DN0654: 31 MARCH 2006
ISSUE 3/0: 21 SEPTEMBER 2009

ARCHITECTURAL DESIGN DOCUMENT FOR THE TECHNOLOGY DEMONSTRATION OF THE JOINT NETWORK DEFENCE AND MANAGEMENT SYSTEM (JNDMS) PROJECT

DRDC-RDDC-2014-C28
CONTRACT NO. W7714-040875/001/SV

DID SD 002

PREPARED FOR:

MARC GREGOIRE
DEFENCE R&D CANADA - OTTAWA
3701 CARLING AVENUE
OTTAWA ON K1A 0Z4

PREPARED BY:
SCOTT MACDONALD
MACDONALD DETTWILER AND ASSOCIATES LTD.
SUITE 60, 1000 WINDMILL ROAD
DARTMOUTH NS B3B 1L7H

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 the Department of National Defence of Canada.

DN0654
Issue 3/0
21 September 2009

DOCUMENT APPROVAL SHEET

ARCHITECTURAL DESIGN DOCUMENT FOR THE TECHNOLOGY DEMONSTRATION OF THE JOINT NETWORK DEFENCE AND MANAGEMENT SYSTEM (JNDMS) PROJECT

CONTRACT NO. W7714-040875/001/SV

DID SD 002

MDA SYSTEMS LTD.

Scott MacDonald
Author (Signature) (Date)

Beverly MacNeil
Quality Assurance (Signature) (Date)

Brett Trask
Project Manager (Signature) (Date)

CHANGE RECORD

Rev. #	Pages Affected	Description	Date of Issue
1/0	All	First Issue (Draft Release)	21 Oct 05
1/1	All	End of phase update	31 Mar 06
2/0	All	Cycle 2 Update	26 Apr 07
3/0	All	Third Issue	21 Sep 09

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 Introduction

Network Enabled Operations may enable Defence and Security forces to operate more effectively, efficiently and quickly than an adversary. This is known as "Decision Superiority", which is the ability to make better and faster decisions than would-be criminals, terrorists and hostile forces. Decision Superiority is dependent on robust Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems and the underlying networks and computer systems.

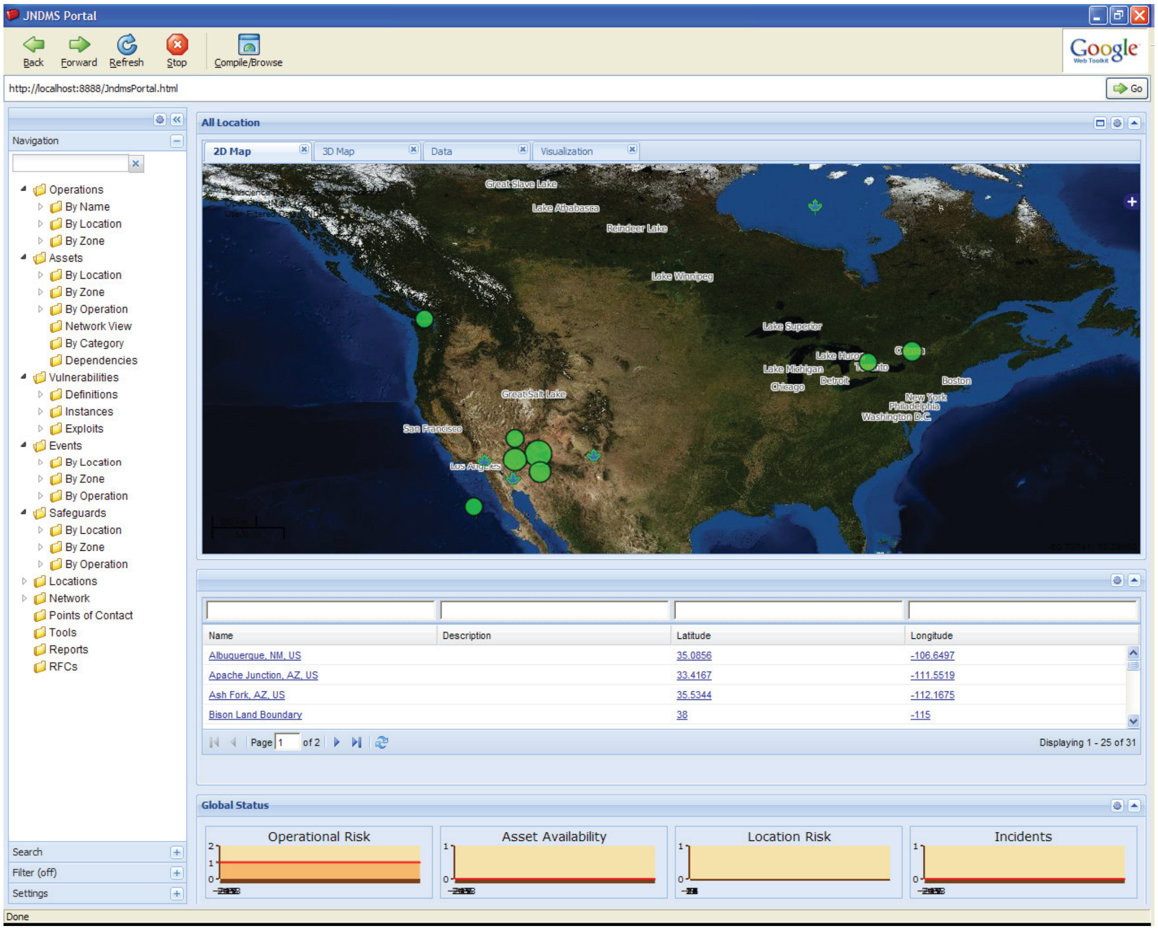
Criminals, terrorists and hostile forces are becoming more sophisticated in their ability to compromise the C4ISR systems of Defence and Security forces. The threat to the Canadian Forces (and our Allies) is here and now - hackers try to compromise our computer and network infrastructures on a daily basis. In future operations the lives of Canadians and Allies could depend on Canada's ability to maintain sustain and defend its Network Enabled Operations. At the highest level, the purpose of JNDMS is to ensure the safety and security of Canadians and our Allies.

"The JNDMS' vision is to combine the network management and the network security domains to provide Situational Awareness (SA) for Computer Network Defence (CND)." (JNDMS Statement of Work)

The JNDMS will enable the Canadian Forces (CF) to be more effective, efficient and successful in conducting military operations. Military Commanders and network operators and maintainers will be able to make better decisions on how best to conduct operations and how to operate and maintain networks in support of current and future operations. JNDMS will help military commanders to be more cognisant of the netcentric dimension of the modern battlefield. It will help ensure that network provided services are available and optimized when they are needed by the CF.

The JNDMS vision is to design and develop a system that integrates network management knowledge, security management knowledge and knowledge of the Department of National Defence (DND) operations. The JNDMS acquires, fuses and correlates both static and dynamic information collected from several sources to achieve SA for the defence of DND's computer networks. SA information must be presented to military personnel in a succinct and contextual form that clearly describes the impact of the network on military operations.

In the JNDMS Portal (see Figure 1), the information system is combined with web-GIS capabilities to provide an immediate geographical context to a situation.



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
Bison Land Boundary		38	-115

Figure 1: JNDMS Portal Information Integrating SA

1.1 Document Purpose and Scope

This document satisfies the requirement for delivery of an Architecture Design Document, Data Item Description (DID) SD 002 for the JNDMS TD as specified by contract no. W7714-040875/001/SV. This document contains the design of the JNDMS software to the system architecture level. Other documents may specify further details for each level of Computer Software Configuration Items (CSCI) described herein. The hierarchy of this document within the project documentation is as shown in Figure 2.

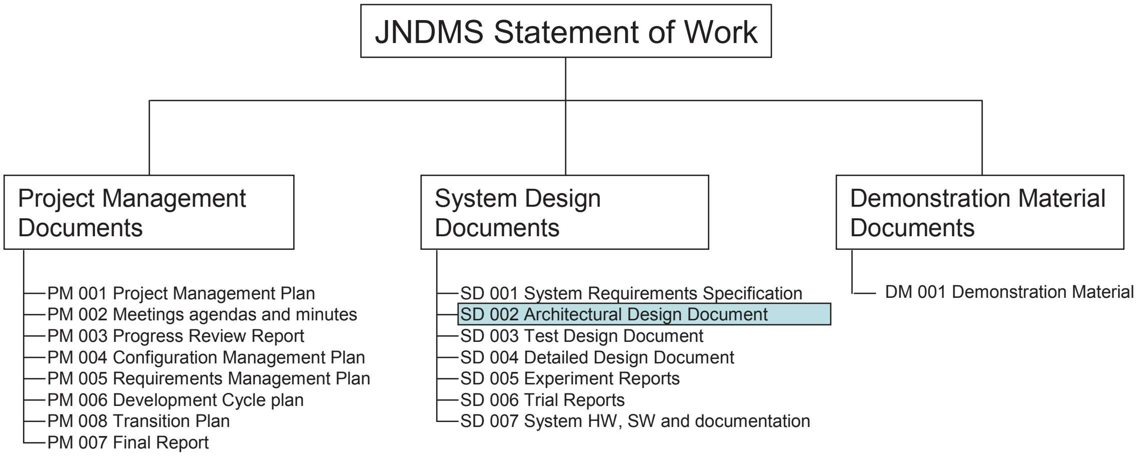

JNDMS Statement of Work
Project Management Documents
PM 001 Project Management Plan
PM 002 Meetings agendas and minutes
PM 003 Progress Review Report
PM 004 Configuration Management Plan
PM 005 Requirements Management Plan
PM 006 Development Cycle plan
PM 008 Transition Plan
PM 007 Final Report
System Design Documents
SD 001 System Requirements Specification
SD 002 Architectural Design Document
SD 003 Test Design Document
SD 004 Detailed Design Document
SD 005 Experiment Reports
SD 006 Trial Reports
SD 007 System HW, SW and documentation
Demonstration Material Documents
DM 001 Demonstration Material

Figure 2: Document Hierarchy

For each JNDMS subsystem, this document outlines the corresponding design, including:

- A brief overview of the configuration item (CI)
- The key design decisions and approaches
- The static and dynamic views, describing the key data flows, classes, and functions
- A summary of the key algorithms needed

1.2 Document Structure

This document is organized as follows:

- Section 1 Introduction – introduction to this document.
- Section 2 Documents – identifies all applicable and reference documents.
- Section 3 JNDMS Software Overview – provides a brief summary of the JNDMS architecture.
- Section 4 Design Decisions – provides some information on the architectural trade-offs that were performed.
- Section 5 CSCI Subsystems – details the architecture of the subsystems.
- Section 6 JNDMS Data – provides a description of the database.
- Section 7 Adaptation to Technology Trends – details the technology trends that will be accommodated by the JNDMS.
- Annex A – Allocated Requirements – details the requirements and how each will be met.

2 Applicable Documents

The applicable documents listed below provide information that either takes precedence over, or forms an intrinsic part of this document, to the extent specified herein.

A-1	W7714-4-040875/A	Request For Proposal
A-2	W7714-4-040875/001/SV	JNDMS Contract
A-3	01-0423	JNDMS Proposal
A-4	DN0665	JNDMS Software Requirements Specification
A-5	DN0678	JNDMS Design

3 JNDMS Software Overview

The principle benefit of JNDMS is improved “Network Situational Awareness” for CF Commanders and network operators and maintainers. This is a significant enhancement to capabilities of the CF. DND can currently detect network faults and security related events. A JNDMS must do more, however. A JNDMS must answer the basic question — so what? The military commander needs to know if and how a security event impacts the mission and JNDMS must present this information in a clear and concise manner.

In order to protect Canada’s military operations, knowledge, information, tactics, and plans, the JNDMS is a system that is designed for the specific purpose of network defence and management. In addition to the management and protection of these networks, we need to allow Military Commanders to assess the health and availability of the networks in the same way that they would any other operational asset, such as a ship, a tank, a plane or a platoon. DND possesses a great deal of information that describes its information technology (IT) assets from an availability and security perspective. Unfortunately, this information is not contextual in terms of DND operations. DND must know what the asset’s purpose is, why a specific server provides a specific service, what type of information is disseminated by a server and how its operations depend on its IT assets.

The JNDMS vision is to design and develop a system that will integrate network management knowledge, security management knowledge and knowledge of DND operations. The JNDMS acquires, fuses and correlates both static and dynamic information collected from several sources to achieve SA for the defence of DND’s computer networks. SA information must be presented to military personnel in a succinct and contextual form that clearly describes the impact of the network on military operations (Figure 3).

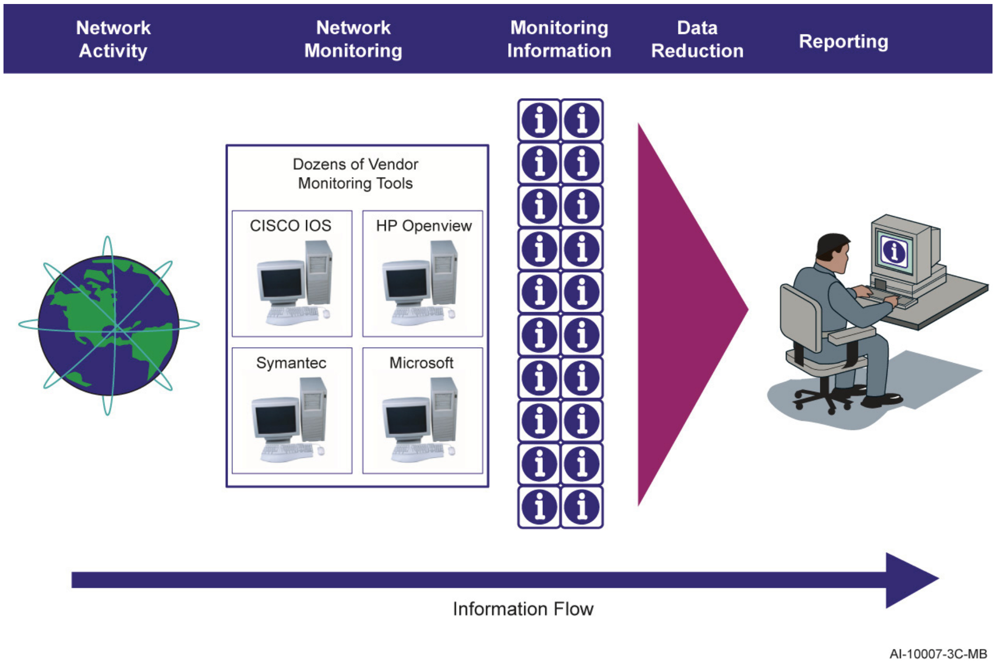


Figure 3: Overall System flow is from Network Activity through Monitoring and Data Reduction to Reporting of Situational Awareness.

One of the key aspects of the JNDMS Technology Demonstrator (TD) is to provide people with information that is understandable and relevant. A key objective of the JNDMS TD is to provide a system to allow military command to be aware of the state of networks and of network activity, to be alerted of attacks in order to identify the location and severity of the attacks, and to quickly assess the impact on its military operations. Information must be reported in a way that the person observing it can understand at a glance:

- What is happening on all networks?
- Where it is happening, geographically?
- In which network classification domain, in which network, and in which system a specific event is happening?
- Why it is happening?
- How does it impact my military operations?
- How to access the system or network; and
- How to remedy the situation or how to limit any propagation of related events?

The JNDMS must be able to exchange network defence and network management information across CF networks, Network Operation Centers (NOC) and C4ISR systems, such as the Canadian Forces Command System (CFCS), Joint Information and Intelligence Fusion Capability (JIIFC), Air Force Command and Control Information System (AFCCIS), Maritime Command Operation Information Network (MCOIN) III and Land Forces Command and Control Information System (LFC2IS). Further, in order to enhance collective defence and security, the JNDMS must be interoperable with the NOCs and C4ISR systems of our Allies.

As depicted in Figure 4, JNDMS provides functionality across multiple networks operating in a multi-level security environment. This capability is significant because network SA can be extended across multiple networks operating at different security classifications.

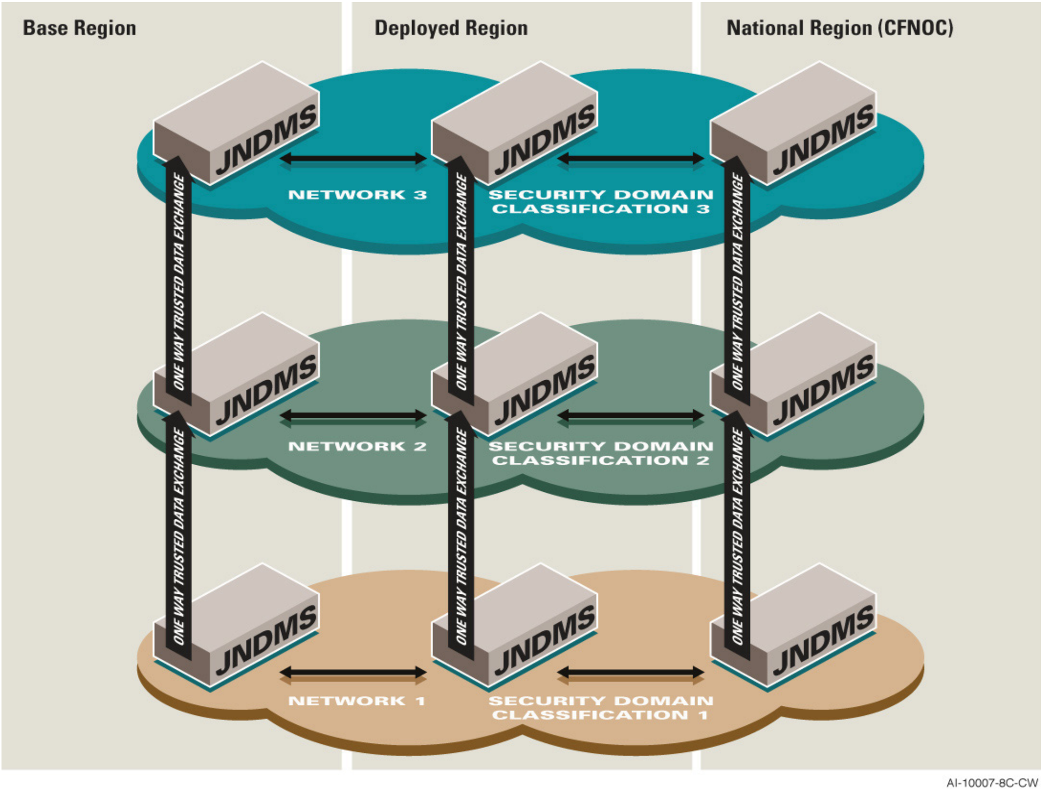

Base Region
Deployed Region
National Region (CFNOC)
JNDMS
NETWORK 3
SECURITY DOMAIN CLASSIFICATION 3
NETWORK 2
SECURITY DOMAIN CLASSIFICATION 2
NETWORK 1
SECURITY DOMAIN CLASSIFICATION 1
ONE WAY TRUSTED DATA EXCHANGE
AI-10007-8C-CW

Figure 4: JNDMS Provides Functionality Across Multiple Levels of Networks

The JNDMS context diagram is shown in Figure 5. The JNDMS provides the following functionality to DND/DRDC:

- Receive Static and Dynamic Data from the network, commercial network service providers, IT staff and operational staff
- Process received data
- Generate SA to operational staff, IT staff, network service providers, and international coalition personnel

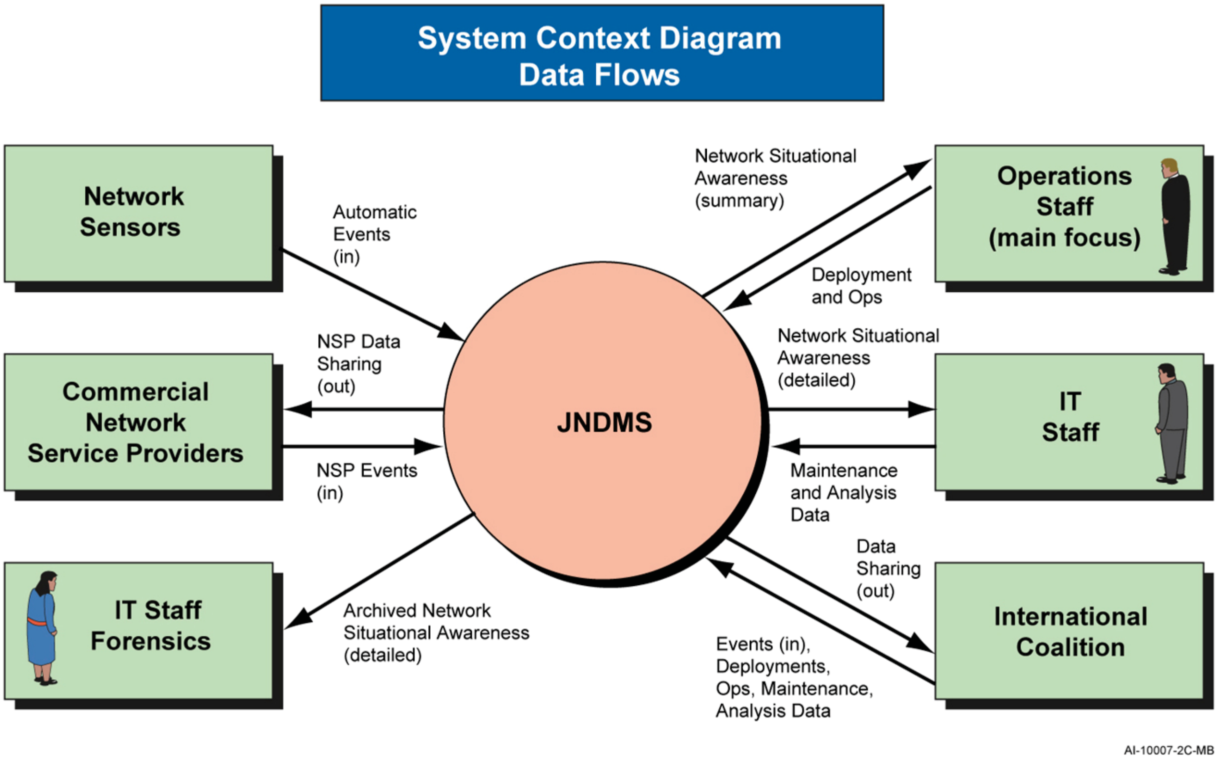

System Context Diagram
Data Flows
Network Sensors
Automatic Events (in)
Commercial Network Service Providers
NSP Data Sharing (out)
NSP Events (in)
IT Staff Forensics
Archived Network Situational Awareness (detailed)
JNDMS
Network Situational Awareness (summary)
Deployment and Ops
Operations Staff (main focus)
Network Situational Awareness (detailed)
Maintenance and Analysis Data
IT Staff
Data Sharing (out)
Events (in), Deployments, Ops, Maintenance, Analysis Data
International Coalition
AI-10007-2C-MB

Figure 5: JNDMS Context Diagram

For a more detailed explanation, refer to the JNDMS Requirements Specification [A-4].

3.1 Software Architecture

The technical purpose of the JNDMS is to collect, manage and present real-time information. The application of the JNDMS is network monitoring, decision making and reporting about network status and events on the networks. This leads to a high-level conceptual architecture (see Figure 6). The network status and events are information being collected at the level of the network and hardware on DND networks and flowing up to a database or data warehouse. Once transformed, the data is normalized, de-conflicted and written to database by the transformer. From the database, decisions are made about which information is routine, which information is important and timely, and which information is urgent in order to require immediate attention. Finally, the presentation system (at the top of the stack in Figure 6) provides a human-friendly SA view on all this information so that people may browse for information when required or be interrupted with alerts about important and urgent events, where required.

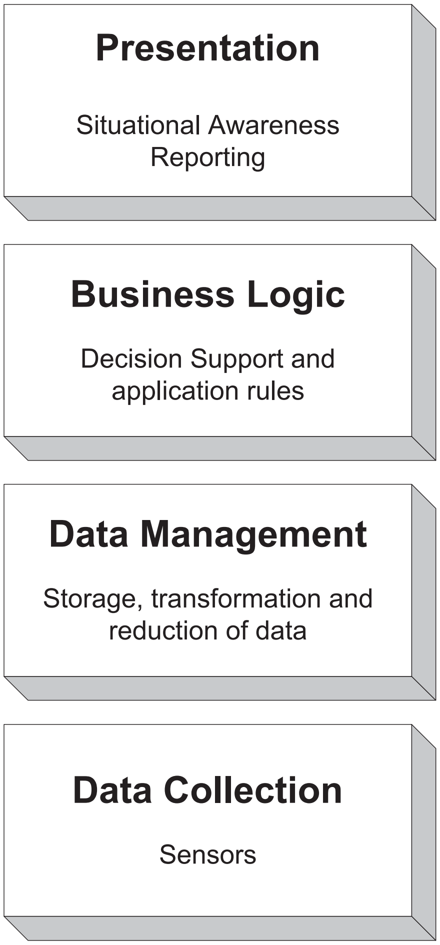


Figure 6: Conceptual Architecture of the JNDMS

The conceptual architecture identifies the following categories of components, identified from the lowest layer to the highest layer:

- Data Collection

  Any information that can be useful in generating conclusions about the state of the network is gathered via the various technical means that will be in place.

- Data Management

  Anticipated large volumes of data from many different sources must be translated into a common representation and stored in a database or data warehouse.

- Business Logic

  The business layer transforms between business processes and raw data. The JNDMS business layer is the implementation of the decision support system, which will:

  - Reduce the amount of information in the database that gets reported to a level of detail required to produce situational awareness
  - Prioritize specific events to get reported as alerts

- Presentation

  Make information available to people through an intuitive interface and share data with other services.

3.2 High-Level System Architecture

The JNDMS Integrated Project Team (IPT) has identified an architecture of specific system components that defines the implementation of the JNDMS, as shown in Figure 7. Each of these components has interfaces and system processes. As this architecture is driven by the architectural themes that we have identified, then each of the system components should have standard interfaces that allow them to interact with other components.

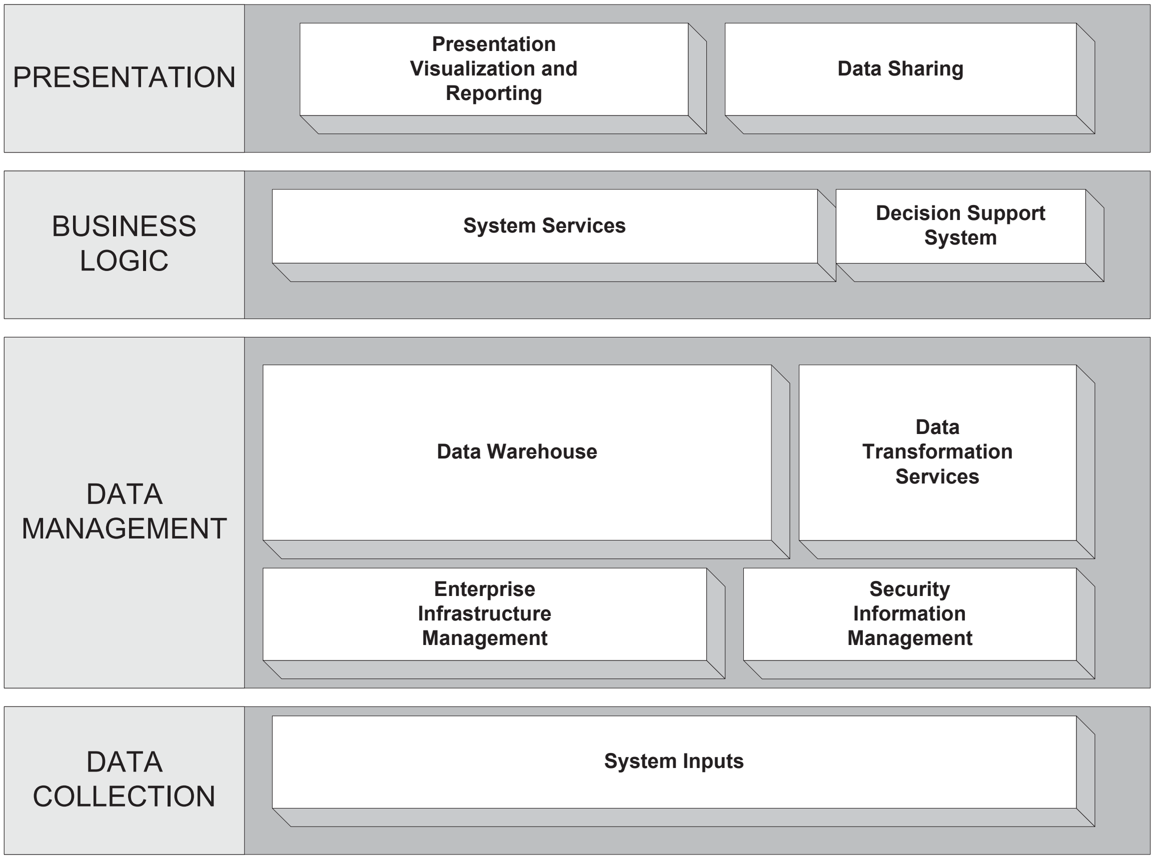

PRESENTATION
Presentation Visualization and Reporting
Data Sharing
BUSINESS LOGIC
System Services
Decision Support System
DATA MANAGEMENT
Data Warehouse
Data Transformation Services
Enterprise Infrastructure Management
Security Information Management
DATA COLLECTION
System Inputs

Figure 7: High-Level Systems Architecture of the JNDMS

Specific functional components and interfaces between them have been identified as the high-level architecture for the JNDMS.

MDA Systems Ltd.'s (MDA) high-level architecture is composed of the following:

- Data Collection Components

  The MDA solution leverages established Commercial Off-The-Shelf (COTS) or open-source products to perform some of the more challenging aspects of CND data acquisition. They include Security Information Management (SIM) products, Enterprise Infrastructure Management (EIM) products, Host Vulnerability Scanners, and Network Infrastructure Discovery and Mapping products. The role of JNDMS is to integrate and manage the results of these tools, and not to provide similar functionality.

- Data Management Components

  DND is a security conscious organization and as a result employs a great deal of security-point products, which generate large volumes of security event data. The SIM component performs initial data fusion and correlation processing on security event data and only inject qualified security events, as well as other interesting security related events into the JNDMS. EIM and Data Collection components also perform some level of data fusion and correlation processing.

  The JNDMS stores all its data, whether acquired or created, in the JNDMS Data Warehouse. The MDA solution implements the JNDMS Data Warehouse with a COTS relational database management system (RDBMS). COTS RDBMS products include the necessary features to achieve data integrity, data replication and data backup. When in persistent storage, JNDMS data maintains contextual attributes, such as temporal, origin, and severity attributes.

- Business Logic Components

  The MDA solution includes a core component (the JSS) that is responsible for initial preprocessing, system I/O, corrdination with the DSS and tasks related to data model integrity.

  The JNDMS Decision Support System (DSS) is responsible for the analysis of incoming events. This componet maintains internal state machines that can identify the current status of the system, including topology and dependency information. This component may, optionally, use a business rules management system to augment its analysis.

- Presentation Components

  The MDA solution includes state-of-the-art visualization technology to convey SA information in highly contextual forms. The JNDMS presentation component supports role-based interactions with the JNDMS operator. Network administrators require the most detailed information, while network and security analysts mandate information pertinent to incidents. Finally, Military Commanders simply demand to know how incidents affect their missions. The JNDMS presentation component provides the correct information to the correct operator at the appropriate time.

  The MDA solution includes mechanisms to permit sharing of SA data with JNDMS installations in the same security domain, with JNDMS installations in other security domains, as well as the information assurance systems of coalition partners. Information sharing policies and information sharing agreements control the flow of shared SA data both in (import) and out (export) of the JNDMS. MDA has also identified a solution to permit information sharing between networks of different security classifications using one-way communication devices commonly referred to as data-diodes.

3.3 COTS Technologies

One of the architectural themes in MDA's solution is to enable best-of-breed COTS technologies. MDA has done an initial assessment of technologies for the JNDMS TD solution and has identified best-of-breed technologies for each of the architectural components.

Each of the JNDMS components is open to the use of different technologies. Specific technologies will not be selected until the end of Phase I of project execution. However, our initial technology comparison draws us to the current best-of-breed landscape of candidate technologies for the JNDMS. The summary of this best-of-breed landscape is provided in Table 1. For a detailed list of products that have been selected, and their interfaces to the system, see the JNDMS Design Document (A-5).

Table 1: Best-of-Breed Technologies for the JNDMS TD

Component	Prelim. (P) Option (O)	Vendor	Product Name	Description	Input Interfaces Supported	Output Interfaces Supported
Sensors (system inputs)	P	CA	eTrust	Network discovery.	Syslog, SMTP, SNMP, FTP, SCP, SMB, NFS, JDBC, ODBC, flat files	XML, SNMP, Flat File
	O	Sun	Java + Eclipse IDE	Java can be used to create custom Import applications.	Any required interface not supplied by COTS	CORBA, JDBC, ODBC, XML, SNMP, Flat File
	P	Intellitactics	ISM	Can process CND periodic inputs.	FTP, SCP, SMB, NFS, JDBC, ODBC, proprietary, C2IEDM	XML, SNMP, Flat File
	O	Sun	Java + Eclipse IDE	Java can create custom import applications.	Any required interface not supplied by COTS	CORBA, JDBC, ODBC, XML, SNMP, Flat File
Enterprise Infrastructure Management	P	CA	Unicenter, BrightStor, eTrust	Unicenter performs enterprise management functions. eTrust performs vulnerability functions.	Syslog, SMTP, SNMP, FTP, SCP, SMB, NFS, JDBC, ODBC, RADIUS, OPSEC LEA, proprietary	XML, SNMP, Flat File

Component	Prelim. (P) Option (O)	Vendor	Product Name	Description	Input Interfaces Supported	Output Interfaces Supported
	P	CA	Spectrum	Spectrum manages network topology and system faults. This product is being integrated into the CA Unicenter suite.	Unicenter bridge, CLI, CORBA	Unicenter bridge, CLI, CORBA
	P	CA	eTrust	eTrust manages network performance metrics. This product is being integrated into the CA Unicenter suite.	Unicenter bridge	Unicenter bridge
	O	Axios	Assyst	Assyst is an IT Service Management product that supports the ITIL best practices.	Bridges to major EIM components, proprietary interfaces, others TBD	Bridges to major EIM components, proprietary interfaces, others TBD
	O	Centennial	Discovery	The Centennial Discovery is a software inventory tool.	Database queries	JDBC.
	O	Ipswitch	What's Up Gold	Network monitoring utility.	SNMP, WMI, Custom agents	Web, Propreitary
	O	Microsoft	SMS/MOM	Can be used as an alternate source of enterprise management functions. Can also be used as a source into the EIM.	XML Based Proprietary API	XML based Proprietary API
Security Information Management	P	Intellitactics	ISM	Discovers interrelationships, prioritizes threats, receives and archives alerts, correlates alerts, performs forensic analysis.	Syslog, SMTP, SNMP, FTP, SCP, SMB, NFS, JDBC/ ODBC, RDEP, RADIUS, OPSEC LEA, LMP, SDW, CSDW, flat files	XML, SNMP, CIDF, IDMEF, IODEF, Flat File
	O	NCircle	IP360	Vulnerability and Risk Management	Propreitary Agents	XML, Propreitary Interfaces

Component	Prelim. (P) Option (O)	Vendor	Product Name	Description	Input Interfaces Supported	Output Interfaces Supported
Data Transformatio n	P	Apache	Xalan	Xalan is an implementation of XSLT (eXtensible Stylesheet Language Transformations)	XML	XML
	P	Apache	iBATIS	iBATIS provides support for mapping database queries to XML or Java objects	XML, JDBC	XML, Java
	P	CA	Advantage, ERWin	Advantage performs Extract, Transform and Load (ETM) functions. Erwin performs data modeling functions.	WBEM, CIM-XML, UML	UML, XML, SQL
	P	Sparx Systems	Enterprise Architect	Performs UML data modeling functions.	UML	UML, XML, XMI, SQL,
	O	Oracle	Oracle	Oracle can be used an alternate for data modeling functions.	XML, Proprietary	SQL, XML, SQL
Data Warehousing	P	Oracle	Oracle	Performs all aspects of RDBMS.	SQL, SQLNet, JDBC, XML	SQL, SQLNet, JDBC, XML
	O	CA	Ingres	INGRES may be an Open-source alternate for database.	SQL, SQLnet, JDBC, XML	SQL, SQLNet, JDBC, XML
	O	Microsoft	SQLServer	SQLServer may be a Microsoft-specific alternate for the database.	SQL, SQLnet, JDBC, XML	SQL, SQLNet, JDBC, XML
System Services	O	JBoss	JBoss	J2EE Applications Server	SOAP, HTTP	SOAP, HTML, HTTP
	O	IBM	Websphere	J2EE Applications Server	SOAP, HTTP	SOAP, HTML, HTTP
	O	BEA	Weblogic	J2EE Applications Server	SOAP, HTTP	SOAP, HTML, HTTP
	P	Apache	Tomcat	J2EE Applications Server	SOAP, HTTP	SOAP, HTML, HTTP

Component	Prelim. (P) Option (O)	Vendor	Product Name	Description	Input Interfaces Supported	Output Interfaces Supported
Decision Support System	P	CA	AION	Performs all DSS functions.	XML, Proprietary	XML, ODBC, JDBC
	P	Sun	Java + Eclipse IDE	Java can create custom output apps.	JDBC, CORBA	<Anything>
Presentation, Visualization, and Alerting	P	Liferay	Liferay Portal	Liferay Portal is an implementation of a J2EE Portal based on JSR standards	Java, SOAP, HTTP, JDBC, many custom	HTML, SOAP, JDBC, Custom
	P	Oracle	Oracle	Custom data visualization services.	Java	
	P	ESRI	ArcGIS	GIS and Web Mapping services.	OpenGIS, WMS, WFS, GML, WCS, SensorML	HTML, Java, XML
	O	CA	Cleverpath	Web portal services	XSL, XML,	HTML, Java, XML
	P	Google	Google Web Toolkit	The Google Web Toolkip provides tools and a framework for rich internet applications.	Java	W3 Standards
	P	Ext	Ext GWT	This provides extensions to the GWT	Java	W3 Standards
	P	Open Layers	Open Layers	This provides an Open Source 2D mapping component	Javascript	Javascript
	P	Google	Google Earth Plugin	This provides a 3D mapping component	Javascript	Javascript
	O	Microsoft	Internet Information Server	IIS is a Microsoft-specific alternative for the presentation functions.	ASP, Java, ActiveX, DLL, HTML, DHTML, SOAP, .NET	HTML, DHTML, XML, Jscript, VBScript, SOAP, .NET
Situational Awareness Data Sharing	P	CA	Advantage	Can perform CND output functions.	IODEF	XML, SMTP, S/MIME, SOAP, HTTP, SCP,
	O	Sun	Java + Eclipse IDE	Java can create custom output apps.	JDBC, CORBA	<Anything>

3.4 Use of Open Standards

The purpose of open standards is the key to facilitating flexibility and evolutionary capabilities of the JNDMS. MDA's TD makes use of existing open standards where they logically fit in the TD architecture. Open standards provide the advantage of independency between the system components - allowing the system to maintain its architectural integrity regardless of the technology used in any one component. The use of open standards will be the key to long-term stability and relevance of the JNDMS.

A large number of standards are available for use today, as described in Table 2. In cases where services or interfaces are required for which no standards exist, a modular approach in the system architecture will mitigate those gaps. With a modular architecture, it is feasible to implement minimal interfaces or components with the objective of replacing them with standards-based interfaces or components, if and when they become available.

Table 2: Standards Available for Use in the JNDMS TD

Standard	Description
.Net	Software development infrastructure for developing, managing and deploying distributed applications and web systems. Microsoft specific.
AES	More secure option for store and forward encryption algorithm are used to ensure security.
C2IEDM	Command and Control Information Exchange Data Model (C2IEDM) is used to exchange military information.
CIM-XML	Common Information Model (CIM) for exchange of management information.
COM	Application Programming Interface (API) for distributed applications and web systems. Microsoft specific.
CORBA	API for computer platform independent data exchange. Java focus, but language independent.
CVE	The Common Vulnerability Enumberation (CVE) is a standard format and identifier for published vulnerabilities.
CVSS	Common Vulnerability Scoring System (CVSS) for exchange of vulnerability impact information.
DES	Store and forward encryption algorithms are used to improve security.
HTTP, HTTPS	Hyper Text Transfer Protocol (HTTP) secure is used to improve security of remote web sessions.
IDEF1x	Industry standard used to describe and exchange data models.
IDMEF	Intrusion Detection Message Exchange Format (IDMEF) is used to exchange intrusion information.
IODEF	Incident Object Description and Exchange Format (IODEF) is used to exchange incident information
ITIL	Information Technology Information Library. OpenGIS® Consortium (OGC).
Javascript (ECMAScript)	Javascript is a standardized (through the ECMAScript specification) method for enhancing the presentation of web pages through scripting. This is a critical component in the new generation of dynamic web pages.
J2EE	A platform-independent, Java-centric infrastructure from Sun for developing, building and deploying Web-based enterprise applications.
JSR-198	Machine and web-engine independent methods for describing portlets.
JSR-88	J2EE APIs
JSR-94	Rules engine independent methods for describing business rules.
JSR-168	Java Specification Request for Portlets.

Standard	Description
JSR-286	Draft Java standard to update Porlet specification.
JSR-170	Java Specification for standard content repository.
Mil-STD 2525A	Standard symbology for military displays.
MIP	Multilateral Interoperability project for interoperability between C4ISR systems.
MQ Series/ CICS	Queued API that permits reliable message delivery for multiple platforms. Microsoft specific.
NVD XML	This represents the schema published by the National Vulnerability Database (NVD) to publish vulnerabilities.
Oasis	The Oasis standards group publishes a number of industry specifications for security, data exchange and web services.
ODBC	Generic database interface used to manipulate databases.
OpenGIS	Standards for geographic views. Newer standards, such as SensorML, could eventually replace this.
RPC	Remote Procedure Calls (RPC) are used to perform multi-platform remote method invocation.
S/MIME	Secure Multipart Internet Message Extensions (S/MIME) is used to export and import information from external sources.
SANS Top 20	List of top 20 vulnerabilities identified by the System Administration, Networking and Security (SANS) Institute imported to identify vulnerabilities.
SMTP	Simple Mail Transfer Protocol (SMTP) is used to export and import information from external sources.
SNML	Simplified Network Mark-up Language (SNML) for exchange of network topologies.
SNMP	Simple Network Management Protocol (SNMP). This is a common method for computing or networking devices to report on configuration and status.
SOAP	Simple Object Access Protocol (SOAP) is used to perform remote invocation and web services through the single web port.
SQL	Industry standard used to define and manipulate data.
SSH, SCP	Secure Socket Shell (SSH) and Secure Copy (SCP) are used to exchange data with external systems.
SSL	Secure Socket Layer (SSL) is used to improve security through third party carriers.
UML	Industry Standard data modeling language.
VulnXML	Vulnerability description in XML from the Open Web Application Security Project.

Standard	Description
W3C Standards	World Wide Web Consortium (W3C) defines web related standards such as HTML and HTTP.
XML	Industry standard used to describe and exchange data models.

3.5 Technical Architecture

Shown in Figure 8, the baseline architecture for the JNDMS adhered to for the technology demonstation. As a result of this detailed analysis, technical solution elements for the JNDMS architecture have been identified.

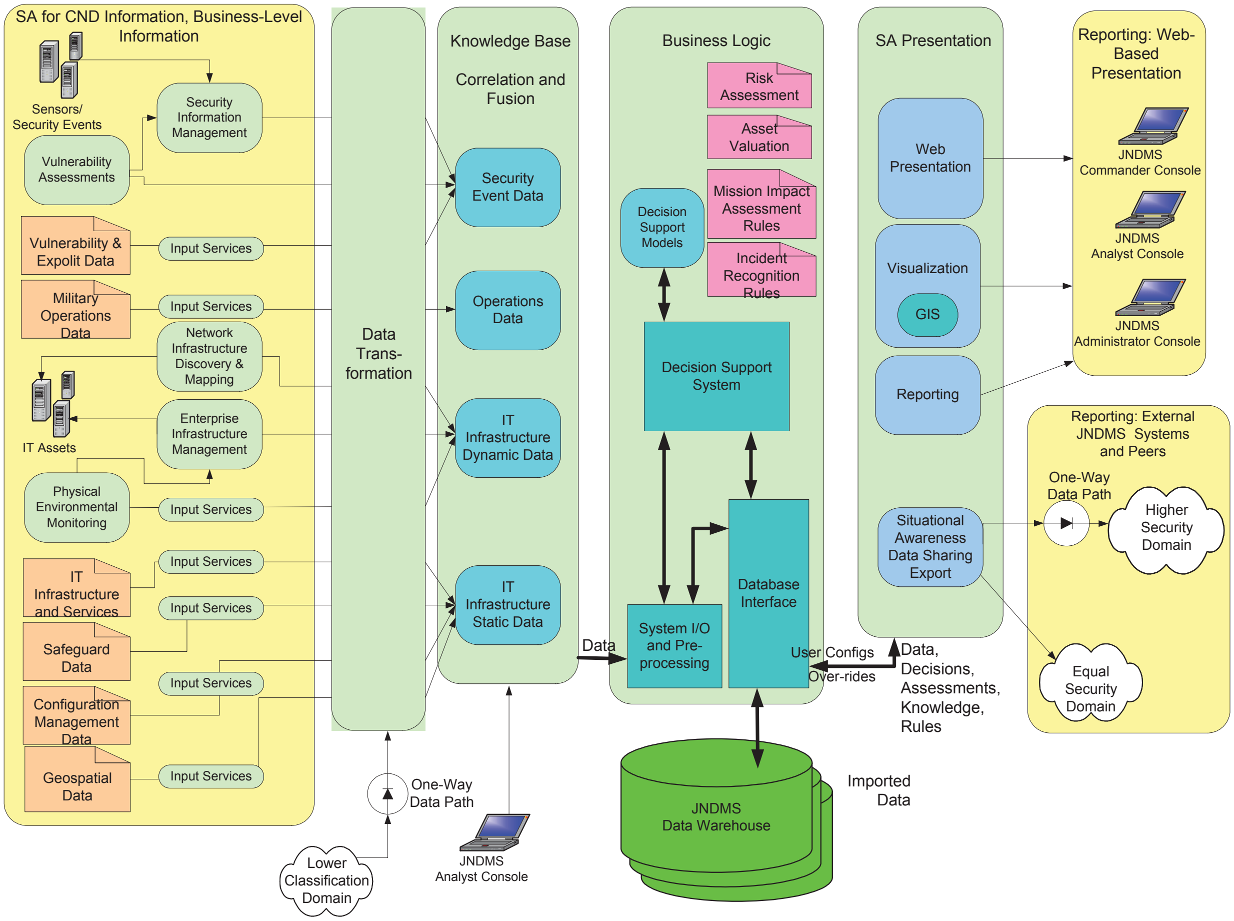

SA for CND Information, Business-Level Information
Sensors/ Security Events
Security Information Management
Vulnerability Assessments
Vulnerability & Expolit Data
Input Services
Military Operations Data
Input Services
Network Infrastructure Discovery & Mapping
IT Assets
Enterprise Infrastructure Management
Physical Environmental Monitoring
Input Services
Input Services
IT Infrastructure and Services
Input Services
Safeguard Data
Input Services
Configuration Management Data
Geospatial Data
Input Services
Data Trans-formation
Knowledge Base
Correlation and Fusion
Security Event Data
Operations Data
IT Infrastructure Dynamic Data
IT Infrastructure Static Data
Business Logic
Risk Assessment
Asset Valuation
Mission Impact Assessment Rules
Incident Recognition Rules
Decision Support Models
Decision Support System
System I/O and Pre-processing
Database Interface
Data
User Configs
Over-rides
SA Presentation
Web Presentation
Visualization
GIS
Reporting
Situational Awareness Data Sharing Export
Data, Decisions, Assessments, Knowledge, Rules
Reporting: Web-Based Presentation
JNDMS Commander Console
JNDMS Analyst Console
JNDMS Administrator Console
Reporting: External JNDMS Systems and Peers
One-Way Data Path
Higher Security Domain
Equal Security Domain
JNDMS Data Warehouse
Imported Data
One-Way Data Path
Lower Classification Domain
JNDMS Analyst Console

Figure 8: The MDA IPT Technical Architecture for the JNDMS

The remainder of this document describes the software design of each of the software components.

3.6 Assumptions

The following assumptions have been made for the JNDMS design:

- Sufficient security is provided by standard login accounts provided by the operating system. User and data security are provided by the operating system.
- Security access controls for JNDMS components will not be implemented. Each user or role will have access to available data.
- Data collected by the JNDMS will be reduced by correlation and coalescing prior to transfer to a higher-level JNDMS system.
- The JNDMS is a tool for assessment, not to determine or take actions.

4 Design Decisions

The following design decisions have been made for the JNDMS software design:

- Near-Real-Time – Response requirements between sensor to user interface (UI) roll-up do not exist at this time, but given the nature of the distributed interface and potential for slow-speed connections, it should be on the order of minutes. Prototyping has confirmed this timing constraint can be met by the Windows 2003 server operating system or Redhat ES operating system.
- Database – For a central point of persistent storage, a database is a logical choice. For the JNDMS, we require an enterprise scale database with built-in replication and transaction integrity mechanisms. This provides the JNDMS with a method to recover the system state after a system crash or power outage.
- Message Queues – For most of the communications in the JNDMS, a high-speed (< 0.5 s) form of inter-process communication (IPC) is not required. Therefore, the primary form of IPC will be provided by the database or by standard network protocols such as SOAP and HTTP. Custom network communications may be required within the system.
- JNDMS Graphical User Interface (GUI) Decoupling – For the JNDMS UI, a framework for communication is used that will allow the UI to be used either locally on the JNDMS or remotely on another Windows computer with network access to the JNDMS. The use of a thin client using Web browser technology allows maximum flexibility in deploying the clients as well as provide an industry supported platform to integrate COTS offerings.
- All performance requirements involving the timing are an average time, meaning that the JNDMS software can exceed the requirement during individual measurements, but on average it meets the requirement.
- Use of COTS – COTS hardware, software and protocols have been chosen where possible.
- Data Storage Throughput – In order to ensure that there is sufficient data storage throughput for playback/recording and processing, copying of raw data files must be avoided. Since these files are possibly tens or hundreds of gigabytes in size, copying a raw data file could take several minutes during which throughput would be severely reduced. To overcome this, summary information is forwarded with linkages back the source information where possible.

.

5 JNDMS Configuration Items

JNDMS has been initially decomposed into nine separate function groupings, referred to as Computer System Configuration Items (CSCI). These CSCIs include:

1. System Inputs
2. Enterprise infrastructure management
3. Security information management
4. Data transformation services
5. Data warehousing
6. Decision support system
7. System Services
8. Presentation, visualization and alerting
9. Situational awareness data sharing

These CSCIs and interactions are described in the following sections.

5.1 System Inputs

There are many sources of real-time or ephemeral data about the CND defensive posture, operations data and security events. These sources include sensors, probes, firewall logs, routers, network intrusion detectors, data from IT infrastructure management systems, application logs or operating system logs, which provide insight into configuration changes or anomalous asset behaviour. JNDMS interfaces with these existing data sources in the DND network infrastructure (Figure 9).

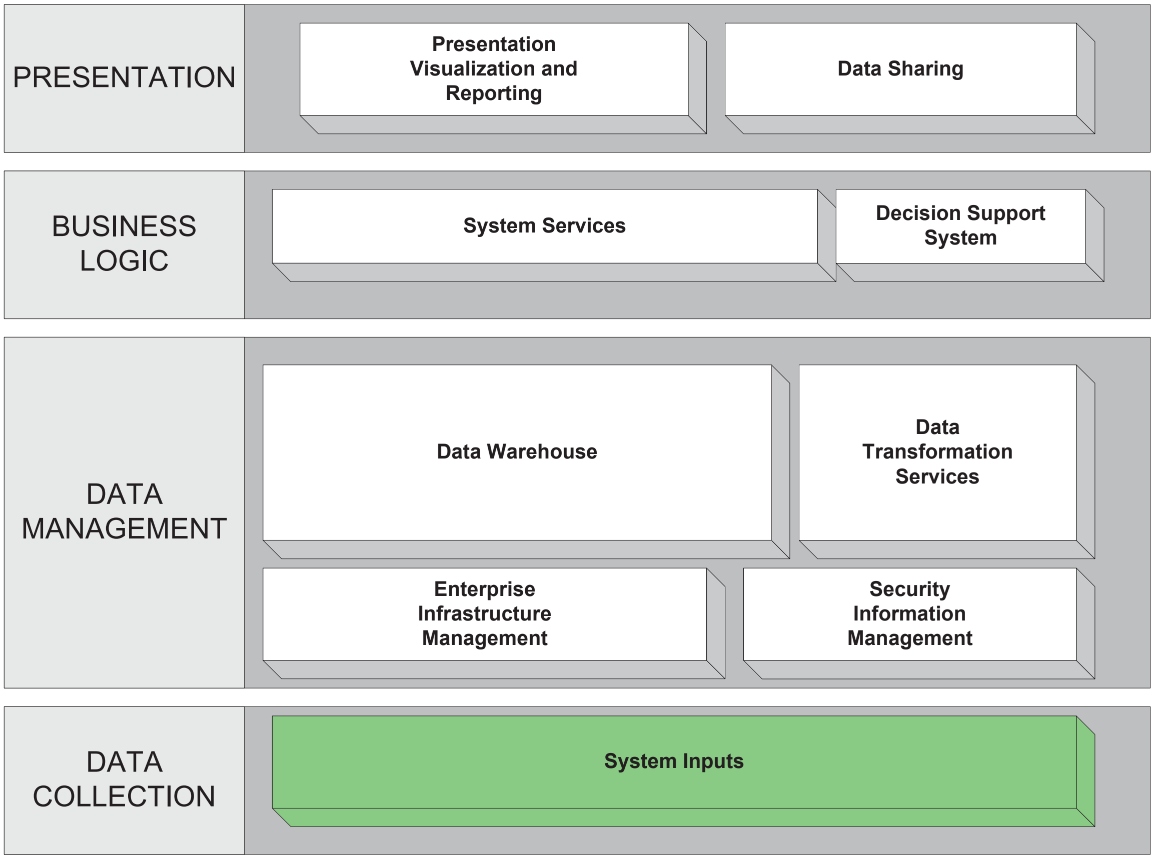

PRESENTATION
Presentation Visualization and Reporting
Data Sharing
BUSINESS LOGIC
System Services
Decision Support System
DATA MANAGEMENT
Data Warehouse
Data Transformation Services
Enterprise Infrastructure Management
Security Information Management
DATA COLLECTION
System Inputs

Figure 9: System Inputs

The Systems Inputs component(s) accept data from many sources, and provide data to the EIM, the SIM or directly to the JNDMS system services. Interfaces to these components consist of standard interfaces available from COTS tools and custom interfaces. For example, both Computer Associates' (CA) Unicenter product and the Intellitactics product currently interface with hundreds of existing systems.

5.1.1 Component Introduction

Data collection is crucial to the success of the JNDMS - all decisions made and alerts raised will only be as capable as the quality and completeness of the data upon which they are based. It is critical that the JNDMS identifies all necessary sources of data input and implements data collection components that are capable of handling the quantity and formats of input data.

The System Inputs component collects data from the DND networks and make that data available to the data management and business logic layers of the JNDMS. Considerations are made to minimize bandwidth using “push technologies”. Use of “pushed” data from the remote sources enables receipt across one-way data diodes. “Push” also allows the receipt of data to activate processing, rather then requiring bandwidth expensive polling systems.

5.1.2 Component Technologies

The sensor inputs report to the rest of the system through either the JNDMS system services interface or through data inputs provided by the EIM or SIM components. Many of the system inputs are in the form of small helper applications, or agents, that understand the sensor and can report to JNDMS.

The SIM (Intellitactics) and EIM (Unicenter) tools have many data inputs preconfigured that address many common interfaces required for JNDMS.

5.1.3 Component Description

The system inputs collect data pertinent to the CND environment, including the defensive posture information, operations data, security events, status of the IT infrastructure and services, safeguard data, security event data, and vulnerability and exploit data.

As implied in the name, the CND Dynamic inputs component collects these inputs and update the JNDMS with these inputs on a near real-time basis. Data will be acquired from different networks spanning different security classifications and requires an accurate time base for each of the segments.

As will be discussed in following sections, after the data has been collected, the JNDMS Data Management layer:

- Transforms
- Filters
- Normalizes
- Aggregates
- De-conflicts
- Appends with metadata (including the source data source, a timestamp, and any information associated with the data)
- Stores the data in the Data Warehouse

5.1.4 Security Data

Security data can come from sources within the networks, such as:

- Firewalls
- Network Intrusion Detection Systems (NIDS)
- Host-based Intrusion Detection Systems (HIDS)
- Intrusion Prevention Systems (IPS)
- Authentication Authorization and Audit servers (AAA)
- Anti-Virus systems (AV)
- Operating system logs
- Application logs
- Database audit logs
- Web proxies
- Web servers
- Authentication servers
- Trouble or incident ticketing systems
- Enterprise Management Systems
- Dynamic Host Configuration Protocol logs (DHCP)
- Public Key Infrastructure systems (PKI)
- Networking devices

DND has already deployed numerous security point products as sensors within their network infrastructure. They include network and host-based firewalls, network and host based intrusion detection systems, filtering routers, vulnerability scanners, and anti-virus solutions. Security point products can generate and transmit a large volume of events or alerts across the network. There are dozens of different data formats and interface mechanisms in which dynamic data is collected. This provides for one of the measures of complexity that the Data Management layer must deal with.

The specific products and deployment options within DND continues to evolve and will change over the course of the project. JNDMS will concentrate on ensuring that examples of key interfaces are met to ensure that eventual transition into DND can be accomplished. This approach ensures, for example, that common IDS inputs can be processed but that the specific IDS products used by DND may be addressed as part of the transition process.

5.1.5 Vulnerability Scan Data

Vulnerability Assessment (VA) scanners on the networks can generate results of targeted host scans rapidly enough to be of use in ongoing or emerging incident investigations.

5.1.6 IT Infrastructure and Services Data

IT Infrastructure and IT Services data are harvested into the JNDMS through the EIM and access through external managed databases. Physical environmental monitoring includes this aspect of IT infrastructure data harvesting, as well as some direct data acquisition and data modeling services, as described in the following paragraphs.

A differentiating facet of the JNDMS-threat landscape from information security perspectives is the much greater need for SA of physical environmental impacts on the CND environment. Dynamic inputs of this nature may include kinetic threats from enemy attacks or mundane threats to field operations IT environments.

Some IT environmental devices, such as Uninterrupted Power Supply (UPS) systems or server room air conditioning systems, have the ability to generate Simple Network Management Protocol (SNMP) packets. These packets are broadcast or retrieved through the network, typically by a network management console. Information is contained in a Management Information Base (MIB), which is a data structure that defines what is obtainable from the device and what can be enabled or disabled.

Examples of IT infrastructure data include:

- Network topology and configuration information
- Physical and logical connections between network assets, their physical and logical interdependencies, functions, redundancies
- Geographic locations of networks and all components on the networks
- Extracts from software distribution and network management tools (such as Microsoft Systems Management Server [SMS] and Microsoft Operations Manager [MOM]) or Big Brother
- Configuration management (CM) databases
- Assets inventory
- Internet Protocol (IP) address allocation schemes or spreadsheets
- Network diagrams
- Circuits and cabling datasets/diagrams
- Network analysis and design tools, etc.

Of these sources, the CM database forms the central basis for managed IT infrastructure data since it should describe all certified and accredited IT network and system assets.

Some types of IT infrastructure static data (such as network or cabling diagrams, and contact lists) are not directly useful during incident analysis, but aid in expeditious incident response. For this reason it has been added into the JNDMS data warehouse and made accessible through a JNDMS Presentation-level component, as a reference to analysts and other system users.

5.1.7 IT Infrastructure Discovery and Mapping

IT infrastructure discovery fills the huge gap between the planned and expected IT infrastructure, and the reality of the deployed and configured IT infrastructure. Network discovery information can validate and update the information obtained from static IT infrastructure data sources; hence, the JNDMS periodically acquires snapshots of the actual state of the CND environment using network discovery tools. An organization cannot manage what it does not know exists and it cannot secure what it does not manage. Active network discovery techniques obtain accurate information about an organization's IT infrastructure.

5.1.8 SA Data Sharing (inbound)

Military operations often include coordination with coalition partners and as such require the sharing of SA data with the partners. An important source of dynamic input to CND SA is inbound information sharing from other JNDMS or JNDMS-like coalition systems. SA data sharing is further described in detail in section 5.9.

5.1.9 JNDMS Console/Human Input

Input by users of the JNDMS is an important part of the dynamic information providing SA of the CND environment. In addition to manual methods for correcting automatically collected data, manual methods will exist for changing the rolled-up severity values of SA for CND and the creation of user-defined rules. This allows for operator control of all JNDMS outputs.

5.1.10 Military Operations Data

The JNDMS acquires specific types of formatted military operations data such as the name of the operations, unit names and main IT assets and requirements involved, criticality of IT assets to the mission, and schedule in terms of time-windows. The JNDMS data model must clearly capture operational IT dependencies and what the effect will be on the operation if the IT asset or service is destroyed or unavailable, if its content is altered, or if it must operate at a reduced service level.

Military operations data includes geospatial data of appropriate precision so that it can be overlaid with contextualized information, such as risks of various kinetic or physical environmental threats that may be present due to the location of mission-critical IT assets. Similarly, mission-critical IT services must be associated with physical IT assets so that a defensive posture assessment can be performed. Providing spatial relationships for both military operations data and IT assets permits all of these to be visually correlated to geography. The JNDMS acquires and links network assets to geographic location with sufficient precision to support SA.

Where military operations data is available in the C2IEDM format, developed by the Multilateral Interoperability Programme (MIP), in an operational database, it can be acquired automatically on a scheduled basis; otherwise it is uploaded in bulk into the JNDMS by system operators.

5.1.11 Vulnerability and Exploit Data

A large variety of vulnerability data is acquired by the JNDMS, including general IT vulnerability and exploit advisories and vulnerability dictionaries, internal or classified sources of vulnerability data, and operational environment-specific vulnerability and threat data. Non-IT vulnerability and exploits are also captured, such as those associated with physical equipment, networks access and backup capabilities, security of rooms, buildings, sites, vehicles and general security related to geographic location (such as potential for natural disaster or the general level of security in a foreign region).

There is a large volume of information in the public domain listing software and configuration vulnerabilities, references to their corresponding safeguards, and details of known exploits of those vulnerabilities. This information is spread among a large number of sources in a number of different formats, including mailing lists, web forums, blog-style websites, formatted vulnerability dictionaries, and vendor patch advisories. Some external sources of periodic vulnerability and exploit information include web resources and email lists, such as Common Vulnerability Exposures (CVE), Neohapsis, Secunia, Bugtraq and NTBugtraq, Full Disclosure, Packet Storm, K-otik, Zone-H, VulnWatch, and Computer Emergency Response Team Coordination Center (CERT/CC).

Enterprises may also have internal repositories of historical information, such as vulnerability tracking/ ticketing tools, or classified sources of vulnerability and exploit information.

Another external repository of vulnerability and threat information must contain physical environmental and kinetic vulnerabilities of IT assets, which may include a lack of access control to server rooms, absence of UPS, limited weather protection of equipment shelter, deployment in a geographic region at risk of kinetic attack, and so on. This data is formatted and pulled into the JNDMS in conjunction with military operations data.

The JNDMS uses data from vulnerability scanners, internal procedures and audits, and military operations imports to identify the relationships between known categorized vulnerabilities that exist within a specific CND environment, and the potential exploits or threats that relate to the involved IT assets.

5.1.12 Safeguard Data

Safeguard data outlines the safeguards available to an IT asset or a set of IT assets. Safeguards can be both physical safeguards and IT-based safeguards. Safeguard data is primarily extracted from CM databases derived from tools that are interfaced to JNDMS. It may also be possible to acquire safeguard data dynamically from devices through mechanisms, such as Host Vulnerability Scanners that harvest data on AV signature file versions, patches installed on systems, and other detailed configuration items.

Other safeguard information, such as IT Security policies, backup and restore procedures, detected password strengths, and security device configurations are uploaded in bulk into the JNDMS database by system operators.

Safeguards, which can be dynamically reconfigured or redeployed to change the defensive posture such as firewall rules, filtering routers, encryption rules, and Virtual Private Network (VPN) links and their access controls, should be captured into the JNDMS Data Warehouse.

Following insertion in the Data Warehouse, these safeguards then become itemized information about the defensive posture, which is useful when responding to an incident identified by the JNDMS.

5.2 Enterprise Infrastructure Management

The EIM component provides the required IT infrastructure information and events information into the JNDMS Data Warehouse (Figure 10). This allows for proper correlation of operational and IT infrastructure data in order to improve SA and to enhance information dissemination and visualization.

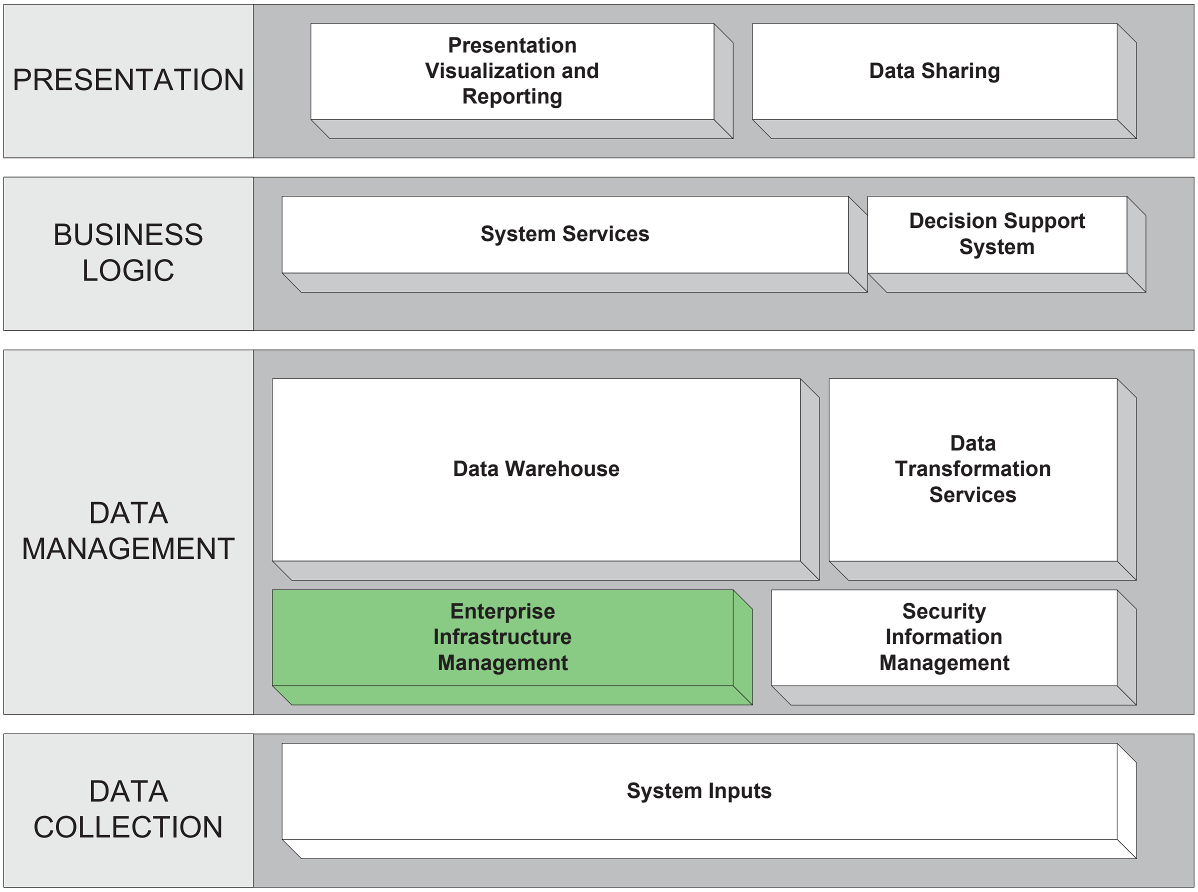

PRESENTATION
Presentation Visualization and Reporting
Data Sharing
BUSINESS LOGIC
System Services
Decision Support System
DATA MANAGEMENT
Data Warehouse
Data Transformation Services
Enterprise Infrastructure Management
Security Information Management
DATA COLLECTION
System Inputs

Figure 10: Enterprise Infrastructure Management

The EIM component accepts input from static and periodic sensors and provides data directly to the Data Transformation and Data Warehouse components. This component is created from COTS systems, such as the CA Unicenter suite of enterprise management tools, customized to support host management, discovery and vulnerability assessment.

5.2.1 Component Introduction

EIM is the process of managing all assets permanently connected or transient on a network. This is often a specially tailored monitoring console or Enterprise Information Portal. Enterprise management involves manipulating assets, allocations and capabilities to optimize a network.

The EIM component of the JNDMS discovers all devices on the network using data from the dynamic inputs and automatically adds them to the Data Warehouse as managed objects. Enhanced monitoring, through proper information gathering and dissemination in this component, increases informational awareness on critical IT infrastructure events and improves the JNDMS operational effectiveness and SA.

5.2.2 Component Technologies

Among the best-of-breed technologies that MDA has identified as candidates for this component in the JNDMS TD are Unicenter, Spectrum, and eHealth from CA, SMS/MOM from Microsoft, What’s Up Gold from Ipswitch and Assyst from Axios Systems. The immediate focus of the JNDMS TD is on the Unicenter, Spectrum and eHalth interfaces while keeping the other interfaces in mind for transition opportunities.

5.2.3 Component Description

EIM, for the purpose of the JNDMS TD, focuses on the discovery, configuration, performance, availability and security policies of IT devices. Monitoring will be extended to identify the relationships between devices. Defining a network topology aids in the understanding of how IT infrastructure affects the availability of IT services and applications. This information is critical to the success of the JNDMS. Figure 11 portrays how events generated by the dynamic input agents flow through the infrastructure.

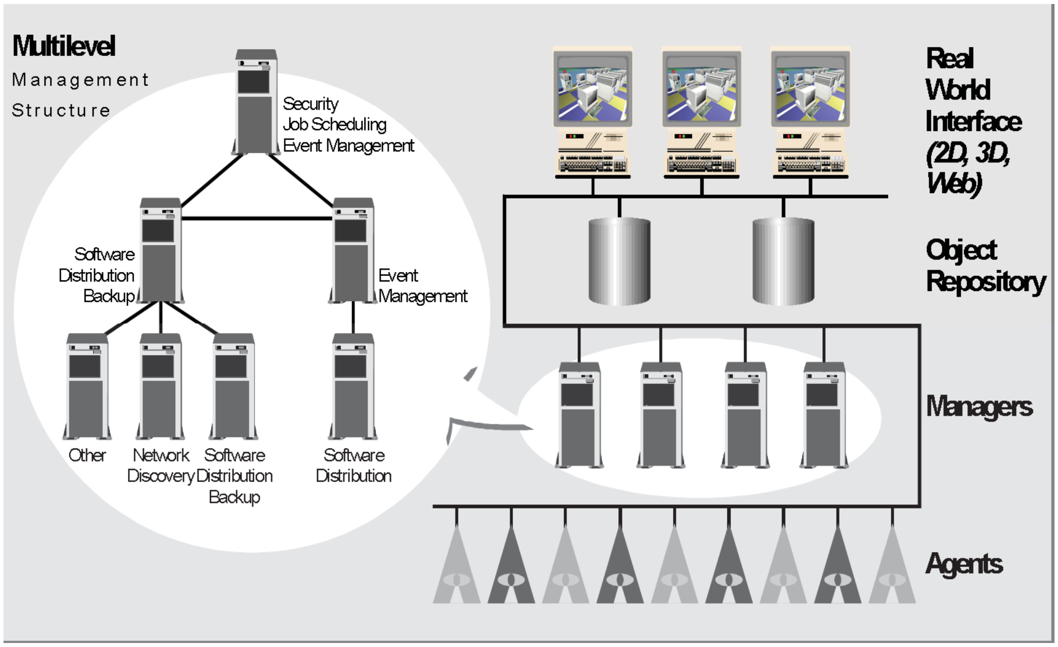


Figure 11: Enterprise Infrastructure Management Architecture

Each module in the EIM component has a management capability that resides on a management server with an agent residing on the managed server. Data and messages are exchanged between the manager and the agent. The manager then does event correlation and feeds the presentation layer.

The JNDMS relies on the set of inputs from the system inputs layer. In the JNDMS architecture, the Real World Interface will be the DSS and Presentation-level components, specific to the business processes of DND. Through the Presentation-level components, the EIM component will enable the JNDMS users to have an enhanced understanding of the current IT infrastructure situation and to have the ability to use historical data to develop a baseline against which future anomalies can be detected and managed on a proactive basis.

Beyond the stand-alone management of the enterprise infrastructure, the JNDMS will have the ability to assess new devices and their corresponding security vulnerabilities. Therefore, identifying where the assets are and how vulnerable a device is to malicious attacks is critical to any operation. The ability of the EIM to understand the network vulnerabilities and to manage them based on severity and potential risk levels will enable improved JNDMS operational efficiency.

5.2.4 Open Standards

An EIM strategy based on open-standards allows the JNDMS to leverage solutions currently deployed at DRDC and DND, such as CA's Unicenter Service Desk, CA's Unicenter Asset Management, Microsoft's MOM, and SMS. Additionally, these open standards will assist DRDC and the JNDMS project to incorporate new technologies as they become available.

EIM provides the required IT and security-based feeds into the JNDMS. This component provides:

- The configuration of IT network baselines and the ability to correlate information against those baselines
- An increased understanding of network vulnerability risks
- An improved definition of the current network topology
- The ability to centralize that data as input to the Translation component

5.3 Security Information Management

The SIM component processes data inputs from the CND environment. From this data stream, significant security events and other events of special interest are injected into the JNDMS TD Data Warehouse (Figure 12). In order to achieve this, the information security data must be efficiently acquired, normalized, correlated and stored in a secure Data Warehouse for future forensic analysis.

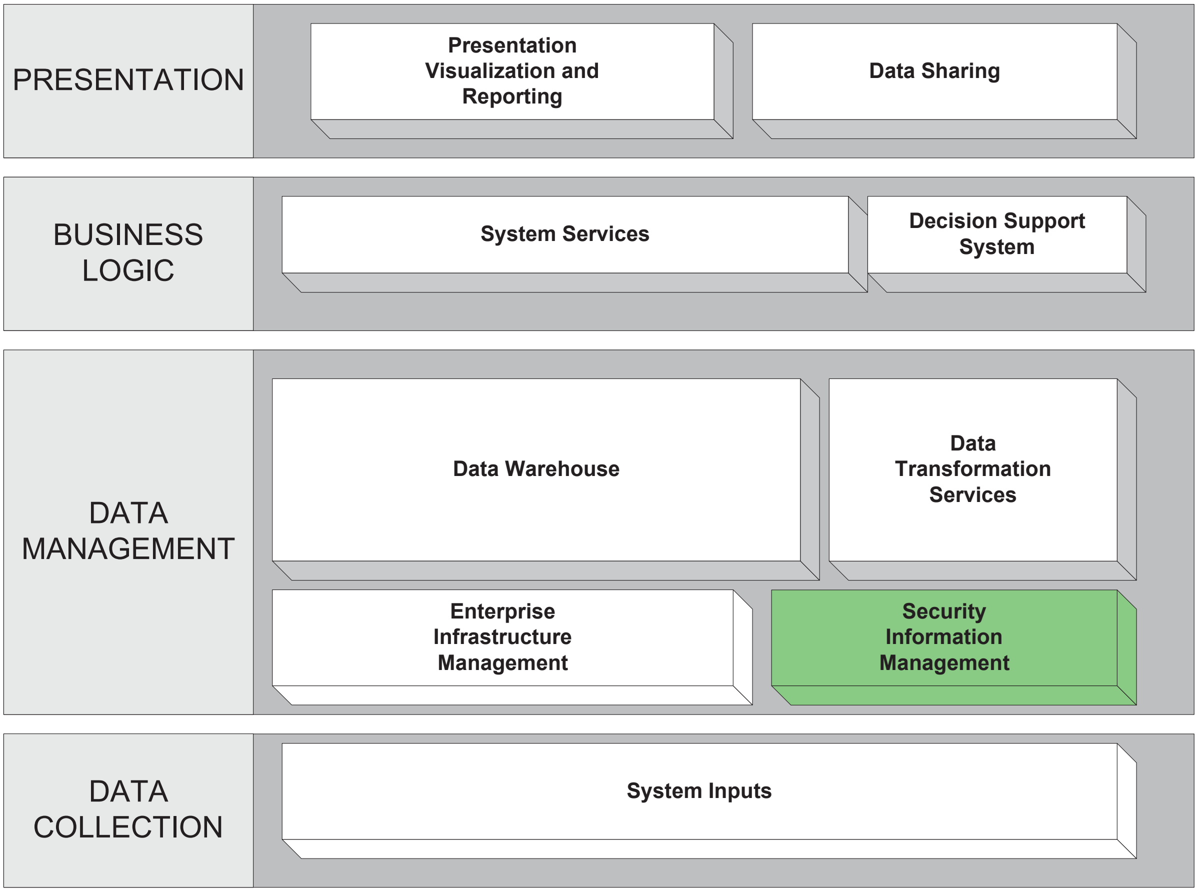

PRESENTATION
Presentation Visualization and Reporting
Data Sharing
BUSINESS LOGIC
System Services
Decision Support System
DATA MANAGEMENT
Data Warehouse
Data Transformation Services
Enterprise Infrastructure Management
Security Information Management
DATA COLLECTION
System Inputs

Figure 12: Security Information Management

The SIM component accepts input from dynamic inputs and provides data directly to the Data Transformation and Data Warehouse components. The SIM component is created from COTS security management systems.

5.3.1 Component Introduction

The SIM component recognizes security events from the stream of data in the CND system inputs layer and make them available to the DSS through the Data Warehouse in the JNDMS to allow for quick reporting and reaction.

5.3.2 Component Technologies

Among the best-of-breed technologies that MDA has identified as candidates for this component in the JNDMS TD is Intellitactics' ISM, which can be configured for operations on the DRDC Lab network.

5.3.3 Component Description

SIM solutions enable security teams to rapidly and comprehensively identify information security incidents, to deploy resources on the threats that pose the greatest risk to the business, to assess and resolve these incidents with the strongest security team productivity and capability, and to affordably scale security coverage enterprise-wide.

Capabilities or features of the SIM component in the JNDMS TD include:

- Acquire security event data, such as logs, alerts, system events and formatted reports, from various sources
- Pre-process and store security event data
- Filter, aggregate, de-conflict, and consolidate security events
- Normalize security event data to a common, complete and consistent format
- Acquire and correlate vulnerability data with security events
- Prioritize individual security events on a normalized severity scale, including supporting evidence of severity assessment
- Summarize the severity of the overall security situation, of ongoing events, and of multiple-simultaneous events including supporting evidence of severity assessment
- Assess the effect of security events on the CND environment

Criteria for selection of a COTS product for the SIM component include the ability to achieve the previously mentioned capabilities, plus the following:

- Preference for a Common-Criteria certified solution
- Aversion to the need for active host-based agents
- A mechanism to validate data integrity as part of a JNDMS data repository
- Interoperability with the existing DND SIM implementations (Intellitactics' ISM). Notably, the DND Computer Incident Response Team (CIRT) has a large investment in their deployed ISM infrastructure, which has been in production for several years, and has a great deal of customization specific to the needs of the Canadian Forces Network Operations Centre (CFNOC).

5.3.4 Detection of Host-Based Intrusion Using the SIM

The SIM component includes host-based intrusion detection. Host-based intrusion involves scanning assets for changes to the software, firmware and policies on a system. Once change is detected, host-based intrusion systems often attempt to take remedial action by applying change to the hosts in an effort to restore system integrity or block potential viral propagation to other systems.

Functionalities of host-based intrusion detection systems include:

- Capture security events data and provide SA from all relevant information domains
- Acquire security events data, such as logs, alerts, system events and formatted reports, from various sources
- Pre-process and store security events data
- Filter data, aggregate data, de-conflict data, consolidate data
- Normalize to a common, complete and consistent format
- Acquire vulnerability data from various sources

5.4 Data Transformation

In the JNDMS, large amounts of data are collected from many different sources. In order to make sense of the data within the business logic, the data must be transformed into a common data model and aggregated into the database (Figure 13). This provides an unambiguous and neutral view of the data. The absence of ambiguity enables the data to be properly interpreted by business processes. Neutrality allows the data to be transformable into both user views and persistent storage views.

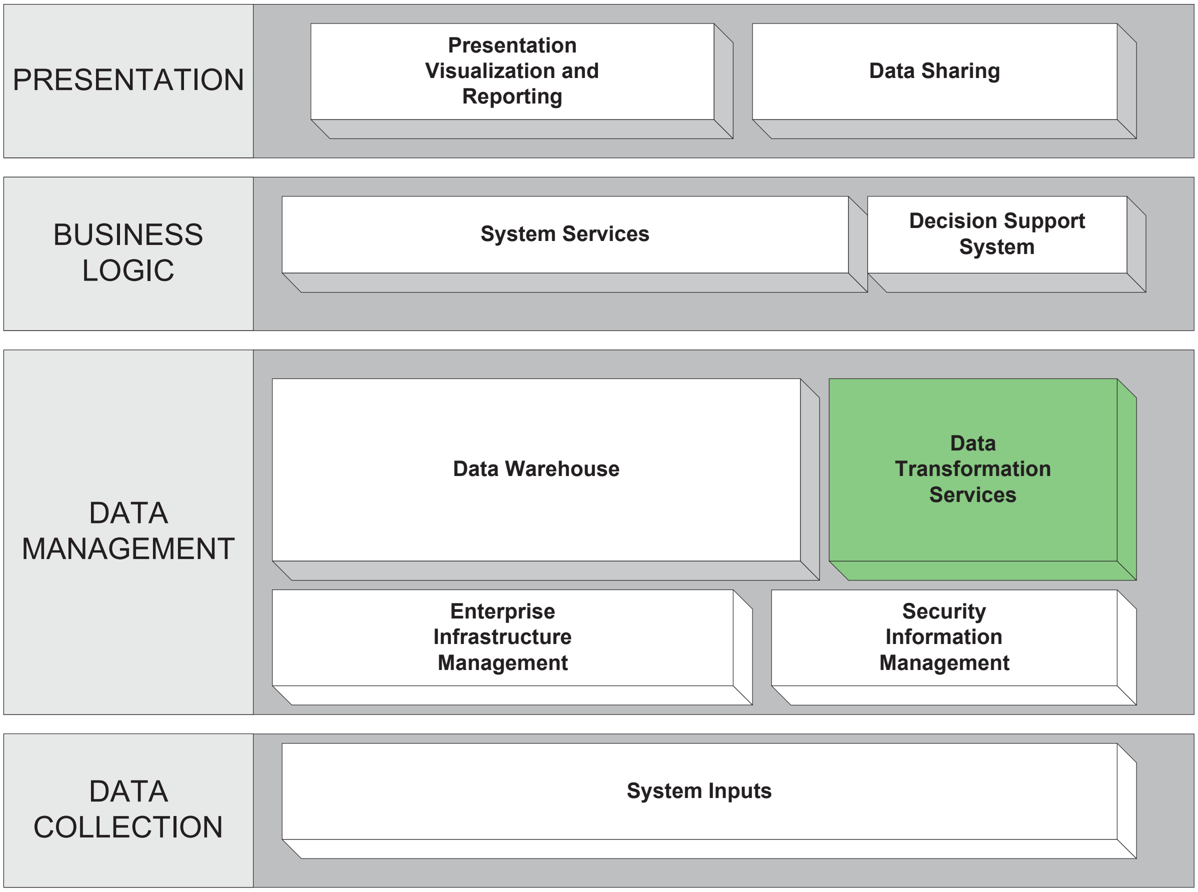

PRESENTATION
Presentation Visualization and Reporting
Data Sharing
BUSINESS LOGIC
System Services
Decision Support System
DATA MANAGEMENT
Data Warehouse
Data Transformation Services
Enterprise Infrastructure Management
Security Information Management
DATA COLLECTION
System Inputs

Figure 13: Data Modelling, Transformation and Fusion

The Transformation Services component provides support for other components to manage data transformational functions. This component is created from a mixture of COTS data transformation engines along with custom interface code in the case that non-standard inputs are being provided.

5.4.1 Component Introduction

Data transformation is critical for enabling the business logic to function efficiently. All of data inputs from the numerous sources in the Data Collection components are transformed into a common data model, aggregated, de-conflicted and fused into a common data repository within the data warehouse.

This component, within JNDMS, provides services that other components can call on to provide transformation functionality. All data flows are not routed through this component; however, a common set of tools are available for transformation purposes.

5.4.2 Component Technologies

Among the best-of-breed technologies that MDA has identified as candidates for this component in the JNDMS TD are Advantage (for real-time ETL) from CA, Enterprise Architect (for data modelling transformations) from Sparx Systems, iBATIS from Apache, and Oracle for the data repository and its related services.

Another part of these services includes language support for XML transformations, through XLST. XML is used to define JNDMS specific interfaces and, because XML is used widely, transformation can be applied directly to the output of some COTS.

Each potentential data source for JNDMS has it's own interface and enforce it's own constraints on JNDMS. One common interface technology that is often used by tools, especially thoses generating events or alarms, is the command line interface (CLI). This interface is supported as part of the data transformation services to translate CLI calls into JNDMS specific interfaces.

5.4.3 Component Description

A data model is a collection of descriptions of data structures and descriptions of operations or functions that manipulate the data. A data model is a graphical and/or textual representation of data objects and relationships. Throughout the JNDMS TD phases, the MDA team will define and refine the data model for all the information that the JNDMS will acquire, manage and query, and produce.

Open standards for data descriptions are utilized where possible to describe the data. One challenge we face is that there are a plethora of standards available to do this. Parts of the initial investigations involve the identification of which of the standards best suits each data description. For example, to represent the interrelationships between networked systems, possible methods could include Web-Based Enterprise Management (WBEM), CIM-XML, Unified Modelling Language (UML) or network diagrams, among many others. Part of the initial phase involves identifying which description technique is best suited for this task. One way to divorce the data and their relationships from the description system is to utilize a data model containing all available information about the data.

5.4.4 Data Transformation

Data transformation engines are used to transform data into the normalized data model. These transformation engines are sensitive to data types, source platform, word sizes and data relationships.

A view of common data transformation flows within JNSMS is shown in Figure 14. This identifies that the data transformation services are spread over several physical components and will be leveraged to support the required data sources.

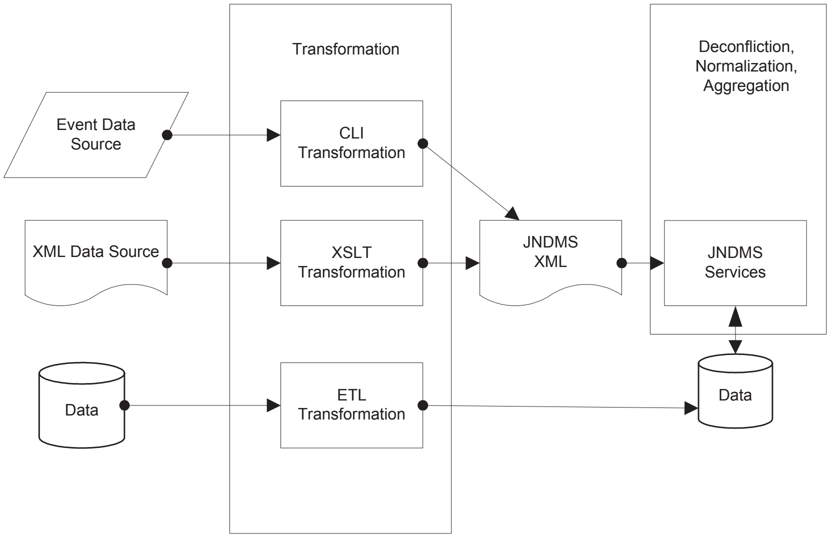


Figure 14: Data transformation in JNDMS.

5.4.5 Transformed Data as the 'Knowledge Base' in the Data Warehouse

Data that is transformed and (i.e., aggregated) form part of the Knowledge Base in the Data Warehouse. This part of the Knowledge Base contains information acquired by external sources that conforms to the JNDMS Data Model. It is important to note that "knowledge", as used by the DSS, may draw from many sources. This knowledge base of transformed data contains static and time sensitive information from both vendor-supplied and environmental sources. Within the JNDMS, this information must conform to the data mode after it has been transformed. The DSS makes extensive use of the Knowledge Base contents.

Knowledge includes static and time sensitive information, such as:

- NIDS signature databases
- CVE information
- Asset IP address allocation data
- Vulnerabilities and exploits
- VA scan results
- Exploit data
- Military operations data
- Safeguard data

- Concept of Operations (CONOPS) documents
- Incident handling procedures
- Network diagrams
- Infrastructure data
- Contact information for key IT resources

5.4.6 Extract, Transform and Load

The Data Transformation component is able to augment the scope of the Data Warehouse adoption of an ETL tool for collecting source data from interim data repositories in lower-level components. This allows for faster analytical processing and decision-making.

5.4.7 Overview of Potential Technologies

One of the more popular data modelling tools, ERWIN, is produced by CA and can be used to describe the data. ERWIN allows the data model to be implemented in different databases. Other tools, such as Enterprise Architect (EA), utilize UML descriptions to accomplish similar objectives. The JNDMS RFP contains a requirement for UML descriptions of the data model, which can be supplied by EA, but the project team is fully capable of transcribing the data model into the multiple Computer Aided Software Engineering (CASE) systems.

Tools are available that can forward and reverse engineer both data model and data contents directly from external data storage. For example, Advantage Data Transformer (ADT), shown in Figure 15, extracts data from source systems, cleanses and transforms the data, then moves the data into a data warehouse, data mart or Operational Data Store (ODS) for decision support processes. It creates graphical mappings of transformations and workflows, and then implements these transformations using a movement server to support large volumes of data movement and transformations. It supports very granular transformations, aggregation and data cleansing algorithms. This capability will be very useful when importing information from existing data sources.

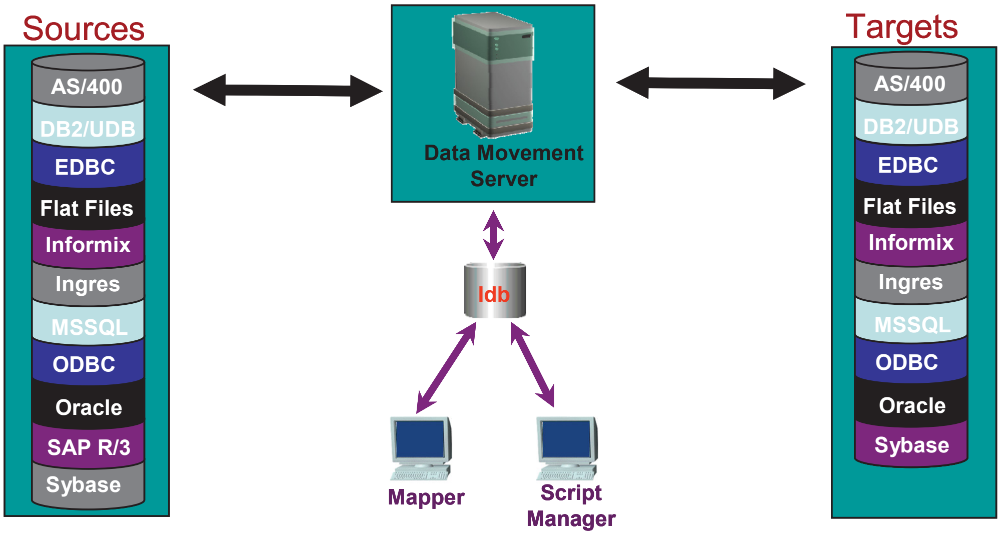


Figure 15: Data Transformer

The data transformer is responsible for extracting data and schemas from one data source and using it to populate another data source. In this example, CA's data transformer product describes the data reductions, correlations, filters or other operations that can be run against the data while it is being transformed.

Once the data has been normalized and filtered, the data will be written to the JNDMS Data Warehouse for storage and subsequent analysis. There are several database systems that can be used as the Data Warehouse, but it is recommended that the chosen database system should have good support for data types, data methods, transactional integrity, security, scalability and replication capabilities. The database system initially identified by MDA for the JNDMS is Oracle, but applications such as ERWIN and ADT can translate this into other databases as required.

5.5 Data Warehousing

A Data Warehouse is a repository of information accumulated from a variety of sources. Prior to being stored in the JNDMS Data Warehouse, this multi-source data is transformed then aggregated so that data from different sources gets stored in a single repository, such as a database table within the Data Warehouse (Figure 16). Follow-on components in the JNDMS architecture, such as the DSS, continually scans this Data Warehouse and attempts to derive patterns, knowledge or alerts regarding the health of the network.

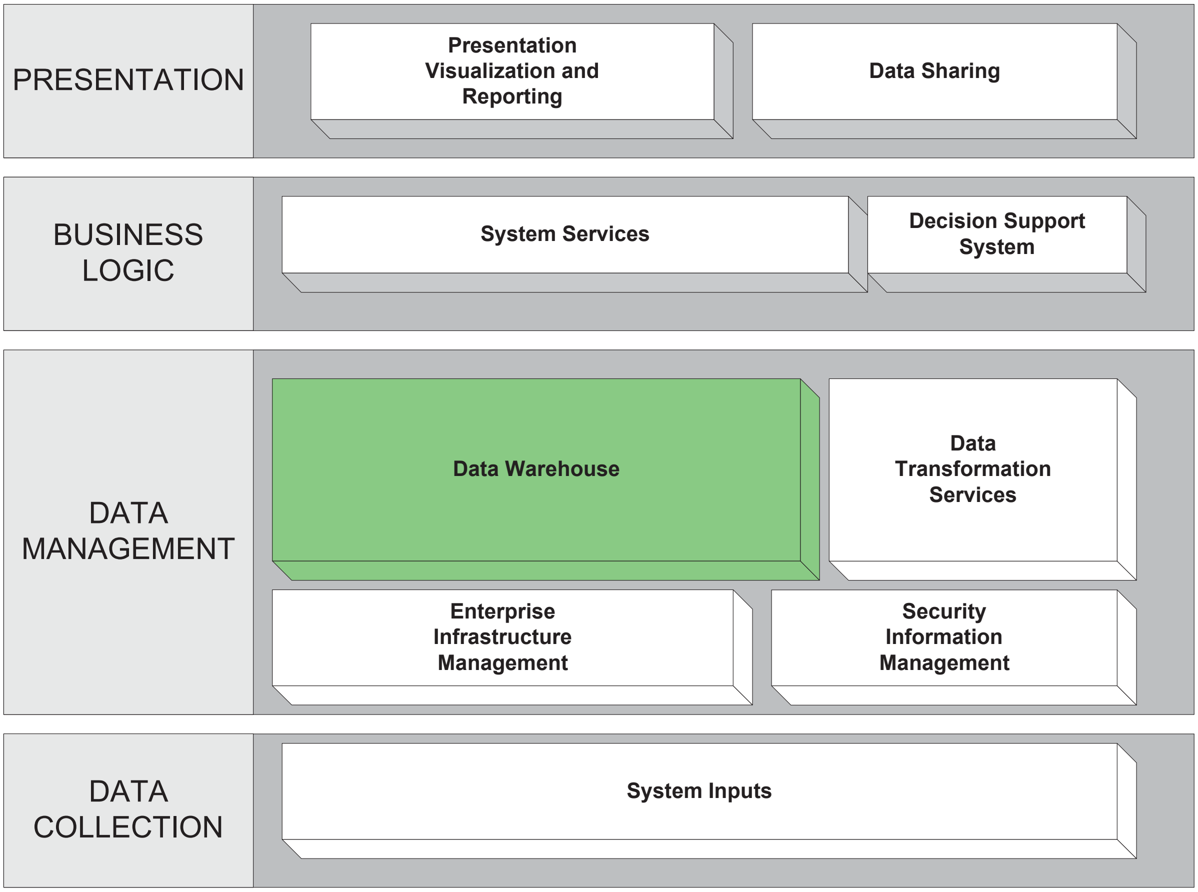

PRESENTATION
Presentation Visualization and Reporting
Data Sharing
BUSINESS LOGIC
System Services
Decision Support System
DATA MANAGEMENT
Data Warehouse
Data Transformation Services
Enterprise Infrastructure Management
Security Information Management
DATA COLLECTION
System Inputs

Figure 16: Data Warehousing

The Data Warehousing component accepts coherent data primarily from the System Services component and stores it for further analysis by the DSS component and further use by the Presentation-level components. The Data Warehousing component is a commercial database which instantiates the data model, configured to support fault tolerance. This component is responsible for enforcing data integrity through transaction management, backups and replication.

5.5.1 Component Introduction

Data retrieval, from a JNDMS perspective, is a three-step process consisting of data collection, data transformation and data storage. The Data Warehouse is the third step in this process, which consists of a data store of large volumes of multi-sources data.

The Data Warehouse component for the JNDMS allows the system to store and manage all data from multiple sources, including:

- CND dynamic inputs
- EIM systems
- Security management systems

The Data Warehouse component accumulates, manages, retrieves and replicates data as required for the JNDMS. This flexibility provides data consistency and rapid data retrieval performance. Flexibility is added with the ability to add additional data sources through the ETL tool as part of the Data Transformation component.

5.5.2 Component Technologies

Among the best-of-breed technologies that MDA has identified as candidates for this component in the JNDMS, the leading technology is Oracle Enterprise Server. Oracle is an industry leader in database management systems. Their databases have built-in features for integrity checking, backups and replication. Oracle databases are currently deployed throughout the CF and IT support personnel are abundant.

5.5.3 Component Description

Definition of a data model is a key aspect of the Data Warehouse component. The data warehouse component must define normalized data and defines the performance and efficiency of the services deployed in the Data Warehouse. Therefore, data management and data retrieval objectives must be considered in the development of the data model.

The data warehouse component is enhanced through the adoption of an entity relationship data modeling tool to analyze data from input sources and to forward engineer the warehouse, as represented in Figure 17. Once the Data Warehouse model is defined and instantiated, then the incoming data from operational applications is transformed and moved into the Data Warehouse environment, thus allowing the data to be leveraged as information. The Data Warehouse is augmented by collecting source data from interim data repositories from lower-level components. This allows for faster analytical processing and decision-making. The transformed data is stored within the warehouse database and is available for further analysis.

The JNDMS data warehouse uses a COTS RDBMS that has the ability to facilitate data integrity, security and automated data backups, which could be used for duplication management. Our recommendation for an enterprise RDBMS is Oracle. The Oracle database products are well known to both DRDC and DND and are able to exceed the transaction and storage performance requirements of feeder systems, such as the previously discussed SIM and EIM software.

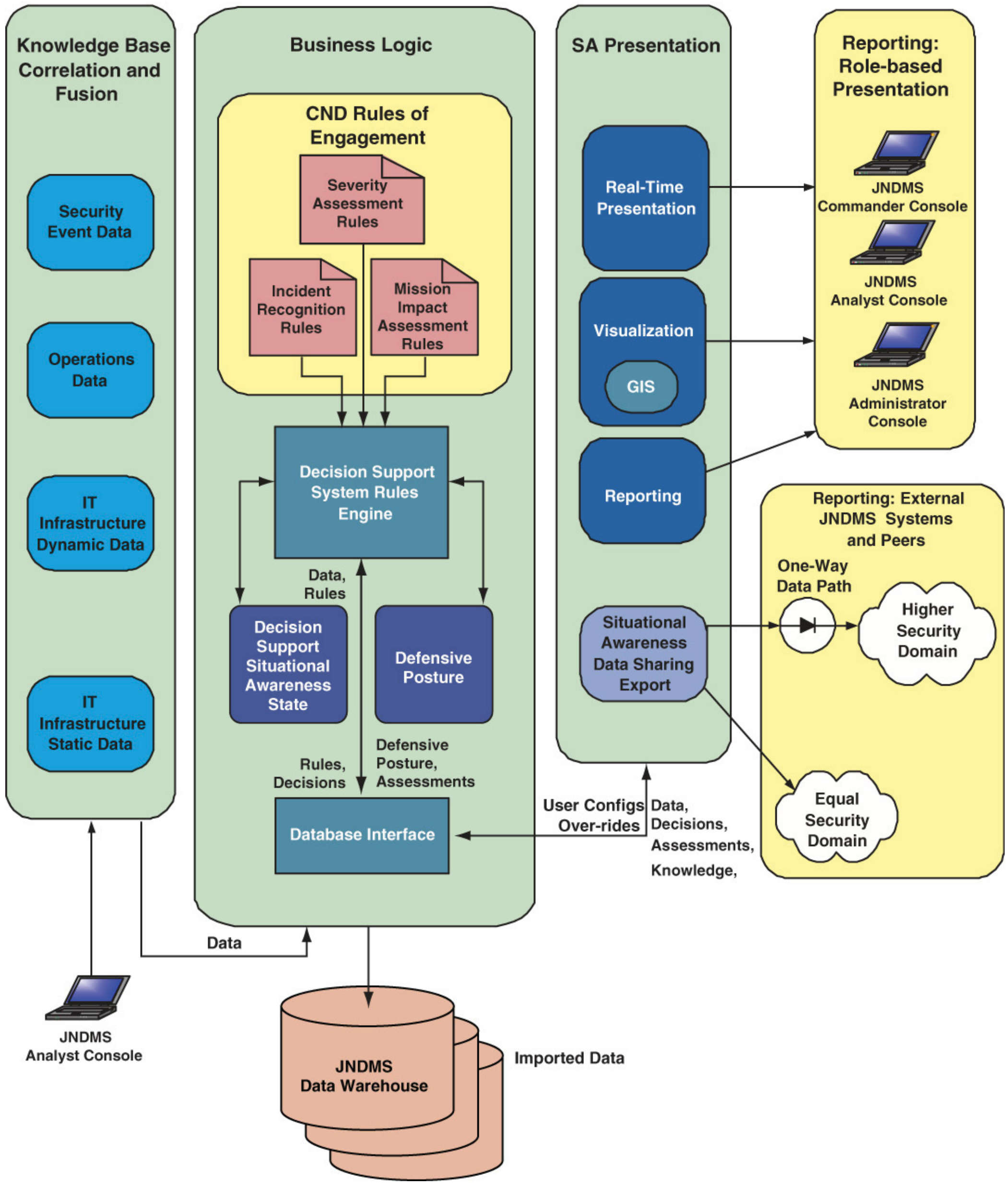

Knowledge Base Correlation and Fusion
Security Event Data
Operations Data
IT Infrastructure Dynamic Data
IT Infrastructure Static Data
Business Logic
CND Rules of Engagement
Severity Assessment Rules
Incident Recognition Rules
Mission Impact Assessment Rules
Decision Support System Rules Engine
Data, Rules
Decision Support Situational Awareness State
Defensive Posture
Rules, Decisions
Defensive Posture, Assessments
Database Interface
SA Presentation
Real-Time Presentation
Visualization
GIS
Reporting
Situational Awareness Data Sharing Export
Reporting: Role-based Presentation
JNDMS Commander Console
JNDMS Analyst Console
JNDMS Administrator Console
Reporting: External JNDMS Systems and Peers
One-Way Data Path
Higher Security Domain
Equal Security Domain
User Configs Over-rides
Data, Decisions, Assessments, Knowledge,
Data
JNDMS Analyst Console
JNDMS Data Warehouse
Imported Data

Figure 17: JNDMS Data Warehouse

5.5.4 Data Replication

The JNDMS Data Warehouse requires an advanced replication capability. Replicating data as a backup not only protects JNDMS data contained within the warehouse, but also protects the investment of time and resources required to create and structure the data contained within that warehouse. Retaining historical versions of the data also help the JNDMS to recover from errors, to facilitate traceability of information if required, and to protect the information if disaster recovery is required. The replication components of the data warehouse enable the JNDMS to define backup policies by specifying critical data.

The detailed requirements for full and partial data replication with peer systems is identified in Phase 1, but many of these requirements, including the development and maintenance of peer systems profiles and policies, may be satisfied by the built-in capabilities and advanced replication features of the recommended Oracle Enterprise RDBMS. The development of these peer system profiles and policies define the access controls and mechanisms required for the JNDMS to exchange with peer systems.

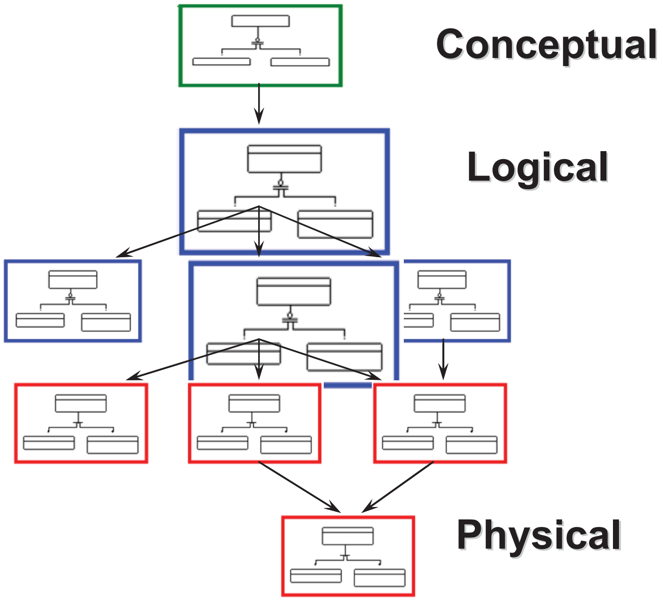


Figure 18: Designing the Data Warehouse from an Entity-Relationship Data Model

An entity-relationship data modeling solution (as shown in Figure 18) supports the building of comprehensive, robust data structures within the Date Warehouse. The design layer architecture allows an organization to create data architectures that support the organization's processes by aligning the models, from the conceptual level to the physical implementation. The JNDMS Data Warehouse model can be created using an entity-relationship data modeling solution at the conceptual level, i.e., identify the conceptual model artefacts and high-level subject areas. This conceptual model can then be used as a basis to design the logical data structures. As required, logical sub-models are derived from the overarching model that include the appropriate logical model objects, but incorporate more detail as required from the various modules.

Finally, the physical data models and associated database structures are created and deployed. Design layer architecture supports model synchronization as models and requirements change with time.

5.5.5 Data

Data that is stored in the Data Warehouse includes the following:

- IT Infrastructure and Services Data
- Military Operations Data
- Security Events Data
- DSS Rules
- Incident Data, DSS Assessments and Defensive Posture Conclusions
- Profiles for Policies for Data Sharing (import and export) with Peers
- Imported Datasets from External Peers
- Maintain Accurate References to the Sources of Data
- Linkage Information to External Data Sources, which may hold accessible information that is relevant to the JNDMS
- Interrelationships
- Metadata for all of the above

5.5.6 Security

The Data Warehouse incorporates a number of security features to ensure the confidentiality, integrity, and availability of the data.

Access control of data will be implemented using combinations of the following strategies:

- Partitioning secure data from non-secure data, or sensitive data from non-sensitive data. This allows access control at the systems level.
- Implementing user-level access control within the database management system.
- Implementing user-level access control within the middleware for the portal application.
- Use of "peer systems profiles" to dictate what data views are synchronized to which JNDMS peers; for example one profile for a CF to CF synchronization, and another for a CF to North Atlantic Treaty Organization (NATO) synchronization.

Encryption is used as appropriate using standards based mechanisms:

- Encapsulation of JDBC/ ODBC calls over the network using SSL or Secure Internet Profile (IPSEC) tunnelling.
- Appropriate use of on-disk encryption using encrypting file systems where host Threat Risk Assessment dictates.

Integrity checking mechanisms are built into the underlying relational database management technology and additional mechanisms, such as inclusion of calculated message digests on input files, can be included in the data schema as well.

Backup and recovery mechanisms that exist within the database technology are leveraged both technically and through CONOPS documentation, including how and when to use full or partial restores.

Additional security can be managed through full database encryption through the use of Oracle 11g.

5.5.7 The Flow of Incoming Data

Operations security events and IT data flows from the input sources into the database using the following mechanisms:

Security Events Data are captured into the database with these inputs:

- Security Advisories
- Alerts and Admin Notes
- Network Forecasted Events
- Intelligence Data
- Network Devices, Logs and Alerts
- Security Devices, Logs and Alerts
- Shared Network Incident Information

Military Operations Data are captured into the database with these inputs:

- Operations Name
- Operation Locations
- Operations IT Assets
- Operation IT Asset Policy
- Operation Priority
- Operation Activity Schedule

IT Data is captured into the database with these inputs:

- IT Data:
    - Bandwidth Usage
    - Device Identification
    - Routing Tables
    - Active Ports
    - OS Version
    - Patch Level
    - Software Versions
    - Anti-Virus Software Status
    - User Rights and Privileges
    - Services

- IP Addresses
- MAC Addresses
- Subnet Network
- Enabled Protocols
- Networking Configuration
- Defensive Posture Architecture
- Network Classification
- Transport Layer Architecture
- Network Architecture and Configuration
- Network Asset Locations
- MIB Data
- System/Application Configuration Data
- Vulnerability Assessment Data
- Safeguard Assessment Data
- Exploit Assessment Data
- Threat and Assessment Data
- Military Operation Locations
- Military Operations IT Assets
- Military Operation IT Asset Policy
- Military Operation Priority
- Military Operation Activity Schedule

5.5.8 Queries

The Data Warehouse supports queries against any metadata or data attribute. Complex queries can combine different attributes or different types of data entities in attempting to identify relationships between different types of inputs. Data may be queried by any combination of timestamp, time range, geographic location, geographic region of interest, network name, security classification, security event type, security event severity, input type, input source, among many other different queryable attributes.

Temporal database features are supported in the JNDMS. Timestamps showing time of creation and reception of the data are saved where available. Preservation of the timestamp information allows temporal queries and analysis. The JNDMS data model is designed to prevent the duplication and loss of records having conflicting timestamps.

5.6 System Services

The System Services provide the core data flow and application logic for the business layer within JNDMS. Figure 19 shows this component within the JNDMS architecture layers.

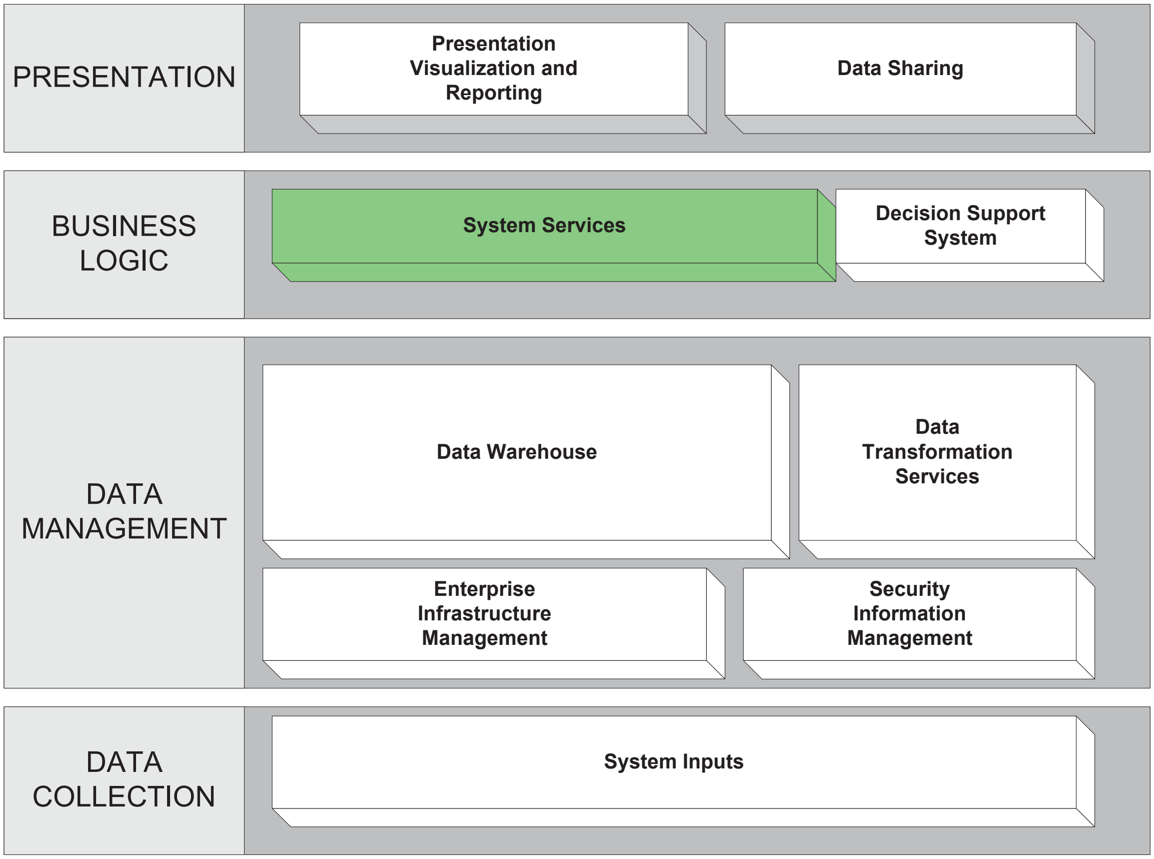

PRESENTATION
Presentation Visualization and Reporting
Data Sharing
BUSINESS LOGIC
System Services
Decision Support System
DATA MANAGEMENT
Data Warehouse
Data Transformation Services
Enterprise Infrastructure Management
Security Information Management
DATA COLLECTION
System Inputs

Figure 19: System Services Component

This component provides the primary interface to data being inserted into the data warehouse and for queries of the JNDMS. This component is a custom application built on an applications server. The interface to this component is defined in XML to be provided as a Web Service to other components.

This component makes use of the Data Transformation Services and is able to apply consistency checks on input data and may also provide some transformational capabilities as well.

This component also interacts with the DSS to supplement the rule based decisions with additional business level logic.

5.6.1 Managing Interfaces

It is not enough to define internal or external interfaces between system components. Given the range of products from different vendors that will supply data to the JNDMS, and the variety of data sources being used, it is desirable to invest in a common data description method. The data model associated with this data description method can contain normalized data structure descriptions from this variety of sources, together with their fields' descriptions, and descriptions of associated operations and functions. Identifying the data model provides a blueprint of information about the data, without tying the description to a particular technology or vendor. The data model is not a physical implementation, but can be applied equally well to different technologies, such as relational databases or distributed objects. Data models usually take a diagrammatic form and often the tool used to construct the forms can apply the data model to a variety of data storage systems.

The system services component defines the interfaces to the data model that other components adhere to. This allows the interfaces to those tools to be defined in a manner logical to those tools, and not in the format of the data model.

5.6.2 Data Modelling and Transformation Techniques and Concepts

A primary requirement that is fulfilled by the JNDMS TD is to handle the proper association to source and context within the JNDMS data model. If source information is not contained within the actual data, fields will be added. In the case of summary information, links will be inserted to point back to the original source of the data, and in some cases to the offset or locations where the source data can be found. The result is a hierarchical distributed JNDMS where time-critical rolled up information propagates to the Business Logic components quickly, and where less time-critical detailed information propagates more slowly (with the options of archiving low-level details on the external systems).

5.6.3 Data Pre-processing

Consistency of data is to be established before attempting normalization of the data. Conflicting data can be identified and resolved. Data can also be filtered so that irrelevant information can be omitted from the aggregated data.

The data is appended with metadata, including the source data source (network, host, etc.), security classification of the data source, a unique identifier, a timestamp from a timeserver, and any context information associated with the data. The benefit of having a unique identifier in the metadata is that data that having identical timestamps may be received and stored. De-conflicting services may later resolve duplicate entries while still allowing genuine storage of records with identical timestamps.

5.6.4 Normalized Data Models

Applications exist that can be used to model and transform data from external sources into the common format for JNDMS. Making sure that all data arrives in a normalized fashion may require transformations of data, including:

- Units - position in degrees, minutes, seconds to decimal degrees
- Types - integer values to floating point
- Precision - 2 digit precision to 10 digit precision
- Nomenclature - tags or field names may require transformation according to standards

Once a consistent data dictionary has been created, relationships between the data are be defined. As is typical with most data description exercises, it is expected that normalized relationships may need to be balanced against performance requirements to suit the target architecture.

5.7 Decision Support System

The DSS identifies security threats and events, and assigns the appropriate level of severity assessment to them (Figure 20). A DSS uses a pre-defined rule-set to effect processing of events from various sources and to arrive at a conclusion or decision. A DSS alleviates the need to modify software to alter the system's decision making process. Instead, a DSS allows the system behaviour to be altered by modifying higher-level business rules.

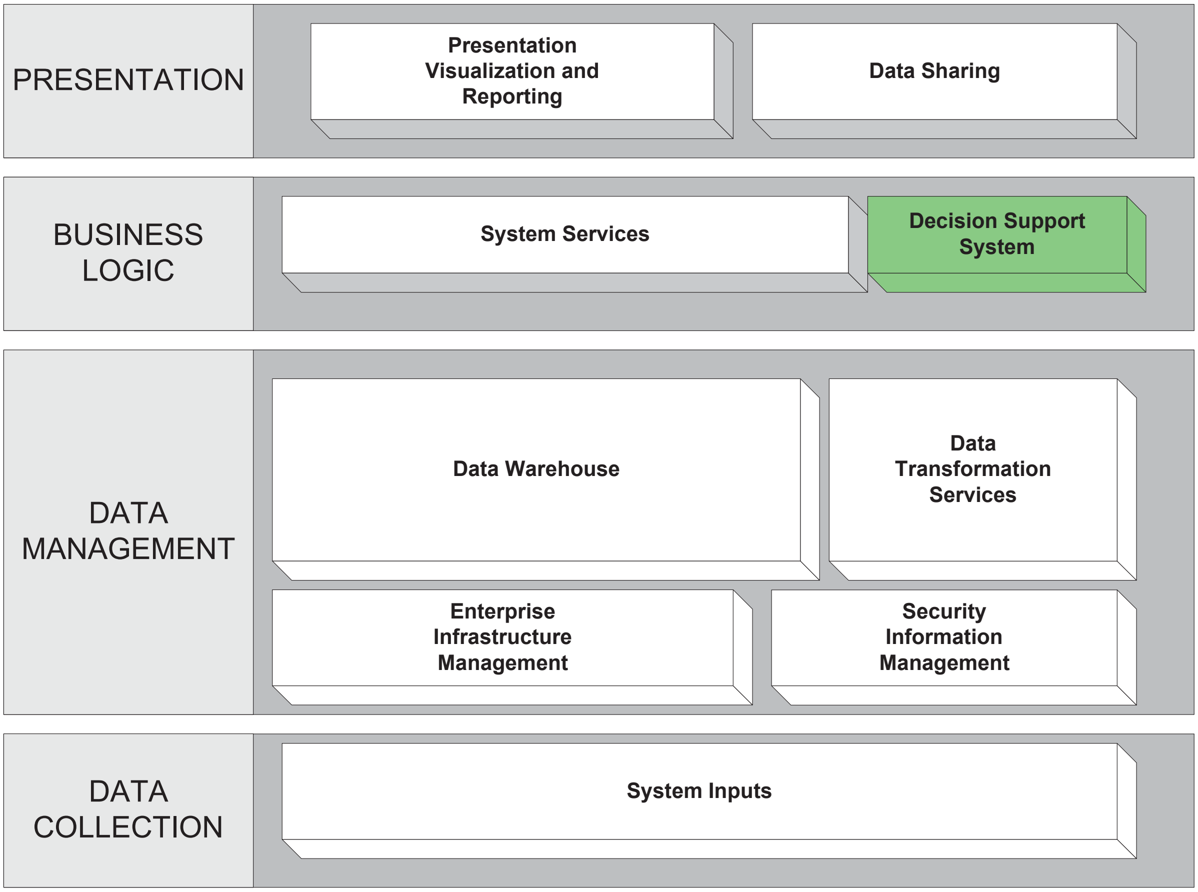

PRESENTATION
Presentation Visualization and Reporting
Data Sharing
BUSINESS LOGIC
System Services
Decision Support System
DATA MANAGEMENT
Data Warehouse
Data Transformation Services
Enterprise Infrastructure Management
Security Information Management
DATA COLLECTION
System Inputs

Figure 20: Decision Support System

The DSS component uses inputs from the Data Warehouse and System Services and applies rules to the content. This component is created from a COTS rules engine. The rules will operate on combinations of current and historical data. This component is also responsible for acting as the interface between the database and the Presentation components.

5.7.1 Component Introduction

Based on a set of business rules, implemented as DSS rules, the DSS generates severity values that provide a measure by which operators can use to prioritise responses to network incidents. These measures are the key to the JNDMS - intrusions and security threat events will be accurately recognized by the DSS and reported on with a timeliness and level of severity assessment that is commensurate to the severity of the detected intrusion or threat. The results of this incident and events calculations will be stored in the Data Warehouse.

5.7.2 Component Technologies

Among the best-of-breed technologies that MDA has identified as candidates for this component in the JNDMS TD, the leading technologies are AION from CA and JRules from Institute of Logistics (ILOG). The rules engine is augmented by the Java programming language to ensure maximum flexibility and ease of integration.

5.7.3 Component Description

The purpose of the JNDMS DSS is to fuse information from the five SAs for CND domains (operations, infrastructure, vulnerability, safeguards, events). The DSS provides recognition and correlation for incidents that affect the network IT infrastructure. The DSS of the JNDMS recognizes incidents that may adversely affect the IT infrastructure. It assesses the damage associated with incidents, and it determines the operational risk for future potential damage associated with incidents. These severity assessments are based on functions of time and incident severity. As there will continually be data coming into the Data Warehouse, the DSS continually updates its severity assessment. Each severity assessment is time stamped and stored in the Data Warehouse. The collection of detected incidents provides overall situational awareness. MDA proposes the use of a commercial BRMS to implement the DSS for the JNDMS. A BRMS includes the necessary tools to model, create, compile, debug, deploy and maintain business rules. These tools are typically graphical in nature to facilitate these tasks.

Types of damage that may be associated with an incident include denial of service, theft of information (confidential or otherwise), loss of data (confidential or otherwise), or loss of integrity (of a network, system, a service on a system or data).

As shown in Figure 21, the JNDMS DSS consumes all data that is collected in the Data Warehouse and make decisions about security assessments, events and the overall defensive posture. These assessments, along with the original rules are all stored in the Data Warehouse.

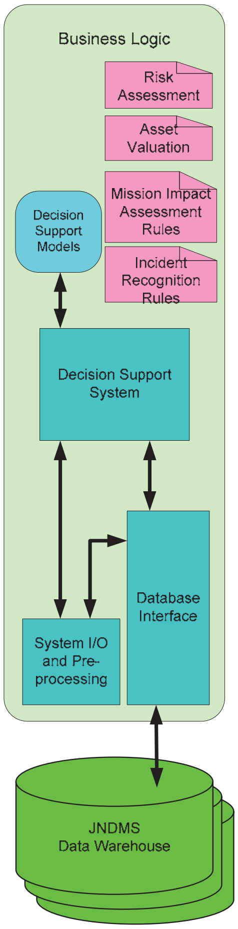


Figure 21: The JNDMS DSS

It should be noted that the Data Warehouse contains DSS knowledge and continually-updated, time stamped severity assessments and incident data generated by the DSS. These are explicitly presented to users via real-time presentation services, or to external systems or higher classification domains via information sharing. It also contains knowledge and rolled-up conclusions that are useful for forecasting, trend analysis, auditing, and reporting, but which have not been explicitly presented to users in real-time. This repository is “append only” in nature and rely on the underlying Data Warehouse technology. The Data Warehouse is also used as the source of the data upon which the decisions are made.

As this data is rolled-up, it is tagged to the original severity assessments and event data as evidence for forensic analysis, security audits, and general reporting.

5.7.4 DSS Rules

A business-rule language describes the grammar for the specific knowledge domain while a business - level model describes the vocabulary. Different rule-sets are required for incident recognition, severity assessment, risk assessment and mission impact assessment. The rule engine employs inferences to emulate the human capability to arrive at a conclusion by reasoning. The rule engine locates the appropriate rule, based on a new event or information, and executes it.

As shown in Figure 22, a person who has the role of Rule Administrator manages the DSS rules. These rules draw from the many data types and attributes available in the Data Warehouse and generate conclusions based on threshold of combined data and heuristic knowledge.

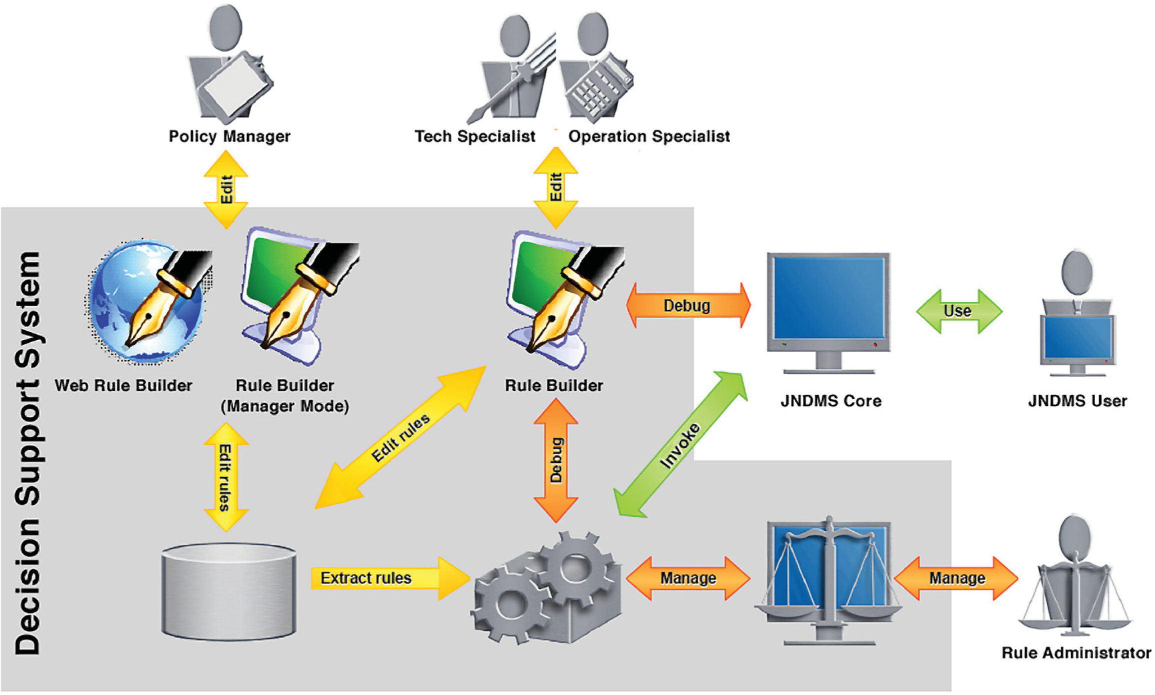


Figure 22: A Typical DSS Architecture

The successful integration of a DSS into an application, such as the JNDMS, requires the participation of different people with different skills: a software developer, a business or system analyst, and a policy manager. The BRMS separates the critical business rules from the source code, thus providing the ability to alter the application behaviour through user-modifiable rules. Database bindings (ODBC, JDBC) allow access to persistent objects, not just memory based objects.

The use of rules often require large data sets or extended periods of training to fully realize the benefit of rule engines. During the execution of JNDMS it is unlikely that this level of input would be available so the integration of the rules engine should be used for experimentation and be entirely optional.

5.7.5 Incident Recognition

The DSS makes use of a distinct set of rules to fuse information from the five SAs for CND domains in order to identify incidents, makes inferences about incidents, activities and situations that adversely affect the IT infrastructure. Examples include:

- Discrepancies between the CM database and information acquired through network discovery
- Evidence of a vulnerability within a host, a subsequent attack against that host, and the future attack on other assets by that same host
- Unusually high bandwidth consumption on links interconnecting assets

The DSS will be capable of processing dynamic events (“transactions”) and providing context to them using periodic data in near-real time, to enable timely response to threats.

The DSS uses correlation techniques to determine if an incident is a single instance, a new local reoccurring trend, a long-standing local reoccurring trend, a new widespread reoccurring trend or a long-standing widespread reoccurring trend. The DSS makes this determination by correlating all incidents with archived incidents generated locally and shared incidents obtained from external organizations. At a high level, the problem the DSS must solve is to find “needles” of threat or exploit in the “haystack” of data from the CND environment. To find these needles, multiple data mining techniques can be employed. The JNDMS TD uses selected techniques from among the following:

- Clustering or the partitioning of data into subsets that share common properties
- Association or the analysis of the structure of relationships and cause-and-effects between data sets
- Statistical analysis or determining the likelihood of properties and associations in data sets
- Rule abduction or the development of if-then-else rules that describe the associations and structures of the data
- Tree abduction or the discovery of relationships between data sets and connecting patterns
- Deviation analysis or the analysis of deviations from normal statistical behaviour
- Neural abduction or training neural networks to match data and local structure

The DSS filters benign incidents and exceptions, and refrain from processing them further. Responsibility for identifying such incidents lies with the JNDMS analyst. The JNDMS maintains a list of such incidents in the JNDMS Data Warehouse, which the DSS consults when processing new incidents.

5.7.6 Severity and Risk Assessment

The DSS uses:

- Information from the five CND information domains
- Dynamic and periodic CND environmental data
- Conclusions previously made by the DSS about the defensive posture

From this, it must assess the probability of occurrence and effect on operations of each given threat or exploit to CND vulnerabilities. The module also has to employ calculations based on 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. It must also consider the net result of all threats and exploits taken together on the operation as a whole. This risk management assessment will then reach conclusions as to the timeframe and frequency of risks being realized, to what degree they affect operations, and at what time.

Given the DSS' conclusions as to the CND risk landscape, it must then detail the nature of the threat/risk impact including disclosure, alteration or destruction of information resources in support of operations, and what corresponding safeguards for confidentiality, integrity or availability are in place or can be deployed in a timely fashion. This must be done for each IT infrastructure or IT service asset, which has been designated as supporting military operations. Further, it rolls up the risk assessments from individual situations into an overall CND risk assessment.

These risk assessments are then used to predict the time to redeploy safeguards or to take preventative action to partially mitigate the threat or exploit agent impact, and the expected time to recover from degraded or destroyed operational capabilities. All such risk assessments are stored and presented to JNDMS users using a meaningful normalized severity scale, and includes supporting evidence statements to justify to human analysts how the system reached its conclusions and assigned the severity value. Then, the system again rolls up individual severity values and evidence statements for all on-going and forecasted incidents to a top level CND-wide severity value and supporting evidence. It keeps tracking these risks or incidents in real time and keeps its assessments continuously updated, along with maintaining a historical record of individual and rolled-up severity values.

The DSS also allows human analysis and input to its decisions, and decision making processes (rules). This includes the ability to permanently or temporarily override system defaults, data flows, or assumptions.

5.8 Presentation, Visualization, and Alerting

The JNDMS is only as useful as the information that it provides to the users of the system. Information content must be specific to the JNDMS application, but abstracted to a level that humans can easily understand. The presentation system must be tailored to enable quick response times, based on accurate and reliable information (Figure 23).

The Presentation, Visualization and Alerting components present SA data to the users and allow user-control of the JNDMS TD. This component is created from a mixture of COTS and custom code, tailored to satisfy the DRDC UI requirements. New information arriving in the Data Warehouse is processed by the DSS, causing changes to the SA information presented by the UI. The UI has capabilities of operating on both historical, real-time current, and forecast information, allowing the presentation to reflect any user-selected date and time.

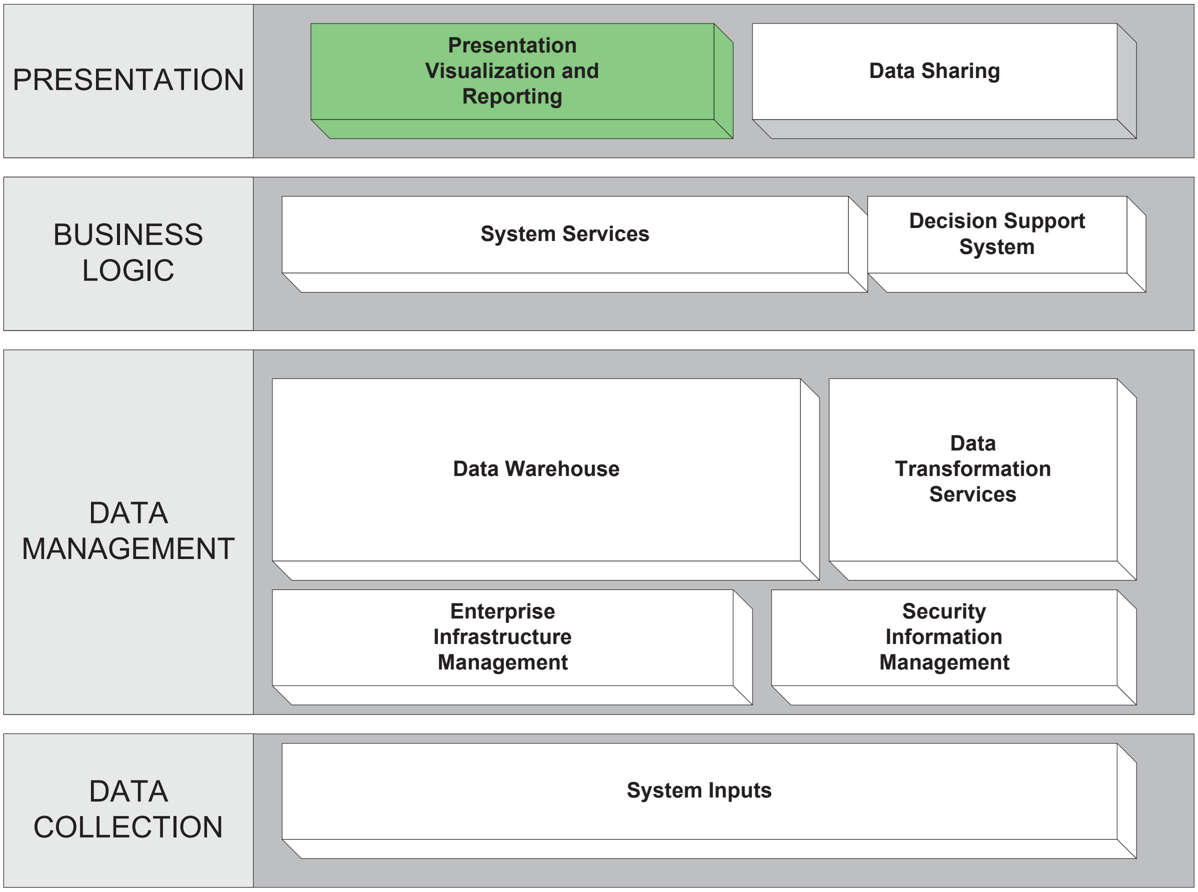

PRESENTATION
Presentation Visualization and Reporting
Data Sharing
BUSINESS LOGIC
System Services
Decision Support System
DATA MANAGEMENT
Data Warehouse
Data Transformation Services
Enterprise Infrastructure Management
Security Information Management
DATA COLLECTION
System Inputs

Figure 23: Presentation, Visualization and Alerting

5.8.1 Component Introduction

The JNDMS Presentation, Visualization and Alerting component presents Military Commanders and network analysts with a deconflicted and decluttered view of the defensive posture of the DND operational networks. All information about the SA, including threatening events, non-threatening events and network environments, is made available to the user. This component is a one-way transfer of information from the database and DSS to the users.

All information provided to the users follows an intuitive navigation and visualization approach. This includes the use of maps, network topology representations, tables, and navigation links as part of the presentation. It is important that the presentation services be made available to a distributed set of users; then these services are made available as web-based services. MDA shares the JNDMS vision for simplifying the numerous complex user interfaces that typically exist in the SA for CND domain. Providing a coherent rolled up view of the SA through merger of multiple data sources simplifies current SA complexity and training.

The proposed JNDMS contains a battle map component that includes many of the functions of a standard C4ISR system, including representations of assets and operations. Geo-referenced network assets are displayed as a map layer where such assets have been mapped to geography. This is displayed in a similar fashion to battle maps for command personnel and as network diagrams for the IT personnel. The JNDMS views have updates in near-real-time. Refresh rates will vary according to the receipt rates of data. The JNDMS provides visual identification of the age of the displayed data.

JNDMS data collection spans several classifications of networks. The five identified information domains' data are collected in near-real-time by the JNDMS to support SA for CND. This data is accessed from a role-based UI that initially constrains users to default functions. However, any additional functions can be made available to all users.

5.8.2 Component Technologies

Among the best-of-breed technologies that MDA has identified as candidates for this component in the JNDMS, the leading technologies are ArcIMS and ArcGIS for Web-GIS from Environmental Systems Research Institute (ESRI), Oracle for component data management, and Liferay Portal from Liferay.

During the development of JNDMS several mapping components other than ESRI matured, including open source offerings such as Open Layers as well as Google's Map API and their Google Earth Plugin. These offerings have shown to be light weight, easier to develop with and provides and more responsive end user experience.

The use of a full J2EE stack, either through JBoss or Liferay also proved to be excessive overhead for our tasks. An alternate version of Liferay was tried that used on Tomcat as the application server. This proved more responsive, however it still had significant development road blocks.

The final portal was built using the Google Web Toolkit. This allowed very quick development cycles and provided better troubleshooting and debugging capabilities. The resulting portal is smaller and better integrated.

5.8.3 Component Description

Presentation, visualization and alerting - these three subcomponents are all related through one concept: information. They are all means of providing information to people.

Presentation simply means the process of making information available to people. The challenges behind presentation are to:

- Abstract the technical content that is generated by the JNDMS into meaningful words and pictures for people to understand.
- Organize content appropriately so that all relevant information for a situation is available to the user, and so that the user can easily access related information.
- Provide information in a timely manner appropriate to the significance of the situation. For example, high priority information can interrupt routine events in the presentation system.

Visualization is a strategy to provide information in a visual display. It includes the following aspects:

- Identify consistent and meaningful terminology and phraseology to provide in the presentation.
- Identify logical flows of information to present to the user.
- Identify graphical cues that can provide users with immediate recognition of physical properties, geographic locations, network configuration topology diagrams, network events or symbolic views of other types of information.
- Develop a system to make the visualization content available to the user in an appealing and understandable format.

Alerting is a concept of timeliness and decision making. It combines the results of the data collection system and the DSS with the presentation system to be able to get high priority information to the user as fast as possible, and to present it with an appropriate level of urgency for the given severity assessment.

Presentation services encompassing all these concepts are provided to users of the JNDMS for the purpose of access to information, i.e., monitoring. In other words, there will be no aspect where a user can, for example, configure networks through the presentation system.

The JNDMS provides a means to visually correlate data from the five SAs for CND information domains identified. This is presented to allow the user to understand the defensive posture, severity assessment, and IT infrastructure status using geospatial maps, graphs, and tables, as appropriate. Playback and play forward capabilities are included.

In the remainder of this section, we examine the strategies that MDA proposes for the JNDMS presentation system and we also examine some technologies that may be used in this system. Table 3 identifies and discusses some of the issues that are important to the JNDMS. MDA will use its expertise in these technical areas in the design and development of a presentation system for the JNDMS that meets the needs and requirements of the TD.

Issue	Discussion
Near Real-Time Presentation	The JNDMS needs to provide multiple role-based interfaces and views of the real-time CND environment suited to the various types of users. This may include a web portal to provide high-level status or historical reporting, and a client application to allow granular control over data presentation, as well as the ability drill down to various tools or more detailed views.
Reporting	The JNDMS provides provide ad-hoc or scheduled reporting from the data repository to meet auditing, trending, and historical query requirements.
Geospatial Data	Geospatial data provides a mapping between IT assets and their real-world location. This mapping may be either static, as in the case of a mission critical server in a datacenter, or dynamic as in the case of a field-deployed unit such as a ship or mobile command post. Another important facet of geospatial data is the real-world position of hostile network entities and tools, such as IP geo-location databases that can estimate the physical locations of their internet IP addresses. Geospatial data can be important for decision-making in the JNDMS. Locations for static assets should be captured in a database so that the DSS can then prioritize decisions based on location. This data can also provide context as to the possible physical location of internet connected hostiles.
Portal - Web Services/Authentication	The advantage of web portals is that they don’t limit the user to a physical location. Web portals with secure protocols can be used to present an organized summary and launching point for a variety of applications. Modern web portals can tailor the same information for multiple customers in different arrangements. Authentication can be used to restrict access of certain information to groups of users, while allowing all users to productively use the single web service.

Issue	Discussion
GIS Mapping Tool	Web-based Geographical Information System (GIS) mapping tools can be used to dynamically exchange and portray geographically referenced data. Views of this data can be combined with network topologies and symbols to show physical locations of networks and situational events.

Table 3: Presentation System Issues for the JNDMS

5.8.4 Portals

A portal can be interpreted as a gateway to information. It provides us with an access point or a view to a large world of information through a “doorway” of limited size.

The nature of this concept is that portal systems are almost exclusively web-based. Using portals for presentation of the JNDMS provides for both advantages and challenges. The advantages are:

- **Portable system**: Users in one geographic location have exactly the same presentation and information as users in other locations. Information may propagate quickly between people. Staff may travel and still maintain their role and responsibilities with regards to the JNDMS.
- **Role-based access**: Specific roles are defined that allow the customization of the presentation based on the logged in user or active role.

Challenges associated with portals are:

- **Security of information passed to the portal**. As the Internet is open to the world, information can be easily detected and used to mount a security threat. Different levels of security may be added to minimize this challenge, such as:
    - Secure web servers that encrypt data with 128-bit encryption
    - The use of server certificates that authenticate the source of data
    - The use of PKIs so that the servers may authenticate the recipients of the data
    - The use of firewalls for an added layer of authentication and encryption
    - Secure browser configurations to prevent the caching of sensitive data in its unencrypted form
    - Stand-alone wide area networks (WAN) that are not connected to the public Internet

      The JNDMS terminals are assumed to reside on a controlled access network such that direct access from public networks is not available.

- **Presentation of information in a near real-time manner**: In an environment where information that is presented to the user must change as events change, the use of portals provides challenges. Information presented in a web portal cannot change unless the user initiates an action. This is called 'pull' technology. If an event occurs in the JNDMS monitoring that is important to be brought to the attention of the user, this may cause a delay in making the information available to the user. There are strategies that can be investigated during the course of the JNDMS-TD to overcome this problem (for example, applying a meta-refresh event in an in-line frame to serve as a notification portion of a portal view).

Other guiding principles that must be considered are:

- Portals should not rely on the use of plug-ins because different users may have different browser configurations.

MDA will accommodate these challenges and issues in the design and development of the JNDMS presentation system. An example of a portal that demonstrates good design principles is shown in Figure 24.

5.8.5 The JNDMS Portal

The portal of the JNDMS TD manages all interactive role-based reporting of the network and situations to all users. The presentation services query the database for all information and presents the users with intuitive views of the network situation and defensive posture, as seen in Figure 24.

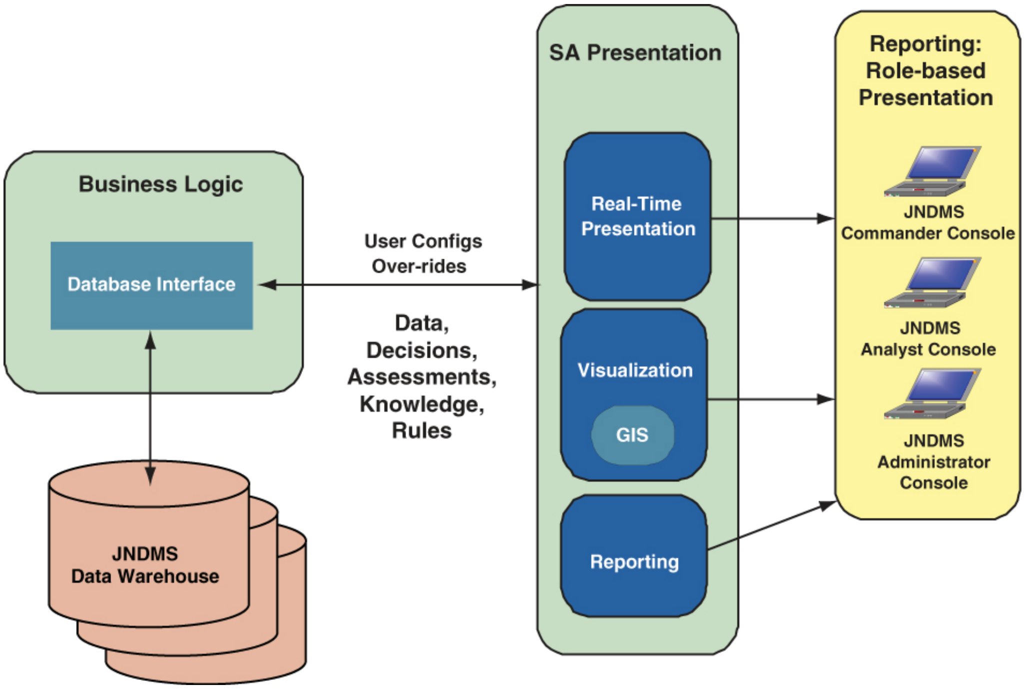


Figure 24: The JNDMS Portal

The JNDMS Portal integrates the concepts described in this section with web technologies to provide the JNDMS workstation functionality. The following information is integrated in a view with a geographic map:

- Network diagrams, with colour coded symbologies used to represent levels of security assessments.
- Threats and the level of invocation of defensive mechanisms against those threats (the defensive posture). As with the network diagrams, this visualization is abstracted with the appropriate scale of the presented map.
- Military operations and their related network configurations.
- Alerts relating to security events on the network.

All of these views are abstracted to a level of detail that is appropriate to the scale of the presented map. This can be done with the use of Web-GIS mapping technologies.

Users are able to navigate these views in the following ways:

- The user is able to follow graphical linkages between computers or between networks. For example, if they select a graphical representation of a network in the portal view, the system assembles a new view showing all network connections and security assessment information for the network that the user selected. This is a form of ‘drill across’ navigation.
- The user is able to pan geographically in the portal view. As they do so, the system assembles a new view showing all the networks and SA information in the new region-of-interest. This is another form of ‘drill across’ navigation.
- The user is able to select a graphical icon for a network or a text description of a network, and request more details. The system assembles a more detailed view of the components of the selected network and will provide more details about the SA information about the components of the network. This is a form of ‘drill down’ navigation. The user is able to drill down until they reach the highest level of granularity of network and systems information stored in the JNDMS.
- The user is able to select a textual or a text description of a situation, and request more details. The system assembles a more detailed view of information that is connected to the situation. This is another form of ‘drill down’ navigation. The user is able to drill down until they reach the level of the five CND Information Domains.
- The user is able to zoom-in on the geographic view. The system assembles a more detailed map of the new region-of-interest and shows more detailed network diagrams and SA information related to the specified region. This is another form of ‘drill down’ navigation. The user is able to drill down until they reach the scale of the highest level granularity of network systems information stored in the JNDMS.
- For each of the representations in the portal view (geography, network diagrams and textual information), the user is always able to drill up to the next highest level of generalization until they reach the lowest level of granularity of information store in the JNDMS.
- At any level of detail within the portal view, the user is able to drill across.

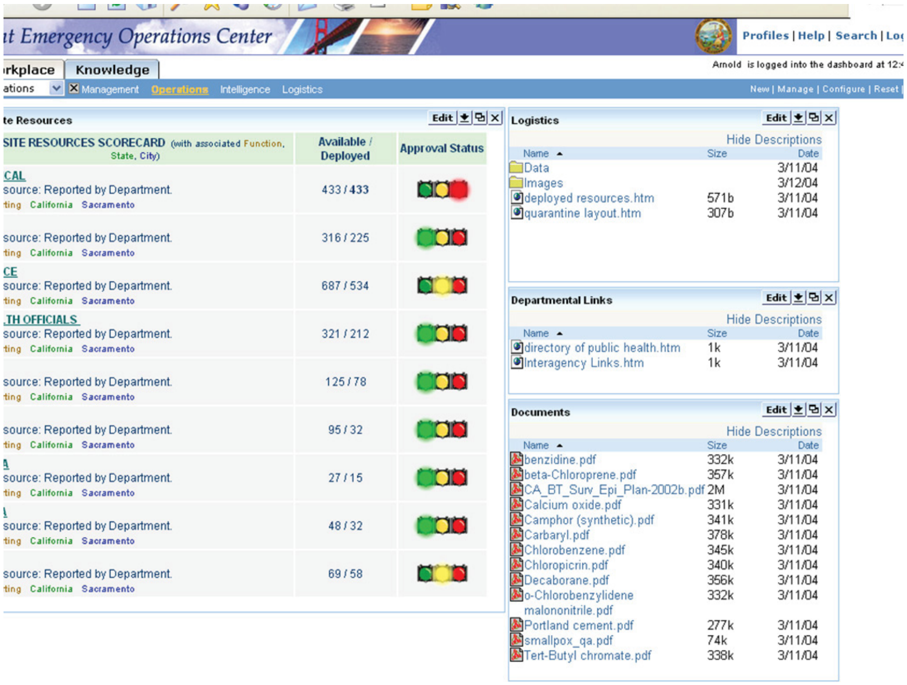
As all information is time stamped in the JNDMS Data Warehouse, the portal is able to show time series of events to allow the user to evaluate the spread and containment of security events. The JNDMS views have updates in near-real-time. Refresh rates will vary according to the receipt rates of data. The JNDMS provides visual identification of the age of the displayed data.

The role in which a user is accessing the portal system will determine the level of information that is available to them, i.e., role-based views. Users are able to (but not required to) authenticate in the JNDMS portal. The non-authenticated users receive the most basic information in the JNDMS view. For authenticated users, the JNDMS provides details, services and capabilities specific to the role that has been assigned to each user.

For some user roles, the users are able to have update privileges. This allows them to add comments to events or to override results of, and add justifications to, the SA where necessary. Overriding results of SA could be in the form of either promoting or demoting the SA.

Users are able to save their viewing preferences and user-defined queries with their profiles so that user-defined views may be configured and used during subsequent sessions.

As previously discussed, there are methods by which the portal is able to interrupt the user view with timely alerts. All information displayed contains the timestamp that the information was generated. SAs and other decisions is also tagged with completeness of all information that formulated the decision, and the level of confidence of the decision.


it Emergency Operations Center
Profiles | Help | Search | Lo
Arnold is logged into the dashboard at 12:
rkplace
Knowledge
ations
Management
Operations
Intelligence
Logistics
New | Manage | Configure | Reset |
Edit

te Resources

SITE RESOURCES SCORECARD (with associated Function, State, City)	Available / Deployed	Approval Status
CAL source: Reported by Department. ting California Sacramento	433 / 433	🟥
source: Reported by Department. ting California Sacramento	316 / 225	🟩
CE source: Reported by Department. ting California Sacramento	687 / 534	🟨
TH OFFICIALS source: Reported by Department. ting California Sacramento	321 / 212	🟩
source: Reported by Department. ting California Sacramento	125 / 78	🟩
source: Reported by Department. ting California Sacramento	95 / 32	🟩
A source: Reported by Department. ting California Sacramento	27 / 15	🟩
A source: Reported by Department. ting California Sacramento	48 / 32	🟩
source: Reported by Department. ting California Sacramento	69 / 58	🟨

Logistics

Hide Descriptions

Name ▲	Size	Date
Data		3/11/04
Images		3/12/04
deployed resources.htm	571b	3/11/04
quarantine layout.htm	307b	3/11/04

Departmental Links

Hide Descriptions

Name ▲	Size	Date
directory of public health.htm	1k	3/11/04
Interagency Links.htm	1k	3/11/04

Documents

Hide Descriptions

Name ▲	Size	Date
benzidine.pdf	332k	3/11/04
beta-Chloroprene.pdf	357k	3/11/04
CA_BT_Surv_Epi_Plan-2002b.pdf	2M	3/11/04
Calcium oxide.pdf	331k	3/11/04
Camphor (synthetic).pdf	341k	3/11/04
Carbaryl.pdf	378k	3/11/04
Chlorobenzene.pdf	345k	3/11/04
Chloropicrin.pdf	340k	3/11/04
Decaborane.pdf	356k	3/11/04
o-Chlorobenzylidene malononitrile.pdf	332k	3/11/04
Portland cement.pdf	277k	3/11/04
smallpox_qa.pdf	74k	3/11/04
Tert-Butyl chromate.pdf	338k	3/11/04

Figure 25: Example of a Consistent Web Portal

In the example shown in Figure 25, views from diverse disciplines are provided in a control-panel layout, where the user can drill down for more detailed information in any one of the views. Similar layouts and graphical cues are provided across these diverse panes - this strategy makes it easy for the user to gather information by scanning the panes without having to concentrate interpreting changes in layout between the panes.

5.8.6 Web-GIS Mapping Standards and Tools

Web-based GIS mapping tools can be used to dynamically exchange and portray geographically referenced data. Views of this data can be combined with network topologies and symbols to show physical locations of networks and situational events.

An ability to view physical locations of networks and events provides decision makers with answers to some important questions with a single glance. Users can quickly understand the geographic location of an event, and are likely to contact people who are close the event in a timely manner. Multiple events may also be associated geographically as a result of a geographic view. Trends and tendencies may be determined by summarizing information with a geographic context.

With the advent of geospatial standards for interoperability in the past 5 years many GIS functions can now be operated through the Internet. The OGC is an international consortium that has developed many standards and architectures that are widely adopted in practical use today. The International Organization has adopted many OGC specifications as international standards for Standardization (ISO). A summary of Web-GIS considerations and OGC specifications is provided in Table 4.

GIS vendors in Canada and around the world have seized opportunities from these emerging standards to provide a wide range of Web-GIS products. Products range from open-source tools with very large install-bases to fit-for-purpose tools than can accommodate specialized engineering requirements.

Table 4: Web-GIS Technologies and Issues

Issue	Discussion
Performance Objectives	The use of web based mapping tools must not result in added delays to the decision maker. Anyone using the web-based reporting system should not be delayed as a result of a request for, and portrayal of, Web-GIS content.
Deployment	Very few Web-GIS standards have security considerations designed into them. The security of the data delivered by web-based mapping tools will be determined by the security levels of the web servers, computers and networks that provide those tools.
Risk Assessment	A risk of any web-based service is that the GIS data delivery system can itself become compromised, resulting in no data or erroneous data delivered to the decision maker from the web server.
Risk Mitigation	Mitigating the risk of web services compromise can be done by using products with significantly sized install bases that security considerations are designed into the products and that patches are available. This risk may also be mitigated using the strategies identified in the Portals discussion in this section.
OGC Specifications	The following are key OGC specifications: **WMS - Web Map Server Interface Specification** This specification defines interfaces requesting maps from web map servers (WMS). One or more raster and/or vector layers may be requested from a WMS. Clients may request maps in a specified projection, and may specify symbology (or styles) for vector or point data. Maps may be saved in Web Map Context documents. **WFS - Web Feature Server Specification** WFS is a specification for requesting and sharing geographic features. For example, a client may request the names and outlines of all lakes within a specified geographic area. The server will respond with a list of lake names, jurisdictions, outlines, and depths of the lakes corresponding to the request. Gazetteers may be encoded using WFS.

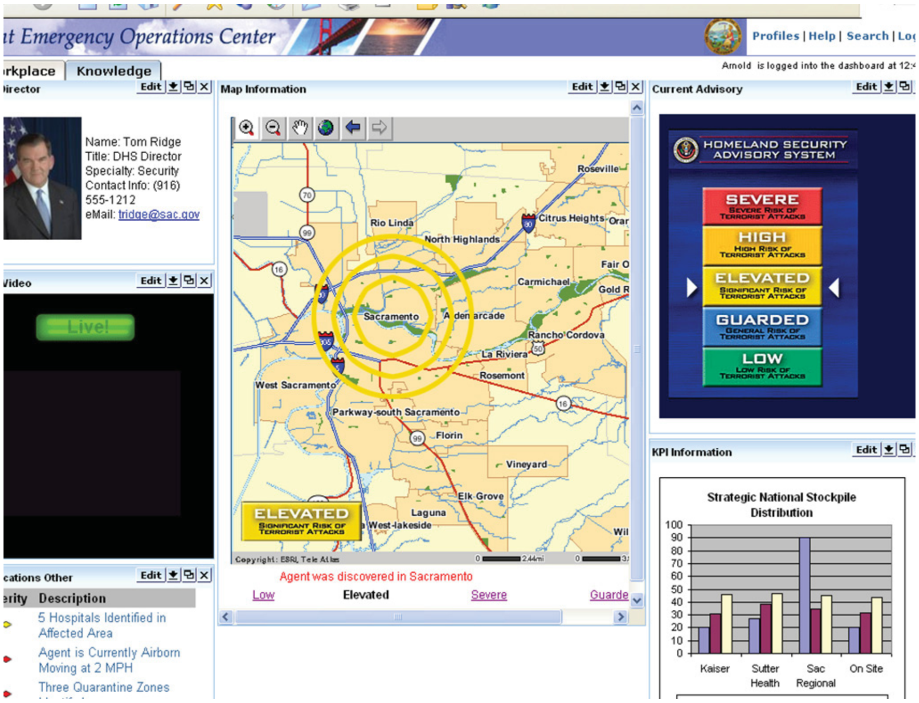
Issue	Discussion
	GML - Geographic Markup Language GML is a means to transport geographic data through the web. GML is an eXtensible Markup Language (XML) specification that may be used to encode entire maps or portions thereof. **WCS - Web Coverage Server Specification** Coverages are raster representations of real-world phenomena. Maps or satellite images may be encoded in coverages. WCS is a specification for requesting and sharing coverages through the Internet. **SensorML** The Sensor Markup Language, or SensorML, while not in wide use today, could prove to be a key technology for the JNDMS. Its purpose is to provide a standard XML to facilitate communication between sensors and other components. Included in the markup language are geolocations, so that geospatial information may be embedded in the data streaming directly from the sensor. **Many OGC specifications, other than these, have been defined and could possibly be used by the JNDMS, but are mostly intended to facilitate the implementation of underlying technologies (such as filter encoding and catalogue services).**

The Canadian Geospatial Data Infrastructure (CGDI) has sponsored and endorsed many of the OGC specifications. In the MDA design of the JNDMS we consider key OGC specifications that are reasonable to apply to the geographic information display of the presentation system.

One key consideration in using Web-GIS services is the availability of data that Web-GIS servers use. For example, a web map server must have a map repository that has accuracy suitable for the application. A web feature server must have a database of geographic features with information that is relevant for the application. One key activity in the development of the JNDMS is to identify reliable sources of data that meet the needs of the TD.

In addition to OGC specification Google has made KML a defacto standard, now supported by many tools. This provides a rich description of geographic entities.

An example of integrating Web-GIS technology with an information system portal is provided in Figure 26.



Name: Tom Ridge
Title: DHS Director
Specialty: Security
Contact Info: (916) 555-1212
eMail: tridge@sac.gov

Agent was discovered in Sacramento

erity	Description
	5 Hospitals Identified in Affected Area
	Agent is Currently Airborn Moving at 2 MPH
	Three Quarantine Zones

Figure 26: Example of Portal Information Integrated with Web-GIS

In this example of a web portal, the information system is combined with Web-GIS capabilities to provide an immediate geographical context to a situation.

5.9 Situational Awareness Data Sharing

The sharing of SA data collected from different geographic locations, as well as from different SA systems increases the size of the dataset and amplifies the possibility of uncovering trends and revealing previously undetected patterns. This data can be shared between installations of the JNDMS in the same security domain, with installations of the JNDMS in other security domains, as well as the information assurance systems of coalition partners (Figure 27).

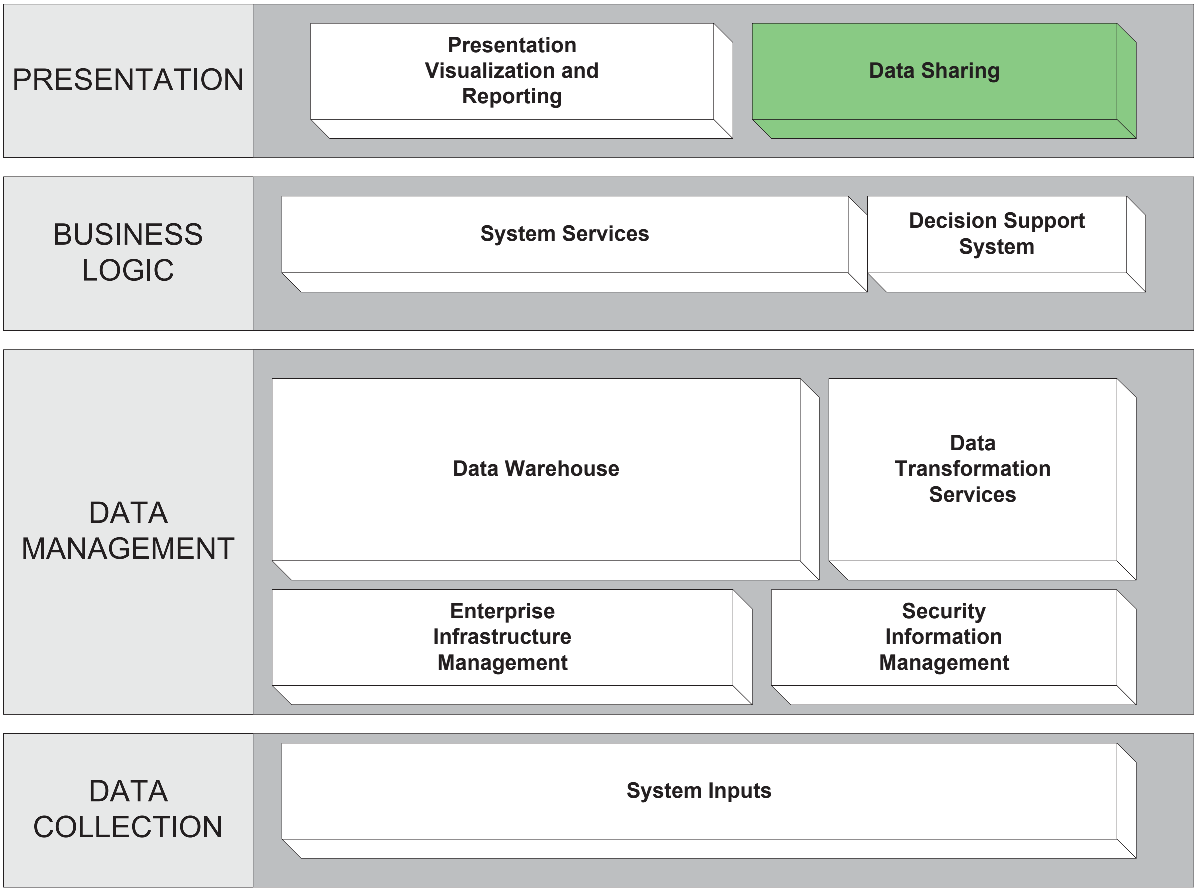

PRESENTATION
Presentation Visualization and Reporting
Data Sharing
BUSINESS LOGIC
System Services
Decision Support System
DATA MANAGEMENT
Data Warehouse
Data Transformation Services
Enterprise Infrastructure Management
Security Information Management
DATA COLLECTION
System Inputs

Figure 27: Decision Support System

The SA Data Sharing component exchanges data with external systems, based upon pre-arranged data exchange policy. Open standards, such as IODEF, are used to provide widest possible support for JNDMS data. This will also be the exit point for data being handed up to a higher-level JNDMS.

5.9.1 Component Introduction

Data sharing is another form of presentation. It is a means of providing information without the requirement for human interpretation of the information. The SA Data Sharing component is provided within the JNDMS so that SA information from the JNDMS may be shared with other instances of the JNDMS and the high-level peer systems of allied and coalition partners. Depending on the final design, the Data Sharing component may make available all SA information that is available to the Presentation, Visualization and Alerting component, or it may make a subset of the SA information available.

It should be noted that the SA Data Sharing component at the Presentation layer only *exports* the SA for CND information that is produced by the DSS. Information from other Network Defence and Management Systems may, depending of the security classifications and service agreements, be imported into the JNDMS Data Warehouse through the SA data sharing input in the CND Dynamic Inputs component.

5.9.2 Component Technologies

Among the best-of-breed technologies that MDA has identified as candidates for this component in the JNDMS, the leading technology is Advantage form CA.

5.9.3 Component Description

The SA Data Sharing component manages and controls the sharing of SA data and associated metadata with other systems, such as other JNDMS installations or information assurance systems of coalition partners. Data sharing is governed by policies that outline data sharing profiles, permissions and attributes, such as classification and direction.

In order to define the data sharing policies, data sharing agreements must be made between organizations to:

- Describe the type of data and metadata that each system is willing and permitted to share with the other system
- Identify the format and encoding of the data and metadata
- Define the expected frequency of data sharing exchanges
- Outline the protocols and mechanisms that enable the information sharing

The JNDMS data model defines a framework for the content, structure, and encoding of both JNDMS data sharing policies and data sharing agreements. For each data sharing request, the contents of the data and metadata exported from the JNDMS are dynamically configured against the data sharing policy available for the client, or partner, who originates the request. The contents that may be configured to specific requests include providing data and metadata only for specific network domains or geographic locations, or limiting data and metadata to include only specific attributes or data sources.

Depending on the data sharing policies and agreements that are in place, data sharing requests may result in either:

- A complete or partial export or all of the JNDMS Data Warehouse so that it may be replicated in another environment
- A complete or partial import of all of the data from an external Network Defence and Management System, so that it may be imported into the JNDMS

Due to the volume of data involved in data exports and imports, it may be prudent to implement full exports and imports as offline batch services. Also, subsequent exports or imports with an external service need only be done as an incremental update to save bandwidth. Only new and modified data need be imported or exported.

Within the JNDMS, data sharing agreements and policies themselves are static arrangements that are agreed to in advance. In the future however, DRDC could leverage work being done by NRNS on Policy Based Network Management (PBNM) that includes an inter-domain policy negotiation capability to enable real-time negotiation of data sharing agreements.

Figure 28 illustrates the JNDMS SA data sharing with:

- An external information assurance system
- A JNDMS installation within the same security domain
- A JNDMS installation in a higher security domain

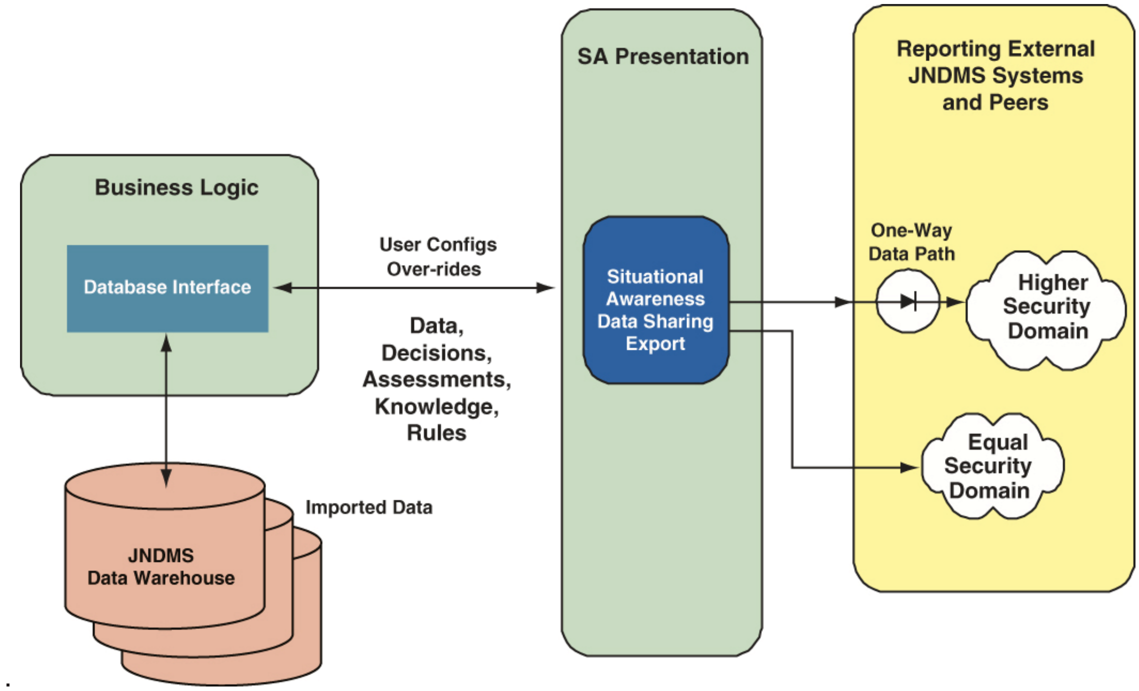


Figure 28: JNDMS Situational Awareness Data Sharing

Data Sharing includes both data export and data import between different levels of security classifications.

5.9.4 Situational Awareness Data Exchange

Since the JNDMS has ownership of its own data model, data sharing between JNDMS installations will not undergo data transformation. Although it is the intention of MDA to employ a standard data model, such as IODEF to facilitate data sharing with external systems, the absence of such a workable standard in some cases may require some form of data transformation when exchanging SA data with external organizations.

5.9.5 Situational Awareness Data Validation

The SA Data Sharing component manages all aspects of SA data sharing. This component validates, filters and sanitizes SA data prior to exporting it to allow for compliance with the data sharing agreement. Moreover, this component validates all received SA data against their origins and enables compliance with the other aspects of the data sharing agreement. The JNDMS data model mandates the content, structure, and encoding of shared SA data. MDA anticipates that the shared SA data is modeled using a standard data model, such as IODEF, and that it is encoded using XML.

5.9.6 Cataloguing and Use of Incoming Situational Awareness Data

The SA Data Sharing component enables accurate cataloguing of all received SA data. This includes the time when the information was received, the identification of the system that provided the information, as well as the information's classification level and caveat. The SA Data Sharing component makes use of cryptography to validate the authenticity, integrity and non-repudiation of shared SA data. To support timeliness and to further support non-repudiation, shared SA data also includes a timestamp to prevent captured information from being be used in replay attacks to create confusion during future attacks. The SA Data Sharing component maintains a log that records all aspects (time, origin, classification) of each data sharing exchange - inbound and outbound.

In addition to real-time updates, the SA Data Sharing component provides periodic bulk updates in support of synchronization after a prolonged system or network outage, or to facilitate the transfer of SA data when network-based communication is strictly prohibited. However, information sharing is achieved, the SA Data Sharing component always records all data attributes: time, source, classification level, etc.

Use of incoming SA data serves more than archival purposes. The DSS component rules are able to use this data to detect trends or new patterns or commonalities that extend beyond its own JNDMS implementation. It is also able to link the information though the DSS to correlate events from external systems with events in the JNDMS, or to identify previously undetected events in the JNDMS with the aid if the new data from the external systems.

5.9.7 Communication Technologies for Situational Awareness Data Sharing

SA data sharing can be accommodated using various communication mechanisms, such as secure messaging using SMTP in conjunction with S/MIME, SOAP to exchange XML encoded objects over HTTP or Secure HTTP (SHTTP) sessions, or SCP protocol from the Secure Shell suite for secure bulk transfers. S/MIME and SOAP are appropriate time sensitive updates, while SCP is better suited for bulk synchronization.

5.9.8 SA Data Sharing Between Different Security Classifications

Military environments include networks of different security classifications. In some cases, security policy requires physical separation in the form of an "air gap" to prevent communication between these networks. The JNDMS provides the capability to transfer SA data generated in a lower classification network to a higher classification network. Under certain circumstances, accredited devices may be used to provide a one-way communication path between a lower priority network and a higher priority network. Products such as the Tenix Interactive Link Data Diode (IL-DD) provide a one-way communication path between two networks, with hardware-enforced prevention of reverse path data flow. The JNDMS recognizes this one-way information flow within the data sharing policy whereby the lower classification JNDMS only exports SA data and will not receive SA data from a higher classification JNDMS. Likewise, the higher classification JNDMS only receives SA data but does will not provide SA data to a lower classification JNDMS. This exchange shall be a “push” and all data is tagged with relevant information as defined by the data model design work in Phase 1 of the project.

MDA recommends that simulation of a one-way data diode by employing simple one-way communication interfaces is sufficient to demonstrate this capability. One possible solution may include a modified Local Area Network (LAN) cable that only permits one-way communication via connectionless User Datagram Protocol (UDP) packets.

When the JNDMS receives data and metadata from a different security classification, it stores that data and metadata in its Data Warehouse. The Data Transformation component adds additional metadata to the incoming data. This additional metadata includes information about the source of the data, including the origin of the data and the security classifications it was received from and delivered to.

The JNDMS contains controls to support profile-based import and export systems. These profiles are a series of policies describing classifications and quantity of data that can be exchanged with recipients. These configurable policies allow exchange mechanisms to be “tailored” for the data sharing requirements of a one JNDMS instance to another, or of a JNDMS to CND system of allies or coalition partners.

5.9.9 Dealing With Transmission Failures

It is likely that there will be cases when data exported from one JNDMS is either not received or interrupted during transmission. Methods to deal with this are dependent on the different security classifications between systems that are transmitting and receiving data. These methods include:

- In the case that data is being transmitted to a JNDMS within an equal security classification, then the receiving system can send a message back to the originating system that it failed to receive the data, or it can simply repeat the request to receive the data.
- In the case that data is being transmitted to a JNDMS of a higher security classification, the high security classification system cannot send a message to the low security classification system that it did not receive the data. However, the data diode that facilitates the transmission contains built-in capability for handling and reporting transmission failures.

6 JNDMS Data

This section describes the entities that are required to be stored in a persistent store within the JNDMS. This data model has been refined to be implemented as a RDBMS schema, for a database that supports SQL-92. This section details:

- Introduction to the database management software
- Database access control
- Data models
- Data base replication
- Estimate of the size of the database

The data entities and some static and dynamic data relationships are created within the Data Warehousing component. Other dynamic relationships may reside within the DSS' rules. Refer to section 5.5 for further details on the relationships between the Data Warehouse component and to section 5.7 for details on the DSS.

6.1 Introduction to the Database Management Software

The purpose of a database in the JNDMS is to be used as both a storage place for commands and messages, but also to allow for history and recoverability. In order to fulfill the need for good recoverability, we need the capability to save the commands and messages that are passed from the user and the JNDMS, and messages that are passed internal to the JNDMS between applications. Furthermore, in the case of a system failure, we must be able to recover the last set of commands and messages, and continue processing, with no loss of data.

The question arises of how this data store can be implemented, whether it should be embedded into a Control and Management application, or set up in such a way that other applications can access it. As most of the JNDMS uses this system to store messages, it should be set up in such a way that other applications can access the data store. In this case, a client server style of access is beneficial, as it allows all of the applications that require access to the data store to connect and have the connection maintained by the server.

Although a fully relational database system is ideal, we have the further need that this system must be efficient, as it cannot interfere with other applications that are running, or interfere with the processing capabilities of the computer in such a way that our timing requirements cannot be met. Trade-offs are made between full normalization of the database to reduce data redundancy and less normalized forms to improve speed.

To implement a reliable storage solution, a relational database solution has been selected, which uses the Oracle RDBMS and a simple database schema. As recoverability is a high priority requirement, Oracle RDBMS is ideal. Most database management systems contain the capability to complete their own error correction and recovery, simplifying the disaster recovery for the JNDMS. The RDBMS further has the capabilities to handle high loading and balancing the query load, in order to efficiently provide a data storage solution that will not affect JNDMS operations.

6.2 Database Access Control

Typical database access control is handled by several means. The first implementation is via the database user. Every connection to the database is done via a database username and password. Table 5: JNDMS Database Users shows the different classes of database users that are created.

User	Description
Admin Users (sys, system)	There are administrative users created by default for the Oracle database these will remain in place such that database administrators can perform the necessary administrative and maintenance functions using standard COTS tools.
JNDMS Owner (jndms)	The JNDMS Owner user is the owner of the schema objects and the data. This account will be used by application developers/ maintainers to create and alter the schema objects, changing the definition of the object stored in the database. By default, this user has full Create/Read/Update/Delete (CRUD) access to the actual data.
JNDMS User(s)	A JNDMS user database account references the JNDMS owner’s objects. This type of user has the ability to update the data but no ability to alter the schema definition. There can be several different users created with different levels of access if this is deemed necessary. Typically, these users only access the database via the specific application, in this case JNDMS. Often, this username and password is contained in a configuration file as is not directly related to an operator’s user account.

Table 5: JNDMS Database Users

The second form of database access control is provided by the application. The rules coded within the applications restrict the access and what data is available and at the same time are able to navigate through the database structure to produce/present the desired results.

6.3 Data Model

Data Model is based upon the requirements that consider the data required to present to the user, the data available from the sensors and the data to be processed by the DSS. The JNDMS data model is unique in that it will correlate data from the distinct domains, namely IT infrastructure, information/data security, and military operations.

6.3.1 IT Infrastructure

The IT infrastructure data represents the network. This data deals first of all with the hardware within the network but as a critical extension, the service that the hardware offers.

There are several sources that can be considered when modelling this portion of the database. It is largely driven by what data is collected via the network discovery tools available/utilized.

In addition to the data provided by the network discovery tools, there are also existing standards for modelling this type of data. Adopting a standards based data model should reduce the dependency of the JNDMS of any given COTS product but is likely to impact integration of the tools. The data model shown in Figure 29: ITI CIM Core, taken from the Impact Assessment Tool (presentation by Luc Beaudoin, DRDC NIO, September 2005) is an example of the infrastructure that needs to be modelled. More details of the CIM standard can be found at <http://www.dmtf.org/home/>.

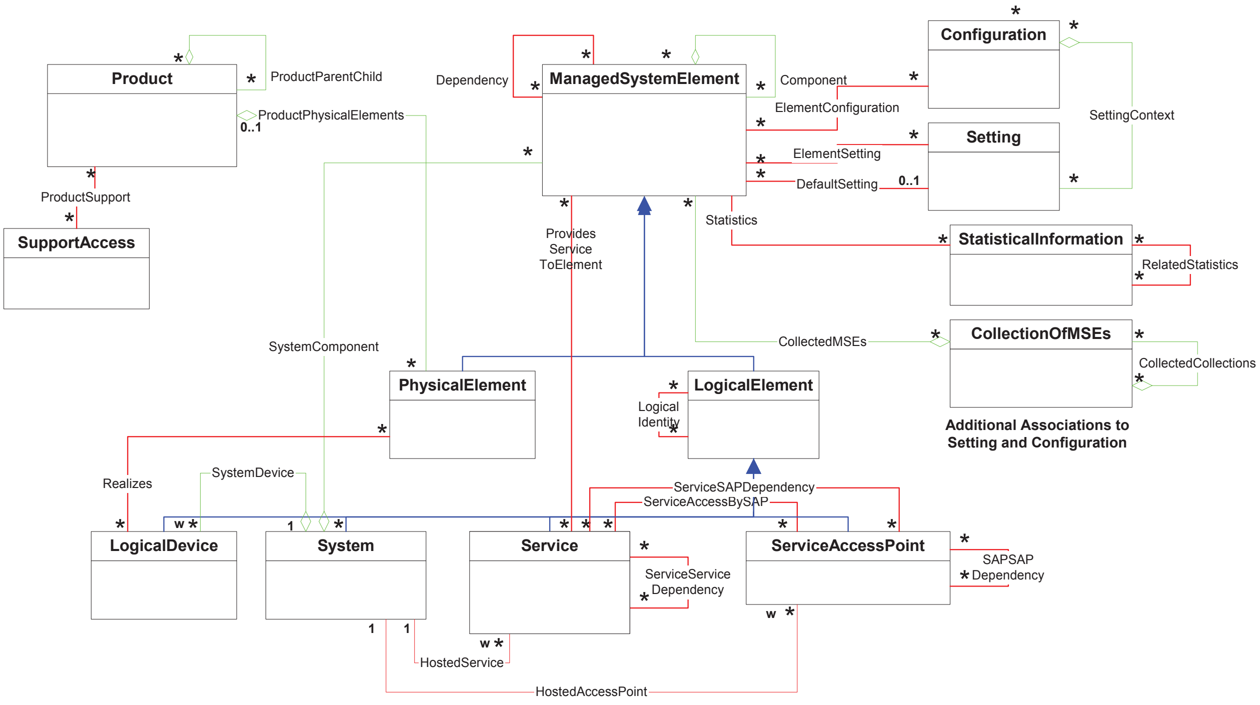


Figure 29: ITI CIM Core

6.3.2 Data Security

The data security domain deals with modelling threats. Modelling threats identifies the data associated with a given threat, and when related to the IT infrastructure data provides a view to system administrators of the impact of a threat on the system.

An example of a data security model is shown in Figure 30. This model highlights the elements of a security incident. Additional information on this model can be found at <http://www.cert.org/research/JHThesis/Start.html>.

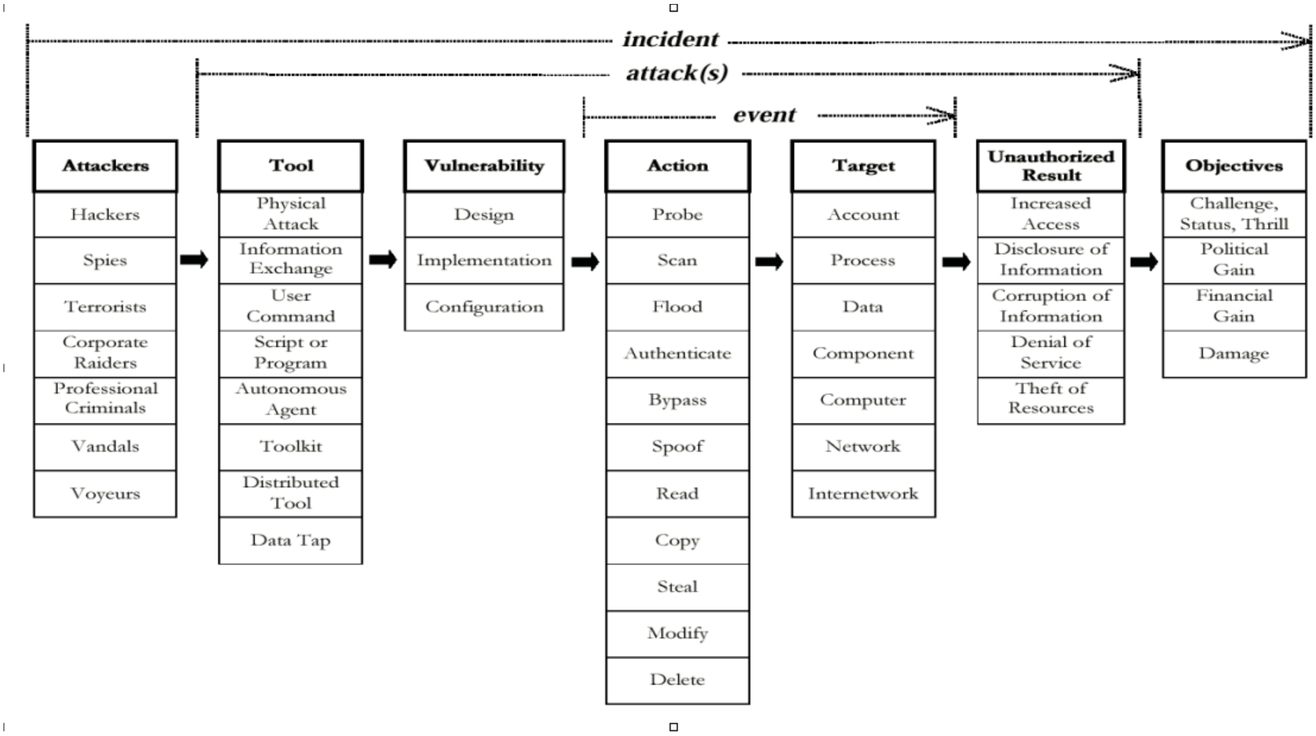


Figure 30: Howard's Model

6.3.3 Operational

Finally, there is the operational model. In reality, each and every C4ISR system implements its own data model, however some standards do exist. The C2IEDM is a NATO standard data model that has been developed to identify a common data structure to be used for command and control (C2) data exchange. The C2 domain is vast and conceivably could encompass the other two model types previously presented. For the purposes of the JNDMS, the focus is on the operational data and linking it to the other data models previously presented. A subset of the C2IEDM is illustrated in Figure 31: C2IEDM – Operational View.

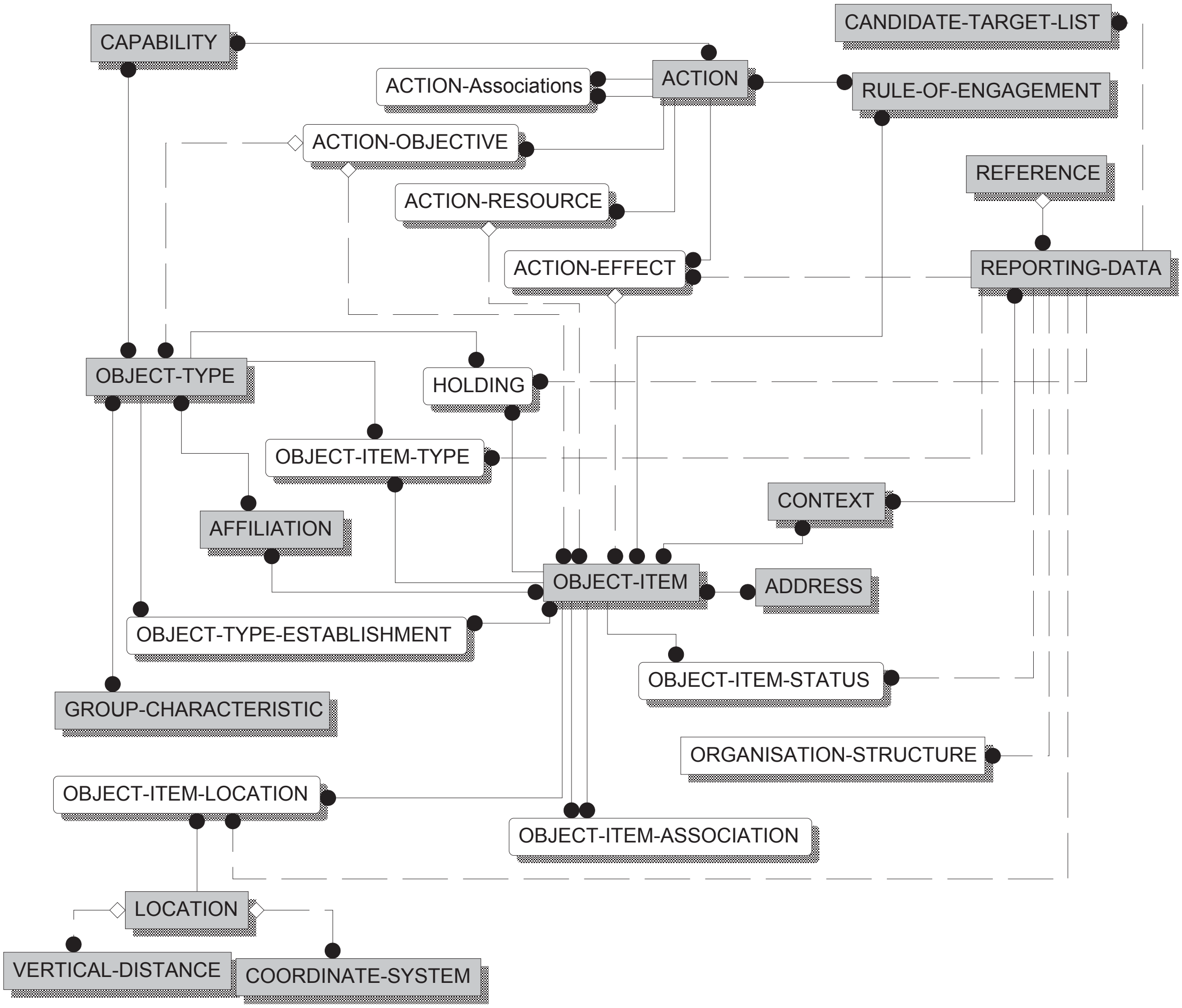


Figure 31: C2IEDM – Operational View

6.3.4 Combining the Models

The area in which the JNDMS truly makes progress is in relating all these models together. By relating the data from all three domains, along with temporal attributes, Commanders are able to identify the real world impact of the various threats. Armed with this knowledge, CND resources can be applied and strategies developed, based upon priorities with an understanding of the impact of a potential action or inaction.

Some initial modelling has been performed as is illustrated in Figure 32: IAT Model, but the task is to progress this model. There are several fundamental questions that need to be answered in order to develop the correct model, as well as sorting out a fully detailed data model. This is the goal of the JNDMS Data Warehouse.

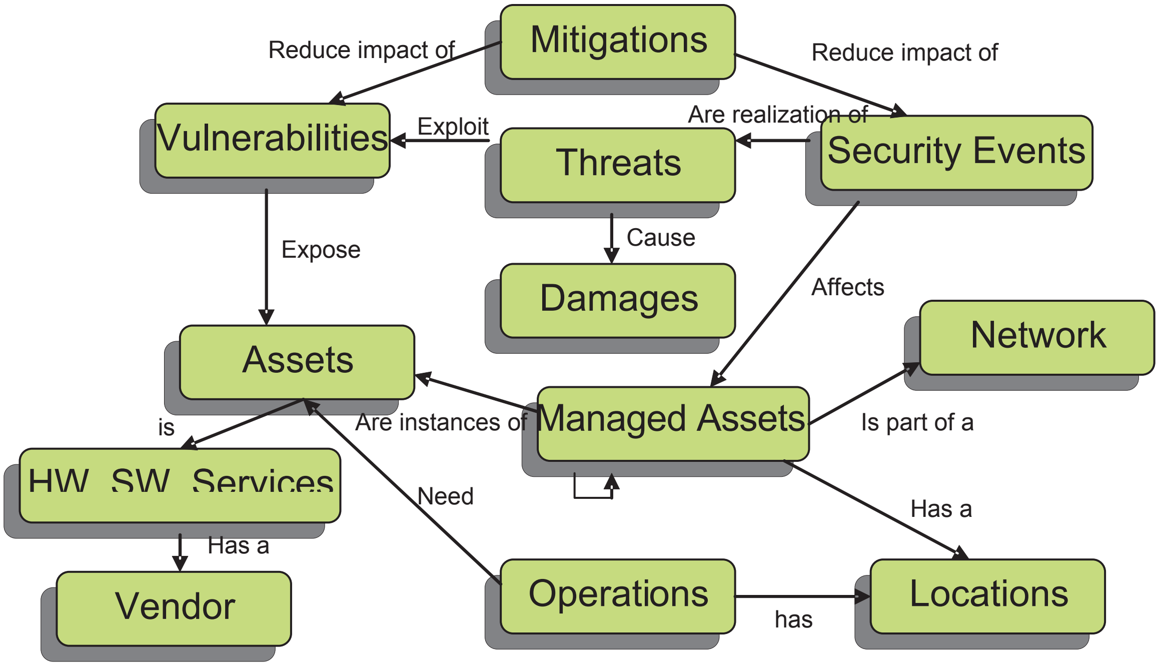


Figure 32: IAT Model

6.4 Database Replication

The JNDMS database employs replication to accomplish two goals. The first goal of replication is for back-up and recovery purposes. Back-up and recovery is important to protect the data itself but also the time and resources consumed to develop the data. The Oracle RDBMS has several powerful back-up and recovery facilities including hot back-ups, incremental back-ups, full back-ups, file system based backups, database exports and more.

The second goal of data replication is to support multiple JNDMS instances within a single IT infrastructure. The shear volume of data that the JNDMS must process limits the scope of the infrastructure it can support. The solution is to allow the processing and by extension the data, to be distributed amongst multiple JNDMS instances.

The JNDMS data can be distributed to support two different distribution structures. A peer-to-peer structure would simply divide the workload based upon some criteria (data) that is not shared. For example, JNDMS' could be assigned to monitor specific portions of the network. In those cases, the IT infrastructure data would not be replicated from instance to instance but rather distributed amongst the instances.

A hierarchy structure could also be supported where an instance of JNDMS would summarize its findings and report the summarized data to a higher level JNDMS. In this model, a lower level JNDMS becomes a “sensor” in the same fashion as the other sensors employed on the network and report to a JNDMS. This type of structure would require a different replication/distribution scheme from the one required for a peer-to-peer structure.

Finally, the two structures could be combined with peers dividing the workload at the lower levels and then each reporting to a higher node in the hierarchy.

The requirements for database replication are further refined during Phase 1 requirements analysis.

6.5 Database Size

Table 6 shows the size estimates for each database table. When creating the size estimates, the following assumptions were made:

- Each table stores 1 month (30 days) worth of records.

The following would be an assumed size of the network for sizing purposes:

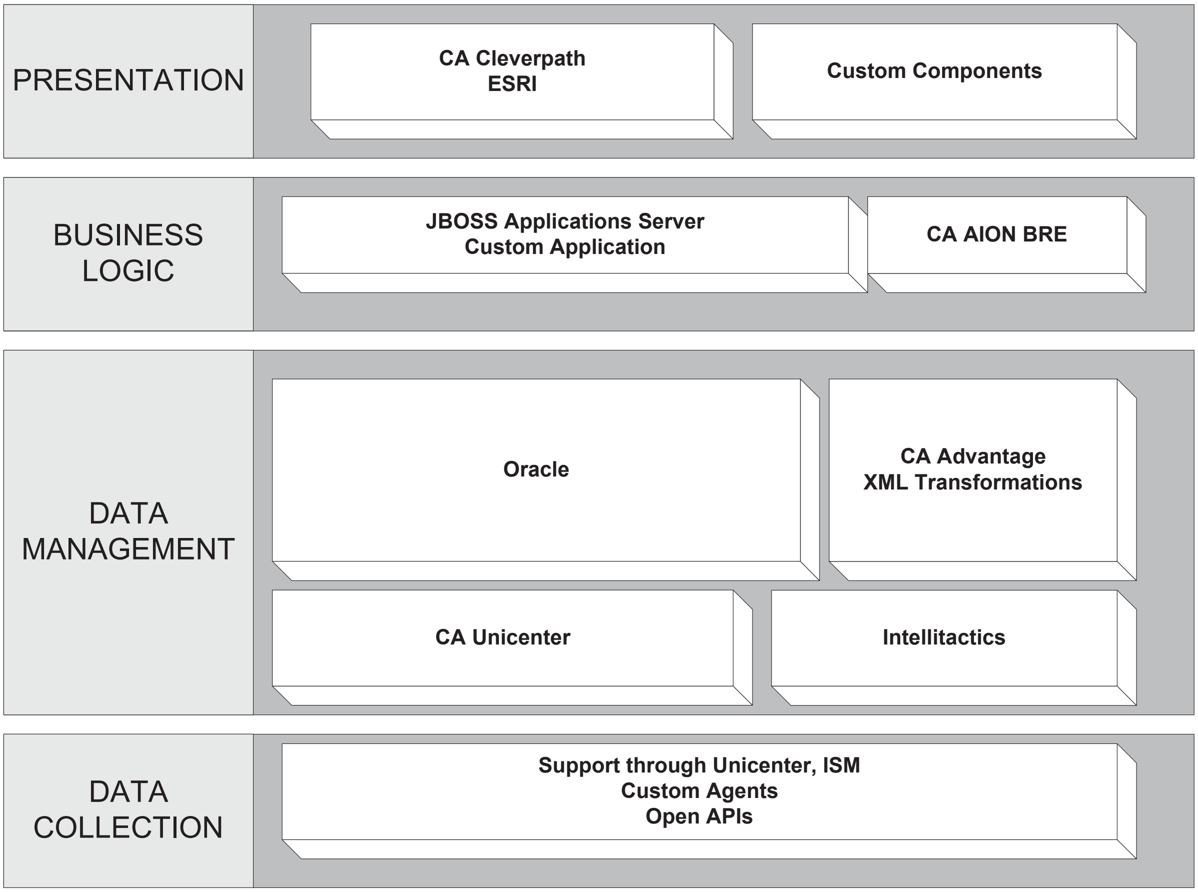
Table 6: Database Size Estimates

Entity	Number	Simulated Data	Record Size (kB)	Record Size (B)	Estimated Size (kB)	Estimated Size (kB) (Simulated)
Hardware Assets	75,000	5200	7	256	525000	1300
Software Assets	350,000	206,000	7	256	2450000	51500
Products	100,000	40,000	1	100	100000	3906
Events	3,000	19	10	300	30000	6
Operation Data	30	7	100	500	3000	3
Security Data	50,000	1400	15	500	750000	684
History / Admin	100,000	1700000	1	75	100000	124512
Relationships / Misc	1,000,000	425000	0.5	100	500000	41504

Per JNDMS node allocation of 130 GB database is fairly large, especially given the number of transactions per second. During the implementation phases, database size and performance is monitored to ensure acceptable database performance is achieved.

7 Adaptation to Technology Trends

The nine components that were identified in section 1 align with discrete areas of technology that are implemented in the JNDMS. For each of these technology areas, we have developed a strategy for the type of technology, the implementation approach and the type of tools required for implementing the technologies. Tools that we recommend for those components are summarized in Figure 33.



PRESENTATION	CA Cleverpath ESRI
	Custom Components
BUSINESS LOGIC	JBOSS Applications Server Custom Application
	CA AION BRE
DATA MANAGEMENT	Oracle
	CA Advantage XML Transformations
	CA Unicenter
	Intellitactics
DATA COLLECTION	Support through Unicenter, ISM Custom Agents Open APIs

Figure 33: Recommended Tools for the Architectural Components

MDA has identified tools that are recommended for implementation of each of the nine components of the architecture. This diagram shows how the tools interact using the same layout as we show for the interaction between the components. The reasons for choosing these tools within each mature or emerging technology area are discussed in this section.

MDA's strategy for the technologies within the nine components proposed for the JNDMS is to have an architecture that is flexible enough to implement either mature or emerging technologies within each component. We have identified this mixture for each component and we propose different reasons for recommending the mix of mature and emerging technologies within each component. These reasons are as follows:

System Inputs

- The success of the JNDMS depends completely on the quality and reliability of the inputs.
- Furthermore, the purpose of the research and development (R&D) to be conducted in the JNDMS focuses on information management, data reduction, decision making and reporting.
- **Conclusion**: These components should use mature technologies and COTS products integrated into the JNDMS architecture because they form the underlying infrastructure behind the TD concept. Custom development only done to accommodate non-standard interfaces. MDA is recommending the eTrust tool from CA for this component.

EIM and SIM

- As with the previous two components, the EIM and the SIM deal with the incoming data stream that provide the source for the data reduction and decision making processes. As a result, it is imperative to have reliable, proven tools that are dedicated for the purposes of the EIM and the SIM.
- **Conclusion:** These components should use mature technologies and COTS products integrated into the JNDMS architecture. As with the data inputs components, custom development will is only done to accommodate non-standard interfaces. MDA is recommending the use of ISM from Intellitactics for this component.

Data Transformation

- Data transformation is a process that must correctly merge sets of data together and store them in the appropriate formats and representations. The keys to data transformation are the flexibility of the transformation tool and the performance to allow the throughput of large amounts of data.
- **Conclusion**: This is a technology area where emerging technologies could be considered to evaluate maximization of capabilities and throughput. While the technology area of data transformation and merging of network intrusion detection data in real-time or near-real-time can be considered to be emerging, the CA data transformer tool is identified as an existing leader for this exact purpose. It is in use today in similar applications, which is why it is recommended by MDA for the JNDMS. We feel that this tool is a significant capability that adds value to an emerging technology area within network intrusion detection.

Data Warehousing

- Without the use of a commercial, robust tool for data warehousing, there would be a significant risk of loss of data integrity. Data warehousing technologies have been mature for decades.
- **Conclusion:** The data warehouse must be as robust as possible, which is why we recommend the use of the RDBMS technology area using Oracle as the underlying tool for the data warehouse.

System Services

- The system services make use of J2EE technology with a COTS application server. This component allows business level logic to be applied to inputs to provide data transformation and consistency checks, as well as providing application logic to complement the decision making of the DSS.
- **Conclusion.** This component is very specific to the JNDMS but leverages COTS to ensure infrastructure issues, such as authentication, programming support, etc, are maximized.

Decision Support System

- Decision system for network intrusion detection is an emerging area of R&D. The use of expert system technologies and inference engines are mature in other applications, but not in network intrusion detection systems. MDA has identified an industry leading COTS tool that has a full API and has the ability to support all the needs of the technology area for the DSS component.
- **Conclusion:** Within the emerging technology area of a DSS for network intrusion detection, we feel that there is a leading COTS tool (AION) available that can be applied to the DSS. The use of this strong and widely used inference engine adda value to the DSS for the JNDMS.
- **The core of the DSS should be available without the use of the rules engine so that issues relating to testing and training the rule set can be mitigated. The internal state and decision making is based primarily within Java components with the option of involking the rules.**

Presentation, Visualization and Reporting

- Technologies for portals and Web-GIS are mature enough and pervasive enough that we don’t feel time would be well spent evaluating emerging tools for this component. It may be worthwhile to evaluate emerging standards, such as SensorML, when tools become available that make use of the standard.
- **Conclusion:** Sufficient tools area available to justify the recommendation to use mature technologies and COTS tools within those technologies (Oracle, Tomcat, Google Earth Plugin, Open Layers, Google’s Web Toolkit and Apache Web Server). SensorML is one technology area to keep a watch on for emerging tools and to evaluate them when they become available.

Situation Awareness Data Sharing

- While data sharing itself is not an emerging technology in any domain, the ability to share data in real-time between computer networks of different classifications is definitely an emerging technology area.
- **Conclusion:** MDA recommends mature technologies for the process of sharing the data. The recommended tool within this technology area is Advantage from CA. The emerging technology of management of data sharing between networks of different security classifications is recommended to use hardware appliances known as one-way diodes.

7.1 Potential COTS Products

Table 7 discusses products that MDA has identified for potential use for the JNDMS. We assess whether each tool is emerging or mature, and provide reasons for the ones that we recommend for the JNDMS.

Table 7: Identification of Technologies for the Solution Components

Technology	COTS/ Open Source/ Custom	Technology Area Mature or Emerging for JNDMS	Preferred for JNDMS	Reason
System Inputs				
CA eTrust	COTS	Mature	√	CA eTrust provides dynamic network discovery.
Java + Eclipse IDE	Custom	Emerging	√	Required for custom development for all non-standard interfaces. We use this to develop custom interfaces where existing COTS does not exist. Java allows a measure of machine independence for multi-platform compatibility. Also allows Java 2 Enterprise Edition (J2EE) compatibility with future DND direction.
Intellitactics Security Manager (ISM)	COTS	Mature	√	Market leader according to Gartner Research and in use at DRDC and DND. Personnel trained on use of this product.
Java + Eclipse IDE	Custom	Emerging	√	Required for custom development for all non-standard interfaces. We use this to develop custom interfaces where existing COTS does not exist. Java allows a measure of machine independence for multi-platform compatibility. Also allows J2EE compatibility with future DND direction.
Lumeta's IPSonar	COTS	Mature		Industry leader, very competitive with Intellitactics. Some unique views of the network space. Not in use at DRDC.

Technology	COTS/ Open Source/ Custom	Technology Area Mature or Emerging for JNDMS	Preferred for JNDMS	Reason
OpenNMS	Open Source	Mature		Inexpensive to purchase, expensive to maintain, unknown stability, uncertain future.
Enterprise Infrastructure Management				
CA Unicenter	COTS	Mature	√	Enterprise wide management system with huge user base and customer support. Large number of installations. CA is mature company with wide product line that integrates with Unicenter. Costs are competitive with other large vendors like IBM and HP for the small DRDC research LAN.
Axios Assyst	COTS	Mature		This is an ITIL support tool that is being evaluated by DND. This is a likely candidate for eventual transition.
Ipswitch What's Up Gold	COTS	Mature		This is a tool that is being used by DND for network views and fault monitoring. This is a likely candidate for eventual transition.
Centennial Discovery	COTS	Mature	√	This provides software inventory.
Microsoft MOM	COTS	Mature		Emerging technology, Microsoft specific so works well for the TD but not a DND wide rollout. Limited API. Will improve over time. Can be used as substitute for Unicenter if TD is limited to Microsoft products.
Security Information Management				
Intellitactics Security Manager (ISM)	COTS	Mature	√	Capable, industry leader. Excellent scalability and speed. DND has already made a considerable investment in this product as the department's SIM solution, including training.
nCircle IP360	COTS	Mature		This is a vulnerability management product that is being used by DND. Its use within DND may be extended in the future. This is a likely candidate for transition.
eTrust	COTS	Mature	√	Hardware appliance used for SIM. Functions include network discovery and vulnerability assessment tools. A part of the eTrust SIM is a hardware appliance that promiscuously monitors in all seven layers of the OSI model for network discovery through traffic analysis.
Data Transformation				
CA Advantage Data Transformer	COTS	Emerging	√	Proven, low cost, and effective technology that is used widely in the industry.

Technology	COTS/ Open Source/ Custom	Technology Area Mature or Emerging for JNDMS	Preferred for JNDMS	Reason
Erwin	COTS	Mature		Generic data modelling tool that can extract database schemas from one database and translate them for use on another. It's in wide use and many of the common schemas for interoperability are described using this tool.
Apache iBATIS	Open Source	Mature	√	
Sparx Enterprise Architect	COTS	Mature	√	Less expensive UML tool than industry leader Rational Rose, but experience has shown it to be equally capable. Forward and reverse engineering capabilities are appropriate for JNDMS.
Database Warehousing				
Oracle	COTS	Mature	√	Oracle is a robust, enterprise wide RDBMS. In use throughout government agencies. Scalability and performance have few equals.
Ingres	Open Source	Emerging		Ingres is a low-cost, low maintenance alternative to other enterprise RDBMS. Leverages open-source development. It is an extremely efficient database, but may be lacking some of the scalability or security features of true enterprise databases.
Decision Support System / Business Logic				
AION Inference Engine	COTS	Emerging	√	Industry leading DSS. Includes capabilities for forward and backward chaining, auto-rules generation and other Artificial Intelligence (AI) capabilities. Full API for integration with other applications. Wide user base.
ILOG JRules Business Rule Management System	COTS	Emerging		In use at DRDC and easy integration into both Java 2 Standard Edition (J2SE) and J2EE environments. Cheaper costs, less capability than AION. May serve as suitable substitute for low volume rules.
Apache Tomcat	Open source	Mature	√	This applicaton server is part of the Apache foundation and forms the basis of many other open source offerings.
Weblogic	COTS	Mature		This is an industry leading application server from BEA.
Websphere	COTS	Mature		This is an industry leading application server from IBM.
JBoss	Open Source	Mature		This open source offering leverages the foundations of the Apache Tomcat application server.

Technology	COTS/ Open Source/ Custom	Technology Area Mature or Emerging for JNDMS	Preferred for JNDMS	Reason
Presentation Visualization and Alerting				
Liferay Portal	Open Source	Mature		The Liferay Portal leverages the Java Community Standards to provide a standard based portal solution that can run on multiple Java Application Servers.
Visualization - Oracle	COTS	Mature		Rapid visualization of data. Industry leader according to Gartner. DND and DRDC have licenses for multiple instances.
Portal—CA Cleverpath	COTS	Mature		Cleverpath is the front-end content and dashboard tool for the enterprise management system and much of the mapping. Wide user base and extensive support makes it suitable for use.
Visualization—ESRI Arc GIS	COTS	Mature		Arc GIS is an industry leading GIS server. Software is integrated with CA Unicenter enterprise management systems. Licensing costs are minimal for development. Full development environment included.
Apache Web Server	Open Source	Mature		Apache is an example of an open-source multi-platform web server in wide use. It supports SSL and has built-in authentication. It can be integrated with Java servlet engines, such as Tomcat, and has native support for the large suite of tools and technologies available from the Apache foundation.
Google Web Toolkit	COTS/ Open Source	Emerging	√	This provides a rich development environment for web applications.
Google Earth Plugin	COTS/Open Source	Emerging	√	This provides 3d mapping.
Google Maps API	COTS/Open Source	Mature	√	This provides 2d mapping.
Open Layers	Open Source	Emeging	√	This provided 2d mapping.
Microsoft Internet Information Server (IIS)	COTS	Mature		IIS is an example of a mature COTS web system. The system includes advanced proprietary operating system interfaces that prohibit port to alternative operating systems, such as Linux.
Situation Awareness Data Sharing				
One-way Diodes	COTS	Emerging	√	Hardware appliance used to insulate transmission across network security levels. Policies are still being identified on proper use and sources of this hardware.

Technology	COTS/ Open Source/ Custom	Technology Area Mature or Emerging for JNDMS	Preferred for JNDMS	Reason
CA Advantage	COTS	Mature		Proven, low cost, and effective technology that used widely in the industry.
Java + Eclipse IDE	Custom	Emerging	√	Required for custom development for all non-standard interfaces. We use this to develop custom interfaces where existing COTS does not exist. Java allows a measure of machine independence for multi-platform compatibility. Also allows J2EE compatibility with future DND direction.

7.2 Potential COTS Hardware

This section describes both the hardware and software that the JNDMS IPT is recommending for the JNDMS, and provides a mapping between software components and the hardware on which they reside. The end of this section contains two parts list tables that provide complete details on each of the software and hardware products that comprise the proposed solution.

The hardware proposed for JNDMS environment of the JNDMS is mature, low-risk COTS Intel-based computers and networking hardware, arranged as shown in Figure 34. All of the Intel computers have similar hardware configurations, permitting different distributions of software during experiments. Similar hardware configurations enable simple content replication using disk-imaging software, allowing units to be easily recovered in the event of failure. The use of mature COTS Intel computers simplifies the development, maintenance and eventual deployment of the JNDMS.

Figure 34 shows the configuration of the four computers, one network switch and a VPN router that are proposed for each JNDMS lab setup. A fifth computer supports the Halifax lab for development. The five computers are dedicated to:

1. The security management workstation runs the Intellitactics Security Management software and the Nessus server.
2. Enterprise Management Software and Web Portal User Interface.
3. JNDMS core components of Data Transformation, Data Warehouse and Decision Support System.
4. The Network Simulation and Development environment supports virtual machines that can be used as a base development environment as well as multiple operating systems for network traffic and host simulation.
5. Documentation and development support for MDA Halifax office JNDMS Program Generation Center (PGC).

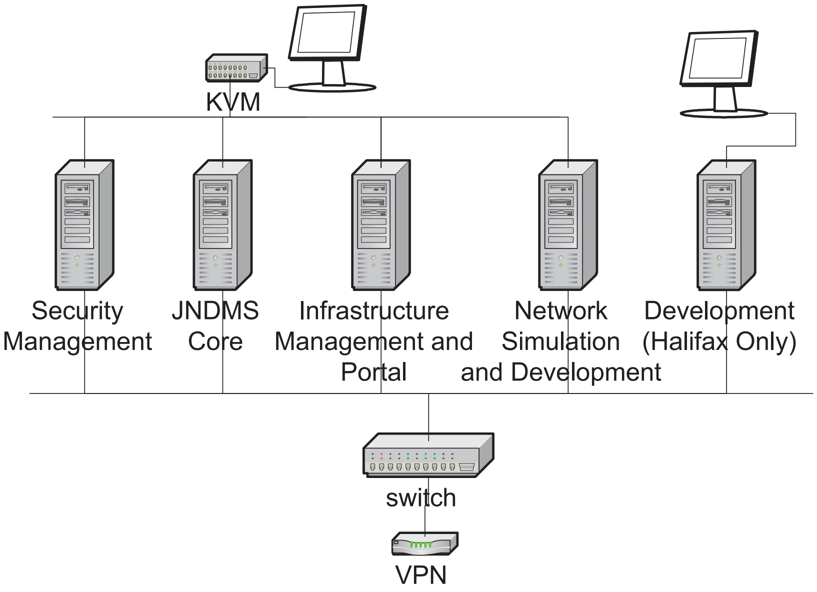

KVM
Security Management
JNDMS Core
Infrastructure Management and Portal
Network Simulation and Development
Development (Halifax Only)
switch
VPN

Figure 34: Hardware Environment of the JNDMS

The JNDMS uses a low-risk COTS hardware environment to simplify the development, maintenance and eventual deployment of the JNDMS.

The configuration of the workstations, the use of virtual environments and the applications installed within each environment is discussed in the JNDMS Design Document (A-5).

ANNEX A – ALLOCATED REQUIREMENTS

Table 8 shows the current requirements that have been extracted from the RFP, the software functional requirements and additional meetings. The table lists these requirements, the proposed method to meet the requirement and what CSC meets the requirement. The following requirements represent the functional requirements at the time of this document and further refinement of these requirements is addressed in the System Requirements Specification and subsequent releases of this document.

Table 8: Functional Compliance Matrix

Functional Requirement	ADD Para
The JNDMS shall provide situational awareness (SA) for Computer Network Defense (CND) through the fusion of Military Operations, IT infrastructure, Security events, Vulnerability, and Safeguards datasets. The JNDMS shall capture, store, process, analyse and present data from these five information domains.	5
The JNDMS shall capture Security Events Data. This function refers to the following sub-functions: acquiring, pre-processing and storing security events data.	5.1, 5.3, 5.4, 5.5, 5.6
Acquiring security events data: The JNDMS shall acquire security events data, such as logs, alerts, system events and formatted reports, from various sources. These sources include network equipments, tools and repositories such as firewalls, IDS/IPS, virus scanner, incident ticketing tools, intelligence community reports and other contextual information reports.	5.3
Pre-processing security events data: The JNDMS shall pre-process security events data so that only “clean” datasets are stored and used for subsequent analysis within the JNDMS. This includes functions such as filtering, aggregating, de-conflicting, consolidating, and normalizing to a common, complete and consistent format (ex: CIDF, IDWG’s Intrusion Detection Message Exchange Format (IDMEF), IODEF), etc.	5.4, 5.6
Storing the security events data: The JNDMS shall write the security events data to the JNDMS database for storage and analysis by subsequent processing functionalities. The data shall be stored with proper association to source and context within the JNDMS data model.	5.5
The JNDMS shall capture military operations data. This function refers to the following sub-functions: acquiring Military Operations data, pre-processing this data, and storing this data.	5.1, 5.4, 5.5, 5.6

Functional Requirement	ADD Para
Acquiring Military Operations Data: The JNDMS shall acquire military operations data such as the name of the operations, locations involved, units and main assets involved, schedule, required IT services and their importance to the operation. The JNDMS shall be able to acquire this data from other data repositories, such as the operational database (ODB) using the C2IEDM format.	5.1
Pre-processing Military Operations Data: The JNDMS shall pre-process the acquired military operation datasets before storage, to assure formatting and content is suited for subsequent JNDMS analysis functionalities. This includes functions such as filtering, aggregating, de-conflicting, and normalizing to the JNDMS data model every data records imported from the operational databases or other sources.	5.4, 5.6
Storing Military Operations Data: The JNDMS shall write the military operations data to the JNDMS database for storage and subsequent processing. The data shall be stored with proper association to source, context and time within the JNDMS data model.	5.5
The JNDMS shall capture IT infrastructure data. This function refers to the following sub-functions: acquiring IT Infrastructure data, pre-processing this data, and writing the IT Infrastructure data to the JNDMS database.	5.1, 5.2, 5.4, 5.5, 5.6
Acquiring IT Infrastructure Data: The JNDMS shall be able to acquire complete IT infrastructure topology and configuration information, including layer 1 to layer 7 assets from the OSI model. The topology and configuration shall include information such as the physical and logical connections between network assets, their physical and logical interdependencies, functions, redundancies, etc. The JNDMS shall be able to acquire this information from various sources such as network management tools exports, configuration management databases, assets inventory, circuits and cabling datasets/diagrams, network analysis and design tools, etc. The JNDMS shall also be able to acquire this data across multiple networks of different classification level (refer to security constraints section of this document).	5.1
Acquiring IT Infrastructure Assets Geospatial Data: The JNDMS shall provide means to acquire network assets location and other geospatial attributes. Each network asset (ex: a software application) can be associated to a piece of equipment which must have a physical location. The JNDMS shall link network assets to a geographic reference of appropriate precision to support situational awareness processes.	5.1, 5.2

Functional Requirement	ADD Para
IT Infrastructure Discovery: The JNDMS shall be able to collect and capture dynamically (also known as "network discovery") pertinent IT infrastructure data such as all active hosts, their identification and status, the logical connections, the actual bandwidth usage, the active ports and services, etc.	5.1, 5.2
Pre-processing IT Infrastructure Data: The JNDMS shall pre-process IT Infrastructure data acquired from sources such as network monitoring agents, network discovery capabilities, host-based and centralized static network management repositories in order to assure formatting and content is suited for subsequent JNDMS analysis functionalities. This includes functions such as filtering, aggregating, deconflicting, and normalizing to the JNDMS data model every data records acquired.	5.4, 5.6
Storing IT Infrastructure Data: The JNDMS shall write the pre-processed IT Infrastructure Data to the JNDMS database for storage and subsequent processing. The data shall be stored with proper association to source, context and time within the JNDMS data model.	5.5
The JNDMS shall capture Vulnerability and Exploit Data. This function refers to the following sub-functions: acquiring Vulnerability and Exploit data, pre-processing this data and writing it to the JNDMS database.	5.1, 5.2, 5.4, 5.5, 5.6
Acquiring Vulnerability Data: The JNDMS shall acquire data from various sources of vulnerability information (e.g., application vulnerabilities, database vulnerabilities, operating system vulnerabilities) such as Nessus Vulnerability Scan results, TRAs, Vulnerability reports from security stakeholders websites (CVE, Sequnia, Bugtrack, etc), vulnerability tracking/ticketing tools, etc. The vulnerabilities acquired shall not only include cyber-space related vulnerabilities but physical/geo-spatial vulnerabilities as well. These vulnerabilities may include no access control to server rooms, absence of UPS, limited weather protection of equipment shelter etc. This vulnerability data may be identified by manual processes such as TRA and reside in static databases.	5.1, 5.2
Acquiring Exploit Data: The JNDMS shall acquire exploit data, such as the status of availability of exploits, methods, popularity, references, and other relevant attributes. The JNDMS shall acquire not only cyber-space related exploits, such as malicious codes, but also physical/geospatial exploits. These exploits may include physical destruction of equipment, or communication channel by external agents such as sun storms, weather, fire, human actions, etc.	5.1

Functional Requirement	ADD Para
Acquiring Vulnerability and Exploit Interrelationship Data: The JNDMS shall acquire the data required to identify the relationships between relevant vulnerabilities, exploits and the applicable systems and system components of DND IT infrastructure.	5.1
Pre-processing Vulnerability and Exploit Data: The JNDMS shall pre-process the acquired Vulnerability and Exploit datasets before storage, to assure formatting and content is suited for subsequent JNDMS analysis functionalities. This includes functions such as filtering, aggregating, de-conflicting, and normalizing to the JNDMS data model every data records acquired.	5.4, 5.6
Storing Vulnerability and Exploit Data: The JNDMS shall write the pre-processed Vulnerability and Exploit Data to the JNDMS database for storage and subsequent processing. The data shall be stored with proper association to source, context and time within the JNDMS data model.	5.5
The JNDMS shall capture IT Infrastructure Safeguards data. This function refers to the following sub-functions: acquiring IT Infrastructure Safeguards data, preprocessing this data, and writing it to the JNDMS database.	5.1, 5.2, 5.5, 5.5, 5.6
Acquiring Safeguard Data: The JNDMS shall acquire Safeguard Data of systems and system components of the IT Infrastructure. These safeguards include detailed configuration items such as Password strength, firewall rules, encryption devices or services, redundant IT services, backups and other tools/methods resulting from security policy implementation.	5.1
Pre-processing Safeguard Data: The JNDMS shall pre-process the acquired Safeguard datasets before storage, to assure formatting and content is suited for subsequent JNDMS analysis functionalities. This includes functions such as filtering, aggregating, de-conflicting, and normalizing to the JNDMS data model every data records acquired.	5.4, 5.6
Storing Safeguard Data: The JNDMS shall write the pre-processed Safeguard Data to the JNDMS database for storage and subsequent processing. The data shall be stored with proper association to source, context and time within the JNDMS data model.	5.5

Functional Requirement	ADD Para
The JNDMS shall capture inter-relationships between Security Events, Military Operations, IT Infrastructure, Vulnerabilities and safeguards. This function refers to the following sub-functions: analysing datasets from the 5 information domains (Operations, Infrastructure, Vulnerability, Safeguards, Events) identifying interrelationships between these 5 information domains, identifying geospatial, connectivity and logical inter-relationships, normalising these inter-relationships, deconflicting these inter-relationships, consolidating these inter-relationships and writing them to the JNDMS database.	5.4, 5.5, 5.6, 5.7
The JNDMS shall assess the Defensive Posture of the IT infrastructure. This function refers to the following sub-functions: analysing the information from datasets, identifying defensive components from the five SA for CND information domains (Operations, Infrastructure, Vulnerability, Safeguards, Events), pre-processing defensive posture components, and writing Defensive Posture attributes to the JNDMS database.	5.7
The JNDMS shall fuse information from the five SA for CND domains (Operations, Infrastructure, Vulnerability, Safeguards, Events) to recognize incident affecting the IT infrastructure and correlate these incidents together. This function refers to the following sub-functions: identifying incidents through the analysis of dataset from the 5 information domains (Operations, Infrastructure, Vulnerability, Safeguards, Events), filtering identified incidents, correlating identified incidents, and writing incidents to the JNDMS database.	5.7
Identify Incidents: The JNDMS shall identify incidents using fusion and user modifiable rules and thresholds applied over the five SA for CND information domains (Operations, Infrastructure, Vulnerability, Safeguards, Events). The JNDMS shall also identify incidents by comparing static and dynamic (network discovery) IT Infrastructure Data and identifying discrepancies. The JNDMS shall also apply metarules to extend basic rules used by Security Events feeder systems such as IDS.	5.7
Correlate Incidents: The JNDMS shall consider new incidents, archived incidents, and shared incidents from other/external organisations in order to identify trends, discover hidden incidents and previously undetected situational patterns, using, when methods such as clustering, association, rule abduction, statistical analysis, deviation analysis, etc.	5.7
Filter Incidents: The JNDMS shall filter identified incidents which represent exceptions and exempt them from further processing. As an example, the system may have a known misconfiguration that results in a known set of alerts. As these alerts have already been processed, and the cause is known, there is no need to process them again.	5.7

Functional Requirement	ADD Para
Store Incident Data: The JNDMS shall store incidents in the JNDMS database. The JNDMS shall assure that incident data is stored with accurate time-stamp and integrity verification.	5.7
Perform near real-time Incident Recognition: The JNDMS shall all incident recognition functions in near real-time to support other JNDMS features and functionalities. Near real-time performance is discussed the quality attributes of the JNDMS (section 11).	5.7
The JNDMS shall perform severity assessment of every network incident identified using SA for CND data and information, such as Incident attributes, the Defensive Posture and the contextual information from the 5 domains (Operations, Infrastructure, Vulnerability, Safeguards, Events). This function refers to the following sub-functions:), assessing damages and their operational relevance, assessing the operational risk associated to incidents as a function of time, assessing incident severity, assessing overall situation and rolled-up severity, and writing incidents severity assessment attributes to the JNDMS database.	5.7
Assess Incident Damages: The JNDMS shall assess the damages caused, or potentially caused by each incident. The JNDMS shall consider the various types of damage, such as availability, confidentiality and integrity for this assessment. The JNDMS shall also consider every interrelationship between IT Infrastructure assets/services to identify those affected and their respective value for operations.	5.7
Assess Risk of Incidents: The JNDMS shall assess the risk of each incident. The JNDMS shall take into account the probability of damage associated with some incident types such as malicious codes and attacks, in order to assess risk as a function of time. The JNDMS shall consider attributes and information which influence the probability of realisation of the full impact associated with an incident. Some of these attributes and information include the Defensive Posture, the time before a preventive action is taken, the expected time to recovery, the spreading rate of a malicious code, etc.	5.7
Assess Incident Severity: The JNDMS shall assess Incident Severity through the analysis of damages, risk, and contextual information from the five information domains of SA for CND. The JNDMS shall make use of user-modifiable rules and thresholds to perform multi-attribute analysis of incident datasets. The JNDMS shall make use of a normalised severity scale meaningful to the JNDMS users. The JNDMS shall generate a severity value and supporting evidence statement.	5.7

Functional Requirement	ADD Para
Assess Rolled-up Severity: The JNDMS shall assess the rolled-up severity associated with the overall situation, including all on-going and forecasted events / incidents. The rolled-up severity assessment shall consist in values and supporting evidence statements.	5.7
Store Severity Assessment Information: The JNDMS shall store Severity Assessment Information in the JNDMS database. The JNDMS shall assure that Severity Assessment Information is stored with accurate time-stamp and integrity verification. The Severity Assessment Information shall be continuously updated. The JNDMS shall store history of incident severity values and rolled-up values.	5.7
The JNDMS shall store and manage SA for CND data. and make it accessible to the different data processing sub-systems. This function includes the following subfunctions: capturing dynamically all SA objects and their attributes, capturing all objects inter-relationships, maintaining accurate temporal references for every record, maintaining data integrity, providing backup and recovery capability, supporting access control mechanism such as authentication and encryption, maintaining accurate references of the source of data, supporting timely access to SA data and queries by all other JNDMS functions, supporting data total and partial replication with other databases.	5.4, 5.5, 5.6
Data Model: The JNDMS shall integrate data standards including Incident data such as those defined by the IODEF and IDMEF, the Military Operation data, such as defined in the C2IEDM, the IT infrastructure data, defined in standards such as the CIM, MIBs and other standard taxonomy/ontology, etc. The data model shall also support physical and logical links/interdependencies between objects.	5.4, 5.5, 5.6
Performance: The database solution shall be able to support data retrieval, data entry and data storage (size) performance required by feeder systems such as enterprise security management software and enterprise network management software. The JNDMS shall be able to store relevant datasets, and point to other data storage systems.	5.5
Temporal Database: The JNDMS shall offer temporal database features including support for temporal queries, precise timestamps of records, and mechanisms preventing the duplication, and loss, of records having conflicting timestamp.	5.5
Data Protection: The JNDMS database shall perform data integrity checks, data access control and data backups / duplication management. The JNDMS database shall support partial replication with peer systems and maintain “peer systems profile" and policies for data exchange privileges and mechanisms.	5.5

Functional Requirement	ADD Para
The JNDMS shall present the relevant data in a way that optimizes the user's situational awareness for computer network defence. This function includes the following sub-functions: capturing different user visualisation profiles, presenting inter-related incidents, impact assessment, defensive posture and the 5 information domains (Operations, Infrastructure, Vulnerability, Safeguards, Events) through a Geospatial Information System (GIS), presenting different logical inter-connectivity schematics/ diagram, deconflicting data views, decluttering data views, layering data views, exporting data views to different formats and projecting data views to the user.	5.8
Performance: The JNDMS views shall be updated in a near-real time fashion. Different level of information may have different refresh rates. The JNDMS shall provide the user with clues as to the general accuracy and "age" of the displayed data.	5.8
User-defined Views and Queries: The JNDMS shall support the creation of userdefined views and queries in support of SA for CND. These user preferences shall be stored in a user profile. The JNDMS shall provide an intuitive interface allowing the user for creating tailored data queries, such as spatial and temporal queries and re-use these queries as required.	5.8
Visual Correlation: The JNDMS shall provide through its user interface a mean to visually correlate complex datasets from the five SA for CDN information domains (Operations, Infrastructure, Vulnerability, Safeguards, Events). The JNDMS shall allow users to rapidly understand the defensive posture, the severity assessment and overall status of the IT infrastructure. The JNDMS shall make use of Geospatial map overlay, logical network graphs, data tables and other data presentation schemes, as required, in order to optimize users' experience. The JNDMS shall support visual correlation of network views as they evolve in time, using features such as "playback" and "play-forward".	5.8
User Interaction: The JNDMS shall allow the user the interact with the interface to accomplish specific tasks. The JNDMS shall allow for "drill-down" "drill-up" and "drill-across", or contextual navigation capabilities to the details of the data repositories. The JNDMS shall also provide ways for the users to override JNDMS Severity Assessment results and record the justification for the override. The JNDMS shall also support the user for the creation of new rules and change of existing rules and thresholds for report generation, incident recognition and severity assessment.	5.8

Functional Requirement	ADD Para
The JNDMS shall allow for sharing of Situation Awareness Data. This function include the following sub-function: managing the SA data recipient/provider permissions, assembling datasets for transmission, interpreting and storing received datasets, verifying transmission integrity, maintaining shared data logs with time, classification, content and recipient/provider information for each shared recordset.	5.9
Data Replication: The JNDMS shall support partial and complete replication of data between different JNDMS instances and other stakeholders' systems. The JNDMS shall also allow periodic synchronization of data (refresh) and maintain data ownership/source attributes.	5.9
Multi-Level Classification Data Exchange: The JNDMS shall be able to exchange data using one-way transfer media such as a data diode. This exchange shall be based on a data "push" approach from low classification level JNDMS instances to higher classification levels. The data collected and stored shall always reside on an instance of JNDMS itself residing at the same level of classification or higher. The data shall be tagged with all relevant classification information, such as the data source name, the level of classification and the caveat.	5.9
Profile-based data sharing: The JNDMS shall be able to adjust data sharing mechanisms based on recipient/provider's profile and based on data attributes, such as classification and direction (inbound Vs outbound). As an example, a coalition partner may only require that data pertaining to a given location be provided, whereas another instance of JNDMS will require total replication of the full database content.	5.9