technology Demonstrator under contract W7714-04-0875/001/SV. This document covers the execution and results of this Technology Demonstration.

Résumé

Le présent document a été rédigé pour répondre aux exigences DID-PM-007 visant le démonstrateur de technologies du Système interarmées de défense et de gestion des réseaux (SIDGR), en vertu du contrat W7714-04-0875/001/SV. Il touche l'exécution et les résultats de cette démonstration technologique.

This page intentionally left blank.

Executive summary

Contractor Final Report: For the Technology Demonstration of the Joint Network Defence and Management System (JNDMS)

Scott MacDonald; DRDC Ottawa CR ; Defence R&D Canada – Ottawa; September 2009.

Introduction or background: The JNDMS Technology Demonstrator has explored how to leverage current enterprise tools to aid in the situational awareness of networks.

Results: The resulting system demonstrated enterprise tools providing information to the JNDMS that was further fused to provide a tool to explore situational awareness. This system was demonstrated a number of times, the final demonstration took place using tools deployed on a live network, the DREnet.

Significance: This demonstrated key functionality in using enterprise tools to fully understand and evolving area of great concern.

Future plans: A transition plan is part of this project to provide some guidance in where to take this technology in the future.

Sommaire

Contractor Final Report: For the Technology Demonstration of the Joint Network Defence and Management System (JNDMS)

Scott MacDonald; DRDC Ottawa CR ; R & D pour la défense Canada – Ottawa; Septembre 2009.

Introduction ou contexte: Le démonstrateur de technologies du SIDGR a étudié comment tirer parti des outils d'entreprise existants afin d'améliorer la connaissance de la situation en réseau.

Résultats: Le système élaboré a démontré que les outils d'entreprise peuvent fournir des données au SIDGR, qui les traite ensuite afin d'obtenir un outil d'aide à la connaissance de la situation. Ce système a fait l'objet de plusieurs démonstrations, et la dernière a utilisé des outils déployés dans DREnet, un réseau opérationnel.

Importance: Nous avons démontré des fonctions cruciales en utilisant des outils d'entreprise pour comprendre en profondeur un domaine préoccupant en constante évolution.

Perspectives: Ce projet comprend un plan de transition visant à recommander où orienter les travaux subséquents sur cette technologie.

Table of contents

List of figures

1 Introduction

1.1 Purpose

This document has been written to fulfill the deliverable DID-PM-007 for the Joint Network Defence and Management System (JNDMS) Technology Demonstrator under contract W7707-03-2091/001/HAL.

1.2 Scope

The document contains the following sections:

- System overview.
- Project execution including details on each project phase and task authorization.

2 System Overview

The Joint Network Defence Management System (JNDMS) was designed as a prototype system to evaluate Situational Awareness. The role of enterprise management tools and security management tools are well entrenched in network management today. The role of these systems and their best practices are captured in accreditation processes such as the Information Technology Infrastructure Library (ITIL). It was one of the goals of the development of JNDMS to leverage these tools and beset practices where possible and to build on top of Commercial-Off -The Shelf (COTS) tools. The project team was keenly aware that the scope and resources available to any commercial offering would overshadow this project and would improve over time. It was therefore beneficial to make use of these tools where possible.

The resulting architecture was a layered system (see Figure 1) in which much of the development concentrated on the data model, business logic and presentation, with integrated COTS providing much of the rest of the system.

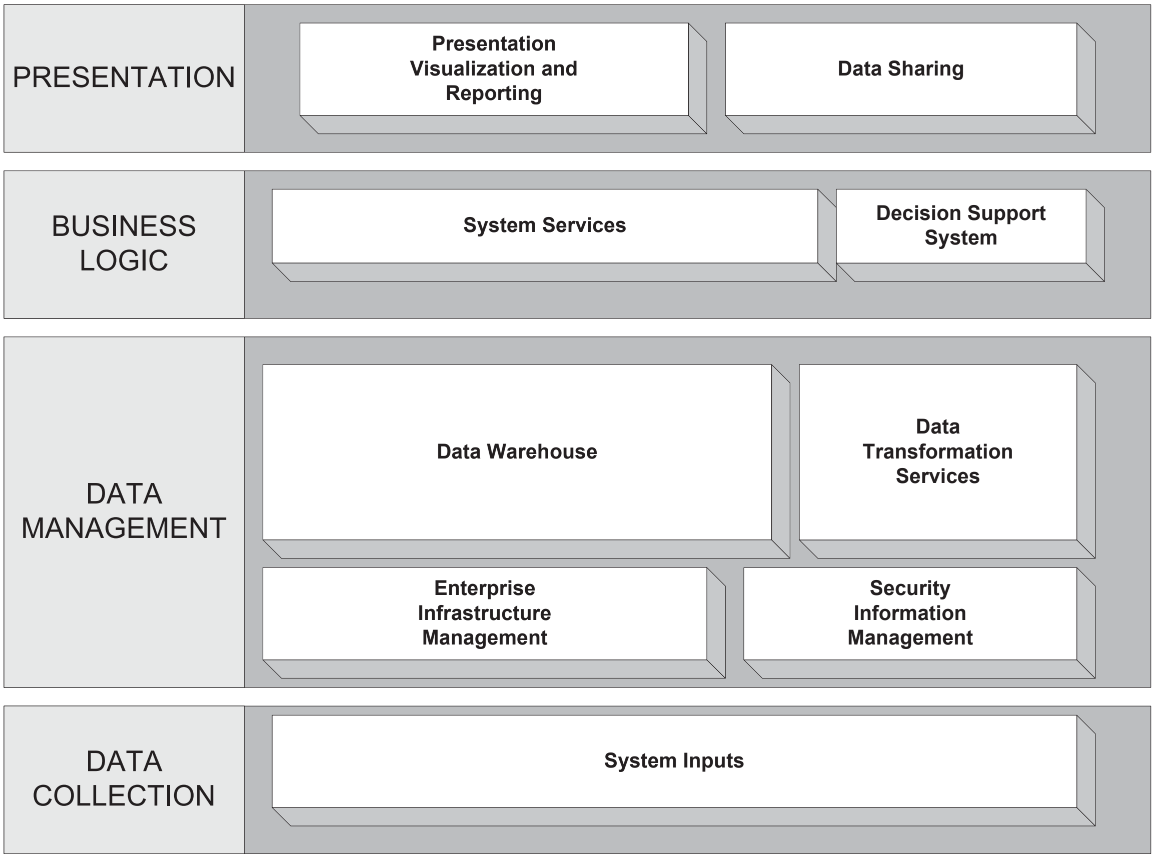

PRESENTATION
Presentation Visualization and Reporting
Data Sharing
BUSINESS LOGIC
System Services
Decision Support System
DATA MANAGEMENT
Data Warehouse
Data Transformation Services
Enterprise Infrastructure Management
Security Information Management
DATA COLLECTION
System Inputs

Figure 1: JNDMS System Architecture

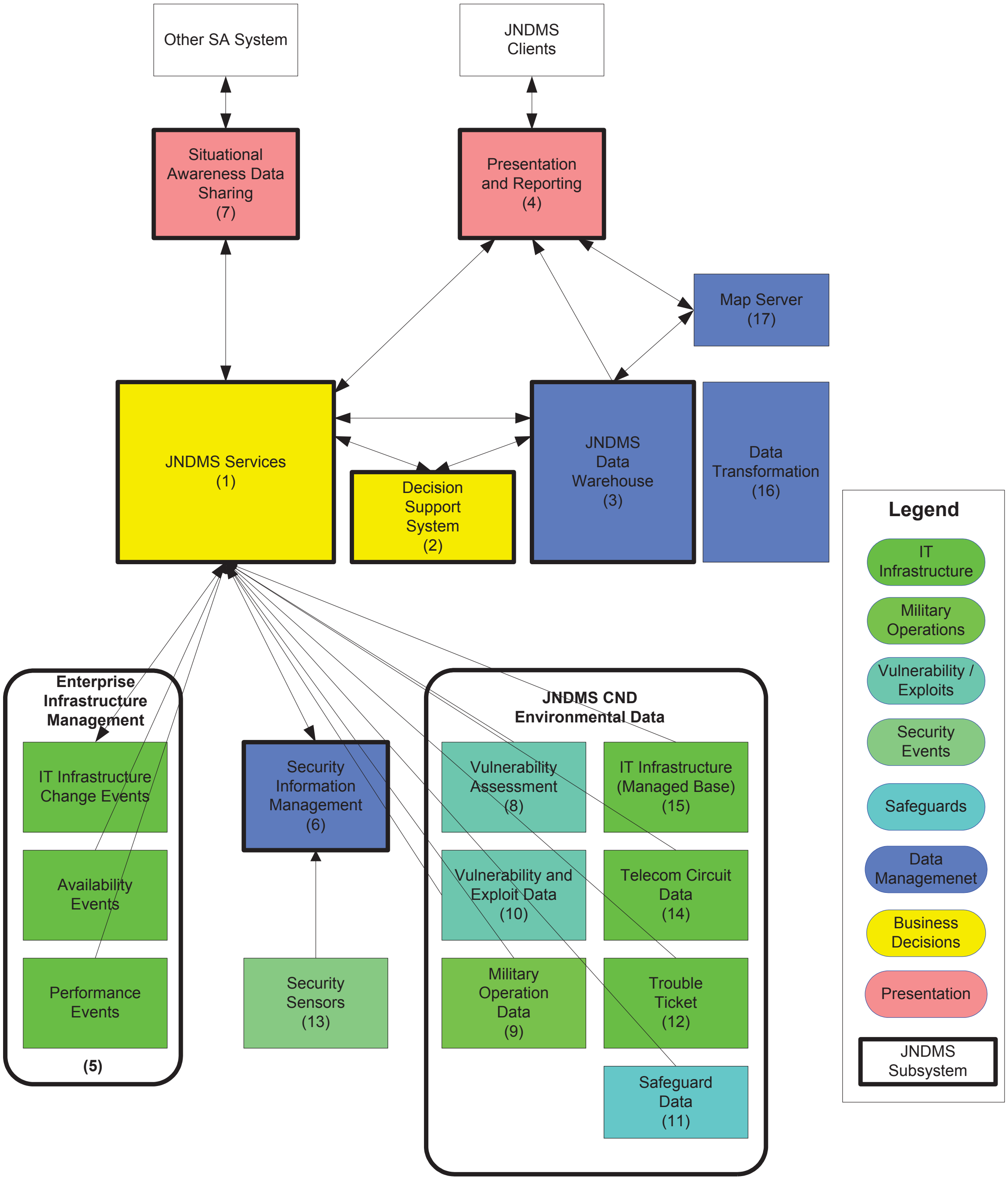

Other SA System
JNDMS Clients
Situational Awareness Data Sharing (7)
Presentation and Reporting (4)
Map Server (17)
JNDMS Services (1)
Decision Support System (2)
JNDMS Data Warehouse (3)
Data Transformation (16)
Enterprise Infrastructure Management
IT Infrastructure Change Events
Availability Events
Performance Events
(5)
Security Information Management (6)
Security Sensors (13)
JNDMS CND Environmental Data
Vulnerability Assessment (8)
IT Infrastructure (Managed Base) (15)
Vulnerability and Exploit Data (10)
Telecom Circuit Data (14)
Military Operation Data (9)
Trouble Ticket (12)
Safeguard Data (11)
Legend
IT Infrastructure
Military Operations
Vulnerability / Exploits
Security Events
Safeguards
Data Managemenet
Business Decisions
Presentation
JNDMS Subsystem

Figure 2: JNDMS Design

The following section will identify the final components of the JNDMS.

2.1 JNDMS Custom Components

- JNDMS System Services (JSS). The JSS represents the system services. This component is responsible for core system I/O and initial pre-processing. This component also interacts with the DSS.
- Decision Support System (DSS). This is the decision support system. The core of the DSS is a custom Java application to provide the system analysis.
- JNDMS Data Warehouse (JDW). The data model for JNDMS is custom work.
- Data transformation. This represents components in clients as well as the JSS to transform data sources or inputs. This component uses custom queries as well as XML translation.
- Data sharing. This represents a component within the JSS for reporting and event sharing.

2.2 JNDMS COTS Components

Significant cots use included:

- Spectrum. This provides the IT infrastructure discovery as well as the availability monitoring. Early development cycles used CA Unicenter Advanced network option.
- Intellitactics. This provides the monitoring and reporting of security events.
- Oracle. This was the database chosen.
- IP360. This is the vulnerability manager used during deployment. Early effort had used CA eTrust and Nessus.
- Centennial. This is the software asset inventory tool used during deployment. Early development cycles used CA Asset management.
- Aion BRE. This is the rules engine used. In later development cycle the functionality of the rules engine was reproduced with Java components. This is no longer necessary for the core of the system.
- Google Earth Plugin. This was used as a prototype of the 3D maps.
- ExtGWT. This provided additional components or widgets for the Google Web Toolkit (GWT).
- Java and Java standards. Much of the custom components were written using Java as well as many of the APIs that are part of the standard and enterprise editions of Java.
- Jep. This is a Java library for evaluating mathematical expressions.
- JGraph. This was used to manage the visual layout and display of graphs within JNDMS.
- Jasper Reports. This provides the ability to create custom reports within JNDMS.

2.3 JNDMS Open Source Components

Significant open source components included:

- Tomcat. This is the application server used.
- Google Web Toolkit. This was used to develop the final version of the portal. This provides a Java environment for the development and maintenance of web portals. Earlier versions used custom Javascript and Dojo.
- XML processing. XML processing components including JAXB and the apache CXF were used. Earlier versions used Apache Axis.
- Open layers. This is used for the display of the 2D map. Early development cycles used ESRI ArcGIS, however it was found that Open Layers and the Google Maps API both provided better performance.
- iBATIS. This is an XML Object/Relational mapping toolkit. This was used to translate between XML and database queries.
- JGraphT. This was used to evaluate decisions based on the internal graphs maintained by JNDMS.

3 Project Execution

3.1 Summary

This project was divided into three phases. The first phase was focused on project initiation and requirements analysis. The second phase was the core of development and the third phase was project wrap up.

The project itself was comprised of an Integrated Project Team (IPT) (see Figure 3). This closely integrated team was leveraged to understand some of the COTS products as well as how the system would be used or deployed.

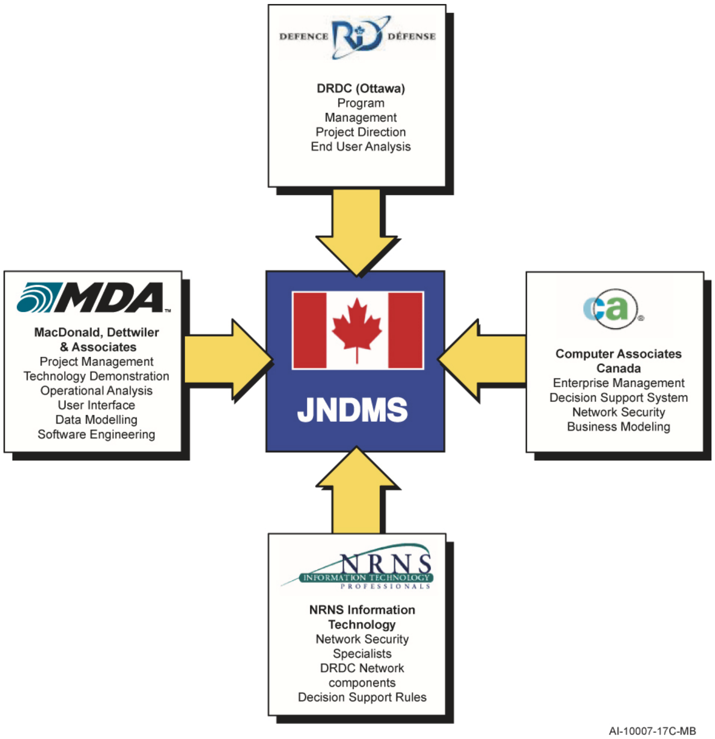


Figure 3: JNDSM IPT

3.2 Phase 1

The Phase 1 represented the initial analysis and design. The result was the creation of the Requirements documentation [10] as well as the Architecture [7] and the Design [8]. These documents were used as a basis for, and updated in, each of the development cycles.

3.3 Phase 2, Cycle 1

3.3.1 Overview

The first development cycle represented the initial effort to build and demonstrate the core JNDMS architecture. This development cycle included the first components of the enterprise tools, the first installation of the security manager and the first version of the JNDMS core components and user interface.

3.3.2 Test Environment

At the end of Cycle 1 the results were demonstrated to DRDC in the Halifax JNDMS lab environment. This environment demonstrated the core components with simulated scenarios. The lab environment consisted of six server or workstation computers (see Figure 4).

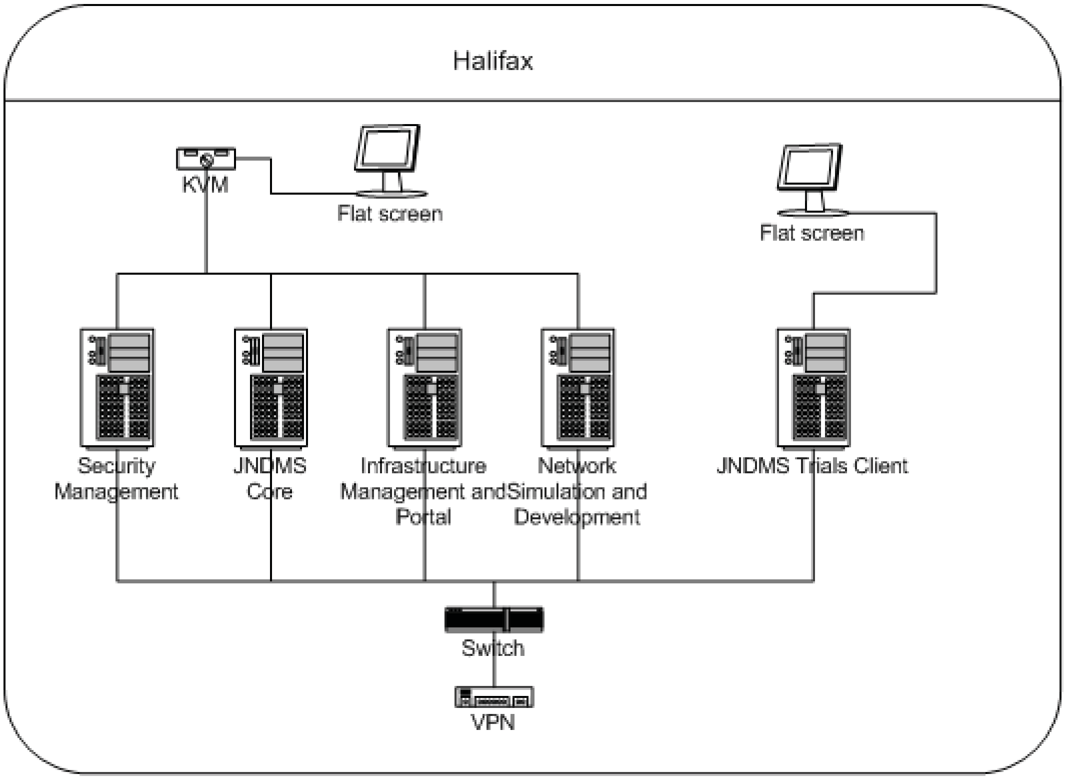


Figure 4: JNDMS Cycle 1 Test Environment

This environment was setup to simulate a small network that would be used to demonstrate the core features of the system. This initial simulated environment consisted of approximately 200 assets (see Figure 5).

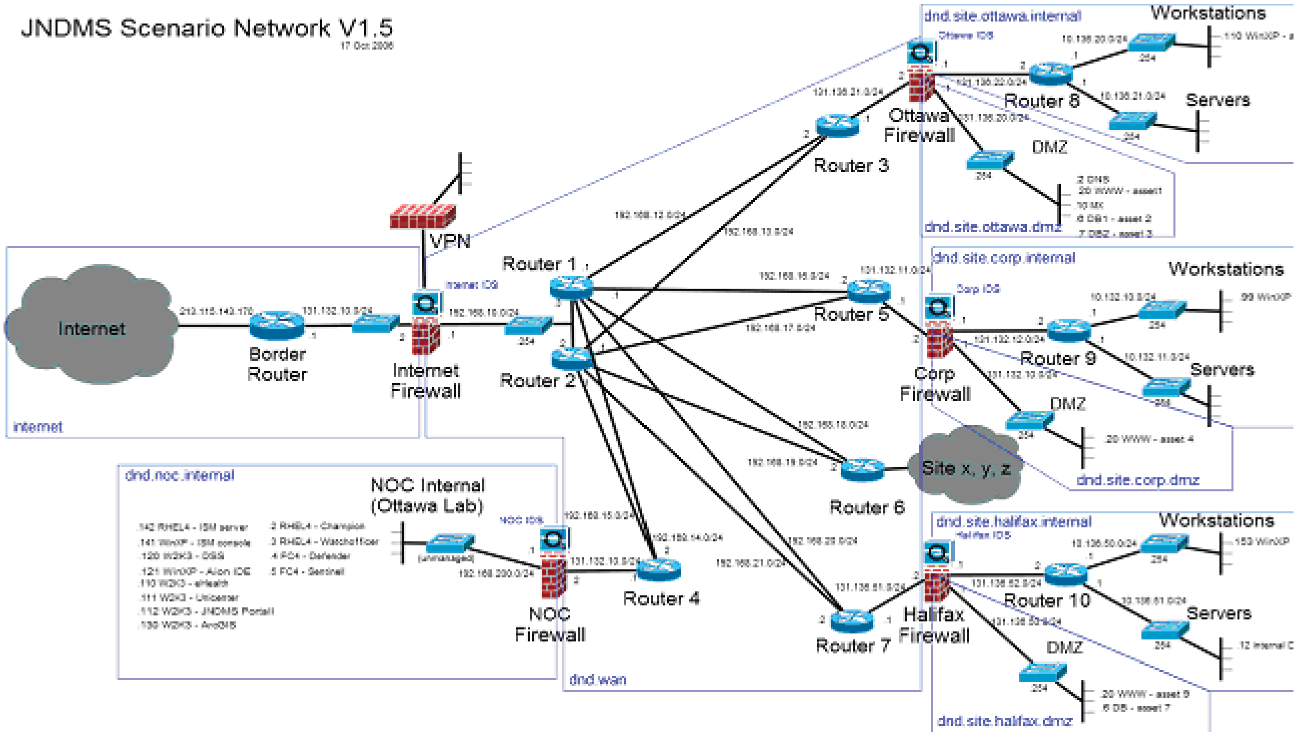


Figure 5: Cycle 1 Simulated Environment.

3.3.3 Objectives and progress

The objectives of the first development cycle were first identified at the beginning of Cycle 1 in the Cycle 1 Development Plan [1]. An overview of these objectives and progress made during the first development cycle are as follows:

- **Build and demonstrate a working prototype of the JNDMS system**. The initial version of the JNDMS was built along with a simulated environment for testing and evaluation.

  The Cycle 1 objectives were refined during the execution of the cycle to identify more specific development goals. These were identified and discussed in the Cycle 1 Trials Report [2] to provide functionality in the following areas:

- **Loading, Processing and Displaying Core Knowledge**. The core knowledge areas identified in Cycle 1 included vulnerability definitions, malware, IDS signatures and software products. Each of these items had an identified source, possible analysis and display within the Cycle 1 system.

- **Loading, Processing and Displaying Environmental Data.** There were 9 identified environmental data types identified in the Cycle 1 Trials Report (Table 4). These concentrated on initial asset and topology information, basic locations, some operational information as well as the relationships to services. The environmental data chosen for Cycle 1 focused on basic inputs from the enterprise tools and allowed the user interface and analysis to explore some of the fundamental ideas for JNDMS.

- The source of data for the environmental data in Cycle 1 included Unicenter tools (Network and Server Management, Advanced Network Operations and Asset Management) as well as manually entered data.
- **Loading, Processing and Displaying Events affecting the Environment**. There were five event types processed for the first cycle. These included:
  - IT asset discovery events. These were modeled after the events generated by Unicenter Network and Server Management (NSM).
  - Basic security events. These were modeled after information available in IDS alarms as broadcast through the Intellitactics Security Manager (ISM).
  - Vulnerability instances. These events were modeled after basic vulnerability scans and Nessus was used as the initial scanner.
  - Trouble tickets. These events were simulated and showed how additional events, not generally processed by common enterprise tools could be analyzed.
  - Physical events. These events were manually inserted and showed another type of event that could impact the state of the network.
- **Implement and refine the design of the JNDMS data model.** The data model in Cycle 1 was modeled using inputs from the JNDMS Phase 1 analysis, the Command and Control Information Exchange Data Model (C2IEDM/JC3IEDM) and an existing data model for the Impact Analysis Tool (IAT). This data model was captured in the tool Enterprise Architect (EA) and presented in the JNDMS Design Document [8].

  The tools to implement the data model were also examined with the initial release of the design document examining issues such as performance and integrity. Oracle was chosen as the database for JNDMS and remained the tool throughout the project.

  The goal of the data model in Cycle 1 was to provide an initial version that would be capable of capturing the data and relationships required for JNDMS to capture, store, analyze and display the network situational awareness. The data model designed and updated throughout Cycle 1 was used throughout the project with updates during each of the following development cycles.
- **Implement and refine the design of the JNDMS user interface (UI).** The initial user interface was designed and implemented during Cycle 1. The user interface was designed to be a web portal to ease deployment issues, to leverage much of industry's move towards web standards and to be able to leverage web views of other tools.

  The initial portal considered was the CA Cleverpath Portal. This portal was part of the enterprise tools chosen for Cycle 1 and was used as the interface to the rules within the Cleverpath Aion Business Rules Engine. It became apparent during the development however that although this would be able to provide the interface to the rules it was not a fully fledged portal system and did not support emerging standards.

  Other portals were examined and the Liferay Portal was chosen for its core feature set, use of common components and adherence to industry standards.

  The design for Cycle 1 provided a portal layout in which the user was presented with multiple tabs, a navigation view, a central data view and a summary view (see Figure 6).

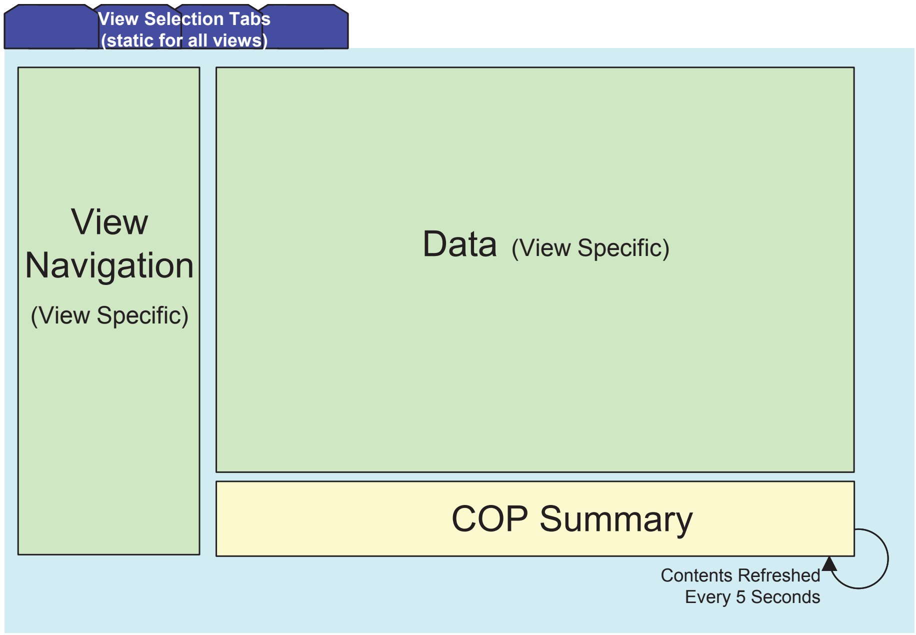


Figure 6: Cycle 1 Portal Layout

Each link available in the navigation view would change what was seen in the data view. The views available could be data (HTML), map or logical views. The tabs at the top of the portal allowed different navigation options to be available. The purpose of these different views was to be able to provide a view focused on specific needs or work flows. The views chosen for Cycle 1 included operations, security events, defensive posture, equipment and topology.

- **Develop the JNDMS system interfaces and test the UI with simulated data.** The portal for Cycle 1 was based on Liferay Enterprise and included a complete J2EE application server (see Figure 7 for example showing a logical view).

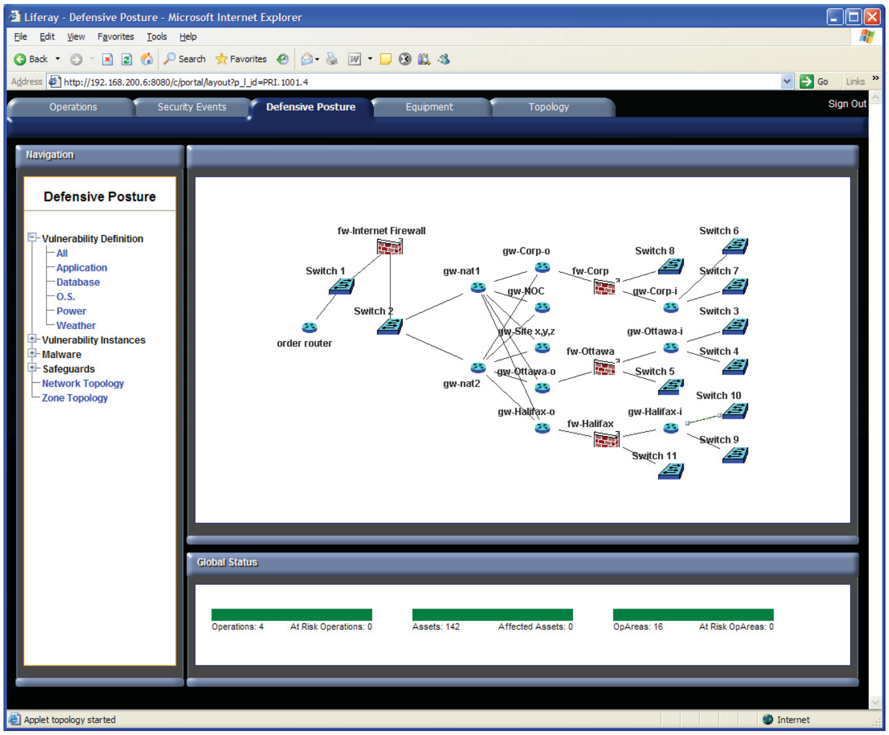


Figure 7: Cycle 1 User Interface

The system built during Cycle 1 allowed simulated data to be entered into the system. During development, snapshots of the outputs of various tools were taken as well as custom text files crafted to provide a basis for the analysis and display. These text and XML files were then generally replayed to the system to provide the ability to test and demonstrate.

- Install the Enterprise Infrastructure Management (EIM) and Security Information Management (SIM) systems within the test environment, and configure for correct operation. The enterprise tools that comprised the EIM for Cycle 1 included Unicenter Network and Server Management (NSM), Unicenter Advanced Network Operations and Unicenter Asset Management. These tools worked together and provided events to JNDMS through the Unicenter Event Console.

  The SIM was comprised of the Intellitactics Security Manager (ISM). This tool was already deployed within the Canadian Forces and provides security management interface as well as the ability to define escalation rules for JNDMS. The ISM was installed and configured as part of Cycle 1.

- Develop the Decision Support Rules Builder for creating and editing the weighted rules that use the incident information, the nature and locations of the affected network systems and other current incidents and vulnerabilities in determining the significance of a particular incident. During Cycle 1 the Cleverpath Aion Business Rules Engine (BRE) was used to implement the component within JNDMS known as the 'Decision Support System'. This component has the responsibility of examining incoming events and providing an analysis as to the impact on the current situational awareness. Aion provided two interfaces for development or updating the rules. The first interface was an Integrated Development Environment (IDE) that was used to create the rule base and to create the required executable components.

  The second interface identified was the Aion Rule manager. This interface could be exposed through the Cleverpath Portal. It was part of the design to explore this interface in future development cycles.

- **Create the initial Decision Support Rules**. These initial rules were developed within Aion for Cycle 1 and integrated with the DSS and JSS though a Java interface. The Aion rules would be triggered whenever a new event was processed by JNDMS.

  The initial rules had the primary responsibility to assess the impact of incidents and to create possible vulnerability instances. In addition to these rules initial versions of rules for incident correlation, risk assessment and severity assessment were created. All processing of incidents for Cycle 1 were done within the Aion rules.

  These initial rules provided the incident processing and provide the first cut at the link to operations through the analysis provided.

- **Create simulated data.** Simulated data was created for Cycle 1 to create the simulated test environment (see Figure 5) and to provide sufficient environmental data and events to be able to develop, test and demonstrate the system.
- **Conduct any approved experiments.** There were no formal experiments in Cycle 1 although the developing system provided a test bed to explore new ideas.
- **Complete a formal trial of the Cycle 1 JNDMS.** The initial version of JNDMS tested at the end of Cycle 1 provided a cross section of the design and identified twenty test cases to evaluate the system. These test cases would test some capability for Cycle 1 and also provide a framework for evaluation of future cycles.

  This system was evaluated in November of 2006 and the resulting system was updated and used for end of cycle demonstrations.

- **Conduct formal and ad hoc demonstrations of the Cycle 1 JNDMS.** The Cycle 1 system was updated and demonstrated in December of 2006 and the results captured in the Cycle 1 Test and Trials Report [2].

  The demonstration consisted of a presentation and a live demonstration of the system using simulated data. The system demonstrated was a subset of the design components (see Figure 8).

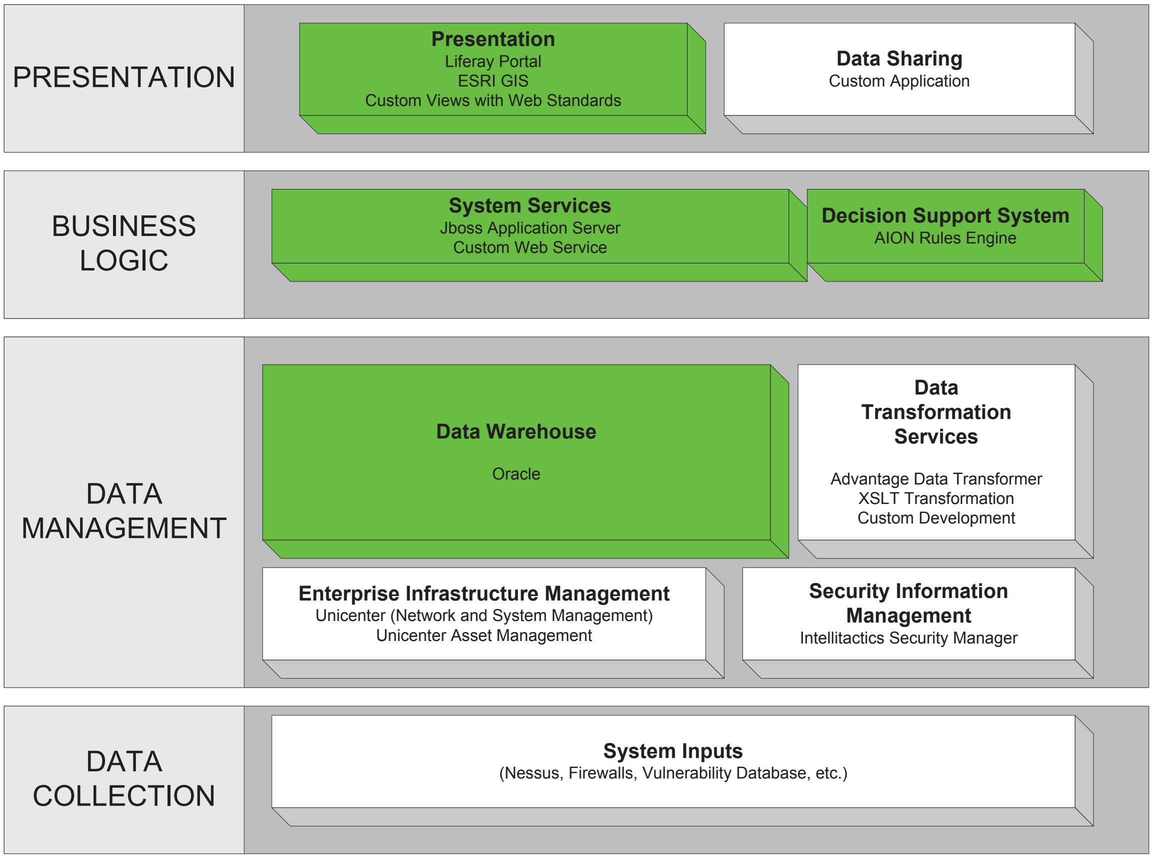

PRESENTATION
Presentation
Liferay Portal
ESRI GIS
Custom Views with Web Standards
Data Sharing
Custom Application
BUSINESS LOGIC
System Services
Jboss Application Server
Custom Web Service
Decision Support System
AION Rules Engine
DATA MANAGEMENT
Data Warehouse
Oracle
Data Transformation Services
Advantage Data Transformer
XSLT Transformation
Custom Development
Enterprise Infrastructure Management
Unicenter (Network and System Management)
Unicenter Asset Management
Security Information Management
Intellitactics Security Manager
DATA COLLECTION
System Inputs
(Nessus, Firewalls, Vulnerability Database, etc.)

Figure 8: Cycle 1 System Demonstrated.

This demonstration discussed the goals of the project and showed how some of the concepts would be displayed. The feedback was generally positive and provided feedback for Cycle 2. The details of the feedback can be found in the Trials Report [2].

- **Conduct further research and development of hypotheses for Defensive Posture and Threat Assessment/Risk Analysis.** The first development cycle concentrated on coming up with a view of situational awareness that could be built and demonstrated.

  Research material was examined (see Design Document [8], rev 1.1 for Cycle 1) and modified slightly for JNDMS. The result was an event flow (see Figure 9) that identified the core processing and resulting analysis that would be required for JNDMS. The basic view of the Situational Awareness provided the basis for event processing throughout the project.

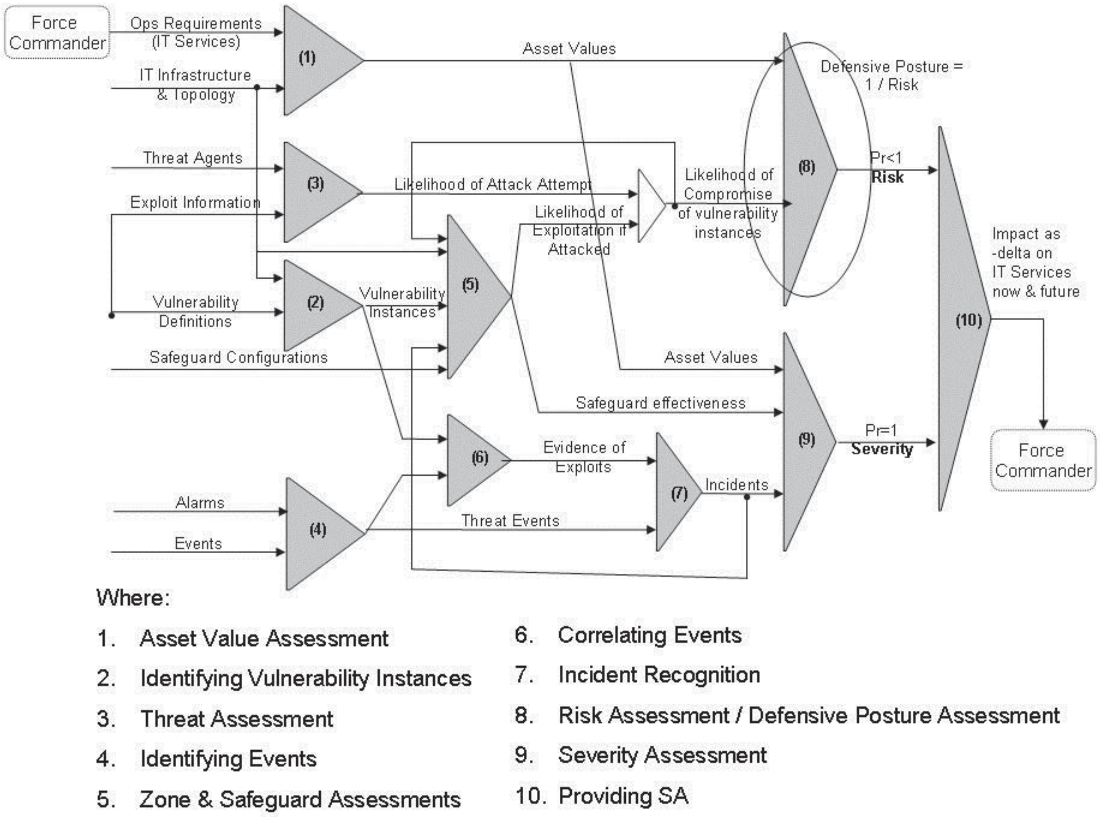

Force Commander
Ops Requirements (IT Services)
IT Infrastructure & Topology
Threat Agents
Exploit Information
Vulnerability Definitions
Safeguard Configurations
Alarms
Events
(1)
(2)
(3)
(4)
(5)
(6)
(7)
(8)
(9)
(10)
Asset Values
Defensive Posture = 1 / Risk
Likelihood of Attack Attempt
Likelihood of Exploitation if Attacked
Likelihood of Compromise of vulnerability instances
Vulnerability Instances
Asset Values
Safeguard effectiveness
Evidence of Exploits
Incidents
Threat Events
Pr<1
Risk
Pr=1
Severity
Impact as -delta on IT Services now & future
Force Commander
Where:
1. Asset Value Assessment
2. Identifying Vulnerability Instances
3. Threat Assessment
4. Identifying Events
5. Zone & Safeguard Assessments
6. Correlating Events
7. Incident Recognition
8. Risk Assessment / Defensive Posture Assessment
9. Severity Assessment
10. Providing SA

Figure 9: Situational Awareness for JNDMS

3.4 Phase 2, Cycle 2

3.4.1 Overview

The second development cycle of JNDMS started in January of 2007. The opportunity of participating in CWID 2007 was available and this formed the focus for Cycle 2. The development was geared toward expanding the core of JNDMS and to be able to demonstrate at CWID. The final demonstrations leveraged this event.

3.4.2 Test Environment

The test environment built and simulated for Cycle 2 revolved around the CWID scenarios. The basic scenario involved a UN Peace Keeping Force in which Canada had a role. This force was to provide a stabilizing force to the fictional country of Terrazona, however as events escalate a NATO Response Force (NRF) is mobilized. The core of the scenario is shared by all participants at CWID.

To examine the role of JNDMS in such an environment a simulated network infrastructure was created. This simulated environment included central command and support services (see Figure 10). These units and the related IT support were spread over several physical, simulated, locations.

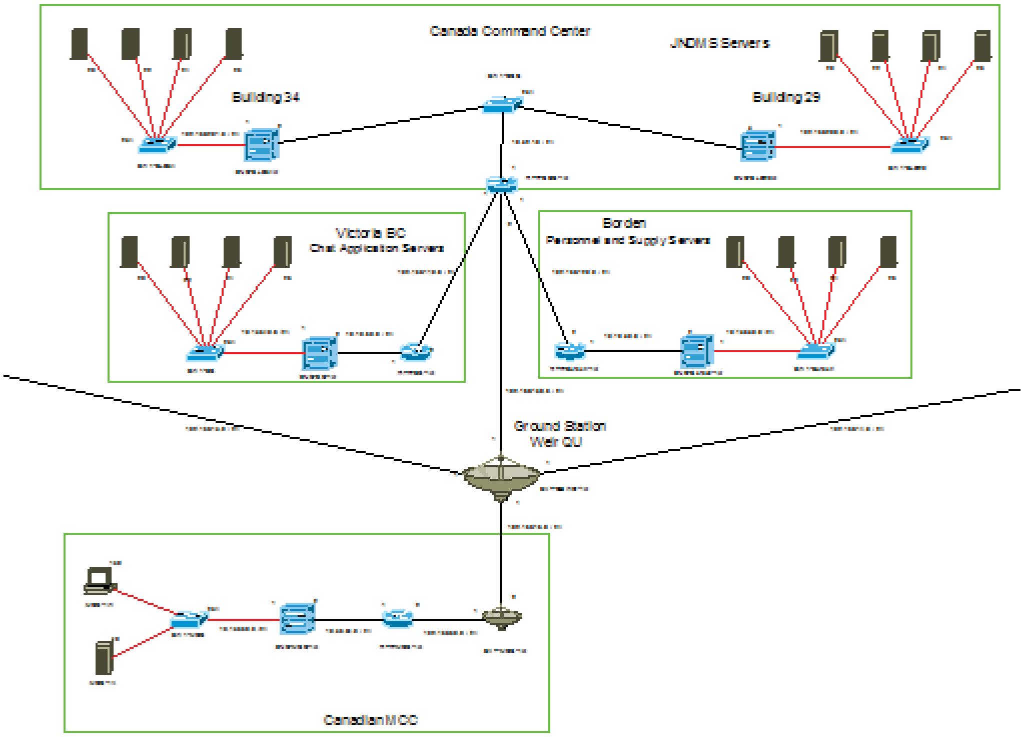


Figure 10: CWID Simulated Command and Support Infrastructure

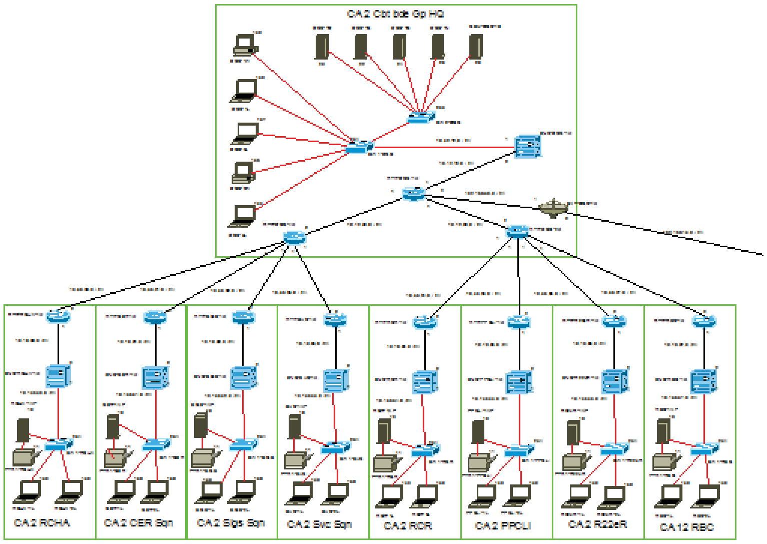


Figure 11: CWID IT Infrastructure for Deployed Ground

The test environment also included the required infrastructure for the deployed air and ground forces. For each of these there was a small command infrastructure and some common equipment layouts for each of the deployed units.

The IT infrastructure for the deployed ground forces can be seen in Figure 11 and the IT infrastructure for the deployed air units can be seen in **Error! Reference source not found.**.

The simulated creation of each of these was done in such a way that the equipment of the units could be added at various points during the CWID scenarios.

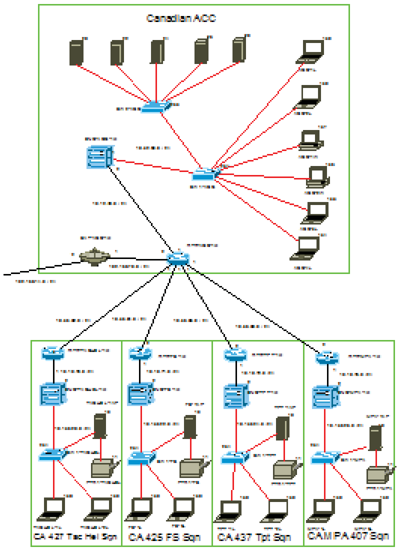


Figure 12: CWID IT Infrastructure for Deployed Air

This test environment represented a significantly more complex environment than the one presented in Cycle 1. The complexity was in both the size of the network as well as the depth of information available, especially for the operational dependencies on the networked assets and services.

3.4.3 Objectives

The objectives for Cycle 2 were originally presented in the Cycle 2 Development Plan [3]. The original objectives as well as the progress made towards them are as follows:

- **Created CND input interfaces where they are not available as inputs to COTS correlation systems.** Input interfaces to JNDMS were updated as required. The majority of the interfaces were updated during Cycle 2 with significant updates to the SIM and EIM interfaces.
- **Expand the data model to accommodate data inputs not included in Cycle 1.** The data model was updated during Cycle 2. As each new input or type of processing was evaluated the data model was examined. The goal of the design of the data model for Cycle 1 was to provide a data model that would support the inputs that were expected during the project, and as the new inputs were supported then the associated components of the data model would be exercised.
- **Create additional rules for the decision support system.** The DSS continued to be updated for cycle 2 with new rules created with Aion. The rules developed during Cycle 1 concentrated on a small initial proof of concept and ensuring that the integration of Aion into JNDMS worked well.

  All of the rules were updated during Cycle 2 with significant updates to the event processing and EIM events. The processing of IT infrastructure and topology was expanded to ensure that outages or interruptions in communications would be evaluated against the operational dependencies.

  The rules were also significantly updated to improve the risk analysis, the impact assessment and the event correlation.
- **Complete the Cycle 2 JNDMS Demonstration (CWID's demonstration).** The CWID demonstrations took place at DRDC Ottawa Shirley's Bay from 04 June to 21 June in 2007. These demonstrations included many months of preparation to understand how these events would be run, how we would interact with the network and how we would provide training and scenarios for the operators that were available.

  The result of participating in the CWID demonstrations was increased depth in the various scenarios and simulated data sets that were used for testing. These events also provided invaluable time with two operators and provided time to see how the end user would view the system and to use it. Comments from the operators can be found in the Cycle 2 Trials report [4].

This event also provided an opportunity to demonstrate the system and its goals to a wider audience. The third week of the CWID demonstrations was the actual demonstration. A number of guests toured the various demonstrations at CWID and this allowed JNDMS to be presented. The demonstrations were generally in the form of short presentations showing some of the features of the system, then the opportunity to ask questions or to see the system in more detail afterwards.

- **Perform post demonstration data analysis.** After the CWID demonstrations there were a number of issues identified during our wrap up. The most significant issues related to the complexity of maintaining the simulated data and the performance of the core system. These issues were partially worked out during the first two weeks of CWID, however this event would set the focus for the Cycle 3 development.
- **Obtain any necessary training from Computer Associates.** The CA product used to scan the network and to provide JNDMS with the topology was changed to Spectrum. Training was provided by CA on the use and integration of this product. Some additional training was provided on the Aion BRE.
- **Perform required design and requirements analysis reviews.** Reviews were performed at the start of the development cycle to evaluate the state of the design and requirements based on the system at the end of Cycle 1. This review provided the basis for the work plan of Cycle 2.
- **Kick-off, analyze and commence with development activities pertaining to contract amendment 002 (IAT implementation)**. The work on IAT commenced during the Cycle 2 development. See section 3.6 for details.
- **Commence with exploitation planning and business process reengineering activities.** Work started informally on the exploitation planning. This included meeting with the DRDC Ottawa exploitation officer and looking at how JNDMS could be leveraged or transitioned after the technology demonstrator.
- **Integrate any new or additional CA purchased equipment into the Cycle 2 baseline configuration.** During the Cycle 2 development updates to the Unicenter Asset management were done as well as some initial integration with CA eTrust Vulnerability manager. The primary change for this cycle, however, was the migration from Unicenter Advanced Network option to Spectrum. CA had purchased another company and was in the progress of integrating the Concord product line of Spectrum and eHealth. These tools were considered the preferred way forward.

  Spectrum was to be integrated into JNDMS through the Unicenter event console and to provide the roles of IT infrastructure discovery and availability monitoring. The work to update the JNDMS interfaces and to provide the customization of both Spectrum and Unicenter was done during this cycle.
- **Deliver a working Cycle 2 hardware and software configuration to DRDC Ottawa.** During Cycle 2 there were generally three environments maintained. These would be the main development lab at MDA Halifax, the development lab at NRNS in Ottawa as well as the environment delivered to DRDC Ottawa for CWID demonstrations.

- **Provide a one (1) day training seminar for DRDC Ottawa and other government agencies prior to the completion of the cycle.** There was formal training as part of the CWID demonstrations as well as informal training as part of general development and through the IAT initiative.
- **Update any CDRL publications required to accurately reflect the Cycle 2 JNDMS configuration and Continue with Monthly Progress Status Reporting and to Facilitate Progress Review Meetings (PRM).** Updates to the documents and status reports were done during the cycle.

The technical objectives of JNDMS were expanded from the above objects, identified in the Cycle 2 Trial Report [4] and identified for each sub system. There were:

- SIM
  - Update to new version of Intellitactics
  - Update interfaces to JSS
  - Integrate virus scanning through SIM
- DSS
  - Expand on defensive posture and zone concepts
  - Include updated interfaces from EIM, SIM and sensors
  - Major improvements to impact analysis
  - Incorporate time scale in decision support
- JSS
  - Update interfaces
  - Major integration of EIM data flows
  - Integrate data flow from IAT
- JDW
  - Provide direct links to operations capabilities and provide their current status
  - Create a log that will chronicle the activity within the system
  - Integrate IAT schema
  - Initial version of global filters and common dynamic queries
  - Incorporate time scale information into the schema
- EIM
  - Install Spectrum
  - Integrate Spectrum data flows for topology and faults
  - Update simulation capability to JNDMS through SNMP simulations

- Data Sharing
  - Implement simple email link
- JUI
  - Update GIS to make the views more dynamic including pop-ups and additional links
  - Integrate IAT
  - Update GIS to include links between icons
  - Integrate dynamic queries including filters and highlights
  - Show Operational status
  - Include context information for decisions made by the system
  - Update visualization applet
  - Expand detail views to include core relationships (incorporated with the dynamic queries) and history
  - Operational input screens
  - Implement key reports for commander and include ability to email results

3.5 Phase 2, Cycle 3

3.5.1 Overview

The Cycle 3 development effort concentrated on completion of the final sub systems such as the sharing module and in added depth to the analysis as well as the user interface. This cycle built on the system developed in previous cycles and started with a review of the system, its design and its requirements.

The end of this development cycle represented the end of phase 2 for JNDMS. The final testing occurred in January of 2008 and represented the final system for the core of JNDMS. This testing event identified a number of issues or questions from DRDC Ottawa and resulted in a 'gap analysis' detailing the questions by DRDC Ottawa.

The results of the post demonstration reviews and the resulting gap analysis were reviewed at MDA Halifax on 13 March 2008 – 14 March 2008. These demonstrations concentrated initially on reviewing system features that required additional explanation from the Cycle 3 tests. These demonstrations then went on to review the structure and content of the new extended test cases. These tests included updates to the sharing module, risk review and safeguards. At the conclusion of the discussions and demonstrations it was clear that additional time would be required to cover all of the extended test cases cleanly.

The execution of these extended test cases was planned over a series of Web demonstrations. The test set up for Cycle 3 was maintained in the Halifax lab and was used in conjunction with an additional demo laptop for some test cases.

The web demonstrations were held over the months from March 2008 to September 2008.

3.5.2 Test Environment

The test environment used for Cycle 3 was based on the CWID demonstration environment, however it had to be significantly updated in several respects.

The first change was to be in the size of the network. It was found during the CWID demonstrations that the scalability of the system was going to be an issue so the test environment would have to plan for this. The core of the network would maintain the basic support facilities found in CWID (see Figure 13).

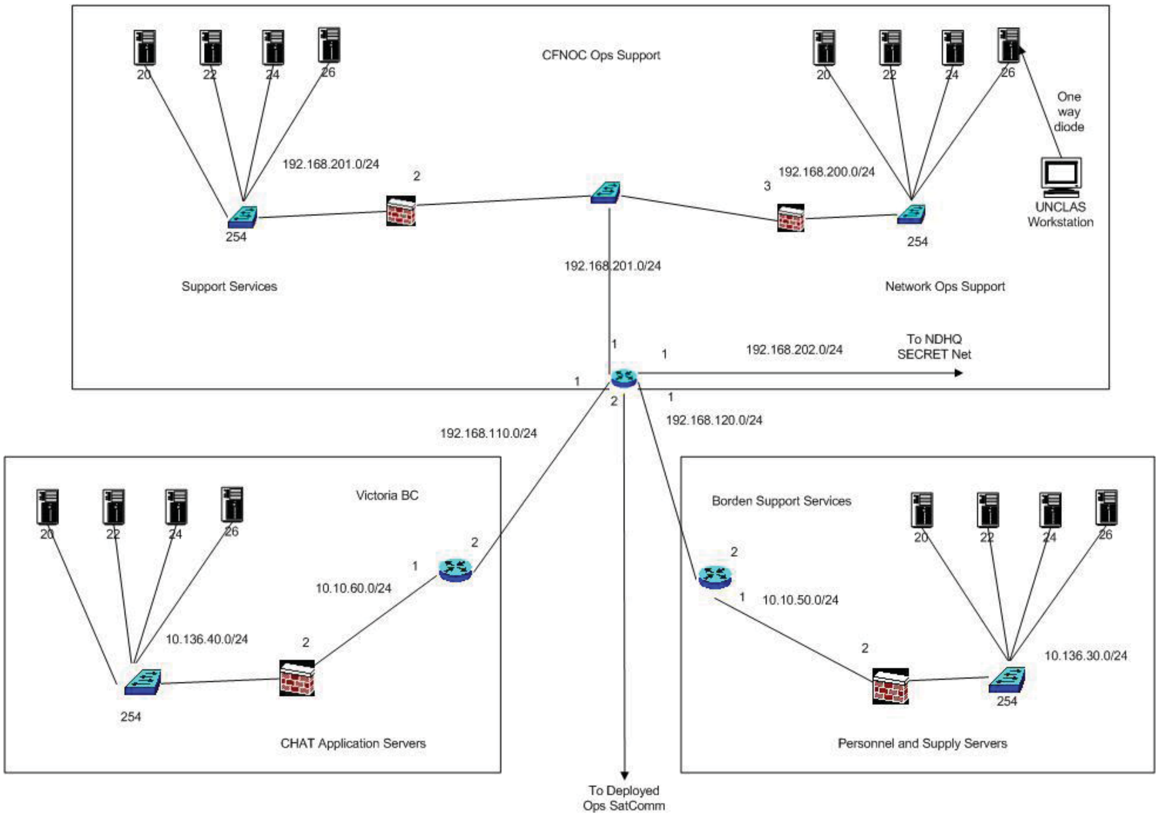


Figure 13: Cycle 3 Support Services

In addition to the support services the structure of the deployed units, as developed during CWID preparation, would be maintained (see Figure 14). In both of these cases the number of assets and the number of network subnets was substantially increased. For example the number of assets was increased from approximately 600 for CWID to approximately 3000 for Cycle 3 demonstrations.

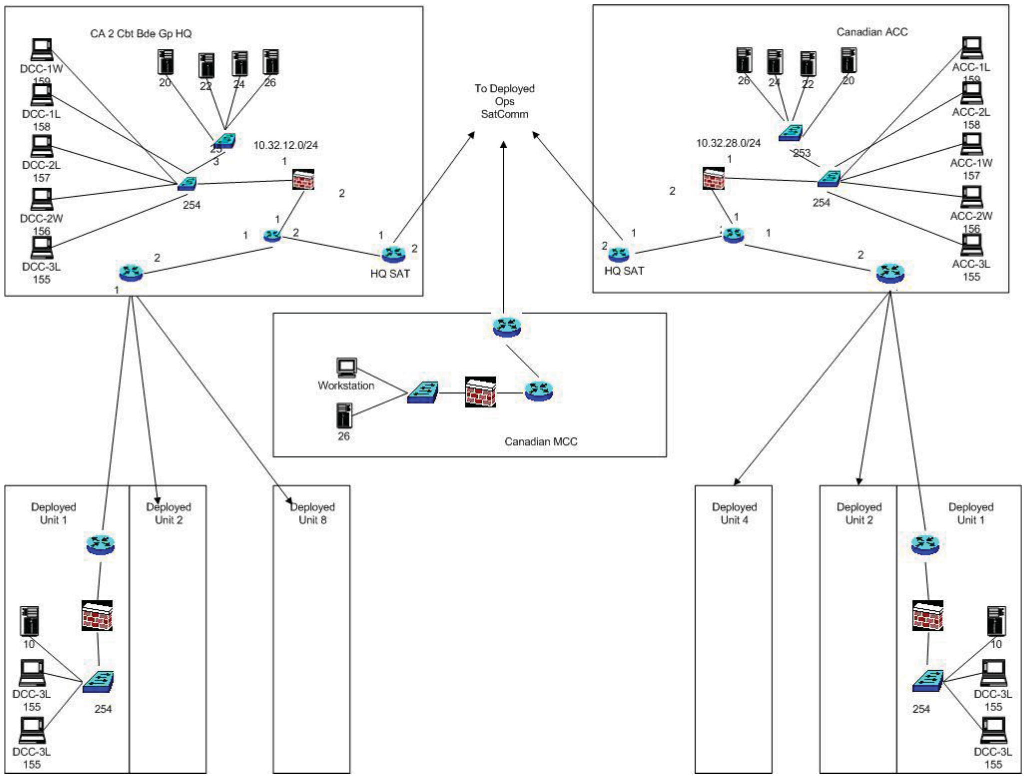


Figure 14: Cycle 3 Deployed Services.

The final simulated environment also included some subnets that were simulated using a router simulator, Dynagen, as well as a captured SNMP image of running hosts. This combination allowed the discovery, using Spectrum, to find and map the simulated network. This test environment was built to be larger and more dynamic than the previous version.

The simulated network also included multiple networks. As part of the updates made during Cycle 3 there was a sharing module added. The testing of this sharing module included the simulation of the one way transfer of data. See Figure 15 for the simulation of the top secret network.

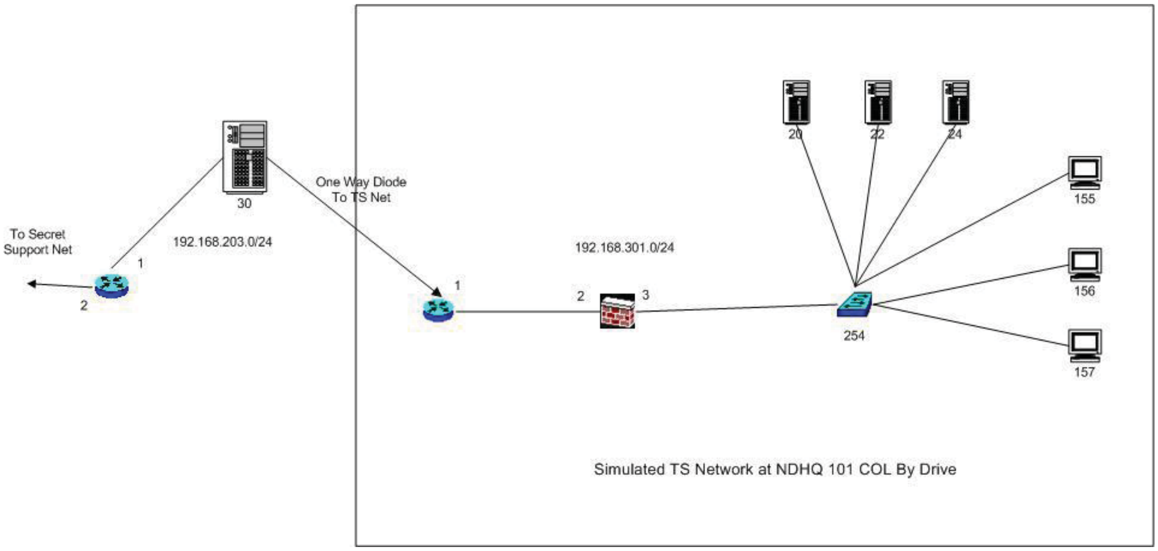


Figure 15: Cycle 3 Simulated Top Secret Network

3.5.3 Objectives and Progress

The objectives identified for Cycle 3 can be found in the Cycle 3 Development Plan [5] and the progress towards these objectives are as follows:

1. **Implementation and enhancement to the Sharing Module including:**

- Movement of data and information within and across domains both laterally and upward (diode) through the JNDMS system structure

  The sharing module was implemented such that event flows into the system could be configured to 'share' with another JNDMS. This configuration allowed information to flow latterly across the domain as well as upward to another domain using a data diode concept. At any point the receiving system could have access to additional event flows that would amalgamate into a new situational awareness.

2. **Improved Decision Support System structure including:**
   - A review of the current DSS rules
   - The implementation of additional DSS rules
   - Advanced Defensive Posture

   The DSS underwent a major overhaul during cycle 3. There had been identified a number of performance issues with the Aion BRE implementation so an analysis of our use of technologies was done. It was found that some of the processing done by the rules engine, such as maintaining and simulating network graphs, was not well aligned with how the rules engine processed the rules. This resulted in undesired performance bottlenecks.

   We examine the overall rule base and came to the conclusion that the core rules would be better implemented within a more traditional programming language. We examined tools that would allow us quick and expressive processing of graphs, then implemented a Java version of the rules.

   We implemented the core rules as both Aion rules and as Java rules, then examined the ease of maintenance as well as the processing speed. The Java version quickly became the preferred implementation.

   It was felt after these experiments that the rules engine would be better utilized on top of the Java processing and that the maintenance and processing of graphs, such as the network topology and service dependencies should remain in the Java modules. The rules in this case could, in the future, provide additional logic paths that the end user could manipulate as well as make use of learning engines that integrate with the rules engine.

3. **Creation of Logical Links: This will enhance users' ability to capture the logical links related to the IT infrastructure relating to a specific system.** There were a number of updates to the user interface to allow for better user interaction. One of these was the ability to create an operation and its associated logical links.

4. **Continue with exploitation planning initiatives, including a scalability study and further business-process reengineering activities**

   During Cycle 3 it was found that although substantial progress would be made towards the scalability that we would have to have a more focused effort to get within the scope of a possible deployment effort. Talks of a test deployment on DREnet after Cycle 3 occurred and this led to discussions about the creation of task authorizations for effort outside of the scope of Cycle 3. See section 3.7 for details.

5. **Improvements to the user interface as follows:**
   - Performance: Improve responsiveness in tracking and reporting actual network activities

   Effort to improve the responsiveness was done in several subsystems. The portal was updated, the database was updated, the system services (JSS) was updated as well as the DSS. The DSS was mostly rewritten to address performance issues.

- Data Exposure: Present more data to end users for exploitation/interpretation. More data exists in the database than is currently readily accessible

  The user interface was updated significantly to allow better user interaction, more control and more information displayed.

6. **Deliver a working Cycle 3 hardware and software configuration to DRDC Ottawa**

   The development labs at MDA and NRNS were maintained as well as a laptop that included a stand alone version of JNDMS for DRDC Ottawa.

7. **Provide a one (1) day training seminar for DRDC Ottawa and other government agencies prior to the completion of the cycle**

   A training day was provided after Cycle 3 to ensure more information of the lab and configuration was known by DRDC Ottawa. During the cycle effort was spent in using the laptop as a training medium. Configuration and use of a subset of the system was done with the laptop.

8. **Update any CDRL publications required to accurately reflect the Cycle 3 JNDMS configuration**

   The documents were updated at the end of Cycle 3.

3.6 Impact Assessment Tool (IAT)

DRDC Ottawa had developed a Microsoft Access database tool called the Impact Assessment Tool. This tool provided functionality to quickly identify the potential impact of events and vulnerabilities. This tool provided feedback from end users and was used in the analysis of JNDMS to determine how the final system would work.

During the development of JNDMS it became apparent that much of the work that went into JNDMS was a duplicate of IAT and so an amendment to JNDMS was drafted to build on the IAT and look at ways to minimize the duplication of effort.

The initial analysis suggested that with relatively minor updates to the JNDMS data model the functionality of IAT could be preserved. We would then have to look at updates to the user interface while trying to maintain consistency with the core of JNDMS. It was felt that as long as the changes could supplement the core of JNDMS, instead of replacing it, then this was a feasible route.

The IAT was developed within the core of JNDMS with updates to the data model and the user interface. The user interface was implemented in such as way that the user would login as ‘IAT’ (or similar) to make use of the IAT views and other users would get the core JNDMS views.

The data stored to represent test scenarios would generally be different, because not all information, such as network topology, would be known to an IAT deployment. An alternate test data set was created for this purpose.

The IAT effort included the following:

- Updates to the core of JNDMS including the data model and user interface.
- Concentration of work flows for NVAT.
- Updated forms to allow better user interaction.
- Addition of SOPs, POCs and RFCs to the core of JNDMS.
- Updates to vulnerability processing including user interface changes, updates to the CVSS and improvements with the Nessus integration.
- The network infrastructure could now be stored and processed as a summary instead of the details of the network topology. This would allow, for example, the creation of 500 workstations without the details of how they connect.
- The addition of a 'Wiki' tab to collect information from end users.

3.7 Task Authorizations

There were two task authorizations as part of JNDMS. The first concentrated on scalability issues and the second on a DREnet deployment.

3.7.1 Task Authorization #1

The first task authorization concentrated on scalability improvements and preparing for a possible DREnet deployment effort. This effort was to address key performance issues, updates to expected integration tools and to provide a potential plan for deployment efforts.

The scalability improvements included many updates to virtually every part of the system, especially in data base queries, data model schema, portal updates, Intellitactics updates and updates to the analysis. The results of testing with different number of asset throughout the project can be seen in Figure 16.

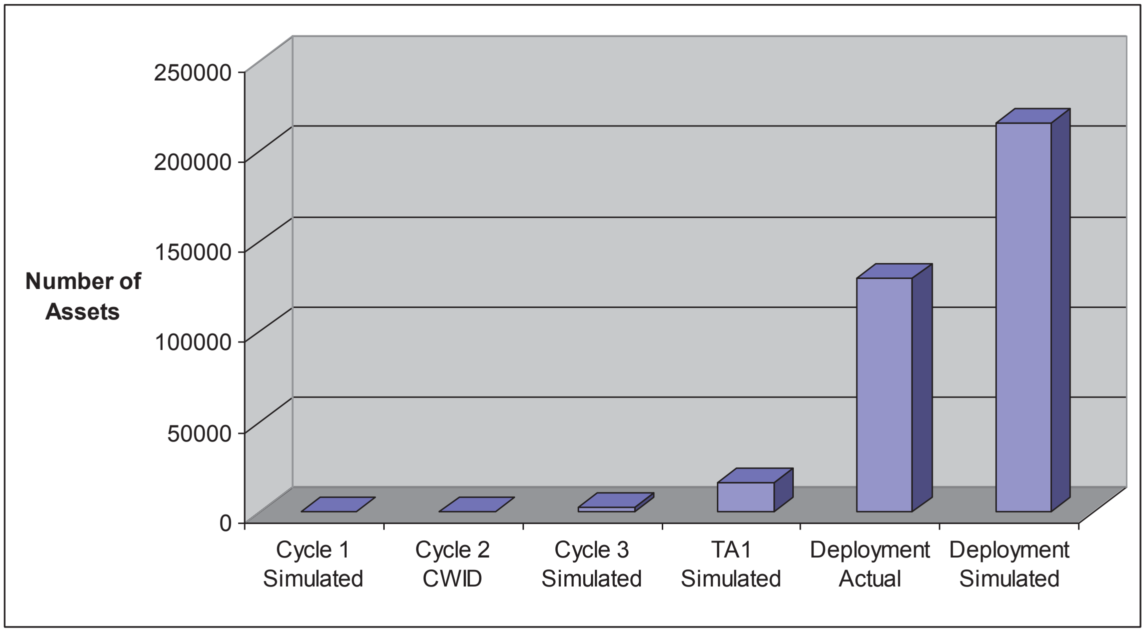


Figure 16: Scalability of asset throughout development.

As part of the scalability efforts the build environment was updated to allow for quick deployments and to better manage the automated tests and various data sets.

The integration efforts included updates to Intellitactics to allow a duplicate copy of the security events to be sent to JNDMS. Updates to Intellitactics also included effort to correlate events before sending to JNDMS.

This task also included effort to procure and integrate nCircle IP360. This vulnerability management tool had been chosen by DND and was seen as the way forward for DRDC.

This task provided a Draft Report [9] on how a deployment effort could occur. This report would identify the remaining issues that would have to be solved as well as the effort required to support the deployment efforts itself.

The final part of this task was an update to the GIS component. The update was done to eliminate much of the performance issues that had been noted with the mapping components. The result of this study was to recommend and provide an initial version of a replacement of the GIS functionality using an open source tool called Open Layers.

3.7.2 Task Authorization #2

The second task authorization was the actual deployment on DREnet. This task included updates to the core of the system for scalability as well as additional integration efforts.

The integration included additional effort for nCircle IP360 as well as integrating with a new software inventory management system, called Centennial.

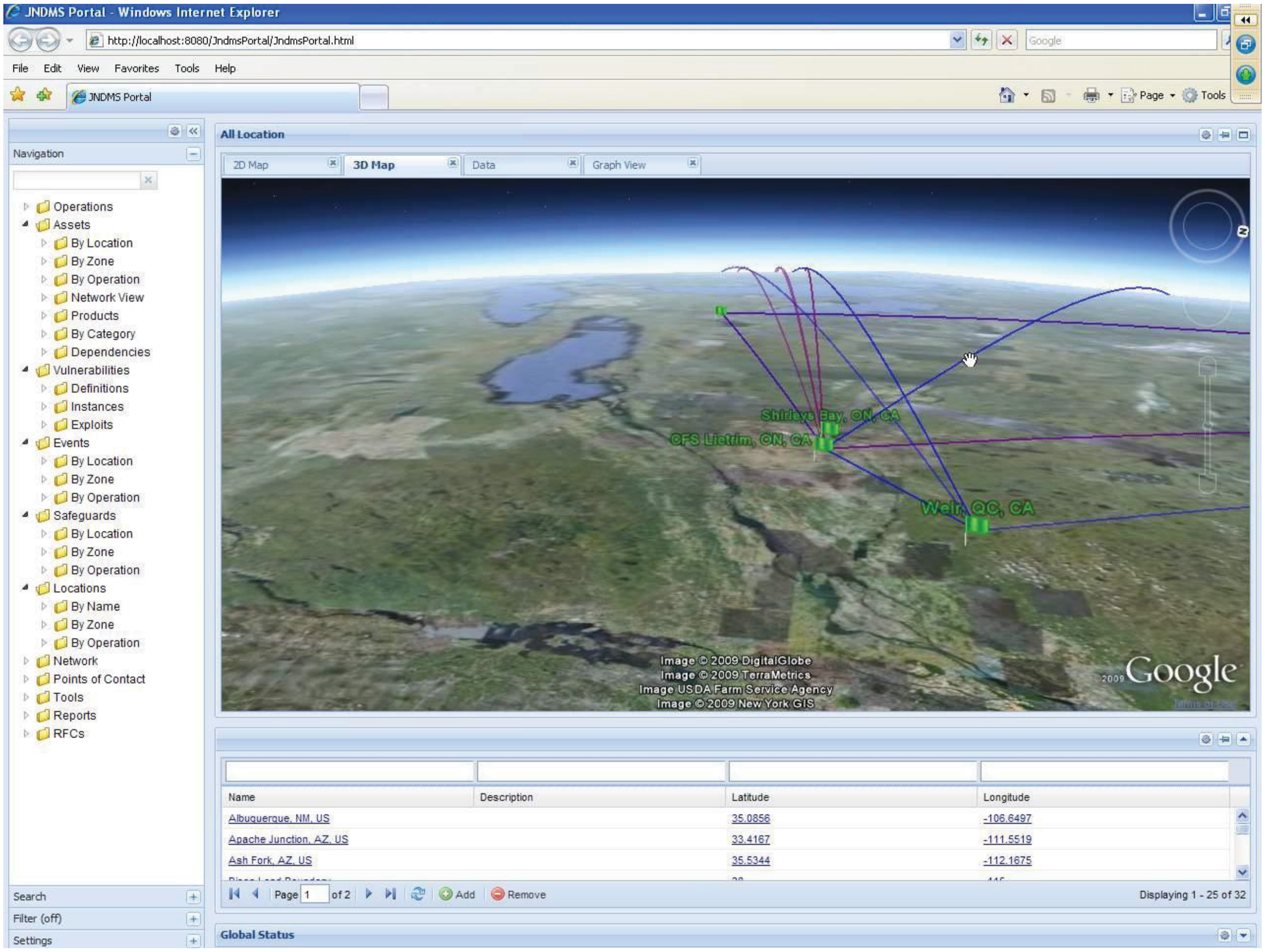
These efforts as well as managing the policy and getting an additional lab setup at the NIO Lab at DRDC Ottawa. This lab had read only access to the security events data, the vulnerability scanning, the software inventory as well as the scanning of the IT infrastructure. The end result was JNDMS running on several sites with the DREnet.

This task also included demonstrations on 25 and 30 June 2009 using the DREnet deployment lab. These final demonstrations were held in the NIO lab at DRDC Ottawa and presented the final version of JNDMS for the TD.

During the final stages of preparation of the demonstration there were still a number of issues relating to the user interface (portal), including some performance issues. A review was held at this point to determine the best way to update the portal. A new technology, the Google Web Toolkit, was evaluated and it was found to provide significant improvements over the current tool set. It was, however, identified as a risk to make such a change this late in the project.

The possible alternatives were reviewed with DRDC Ottawa and it was decided that the improvements to the look and feel as well as the user interaction warranted the risk to migrate the portal to this new technology. This was done as part of TA2.

The new, updated, portal included an updated 2D map using Open Layers, a new 3D map using Google Earth, new components using the Google Web Toolkit as well as updates to all previous components such as the visualization applet. See Figure 17 below.



Name	Description	Latitude	Longitude
Albuquerque, NM, US		35.0856	-106.6497
Apache Junction, AZ, US		33.4167	-111.5519
Ash Fork, AZ, US		35.5344	-112.1675

Figure 17: The update JNDMS Portal

3.8 Phase 3

Phase 3 included a number of efforts including updates to system documentation, the creation of a Transition Report, the authoring of this report and final demonstrations.

As part of phase 3 there was an additional demonstration to NATO. This was done remotely and presented the final version of JNDMS with simulated data. This demonstration was required to see if the JNDMS concept could be exploited by NATO for further development of their Computer Incident Response Capability (CIRC).

4 Lessons Learned

Throughout the project there were a number of Lessons learned. These included:

- The complexity of simulated data was often underestimated. This started to become apparent during the development of the CWID datasets. The increase in depth of the scenarios meant that all aspects of the simulated data had to be maintained. As the size of the data grew and as the complexity of the scenarios or operations grew, so did the complexity of the maintenance of the data.
- Related to the above lesson was the complexity of live networks. The number of integration points and the number of events that could deviate from the simulated events proved to be a significant effort.
- It was also found, however, that the live network was the only way to really test or evaluate the system in the end. For future efforts it would be recommended to ensure that a live network is available at all times. This could allow for a reduction in the effort to maintain the simulated data as well as provide a more realistic data set to test on.
- The creation of automated build environment was beneficial and should have been done earlier.
- Support of long standing relationships through the IPT was found to be essential, especially in working through the policy issues of the deployment.
- Don’t underestimate (possibly part of above) the sometime nebulous requirements for certification.
- Getting vendors involved / CA
  - Tool support / creation of early versions
  - On going support in a timely manner
  - Support on changing tools / when to change
  - License support, especially in deployment efforts
- Web technologies / early adopters. The use of some early versions of technologies has a potential cost.
- Concentrate on key inputs (system simplified as time went on).
- Help/usefulness of focused workflows (IAT role).
- The benefit of keeping appraised of direction of stake holders (use of tools, especially IP360, Centennial).
- Benefit of interfaces to core (separation of components, ease of integration of new tools).

5 Further Research and Development

For further research and development activities could include:

- Scalability. The current system was built to scale to the DREnet deployment. This amounted to about 120k assets with a simulated data set at about 216k assets. Any DND sized deployment would be an order of magnitude beyond this. Here are several areas to look at:
    - The DSS must be able to scale the analysis to the new data size. This could be done by improving its algorithms and by distributing the analysis across multiple machines.
    - The schema could be reviewed to improve common queries. This could include how secondary assets are stored, the creation of indexes or the use of views.
    - The JSS would have to be updated to ensure that data model updates could be maintained under increased load. This is another candidate for using updated hardware or distributing its load.
    - Each of the input subsystems, such as Intellitactics and Spectrum, would have to be configured to scale. This would include updates to the interface to JNDMS in some circumstances.
    - Filtering of software assets from Centennial should be done. There are a lot of very minor software tools, such as fonts, that are reported separately. These should not generally be shown to the user. One option may be to have another class of software that is not generally shown but still recorded.
    - The scalability efforts would have to ensure that the end user's experience remain responsive.
- Stability. Any full deployment would require an updated testing regime that could test all aspects of the system under full load. This would include general bug fixes.
- Focused workflows. It was noted that some common questions or workflows could be implemented as single click options within the current interface. Some effort would be required to identify the key workflows, then provide links and possibly reports to accommodate these specific areas.
- Updates to the analysis. The analysis algorithms should be reviewed as the system scales to ensure that it maintains relevancy and to examine better ways to express the situational awareness. Some options include:
    - The use of a rules engine could be investigated again. The rules engines required significant amounts of data to prove their worth and it was found that they were better utilized in conjunction with other programming models instead of stand alone. It is still believed however that rules engines could provide key benefits in allowing the system to adapt to changing environments or threats and they could also allow operators more control over the analysis. In either case having the system deployed and measuring the events would be essential.

  - Updates to the algorithms to allow the DSS to be distributed over multiple machines.
  - Ensure appropriate controls are exposed to the operators so that the analysis can be tweaked.
  - Examine the possibility of having multiple, parallel, analysis engines. It has been noted that different audiences view risk and impact in different ways. The existing filters allow the focus of the operators to change, but the underlying risk remains constant for all users.
  - As the system gets used the impact of new threats should be reviewed and the analysis updated to reflect new environments.
  - There are a number of special cases noted during the final phases on how certain relationships are expressed. Part of the updates to the analysis would be to ensure that whatever combination the user expresses in the portal would be addressed appropriately.
- The mapping views should be updated to included:
  - Google Earth was shown to be beneficial. This should be integrated into JNDMS through the use of Google Enterprise so that there are no issues with license keys or Internet connectivity.
  - Google Maps should be examined as the 2D API. The current Openlayers has shown that we are pushing the system to the limits. There is a newer version of Openlayers available; however it is felt that any significant updates to the system would be best served by a migration towards Google Maps. Google is already used for the demonstration of the 3D maps and this would provide added consistency as well as the improved feature set of the Google Maps API.
  - The geographical views have shown to be beneficial and it would help the overall interface if there was more interaction with the map through the portal. This could include options such as drawing a polygon on the map and having a search done within this area. This option may require either the GIS extensions to Oracle or other database tools such as PostGIS.
- The applet could be updated so that the layouts scale better and the more focused workflows are integrated into the applet.
- General updates to the portal could include:
  - The ability to add or edit more relationships.
  - General testing
  - Direct links to external tools. Some tools provide a web interface that we could leverage if we knew an asset's IP address, for example.
  - Updates to input forms to allow faster inputs of common data.
  - Updates to the filter and searches to support common queries and to include additional user tools such as the ability to highlight a subset of a search.
  - Update to the new portal to ensure all functionality is available.

- General updates to the core inputs could include:
  - The vulnerability definitions and possibly other schemas should be updated to the most current version.
  - Examining additional sources of data and how they would be imported into JNDMS.
  - Updates to the firewall processing rules to support more platforms and provide more information to the operators.

References

[1] Cycle 1 Development Plan, MDA Reference # DN0681 dated 27 April 2006

[2] Cycle 1 Trial Report, MDA Reference # DN0736 dated 21 March 2007

[3] Cycle 2 Development Plan, MDA Reference # DN0681 dated 02 February 2007

[4] Cycle 2 Trial Report, MDA Reference # DN0736 dated 21 August 2007

[5] Cycle 3 Development Plan, MDA Reference # DN0681 dated 26 October 2007

[6] Cycle 3 Trial Report, MDA Reference # DN0859 dated 28 January 2009

[7] Architecture Document, MDA Reference # DN0654 dated 26 April 2007

[8] Design Document, MDA Reference # DN0678 dated 03 December 2008

[9] TA1 Final Report, MDA Reference # DN0935 dated 30 January 2009

[10] Requirements Document, MDA Reference # DN0658 dated 28 October 2005

[11] TA2 Final Report, MDA Reference # DN1011 dated September 2009

[12] Transition Report, MDA Reference # DN0773 dated September 2009

List of symbols/abbreviations/acronyms/initialisms

DND	Department of National Defence
DRDC	Defence Research & Development Canada
DRDKIM	Director Research and Development Knowledge and Information Management
DSS	Decision Support System. Part of JNDMS
EIM	Enterprise Information Management. Part of JNDMS
GWT	Google Web Toolkit
JDW	JNDMS Data Warehouse
JNDMS	Joint Network and Defence Management System
JSS	JNDMS System Services
R&D	Research & Development
SIM	Security Information Management. Part of JNDMS

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.) MDA Systems Ltd. Suite 60, 1000 Windmill Road Dartmouth NS B3B 1L7	2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.) UNCLASSIFIED (NON_CONTROLLED GOODS) DMC A REVIEW: GCEC JUNE 2010

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

Contractor Final Report: For the Technology Demonstration of the Joint Network Defence and Management System (JNDMS)

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

MacDonald, S.

5. DATE OF PUBLICATION (Month and year of publication of document.) October 2013	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.) 45	6b. NO. OF REFS (Total cited in document.) 12

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.)

Contract Report

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

Defence R&D Canada – Ottawa
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4

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.) 15BJ	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.) W7714-040875/001/SV
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 Ottawa CR	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.) MDA Reference # DN1011

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

UNLIMITED

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.))

UNLIMITED

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

This document has been written to fulfill the deliverable DID-PM-007 for the Joint Network Defence and Management System (JNDMS) Technology Demonstrator under contract W7714-04-0875/001/SV. This document covers the execution and results of this Technology Demonstration.

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.)

Computer Network Defence // Cyber Situational Awareness