# System requirements specification for the technology demonstration of the Joint Network Defence and Management System (JNDMS) Project

Prepared by:
Scott MacDonald
MacDonald Dettwiler and Associates Ltd.
Suite 60, 1000 Windmill Rd.
Dartmouth, NS  B3B 1L7

PWGSC Contract Number:
W7714-040875/001/SV
DID SD-001

Contract Scientific Authority:
Marc Gregoire (Contact Maxwell Dondo 613-998-2073)

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.

Contract Report Number DRDC-RDDC-2014-C95

DN0665: 28 NOVEMBER 2005
ISSUE 2/0: 17 JANUARY 2006

# SYSTEM REQUIREMENTS SPECIFICATION FOR THE TECHNOLOGY DEMONSTRATION OF THE JOINT NETWORK DEFENCE AND MANAGEMENT SYSTEM (JNDMS) PROJECT

CONTRACT NO. W7714-040875/001/SV

DID SD-001

PREPARED FOR:

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

PREPARED BY:

MACDONALD DETTWILER AND ASSOCIATES LTD.
SUITE 60, 1000 WINDMILL ROAD
DARTMOUTH NS  B3B 1L7

DN0665
Issue 2/0
17 January 2006

# DOCUMENT APPROVAL SHEET

# SYSTEM REQUIREMENTS SPECIFICATION FOR THE TECHNOLOGY DEMONSTRATION OF THE JOINT NETWORK DEFENCE AND MANAGEMENT SYSTEM (JNDMS) PROJECT

## CONTRACT NO. W7714-040875/001/SV

## DID SD-001

## MACDONALD DETTWILER AND ASSOCIATES LTD.

| | | |
|---|---|---|
| Scott MacDonald | | |
| Author | (Signature) | (Date) |
| Troy Kennedy | | |
| Quality Assurance | (Signature) | (Date) |
| John Moloney | | |
| Project Manager | (Signature) | (Date) |

# CHANGE RECORD

| Rev. # | Pages Affected | Description | Date of Issue |
|---|---|---|---|
| 1/0 | All | First Issue (Initial Release) | 28 Nov 05 |
| 2/0 | All | Second Issue | 17 Jan 06 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# 1 Purpose

The purpose of this document is to specify the JNDMS requirements and satisfy the Contract Data Requirements List (CDRL) 4/Data Item Description (DID) SD-001 deliverable as stated in Contract No. W7714-040875/001/SV.

This System Requirement Specification (SRS) represents a ‘live’ document with an initial release during phase 1 of the JNDMS Technology Demonstration (TD) followed by a Technical Review Meeting to complete the phase 1 requirements analysis. This document will be updated during each of the development cycles with the final version being delivered during phase 3.

# 2 Introduction

Military forces are becoming increasingly reliant on communications and computer-based networks to perform their operations. This is true for all phases of an operation, from strategic intelligence gathering and dissemination, operational planning, logistics support, command and control, to time-critical tactical sensing and decision-making in the field. Because networks underlie so many military activities, understanding the state of the required networks and maintaining their health is extremely important, particularly as the networks themselves become targets of potential adversaries. The network environment is being viewed today as another battlespace that must be controlled and defended.

The cyber domain can be presented as a battlefield using common military symbology. In this abstraction of the cyber-battlefield, the Computer Network Exploitation (CNE) and Computer Network Defence (CND) rectangles represent operational units, analogous to reconnaissance patrols and defensive position observation posts in traditional warfare. The protected regions are presented as cyber domains, but may also include physical network assets. The casualties suffered in this battlespace can undoubtedly translate into decreased operational capabilities for the entire defence organization.

In order to provide CND in this modern battlespace, one must maintain situational awareness (SA), analogously to other Command and Control (C2) activities in the land, airspace and sea elements. SA for CND can be seen as a process by which one perceives its network environment, as well as understands and continuously predicts the risk and its evolution in time and space. The primary purpose of SA for CND is the efficient defence of the Information Technology (IT) infrastructure and services, in support of military operations.

This implies that the information requirements for SA ought to include military operations and their dependencies on IT services. However, bringing SA for CND in the military operation context is a significant challenge, which must be addressed so that CND decisions take operational risk into consideration. Information requirements for SA for CND can be grouped into five information domains: Military Operations, IT Infrastructure and Services, Vulnerabilities and Exploits, Safeguards and Security Events. The integration and analysis of these domains provide decision makers with knowledge about the defensive posture of the networks and the severity assessment of network incidents.

The provision of SA for CND to the decision maker also involves the continuous processing of a very large volume of data, which is generated at a fast rate. In an organization such as the Department of National Defence (DND), there are a number of people and departments, both internal and external, involved in the capture and processing of the data relevant to SA for CND. This complexity adds to the challenge of building a system to provide SA for CND. The JNDMS TD Project (TDP) is an initiative of the Network Information Operations (NIO) Section at Defence R&D Canada - Ottawa (DRDC Ottawa) whose objective is to provide SA for CND.

# 3 Scope

This document is the SRS for the JNDMS TDP. This document provides the traceability of the initial requirements into the use case analysis, and forms the basis of the design work and will be used to provide test case traceability.

This document also forms the technical foundation for development of the JNDMS TD, which addresses the expressed needs of the Canadian Forces (CF) and the operational units involved CND. The JNDMS is focused on bringing to decision makers the right network information at the right time.

The JNDMS' goals are to:

- Provide commanders, network controllers and security analysts with an integrated computer network defence SA picture of the computer networks being used for military operations
- Support operation-centric computer network defence and network management
- Support sharing of network information among CF and international coalition partners to enhance the CF ability to identify network threats and support network defence within coalition operations

The JNDMS TDP will provide a fundamental step toward a comprehensive, near real-time, decision support system for integrated computer network defence and management.

# 4 JNDMS Use Cases

The JNDMS requirements are documented and maintained in a Requirements Traceability Matrix (RTM), as found in Annex A - Use Case Traceability, Annex B - Functional Requirements, and Annex C - Associated Requirement Traceability. Further elaboration of those requirements, and their inter-dependencies are held in a Unified Modeling Language (UML) Model. The UML Model allows -requirements to be represented as use cases and provides a powerful notation for documenting the requirements, as well as their relationship to one another. Requirements within the model are grouped into packages to allow management of complexity.

This requirements document will present the use cases and their relationship to the functional requirements. For a use case to be appropriately implemented all of the associated requirements must be met. The use case model must address all of the functional requirements to be complete.

## 4.1 Actors

The actors of the use cases are presented first to define the people systems and subsystems that will interact with the JNDMS. These actors may be external to the system to show how the system as a whole is used, or they may be internal to show how subsystems behave.

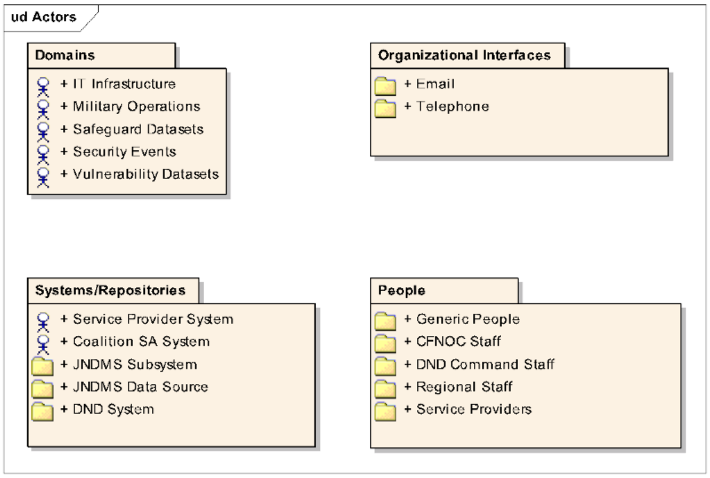


**Figure 1: Actors**

### 4.1.1 Domains

The domain actors in this section are derived from the five core domains of the input data sets. JNDMS is built on the fusion of these five domains and these actors represent the most general case of these data inputs.

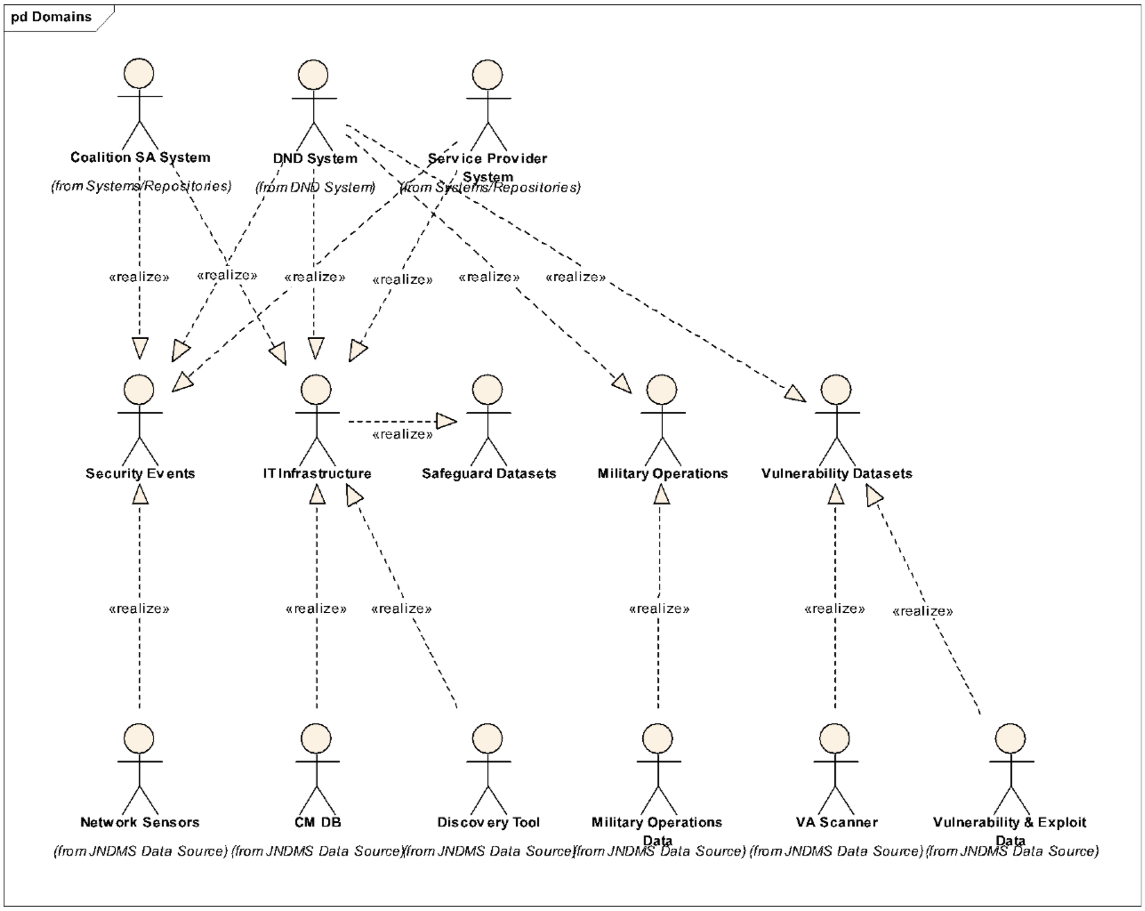


**Figure 2: Domains**

The actors in this section are derived from the five core domains of the input data sets.

## Actor: IT Infrastructure -

### Description:

The IT infrastructure includes the IT assets as well as their dependencies.

### Relationships:

| Source | Type | Target |
|---|---|---|
| IT Infrastructure | Realisation | Safeguard Datasets |
| Present Situational Awareness | UseCase | IT Infrastructure |
| CM DB | Realisation | IT Infrastructure |
| DND System | Realisation | IT Infrastructure |
| Coalition SA System | Realisation | IT Infrastructure |
| Service Provider System | Realisation | IT Infrastructure |
| Discovery Tool | Realisation | IT Infrastructure |

**Table 1: Relationships for IT Infrastructure**

## Actor: Military Operations -

### Description:

The military operations data must be able to describe key inputs of the operation including priorities and IT services required.

### Relationships:

| Source | Type | Target |
|---|---|---|
| Present Situational Awareness | UseCase | Military Operations |
| DND System | Realisation | Military Operations |
| Military Operations Data | Realisation | Military Operations |

**Table 2: Relationships for Military Operations**

## Actor: Safeguard Datasets -

### Description:

This data set represents the safeguards that have been applied to the assets.

### Relationships:

| Source | Type | Target |
|---|---|---|
| IT Infrastructure | Realisation | Safeguard Datasets |
| Present Situational Awareness | UseCase | Safeguard Datasets |

**Table 3: Relationships for Safeguard Datasets**

## Actor: Security Events -

### Description:

This is a generalization of any security event. The events can be network related, as collected by a security management tool, or could be information through email or manual entry.

### Relationships:

| Source | Type | Target |
|---|---|---|
| Service Provider System | Realisation | Security Events |
| Present Situational Awareness | UseCase | Security Events |
| Network Sensors | Realisation | Security Events |
| DND System | Realisation | Security Events |
| Coalition SA System | Realisation | Security Events |

**Table 4: Relationships for Security Events**

### Actor: Vulnerability Datasets -

**Description:**

These data sets represent the known vulnerabilities.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| Present Situational Awareness | UseCase | Vulnerability Datasets |
| DND System | Realisation | Vulnerability Datasets |
| VA Scanner | Realisation | Vulnerability Datasets |
| Vulnerability & Exploit Data | Realisation | Vulnerability Datasets |

**Table 5: Relationships for Vulnerability Datasets**

## 4.1.2 Organizational Interfaces

The organizational interfaces represent boundaries that cannot be easily automated. This may be in the form, for example of phone conversations between JNDMS users and external points of contact. System or organizational boundaries that can be automated are modeled in the software section of the actors. These may take the form of external systems with programming interfaces or databases.

Some of the interfaces modeled in this section may be software, such as email, that is managed through other software systems such as a trouble ticket system.

### 4.1.2.1 Email

This package contains the email interface.

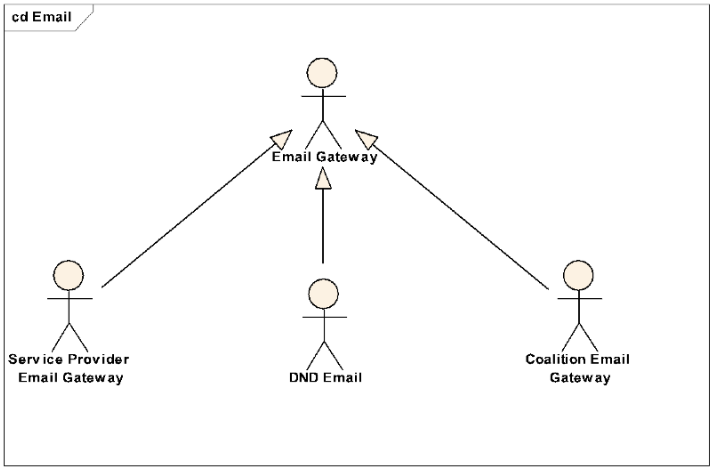


**Figure 3: Email**

This shows the relationships between email gateways.

### Actor: Email Gateway -

**Description:**

This represents a generalization of an email interface.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| Service Provider Email Gateway | Generalization | Email Gateway |
| DND Email | Generalization | Email Gateway |
| Coalition Email Gateway | Generalization | Email Gateway |

**Table 6: Relationships for Email Gateway**

## Actor: Coalition Email Gateway -

### Description:

Slightly higher classification email interface than unclassified Bell email. Less secure than DND internal email system. Used to communicate with coalition forces.

### Relationships:

| Source | Type | Target |
|---|---|---|
| Coalition Email Gateway | Generalization | Email Gateway |

**Table 7: Relationships for Coalition Email Gateway**

## Actor: DND Email -

### Description:

Internal DND email that may or may not traverse the 3 levels of security. Assumption is it is typed in at the appropriate level, or sent up using data diodes. There may be no means of sending email down to a lower security network except to manually transcribe or use sneaker net.

### Relationships:

| Source | Type | Target |
|---|---|---|
| DND Email | Generalization | Email Gateway |

**Table 8: Relationships for DND Email**

## Actor: Service Provider Email Gateway -

### Description:

Interface to external email. This is a specific gateway to a Service Provider that may or may not be tunnelled.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| Service Provider Email Gateway | Generalization | Email Gateway |
| Service Provider Email Gateway | Dependency | Service Interruption Coordinator |

**Table 9: Relationships for Service Provider Email Gateway**

### 4.1.2.2 Telephone

This package contains the telephone interface.

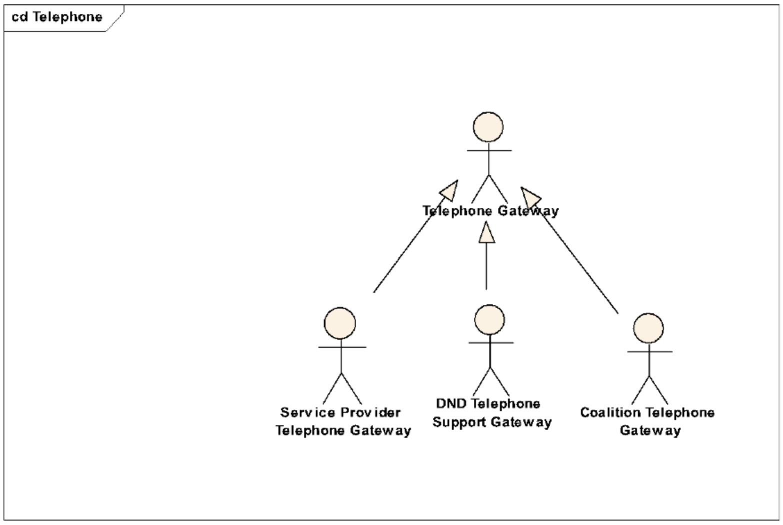

cd Telephone
Telephone Gateway
Service Provider Telephone Gateway
DND Telephone Support Gateway
Coalition Telephone Gateway

**Figure 4: Telephone**

This shows interfaces that rely primarily on phone.

## Actor: Telephone Gateway -

### Description:

This represents a generalization of a telephone interface.

### Relationships:

| Source | Type | Target |
|---|---|---|
| Service Provider Telephone Gateway | Generalization | Telephone Gateway |
| DND Telephone Support Gateway | Generalization | Telephone Gateway |
| Coalition Telephone Gateway | Generalization | Telephone Gateway |

**Table 10: Relationships for Telephone Gateway**

## Actor: Coalition Telephone Gateway -

### Description:

Trusted to a better degree than the Bell Telephone gateway, but less so than the DND telecom gateway.

### Relationships:

| Source | Type | Target |
|---|---|---|
| Coalition Telephone Gateway | Generalization | Telephone Gateway |

**Table 11: Relationships for Coalition Telephone Gateway**

## Actor: DND Telephone Support Gateway -

### Description:

Internal DND telecom's systems. Some of this infrastructure may include RF and satellite communications.

### Relationships:

| Source | Type | Target |
|---|---|---|
| DND Telephone Support Gateway | Generalization | Telephone Gateway |

**Table 12: Relationships for DND Telephone Support Gateway**

## Actor: Service Provider Telephone Gateway -

### Description:

Unsecured telecommunications with Service Provider employees.

### Relationships:

| Source | Type | Target |
|---|---|---|
| Service Provider Telephone Gateway | Generalization | Telephone Gateway |

**Table 13: Relationships for Service Provider Telephone Gateway**

### 4.1.3 People

This package contains the actors that represent people or users of the system. This package is divided into sub packages that represent major groups that use or interact with JNDMS.

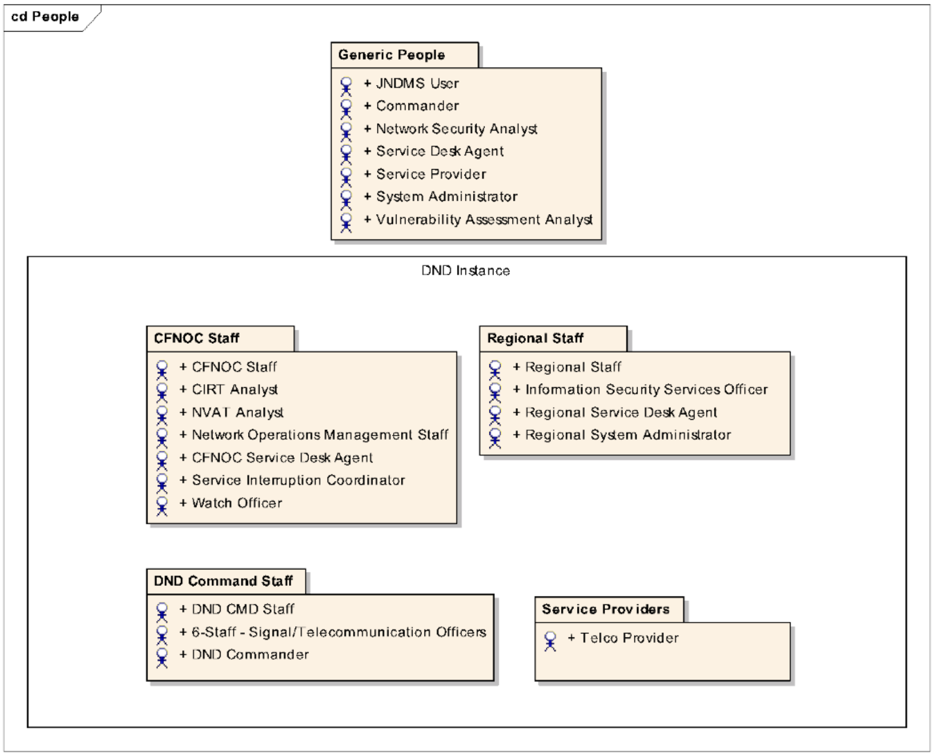

cd People
Generic People
+ JNDMS User
+ Commander
+ Network Security Analyst
+ Service Desk Agent
+ Service Provider
+ System Administrator
+ Vulnerability Assessment Analyst
DND Instance
CFNOC Staff
+ CFNOC Staff
+ CIRT Analyst
+ NVAT Analyst
+ Network Operations Management Staff
+ CFNOC Service Desk Agent
+ Service Interruption Coordinator
+ Watch Officer
Regional Staff
+ Regional Staff
+ Information Security Services Officer
+ Regional Service Desk Agent
+ Regional System Administrator
DND Command Staff
+ DND CMD Staff
+ 6-Staff - Signal/Telecommunication Officers
+ DND Commander
Service Providers
+ Telco Provider

**Figure 5: People**

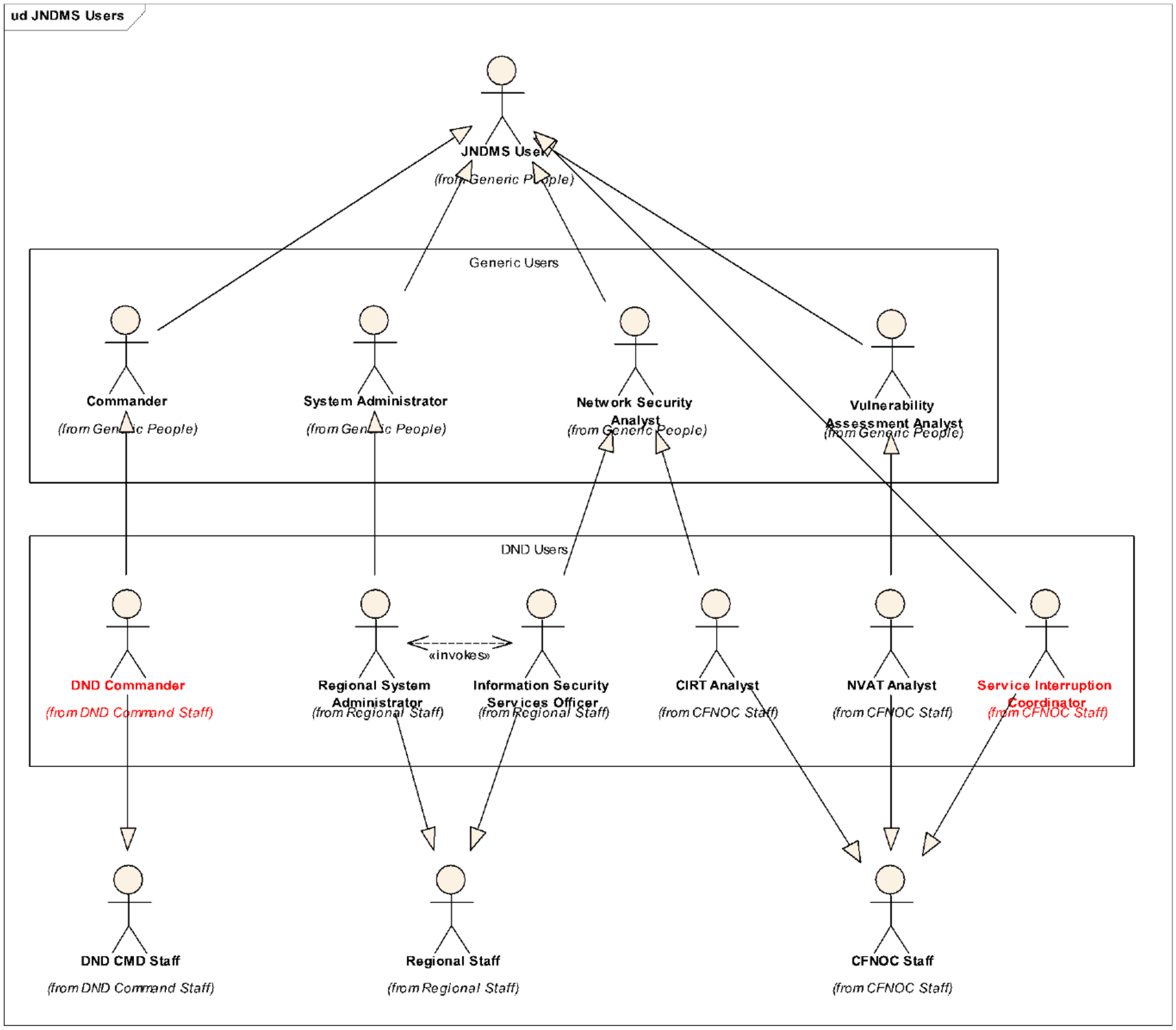


**Figure 6: JNDMS Users**

#### 4.1.3.1 Generic People

This package contains actors that represent people with generic roles. Other packages will contain more specific roles and be related to the roles within this package.

### Actor: JNDMS User -

**Description:**

This actor represents a generic JNDMS user. This role can be attributed to any one that uses or interacts with the JNDMS. Other, more specific, roles are derived from this generic role.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| Service Interruption Coordinator | Generalization | JNDMS User |
| Network Security Analyst | Generalization | JNDMS User |
| System Administrator | Generalization | JNDMS User |
| Vulnerability Assessment Analyst | Generalization | JNDMS User |
| Commander | Generalization | JNDMS User |
| JNDMS User | UseCase | Present Situational Awareness |
| JNDMS User | UseCase | Views (GIS) |
| JNDMS User | UseCase | User Interactions |

**Table 14: Relationships for JNDMS User**

### Actor: Commander -

**Description:**

This actor represents the generic commander in charge of an operation, or organisation.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| DND Commander | Generalization | Commander |
| Commander | Generalization | JNDMS User |

**Table 15: Relationships for Commander**

## Actor: Network Security Analyst -

**Description:**

This represents the generic analyst responsible for the network security component of an organisation.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| Information Security Services Officer | Generalization | Network Security Analyst |
| Network Security Analyst | Generalization | JNDMS User |
| Network Security Analyst | Association | Create / Update SIM Rules |
| CIRT Analyst | Generalization | Network Security Analyst |

**Table 16: Relationships for Network Security Analyst**

## Actor: Service Desk Agent -

**Description:**

This represents the generic Service Desk Agent responsible for the helpdesk component of an organisation.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| Regional Service Desk Agent | Generalization | Service Desk Agent |
| CFNOC Service Desk Agent | Generalization | Service Desk Agent |

**Table 17: Relationships for Service Desk Agent**

### Actor: Service Provider -

**Description:**

This is a generic actor representing the subcontracted services.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| Telco Provider | Generalization | Service Provider |

**Table 18: Relationships for Service Provider**

### Actor: System Administrator -

**Description:**

This represents the generic System Administrator actor responsible for the IT infrastructure administration of an organisation.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| Regional System Administrator | Generalization | System Administrator |
| System Administrator | Generalization | JNDMS User |

**Table 19: Relationships for System Administrator**

### Actor: Vulnerability Assessment Analyst -

**Description:**

This represents the generic analyst responsible for the network vulnerability assessment component of an organisation. The network is assessed against known vulnerabilities to uncover security weaknesses. This includes searching security web sites or intelligence reports for up-to-date vulnerability information, and also includes resolving any related security issues.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| Vulnerability Assessment Analyst | Generalization | JNDMS User |
| NVAT Analyst | Generalization | Vulnerability Assessment Analyst |

**Table 20: Relationships for Vulnerability Assessment Analyst**

#### 4.1.3.2 CFNOC Staff

This package documents the staff within the CFNOC that are involved in the JNDMS use cases. The following diagram shows an overview of the structure and the relationship between group references within the use cases.

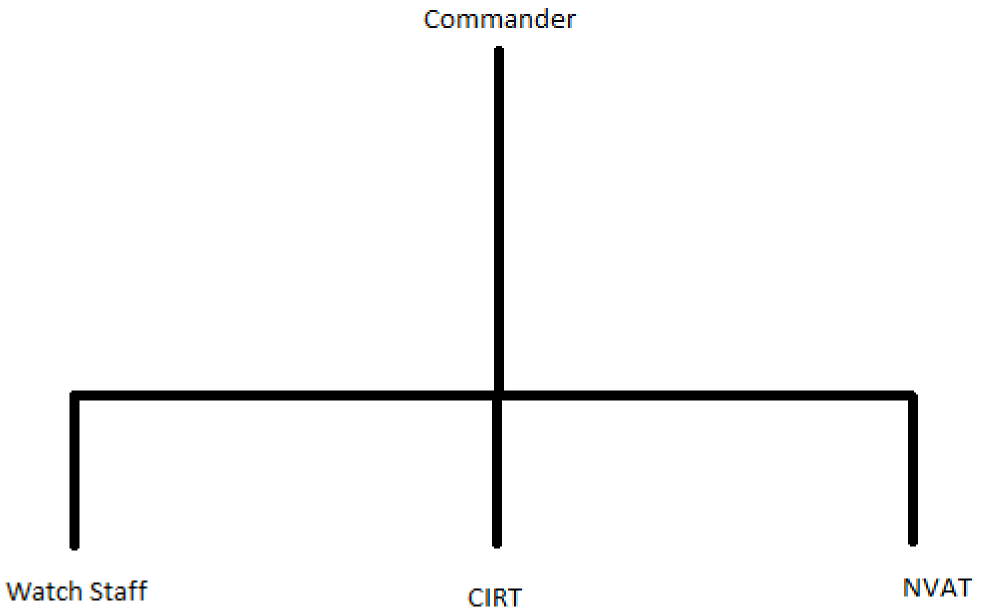


**Figure 7: CFNOC Structure Overview**

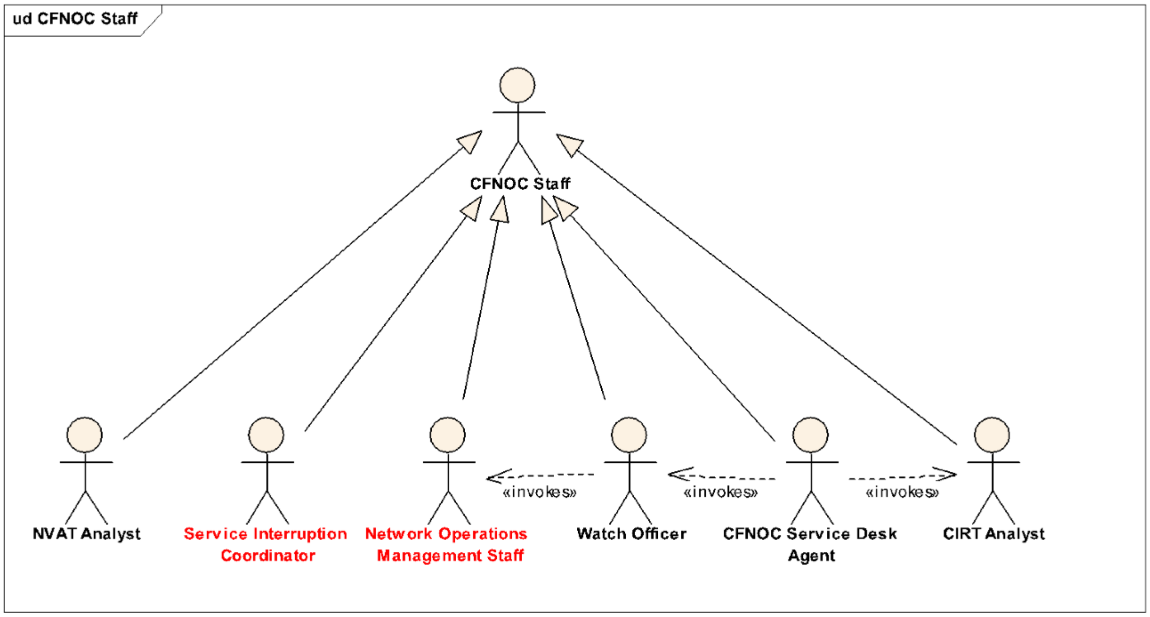


**Figure 8: CFNOC Staff**

## Actor: CFNOC Staff -

### Description:

These DND people reside within the CFNOC.

### Relationships:

| Source | Type | Target |
|---|---|---|
| Watch Officer | Generalization | CFNOC Staff |
| CFNOC Service Desk Agent | Generalization | CFNOC Staff |
| Network Operations Management Staff | Generalization | CFNOC Staff |
| Service Interruption Coordinator | Generalization | CFNOC Staff |
| CIRT Analyst | Generalization | CFNOC Staff |
| NVAT Analyst | Generalization | CFNOC Staff |

**Table 21: Relationships for CFNOC Staff**

## Actor: CIRT Analyst -

### Description:

This actor represents the network security analyst within CFNOC. These analysts are part of the Computer Incident Response Team (CIRT) and are the primary users of the Intellitactics Network Security Manager (NSM).

### Relationships:

| Source | Type | Target |
|---|---|---|
| CIRT Analyst | Association | Prioritize the Response to Incidents |
| CIRT Analyst | Association | Detection of traffic pattern raises alarms |
| CIRT Analyst | Association | View Incident Severity View |
| CIRT Analyst | Association | View Incident Details |
| CIRT Analyst | Association | View Severity Details Calculation |
| CIRT Analyst | Association | Issue Corrective Procedures |
| CIRT Analyst | Generalization | Network Security Analyst |
| CIRT Analyst | Generalization | CFNOC Staff |
| CIRT Analyst | Association | View Status of Canadian and Coalition Networks |
| CIRT Analyst | Association | View Defensive Posture View |
| CIRT Analyst | Association | Clean Infection and Secure Server |
| CIRT Analyst | Association | View Security Incidents View |
| CIRT Analyst | Association | View Services Status View |
| CFNOC Service Desk Agent | Dependency | CIRT Analyst |
| CIRT Analyst | Association | Query - Operations depending on Specific IT Infrastructure |
| CIRT Analyst | Association | Examine External Sources of Exploit and Vulnerability Information |

**Table 22: Relationships for CIRT Analyst**

## Actor: NVAT Analyst -

### Description:

The Network Vulnerability Assessment Team (NVAT) reviews Intelligence reports and researches the Internet for known vulnerabilities and assesses if they apply to DND hardware or software.

### Relationships:

| Source | Type | Target |
|---|---|---|
| NVAT Analyst | Generalization | Vulnerability Assessment Analyst |
| NVAT Analyst | Generalization | CFNOC Staff |
| NVAT Analyst | Association | Examine External Sources of Exploit and Vulnerability Information |
| NVAT Analyst | Association | View Risk Assessment Details |
| NVAT Analyst | Association | Plan and Request Appropriate Risk Mitigation |
| NVAT Analyst | Association | Update Vulnerability Status once the Mitigation is Validated |
| NVAT Analyst | Association | Investigate Potential Vulnerability |
| NVAT Analyst | Association | View Defensive Posture View |
| NVAT Analyst | Association | View Risk Assessment View |

**Table 23: Relationships for NVAT Analyst**

## Actor: Network Operations Management Staff -

### Description:

These are staff that maintain the network infrastructure. In the NOC, these people are responsible for the LAN that CFNOC uses to coordinate the status of the WAN.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| Watch Officer | Dependency | Network Operations Management Staff |
| Network Operations Management Staff | Generalization | CFNOC Staff |
| Network Operations Management Staff | Association | Isolate/Reconnect Subset of Network |

**Table 24: Relationships for Network Operations Management Staff**

## Actor: CFNOC Service Desk Agent -

**Description:**

Personnel that man the front-line helpdesk at the CFNOC, logging trouble tickets. In some cases, they do not actually remedy the troubles, but do know who to send the trouble ticket on to for action.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| CFNOC Service Desk Agent | Generalization | CFNOC Staff |
| CFNOC Service Desk Agent | Dependency | Watch Officer |
| CFNOC Service Desk Agent | Generalization | Service Desk Agent |
| Contact CFNOC and Make Recommendations | Association | CFNOC Service Desk Agent |
| CFNOC Service Desk Agent | Association | Close Trouble Ticket |
| CFNOC Service Desk Agent | Dependency | CIRT Analyst |

**Table 25: Relationships for CFNOC Service Desk Agent**

## Actor: Service Interruption Coordinator -

**Description:**

This team coordinates service interruption with local NOCs, J6, Engineering and Bell Nexxia.

### Relationships:

| Source | Type | Target |
|---|---|---|
| Service Interruption Coordinator | Association | Log Trouble Ticket |
| Service Interruption Coordinator | Generalization | JNDMS User |
| Service Interruption Coordinator | Generalization | CFNOC Staff |
| Service Provider Email Gateway | Dependency | Service Interruption Coordinator |
| Service Interruption Coordinator | Association | Reject Service Outage |
| Service Interruption Coordinator | Association | Identify Network Outage Options |
| Service Interruption Coordinator | Association | Query - Operations affected by Outage |
| Service Interruption Coordinator | Association | Provide Outage Options to Service Provider |
| Issue Maintenance Request | Association | Service Interruption Coordinator |

**Table 26: Relationships for Service Interruption Coordinator**

## Actor: Watch Officer -

### Description:

This person is in charge of coordinating the Watch Staff within the CFNOC. The Watch Staff includes a Duty Watch position, which is manned 24 hours a day, 7 days a week (24/7). The Watch Staff monitors the timely flow of actions through the NOC workflows.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| Watch Officer | Generalization | CFNOC Staff |
| Watch Officer | Dependency | Network Operations Management Staff |
| Watch Officer | Association | Make Decision to Isolate/Reconnect a Domain |
| CFNOC Service Desk Agent | Dependency | Watch Officer |

Table 27: Relationships for Watch Officer

### 4.1.3.3 DND Command Staff

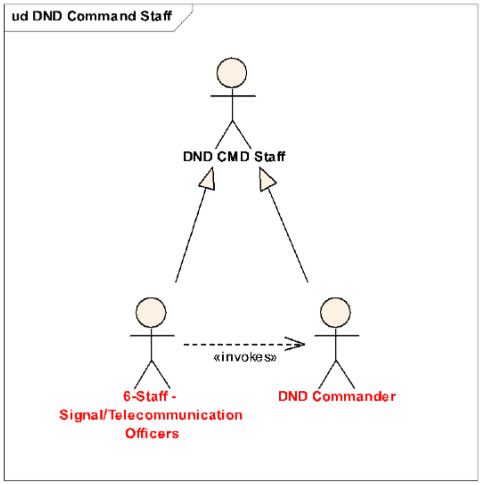


Figure 9: DND Command Staff

## Actor: DND CMD Staff -

### Description:

This actor represents the DND Command (CMD) staff.

### Relationships:

| Source | Type | Target |
|---|---|---|
| DND Commander | Generalization | DND CMD Staff |
| 6-Staff - Signal/Telecommunication Officers | Generalization | DND CMD Staff |

**Table 28: Relationships for DND CMD Staff**

## Actor: 6-Staff - Signal/Telecommunication Officers -

### Description:

Signal/Telecommunication officers are responsible for operations IT requirements and planning the circuits that the DND traffic flows across, for wireless infrastructure and recommendations for change to accommodate ongoing operations.

### Relationships:

| Source | Type | Target |
|---|---|---|
| 6-Staff - Signal/ Telecommunication Officers | Generalization | DND CMD Staff |
| 6-Staff - Signal/ Telecommunication Officers | Dependency | DND Commander |
| Identify Network Outage Options | Association | 6-Staff - Signal/ Telecommunication Officers |

**Table 29: Relationships for 6-Staff - Signal/Telecommunication Officers**

### Actor: DND Commander -

**Description:**

DND Command staff at the National Defence Command Centre (NDCC). These people consume the network threat level and prioritize the network assets (more specifically, network services like C2 systems, email, phone, etc.) for current operations. They don't necessarily know how communications are set-up, but do identify which IT service is important for operations.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| DND Commander | Generalization | DND CMD Staff |
| 6-Staff - Signal/Telecommunication Officers | Dependency | DND Commander |
| DND Commander | Generalization | Commander |
| DND Commander | Association | Headquarters staff checks network status |

**Table 30: Relationships for DND Commander**

## 4.1.3.4 Regional Staff

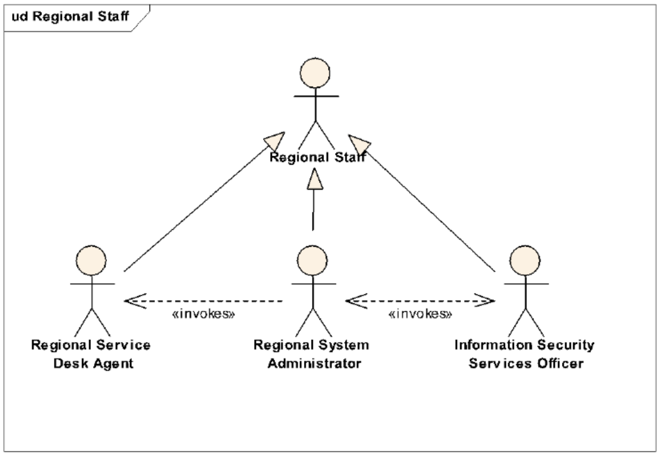

ud Regional Staff
Regional Staff
«invokes»
«invokes»
Regional Service Desk Agent
Regional System Administrator
Information Security Services Officer

**Figure 10: Regional Staff**

## Actor: Regional Staff -

### Description:

This actor represents DND people at the regional level.

### Relationships:

| Source | Type | Target |
|---|---|---|
| Regional System Administrator | Generalization | Regional Staff |
| Regional Service Desk Agent | Generalization | Regional Staff |
| Information Security Services Officer | Generalization | Regional Staff |

**Table 31: Relationships for Regional Staff**

## Actor: Information Security Services Officer -

### Description:

This DND personnel is responsible for the network security component at the regional level.

### Relationships:

| Source | Type | Target |
|---|---|---|
| Information Security Services Officer | Generalization | Network Security Analyst |
| Information Security Services Officer | Association | View Incident Details |
| Issue Corrective Procedures | Dependency | Information Security Services Officer |
| Information Security Services Officer | Dependency | Regional System Administrator |
| Information Security Services Officer | Generalization | Regional Staff |
| Information Security Services Officer | Association | View Security Incidents View |
| Information Security Services Officer | Association | View Services Status View |
| Information Security Services Officer | Association | Contact CFNOC and Make Recommendations |
| Regional System Administrator | Dependency | Information Security Services Officer |
| Information Security Services Officer | Association | Query - Operations depending on Specific IT Infrastructure |

**Table 32: Relationships for Information Security Services Officer**

## Actor: Regional Service Desk Agent -

### Description:

This represents DND helpdesk personnel at the regional level.

### Relationships:

| Source | Type | Target |
|---|---|---|
| Regional Service Desk Agent | Generalization | Service Desk Agent |
| Regional Service Desk Agent | Generalization | Regional Staff |
| Regional System Administrator | Dependency | Regional Service Desk Agent |
| Regional Service Desk Agent | Association | Log Trouble Ticket |

**Table 33: Relationships for Regional Service Desk Agent**

## Actor: Regional System Administrator -

### Description:

Personnel responsible for configuring and operating the hardware and software at the regional level.

### Relationships:

**Table 34: Relationships for Regional System Administrator**

| Source | Type | Target |
|---|---|---|
| Regional System Administrator | Association | Query - What network each piece of equipment runs on |
| Regional System Administrator | Association | Query - What services each piece of equipment supports |
| Plan and Request Appropriate Risk Mitigation | Dependency | Regional System Administrator |
| Regional System Administrator | Association | Query - Point of contact for each equipment |
| Regional System Administrator | Association | Query - Operations depending on Specific IT Infrastructure |
| Regional System Administrator | Association | Contact "Point of Contacts" |

| Source | Type | Target |
|---|---|---|
| Regional System Administrator | Association | Disable Equipment |
| Regional System Administrator | Association | Enable Equipment |
| Regional System Administrator | Generalization | System Administrator |
| Information Security Services Officer | Dependency | Regional System Administrator |
| Regional System Administrator | Generalization | Regional Staff |
| Regional System Administrator | Dependency | Information Security Services Officer |
| Regional System Administrator | Dependency | Regional Service Desk Agent |

### 4.1.3.5 Service Providers

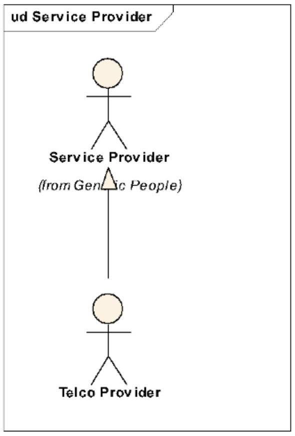


**Figure 11: Service Provider**

## Actor: Telco Provider -

### Description:

This represents the telecommunications provider's helpdesk personnel responsible for entering TSRP trouble tickets into the Remedy system and keeping those tickets updated.

### Relationships:

| Source | Type | Target |
|---|---|---|
| Telco Provider | Generalization | Service Provider |
| Provide Outage Options to Service Provider | Association | Telco Provider |
| Telco Provider | Association | Issue Maintenance Request |

**Table 35: Relationships for Telco Provider**

### 4.1.4 Systems/Repositories

This package contains major subsystems or repositories of data that interact with the JNDMS.

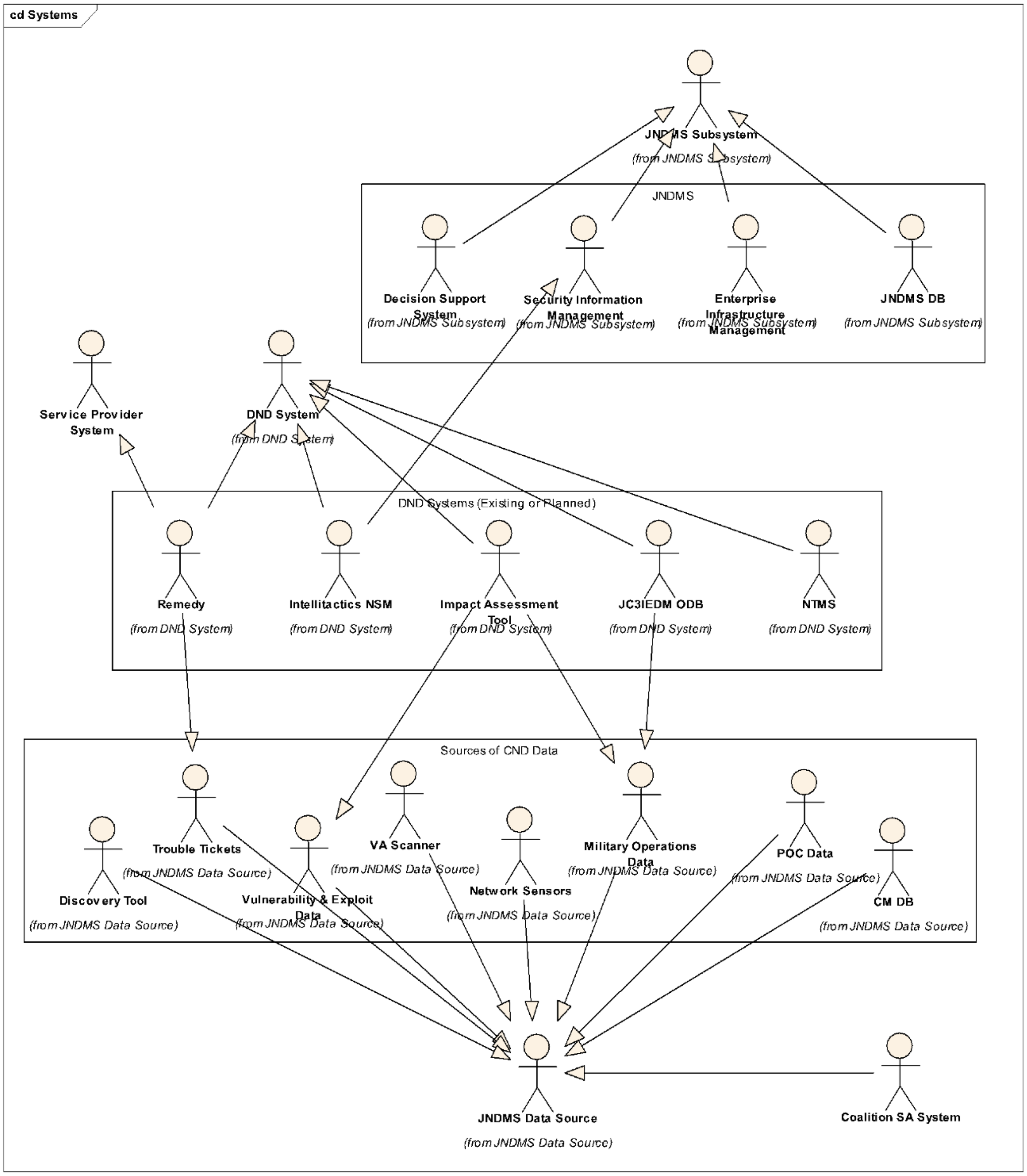


**Figure 12: Systems**

## Actor: Service Provider System -

### Description:

This actor represents a generic service provider system.

### Relationships:

| Source | Type | Target |
|---|---|---|
| Remedy | Generalization | Service Provider System |
| Service Provider System | Realisation | Security Events |
| Service Provider System | Realisation | IT Infrastructure |

**Table 36: Relationships for Service Provider System**

## Actor: Coalition SA System -

### Description:

This a coalition partner with whom DND may have decided to share situational awareness data.

### Relationships:

| Source | Type | Target |
|---|---|---|
| Exchange data across classification layer | Association | Coalition SA System |
| Coalition SA System | Generalization | JNDMS Data Source |
| Coalition SA System | Realisation | Security Events |
| Coalition SA System | Realisation | IT Infrastructure |

**Table 37: Relationships for Coalition SA System**

### 4.1.4.1 JNDMS Subsystem

This package regroups the major JNDMS subsystems.

#### Actor: JNDMS Subsystem -

**Description:**

This represents a generic actor for a subsystem within JNDMS.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| Security Information Management | Generalization | JNDMS Subsystem |
| Enterprise Infrastructure Management | Generalization | JNDMS Subsystem |
| Decision Support System | Generalization | JNDMS Subsystem |
| JNDMS DB | Generalization | JNDMS Subsystem |

**Table 38: Relationships for JNDMS Subsystem**

#### Actor: Decision Support System -

**Description:**

This actor represents the Decision Support System within the Business Logic layer of the JNDMS. This actor is used where this subsystem acts on other subsystems.

**Relationships:**

**Table 39: Relationships for Decision Support System**

| Source | Type | Target |
|---|---|---|
| Decision Support System | Association | Assess Current Threat Level |
| Decision Support System | Association | Vulnerability Severity Assessment |
| Decision Support System | Association | Incident Severity Assessment |
| Decision Support System | Association | Assess Rolled-up Severity Value |

| Source | Type | Target |
|---|---|---|
| Decision Support System | Association | Correlate Incidents |
| Decision Support System | Association | Filter Incidents |
| Decision Support System | Association | Identify Defensive Components |
| Decision Support System | Association | Pre-Process Defensive Posture Components |
| Decision Support System | Generalization | JNDMS Subsystem |

## Actor: Enterprise Infrastructure Management -

### Description:

This actor represents the Enterprise Infrastructure Management (EIM) subsystem within JNDMS.

### Relationships:

| Source | Type | Target |
|---|---|---|
| Acquire Infrastructure Incidents | Dependency | Enterprise Infrastructure Management |
| Acquire IT Infrastructure Data | Dependency | Enterprise Infrastructure Management |
| Enterprise Infrastructure Management | Association | Identify Infrastructure Incidents |
| Enterprise Infrastructure Management | Association | Acquire Static IT Data and Location |
| Enterprise Infrastructure Management | Association | Acquire IT Infrastructure Discovery |
| Enterprise Infrastructure Management | Generalization | JNDMS Subsystem |

**Table 40: Relationships for Enterprise Infrastructure Management**

## Actor: JNDMS DB -

### Description:

This actor represents the central database of the JNDMS data warehouse.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| JNDMS DB | Association | Data Warehousing |
| JNDMS DB | Generalization | JNDMS Subsystem |

**Table 41: Relationships for JNDMS DB**

### Actor: Security Information Management -

**Description:**

This actor represents the Security Information Management (SIM) subsystem within JNDMS. It processes security events and identifies information security incidents.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| Intellitactics NSM | Generalization | Security Information Management |
| Security Information Management | Generalization | JNDMS Subsystem |

**Table 42: Relationships for Security Information Management**

## 4.1.4.2 JNDMS Data Source

This package regroups data sources required for Situational Awareness.

### Actor: JNDMS Data Source -

**Description:**

This represents the generic actor for a source of data for JNDMS.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| CM DB | Generalization | JNDMS Data Source |
| Vulnerability & Exploit Data | Generalization | JNDMS Data Source |
| Trouble Tickets | Generalization | JNDMS Data Source |
| Network Sensors | Generalization | JNDMS Data Source |
| VA Scanner | Generalization | JNDMS Data Source |
| Discovery Tool | Generalization | JNDMS Data Source |
| Military Operations Data | Generalization | JNDMS Data Source |
| POC Data | Generalization | JNDMS Data Source |
| Coalition SA System | Generalization | JNDMS Data Source |

**Table 43: Relationships for JNDMS Data Source**

## Actor: CM DB -

**Description:**

This actor represents the asset configuration management data. This database represents the known or tracked assets and associated information.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| CM DB | Generalization | JNDMS Data Source |
| Acquire Static IT Data and Location | Dependency | CM DB |
| CM DB | Realisation | IT Infrastructure |

**Table 44: Relationships for CM DB**

### Actor: Discovery Tool -

**Description:**

This actor represents an automated network discovery tool. This tool must be able to collect information on IT assets and their interconnections.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| Acquire IT Infrastructure Discovery | Dependency | Discovery Tool |
| Discovery Tool | Generalization | JNDMS Data Source |
| Discovery Tool | Realisation | IT Infrastructure |

**Table 45: Relationships for Discovery Tool**

### Actor: Military Operations Data -

**Description:**

The military operations data includes operation locations and their IT requirements.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| Acquire Operations Details | Dependency | Military Operations Data |
| Acquire Ops. IT Requirements | Dependency | Military Operations Data |
| Impact Assessment Tool | Generalization | Military Operations Data |
| Military Operations Data | Generalization | JNDMS Data Source |
| JC3IEDM ODB | Generalization | Military Operations Data |
| Military Operations Data | Realisation | Military Operations |

**Table 46: Relationships for Military Operations Data**

## Actor: Network Sensors -

### Description:

The network sensors represent the generalization of input devices on the sensors.

### Relationships:

| Source | Type | Target |
|---|---|---|
| Firewall Logs | Generalization | Network Sensors |
| Security Alarms | Generalization | Network Sensors |
| Performance Metrics | Generalization | Network Sensors |
| Network Events | Generalization | Network Sensors |
| Application Events | Generalization | Network Sensors |
| Network Sensors | Generalization | Information Sources |
| Network Sensors | Realisation | Security Events |
| Acquire Security Events | Dependency | Network Sensors |
| Network Sensors | Generalization | JNDMS Data Source |

**Table 47: Relationships for Network Sensors**

## Actor: POC Data -

### Description:

A Point of Contact (POC) database is used to find a point of contact for a specific piece of equipment.

### Relationships:

| Source | Type | Target |
|---|---|---|
| POC Data | Generalization | JNDMS Data Source |

**Table 48: Relationships for POC Data**

## Actor: Trouble Tickets -

### Description:

This actor represents a generalization of any trouble ticket.

### Relationships:

| Source | Type | Target |
|---|---|---|
| Log Trouble Ticket | Dependency | Trouble Tickets |
| Close Trouble Ticket | Dependency | Trouble Tickets |
| Acquire Trouble Tickets | Dependency | Trouble Tickets |
| Trouble Tickets | Generalization | JNDMS Data Source |
| Remedy | Generalization | Trouble Tickets |

**Table 49: Relationships for Trouble Tickets**

## Actor: VA Scanner -

### Description:

This actor represents a Vulnerability Assessment Scanner.

### Relationships:

| Source | Type | Target |
|---|---|---|
| Acquire Vulnerability Assessment Scans | Dependency | VA Scanner |
| Acquire Scanners Vulnerability Dictionary | Dependency | VA Scanner |
| VA Scanner | Generalization | JNDMS Data Source |
| VA Scanner | Realisation | Vulnerability Datasets |

**Table 50: Relationships for VA Scanner**

### Actor: Vulnerability & Exploit Data -

**Description:**

This data may come from sources like advisories or security web sites. It has been parsed and is of a known format.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| Acquire Vulnerability Data | Dependency | Vulnerability & Exploit Data |
| Acquire Exploit Data | Dependency | Vulnerability & Exploit Data |
| Vulnerability & Exploit Data | Generalization | JNDMS Data Source |
| Impact Assessment Tool | Generalization | Vulnerability & Exploit Data |
| Vulnerability & Exploit Data | Realisation | Vulnerability Datasets |

**Table 51: Relationships for Vulnerability & Exploit Data**

## 4.1.4.3 DND System

This package regroups systems or repositories that are currently used by DND.

### Actor: DND System -

**Description:**

This represents the generic actor for systems, tools or repositories currently used by DND.

**Relationships:**

**Table 52: Relationships for DND System**

| Source | Type | Target |
|---|---|---|
| NTMS | Generalization | DND System |
| Remedy | Generalization | DND System |
| Impact Assessment Tool | Generalization | DND System |
| Intellitactics NSM | Generalization | DND System |
| JC3IEDM ODB | Generalization | DND System |

| Source | Type | Target |
|---|---|---|
| DND System | Realisation | Security Events |
| DND System | Realisation | IT Infrastructure |
| DND System | Realisation | Military Operations |
| DND System | Realisation | Vulnerability Datasets |

## Actor: Impact Assessment Tool -

### Description:

This actor represents the Impact Assessment Tool.

### Relationships:

| Source | Type | Target |
|---|---|---|
| Impact Assessment Tool | Generalization | DND System |
| Impact Assessment Tool | Generalization | Vulnerability & Exploit Data |
| Impact Assessment Tool | Generalization | Military Operations Data |
| Enter Potential Vulnerability in IAT | Dependency | Impact Assessment Tool |
| Update Vulnerability Status once the Mitigation is Validated | Dependency | Impact Assessment Tool |

**Table 53: Relationships for Impact Assessment Tool**

## Actor: Intellitactics NSM -

### Description:

Intellitactics Network Security Manager (NSM) is the SIM solution currently deployed at CFNOC. It fully integrates the best features of security information management with automated event management.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| Intellitactics NSM | Generalization | Security Information Management |
| Acquire Security Incidents | Dependency | Intellitactics NSM |
| Intellitactics NSM | Association | Identify Security Incidents |
| Intellitactics NSM | Association | Acquire Security Events |
| Intellitactics NSM | Association | Pre-Process Security Events |
| Intellitactics NSM | Association | Store Security Events |
| Intellitactics NSM | Association | Acquire Vulnerability Assessment Scans |
| Intellitactics NSM | Association | Acquire IT Infrastructure Data |
| Intellitactics NSM | Generalization | DND System |

**Table 54: Relationships for Intellitactics NSM**

## Actor: JC3IEDM ODB -

**Description:**

This actor represents the operations database (ODB) using the Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM) format. It contains information related to an operation, such as dates, IT assets and required IT services. This database is not yet available from DND; it is planned.

**Relationships:**

| Source | Type | Target |
|---|---|---|
| JC3IEDM ODB | Generalization | DND System |
| JC3IEDM ODB | Generalization | Military Operations Data |

**Table 55: Relationships for JC3IEDM ODB**

## Actor: NTMS -

### Description:

This is the National Telecommunication Management System used between Bell and DND. It provides circuit and connectivity information.

### Relationships:

| Source | Type | Target |
|---|---|---|
| NTMS | Generalization | DND System |

**Table 56: Relationships for NTMS**

## Actor: Remedy -

### Description:

Remedy is the Ticketing Tool currently deployed. It is jointly maintained between Bell and the Engineering staff (IMGIS).

### Relationships:

| Source | Type | Target |
|---|---|---|
| Remedy | Generalization | Service Provider System |
| Remedy | Generalization | DND System |
| Remedy | Generalization | Trouble Tickets |

**Table 57: Relationships for Remedy**

## 4.2 Use Cases

The use cases in this section are presented in a structured format generated from the underlying UML model.

The use cases are structured according to the draft architecture to facilitate further decomposition and traceability through the design phases. The following diagram shows the Computer System Configuration Items (CSCI) and associated architecture layers.

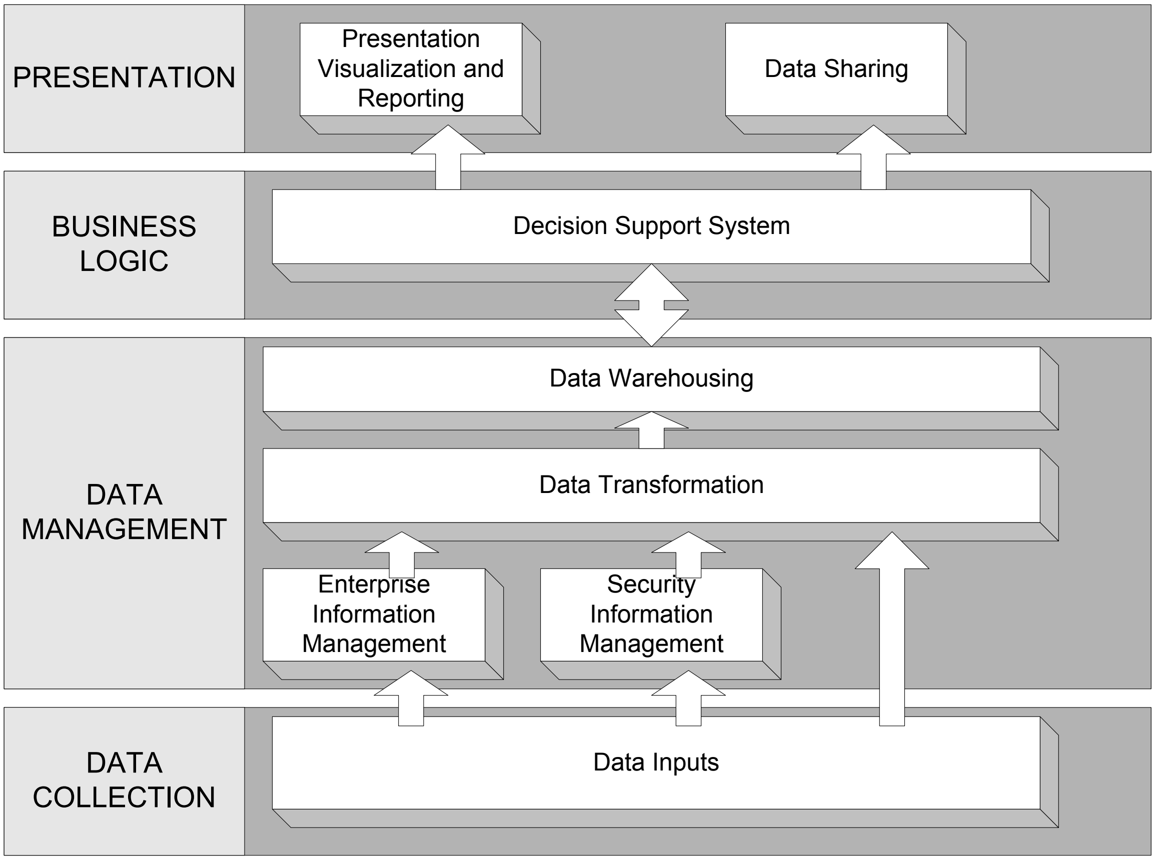


**Figure 13: JNDMS CSCIs**

Each use case will have a description that briefly describes the use case. Following the description there will be one or more of the following elements associated with the use case:

- A context diagram. Some of the use cases or use case packages have an associated diagram showing the relationship between this use case and other use cases and actors.

- An association table. This table will show the relationships between this use case and other use cases and actors. Each table has three columns, the source, type and target. The source shows the source of the relationship. Some relationships are directional so the name of the current use case may be either the source or target of this relationship. The type of the relationship refers to UML "stereotypes". The following relationships are common and may be found within this model:

    - Use: This relationship shows that the source element makes use of the target element. This is often the relationship between actors and the use cases.

    - Associate: This relationship is any general relationship. It simply means that the model does not specify the details of the relationship, just that they are related. In the following tables this relationship just shows as a blank field for the type.

    - Generalize: This relationship shows a hierarchal relationship. This shows that some use cases are specializations of more general use cases.

    - Include: This relationship allows use case to be broken up in to more manageable units. This shows when one use case includes one or more other use cases.

    - Realize: This relationship shows when one use case is a realization of another. In this model use cases realize associated requirements, for example.

    - Dependency: This relationship allows use cases to show when they depend on the behaviour of another use case.

    - Invokes: This relationship shows when one use case or actor invokes another use case or actor. This may be used in showing subsystem interaction, for example.

    - Precedes: This relationship allows ordering information to be modeled. This relationship shows when one use case must precede another.

### 4.2.1 Data Collection

The data collection package contains the use cases related to the inputs of the JNDMS. The architecture document refers to dynamic and static inputs, however these have been combined in a single package. The architecture will be updated to reflect the results of the requirement analysis efforts.

The Acquire Domain Data use case shows how the data collection use cases interact with each other.

## Use Case: Acquire Domain Data -

### Description:

This use case provides a generalization for the collection of the core domain data sets. The input data from these domains, as defined in the actor package 'domains', represents the key data inputs, which are fused to provide the overall situational awareness.

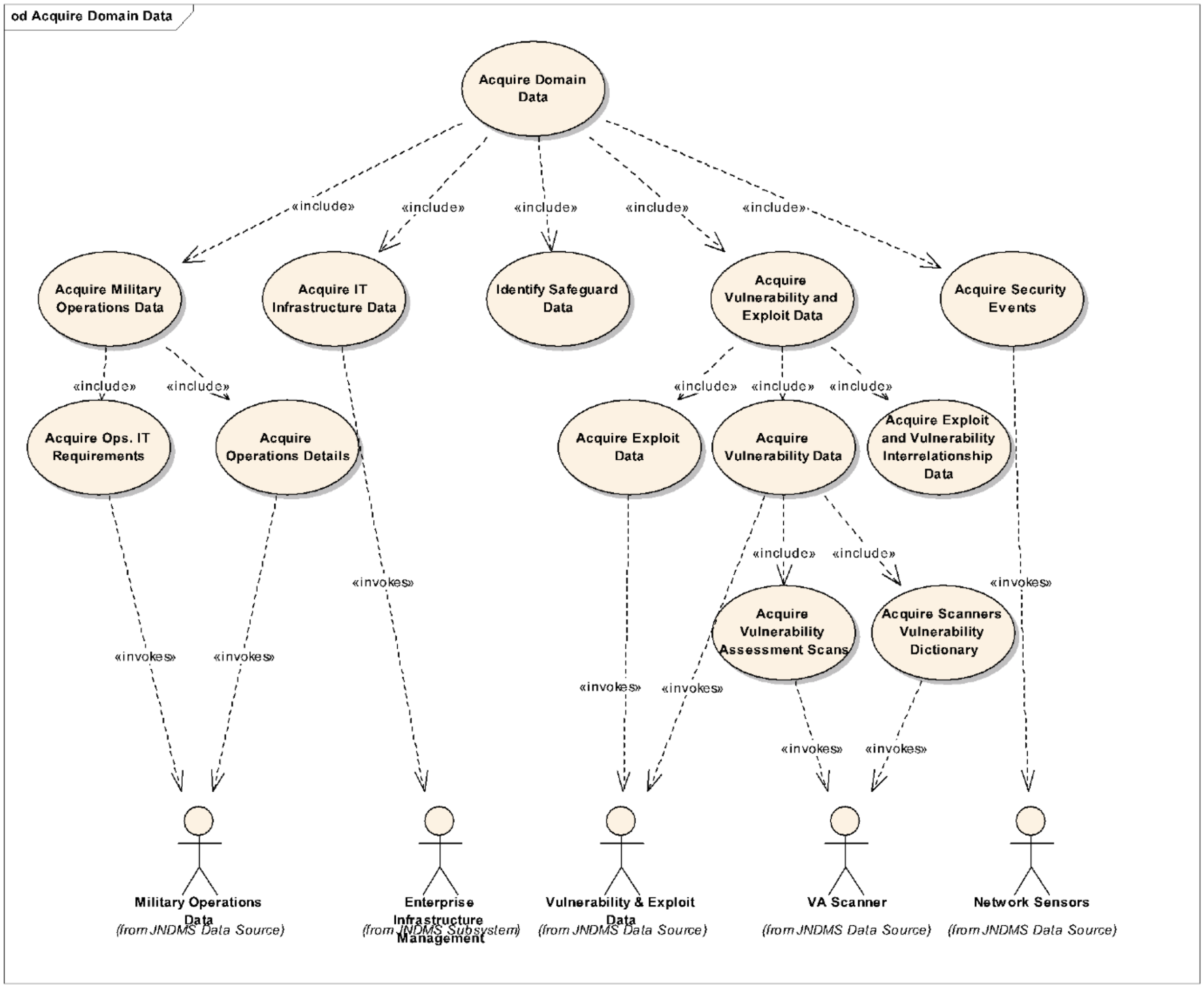


**Figure 14: Acquire Domain Data**

| Source | Type | Target |
|---|---|---|
| Acquire Domain Data | include | Acquire Military Operations Data |
| Acquire Domain Data | include | Acquire IT Infrastructure Data |
| Acquire Domain Data | include | Acquire Vulnerability and Exploit Data |
| Acquire Domain Data | include | Identify Safeguard Data |
| Acquire Domain Data | | DID-JNDMS-0 |
| Acquire Domain Data | include | Acquire Security Events |

**Table 58: Relationships for Acquire Domain Data**

**Requirements:**

**DID-JNDMS-0**

The JNDMS shall provide situational awareness (SA) for Computer Network Defence (CND) through the fusion of Military Operations, IT infrastructure, Security events, Vulnerability, and Safeguards data sets. The JNDMS shall capture, store, process, analyze and present data from these five information domains**.**

## Use Case: Acquire IT Infrastructure Data -

**Description:**

JNDMS will acquire static and dynamic IT infrastructure data. This information will be saved in two separate data sets. This information is available in EIM.

**Table 59: Relationships for Acquire IT Infrastructure Data**

| Source | Type | Target |
|---|---|---|
| Acquire IT Infrastructure Data | include | Acquire Static IT Data and Location |
| Acquire IT Infrastructure Data | invokes | Enterprise Infrastructure Management |
| Acquire IT Infrastructure Data | include | Acquire IT Infrastructure Discovery |

| Source | Type | Target |
|---|---|---|
| Acquire IT Infrastructure Data | precedes | Pre-Process IT Infrastructure Data |
| Acquire Domain Data | include | Acquire IT Infrastructure Data |
| Intellitactics NSM | | Acquire IT Infrastructure Data |

## Use Case: Acquire IT Infrastructure Discovery -

### Description:

This is the "dynamic" IT data "discovered" through a Discovery tool.

| Source | Type | Target |
|---|---|---|
| Acquire IT Infrastructure Data | include | Acquire IT Infrastructure Discovery |
| Acquire IT Infrastructure Discovery | | DID-ITID-3 |
| Enterprise Infrastructure Management | | Acquire IT Infrastructure Discovery |
| Acquire IT Infrastructure Discovery | | DID-ITID-0 |
| Acquire IT Infrastructure Discovery | invokes | Discovery Tool |

**Table 60: Relationships for Acquire IT Infrastructure Discovery**

### Requirements:

**DID-ITID-0**

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.

**DID-ITID-3**

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.

## Use Case: Acquire Static IT Data and Location -

### Description:

Static IT infrastructure data is the data that should be available in a Configuration Management Database. It is the configuration and topology as planned by the organization. JNDMS may have to acquire this information through an existing network management tool export. The EIM subsystem is also responsible for capturing asset locations. This asset information and the associated locations are considered static IT data.

| Source | Type | Target |
|---|---|---|
| Acquire IT Infrastructure Data | include | Acquire Static IT Data and Location |
| Acquire Static IT Data and Location | | DID-ITID-2 |
| Acquire Static IT Data and Location | invokes | CM DB |
| Enterprise Infrastructure Management | | Acquire Static IT Data and Location |
| Acquire Static IT Data and Location | | DID-ITID-0 |
| Acquire Static IT Data and Location | | DID-ITID-1 |
| Acquire Static IT Data and Location | include | Import Circuit Information |

**Table 61: Relationships for Acquire Static IT Data and Location**

### Requirements:

**DID-ITID-0**

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.

**DID-ITID-1**

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 data sets/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)**.**

**DID-ITID-2**

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**.**

## Use Case: Import Circuit Information -

### Description:

JNDMS collects and stores telecom circuit information.

| Source | Type | Target |
|---|---|---|
| Acquire Static IT Data and Location | include | Import Circuit Information |

**Table 62: Relationships for Import Circuit Information**

## Use Case: Acquire Military Operations Data -

### Description:

This represents the general case of collecting military operations data. This most likely source is through the J6 operational planning phase although other sources may be identified (such as through the data export/import mechanism and JC3IEDM).

| Source | Type | Target |
|---|---|---|
| Acquire Military Operations Data | include | Acquire Operations Details |
| Acquire Domain Data | include | Acquire Military Operations Data |
| Acquire Military Operations Data | include | Acquire Ops. IT Requirements |
| Acquire Military Operations Data | | DID-OD-0 |
| Acquire Military Operations Data | | DID-OD-1 |
| Acquire Military Operations Data | precedes | Pre-Process Operations Data |

**Table 63: Relationships for Acquire Military Operations Data**

**Requirements:**

**DID-OD-0**

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.

**DID-OD-1**

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**.**

## Use Case: Acquire Operations Details -

### Description:

This is acquiring details of military operations.

| Source | Type | Target |
|---|---|---|
| Acquire Military Operations Data | include | Acquire Operations Details |
| Acquire Operations Details | invokes | Military Operations Data |

**Table 64: Relationships for Acquire Operations Details**

## Use Case: Acquire Ops. IT Requirements -

### Description:

The IT services required for the operation are selected and their importance for the operation is selected and entered into the JNDMS database. JNDMS knows what IT assets provide the required services.

| Source | Type | Target |
|---|---|---|
| Acquire Ops. IT Requirements | invokes | Military Operations Data |
| Acquire Military Operations Data | include | Acquire Ops. IT Requirements |
| Acquire Ops. IT Requirements | | DID-OD-0 |
| Acquire Ops. IT Requirements | | DID-OD-1 |

**Table 65: Relationships for Acquire Ops. IT Requirements**

### Requirements:

**DID-OD-0**

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.

**DID-OD-1**

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**.**

## Use Case: Identify Safeguard Data -

### Description:

The description of the currently applied safeguards will be entered into the JNDMS. The IT assets and features representing safeguards are identified as such. The safeguards are a critical component of building the defensive posture.

| Source | Type | Target |
|---|---|---|
| Identify Safeguard Data | precedes | Pre-Process Safeguard Data |
| Acquire Domain Data | include | Identify Safeguard Data |
| Identify Safeguard Data | | DID-SAFD-0 |
| Identify Safeguard Data | | DID-SAFD-1 |

**Table 66: Relationships for Identify Safeguard Data**

### Requirements:

**DID-SAFD-0**

The JNDMS shall capture IT Infrastructure Safeguards data. This function refers to the following sub-functions: acquiring IT Infrastructure Safeguards data, pre-processing this data, and writing it to the JNDMS database.

**DID-SAFD-1**

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.

## Use Case: Acquire Vulnerability and Exploit Data -

### Description:

This use case represents the general case of collecting vulnerability and exploit data. The use case is separated into the acquisition of the vulnerability data and exploit data so that each case may be addressed individually.

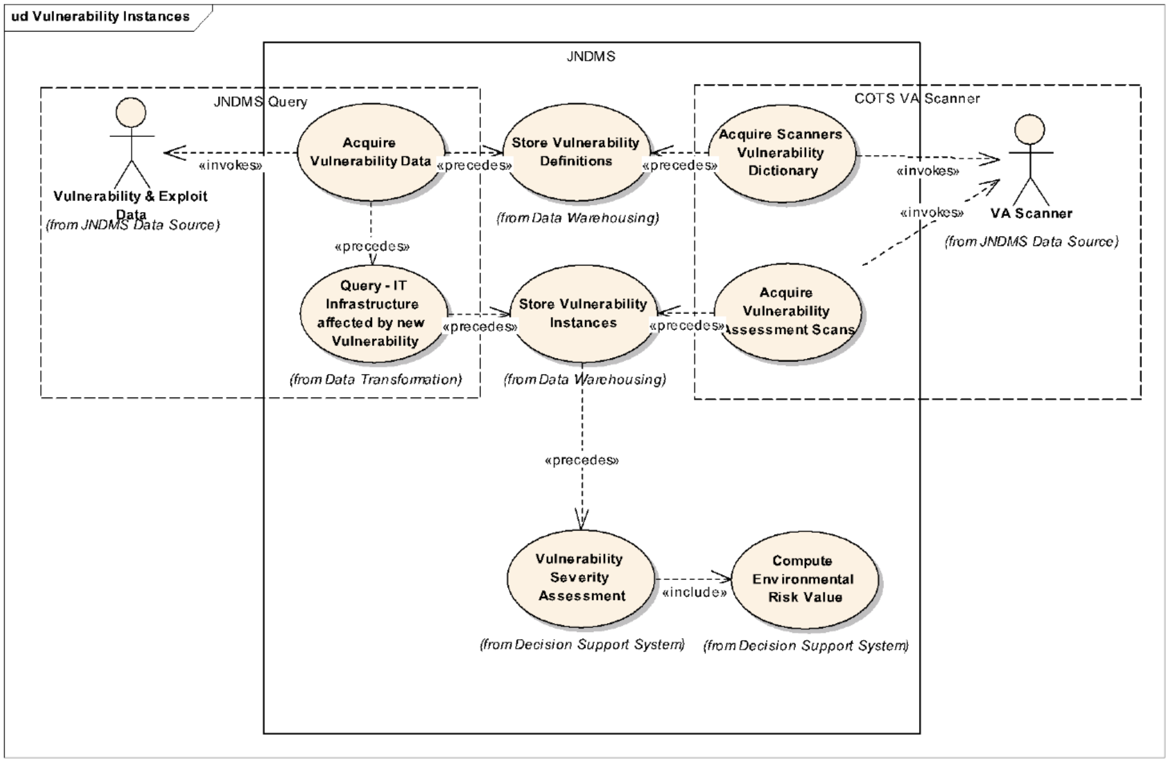

ud Vulnerability Instances
JNDMS
JNDMS Query
COTS VA Scanner
Vulnerability & Exploit Data
(from JNDMS Data Source)
«invokes»
Acquire Vulnerability Data
«precedes»
Store Vulnerability Definitions
(from Data Warehousing)
«precedes»
Acquire Scanners Vulnerability Dictionary
«invokes»
«invokes»
VA Scanner
(from JNDMS Data Source)
«precedes»
Query - IT Infrastructure affected by new Vulnerability
(from Data Transformation)
«precedes»
Store Vulnerability Instances
(from Data Warehousing)
«precedes»
Acquire Vulnerability Assessment Scans
«precedes»
Vulnerability Severity Assessment
(from Decision Support System)
«include»
Compute Environmental Risk Value
(from Decision Support System)

**Figure 15: Vulnerability Instances**

**Table 67: Relationships for Acquire Vulnerability and Exploit Data**

| Source | Type | Target |
|---|---|---|
| Acquire Vulnerability and Exploit Data | precedes | Pre-Process Vulnerability and Exploit Data |
| Acquire Vulnerability and Exploit Data | include | Acquire Exploit and Vulnerability Interrelationship Data |

| Source | Type | Target |
|---|---|---|
| Acquire Domain Data | include | Acquire Vulnerability and Exploit Data |
| Acquire Vulnerability and Exploit Data | include | Acquire Vulnerability Data |
| Acquire Vulnerability and Exploit Data | include | Acquire Exploit Data |
| Acquire Vulnerability and Exploit Data | | DID-VED-0 |

**Requirements:**

**DID-VED-0**

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.

## Use Case: Acquire Exploit Data -

**Description:**

The exploit data is collected from security management tools or harvested from web sites, such as the Computer Emergency Response Team (CERT).

| Source | Type | Target |
|---|---|---|
| Acquire Exploit Data | | DID-VED-2 |
| Acquire Exploit Data | invokes | Vulnerability & Exploit Data |
| Acquire Vulnerability and Exploit Data | include | Acquire Exploit Data |
| Acquire Exploit Data | | DID-VED-0 |

**Table 68: Relationships for Acquire Exploit Data**

**Requirements:**

**DID-VED-0**

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.

**DID-VED-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.

## Use Case: Acquire Exploit and Vulnerability Interrelationship Data -

**Description:**

The relationships between exploit and vulnerability data will be captured. The CVE number will be used when available. An exploit can be related to one or more vulnerabilities.

| Source | Type | Target |
|---|---|---|
| Acquire Exploit and Vulnerability Interrelationship Data | | DID-VED-3 |
| Acquire Vulnerability and Exploit Data | include | Acquire Exploit and Vulnerability Interrelationship Data |
| Acquire Exploit and Vulnerability Interrelationship Data | | DID-VED-0 |

**Table 69: Relationships for Acquire Exploit and Vulnerability Interrelationship Data**

**Requirements:**

**DID-VED-0**

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.

**DID-VED-3**

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.

## Use Case: Acquire Scanners Vulnerability Dictionary -

**Description:**

JNDMS will know the entire set of vulnerabilities that the scanners can scan for.

| Source | Type | Target |
|---|---|---|
| Acquire Vulnerability Data | include | Acquire Scanners Vulnerability Dictionary |
| Acquire Scanners Vulnerability Dictionary | invokes | VA Scanner |
| Acquire Scanners Vulnerability Dictionary | precedes | Store Vulnerability Definitions |

**Table 70: Relationships for Acquire Scanners Vulnerability Dictionary**

## Use Case: Acquire Vulnerability Data -

**Description:**

Vulnerability data must be collected. The source of the data can be from a VA tool or from vulnerability assessment data sources such as CVE.

**Table 71: Relationships for Acquire Vulnerability Data**

| Source | Type | Target |
|---|---|---|
| Acquire Vulnerability Data | | DID-VED-1 |

| Source | Type | Target |
|---|---|---|
| Acquire Vulnerability Data | invokes | Vulnerability & Exploit Data |
| Acquire Vulnerability Data | include | Acquire Scanners Vulnerability Dictionary |
| Acquire Vulnerability and Exploit Data | include | Acquire Vulnerability Data |
| Acquire Vulnerability Data | include | Acquire Vulnerability Assessment Scans |
| Acquire Vulnerability Data |  | DID-VED-0 |
| Acquire Vulnerability Data | precedes | Store Vulnerability Definitions |
| Acquire Vulnerability Data | precedes | Query - IT Infrastructure affected by new Vulnerability |

**Requirements:**

**DID-VED-0**

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.

**DID-VED-1**

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 web sites (CVE, Secunia, Bugtraq, 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.

### Use Case: Acquire Vulnerability Assessment Scans -

**Description:**

A Vulnerability Scanner will be used to scan the network for known vulnerabilities.

| Source | Type | Target |
|---|---|---|
| Acquire Vulnerability Assessment Scans | invokes | VA Scanner |
| Acquire Vulnerability Data | include | Acquire Vulnerability Assessment Scans |
| Intellitactics NSM | | Acquire Vulnerability Assessment Scans |
| Acquire Vulnerability Assessment Scans | precedes | Store Vulnerability Instances |

**Table 72: Relationships for Acquire Vulnerability Assessment Scans**

### Use Case: Acquire Security Events -

**Description:**

JNDMS processes security events collected from security devices (Intrusion Detection Systems [IDS], firewalls, virus scanners, ...) and from network devices ( routers, switches, servers, printers, ...).

| Source | Type | Target |
|---|---|---|
| Acquire Domain Data | include | Acquire Security Events |
| Acquire Security Events | | DID-SED-1 |
| Intellitactics NSM | | Acquire Security Events |
| Acquire Security Events | invokes | Network Sensors |
| Acquire Security Events | precedes | Pre-Process Security Events |
| Acquire Security Events | | DID-SED-0 |

**Table 73: Relationships for Acquire Security Events**

**Requirements:**

**DID-SED-0**

The JNDMS shall capture Security Events Data. This function refers to the following sub-functions: acquiring, pre-processing and storing security events data.

**DID-SED-1**

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 equipment, tools and repositories such as firewalls, IDS/IPS, virus scanner, incident ticketing tools, intelligence community reports and other contextual information reports

### 4.2.2 Data Transformation

The data transformation CSCI is a module that is responsible for manipulating data between other CSCIs, and possibly between JNDMS and external sources.

#### Use Case: Data Transformation -

**Description:**

This represents the most general case where data must be transformed from one type to another.

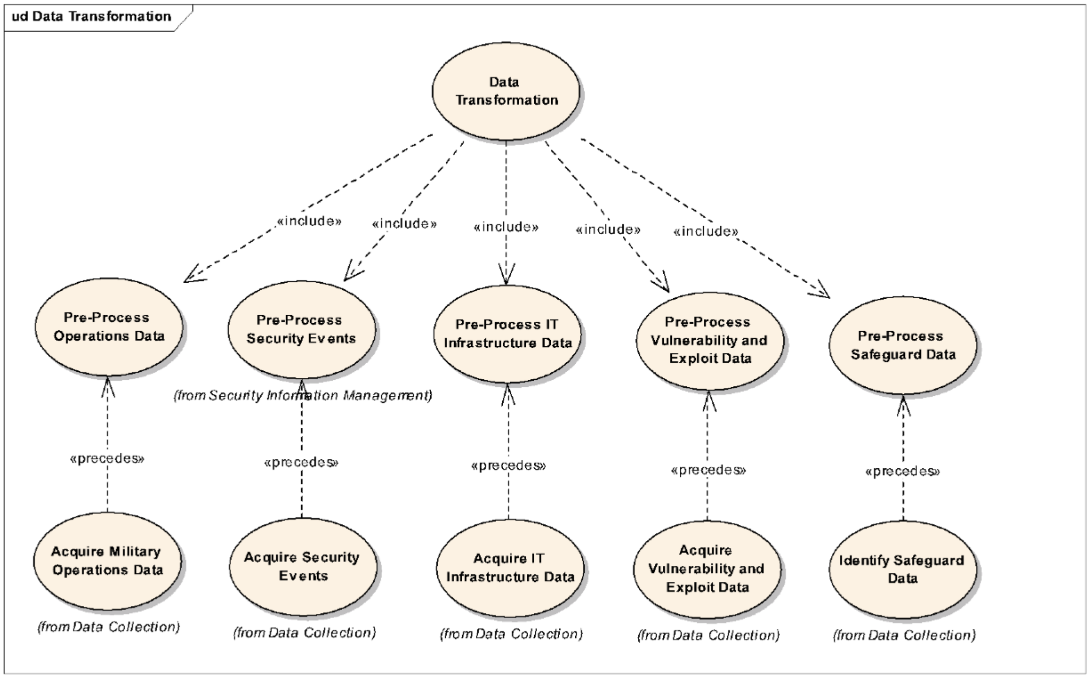

ud Data Transformation
Data Transformation
«include»
«include»
«include»
«include»
«include»
Pre-Process Operations Data
Pre-Process Security Events
(from Security Information Management)
Pre-Process IT Infrastructure Data
Pre-Process Vulnerability and Exploit Data
Pre-Process Safeguard Data
«precedes»
«precedes»
«precedes»
«precedes»
«precedes»
Acquire Military Operations Data
(from Data Collection)
Acquire Security Events
(from Data Collection)
Acquire IT Infrastructure Data
(from Data Collection)
Acquire Vulnerability and Exploit Data
(from Data Collection)
Identify Safeguard Data
(from Data Collection)

**Figure 16: Data Transformation**

| Source | Type | Target |
|---|---|---|
| Data Transformation | | DID-JNDMS-0 |
| Data Transformation | include | Pre-Process Operations Data |
| Data Transformation | include | Pre-Process Security Events |
| Data Transformation | include | Pre-Process IT Infrastructure Data |
| Data Transformation | include | Pre-Process Vulnerability and Exploit Data |
| Data Transformation | include | Pre-Process Safeguard Data |

**Table 74: Relationships for Data Transformation**

**Requirements:**

**DID-JNDMS-0**

The JNDMS shall provide situational awareness (SA) for Computer Network Defence (CND) through the fusion of Military Operations, IT infrastructure, Security events, Vulnerability, and Safeguards data sets. The JNDMS shall capture, store, process, analyze and present data from these five information domains**.**

## Use Case: Pre-Process IT Infrastructure Data -

### Description:

The collected IT infrastructure data must be pre-processed. The pre-processing functions may include filtering, aggregating, de-conflicting and normalization.

| Source | Type | Target |
|---|---|---|
| Pre-Process IT Infrastructure Data | precedes | Store IT Infrastructure Data |
| Acquire IT Infrastructure Data | precedes | Pre-Process IT Infrastructure Data |
| Pre-Process IT Infrastructure Data | | DID-ITID-4 |
| Pre-Process IT Infrastructure Data | | DID-IRELD-0 |
| Pre-Process IT Infrastructure Data | | DID-ITID-0 |
| Data Transformation | include | Pre-Process IT Infrastructure Data |

**Table 75: Relationships for Pre-Process IT Infrastructure Data**

### Requirements:

**DID-IRELD-0**

The JNDMS shall capture inter-relationships between Security Events, Military Operations, IT Infrastructure, Vulnerabilities and safeguards. This function refers to the following sub-functions: analyzing data sets from the 5 information domains (Operations, Infrastructure, Vulnerability, Safeguards, Events) identifying interrelationships between these 5 information domains, identifying Geospatial, connectivity and logical inter-relationships, normalizing these inter-relationships, de-conflicting these inter-relationships, consolidating these inter-relationships and writing them to the JNDMS database.

**DID-ITID-0**

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.

**DID-ITID-4**

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 functions. This includes functions such as filtering, aggregating, de-conflicting, and normalizing to the JNDMS data model every data record acquired**.**

## Use Case: Pre-Process Operations Data -

### Description:

The pre-processing may include filtering, aggregating, de-conflicting and normalization.

| Source | Type | Target |
|---|---|---|
| Pre-Process Operations Data | precedes | Store Operations Data |
| Pre-Process Operations Data | | DID-OD-2 |
| Pre-Process Operations Data | | DID-IRELD-0 |
| Acquire Military Operations Data | precedes | Pre-Process Operations Data |
| Pre-Process Operations Data | | DID-OD-0 |
| Data Transformation | include | Pre-Process Operations Data |

**Table 76: Relationships for Pre-Process Operations Data**

### Requirements:

**DID-IRELD-0**

The JNDMS shall capture inter-relationships between Security Events, Military Operations, IT Infrastructure, Vulnerabilities and safeguards. This function refers to the following sub-functions: analyzing data sets from the 5 information domains (Operations, Infrastructure, Vulnerability, Safeguards, Events) identifying interrelationships between these 5 information domains, identifying Geospatial, connectivity and logical inter-relationships, normalizing these inter-relationships, de-conflicting these inter-relationships, consolidating these inter-relationships and writing them to the JNDMS database.

**DID-OD-0**

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.

**DID-OD-2**

Pre-processing Military Operations Data: The JNDMS shall pre-process the acquired military operation data sets before storage, to assure formatting and content is suited for subsequent JNDMS analysis functionality. This includes functions such as filtering, aggregating, de-conflicting, and normalizing to the JNDMS data model every data record imported from the operational databases or other sources.

## Use Case: Pre-Process Safeguard Data -

### Description:

The pre-processing may include filtering, aggregating, de-conflicting and normalization.

| Source | Type | Target |
|---|---|---|
| Pre-Process Safeguard Data | precedes | Store Safeguard Data |
| Identify Safeguard Data | precedes | Pre-Process Safeguard Data |
| Pre-Process Safeguard Data | | DID-IRELD-0 |
| Pre-Process Safeguard Data | | DID-SAFD-2 |
| Pre-Process Safeguard Data | | DID-SAFD-0 |
| Data Transformation | include | Pre-Process Safeguard Data |
| Pre-Process Safeguard Data | | Safeguards |

**Table 77: Relationships for Pre-Process Safeguard Data**

### Requirements:

**DID-IRELD-0**

The JNDMS shall capture inter-relationships between Security Events, Military Operations, IT Infrastructure, Vulnerabilities and safeguards. This function refers to the following sub-functions: analyzing data sets from the 5 information domains (Operations, Infrastructure, Vulnerability, Safeguards, Events) identifying interrelationships between these 5 information domains, identifying Geospatial, connectivity and logical inter-relationships, normalizing these inter-relationships, de-conflicting these inter-relationships, consolidating these inter-relationships and writing them to the JNDMS database.

**DID-SAFD-0**

The JNDMS shall capture IT Infrastructure Safeguards data. This function refers to the following sub-functions: acquiring IT Infrastructure Safeguards data, pre-processing this data, and writing it to the JNDMS database.

**DID-SAFD-2**

Pre-processing Safeguard Data: The JNDMS shall pre-process the acquired Safeguard data sets before storage, to assure formatting and content is suited for subsequent JNDMS analysis functionality. This includes functions such as filtering, aggregating, de-conflicting, and normalizing to the JNDMS data model every data record acquired.

## Use Case: Pre-Process Vulnerability and Exploit Data -

### Description:

The pre-processing may include filtering, aggregating, de-conflicting and normalization.

| Source | Type | Target |
|---|---|---|
| Acquire Vulnerability and Exploit Data | precedes | Pre-Process Vulnerability and Exploit Data |
| Pre-Process Vulnerability and Exploit Data | | DID-VED-4 |
| Pre-Process Vulnerability and Exploit Data | | DID-IRELD-0 |
| Pre-Process Vulnerability and Exploit Data | | DID-VED-0 |
| Data Transformation | include | Pre-Process Vulnerability and Exploit Data |
| Pre-Process Vulnerability and Exploit Data | precedes | Store Vulnerability and Exploit Data |
| Pre-Process Vulnerability and Exploit Data | | Exploit |
| Pre-Process Vulnerability and Exploit Data | | VulnerabilityDefinition |

**Table 78: Relationships for Pre-Process Vulnerability and Exploit Data**

**Requirements:**

**DID-IRELD-0**

The JNDMS shall capture inter-relationships between Security Events, Military Operations, IT Infrastructure, Vulnerabilities and safeguards. This function refers to the following sub-functions: analyzing data sets from the 5 information domains (Operations, Infrastructure, Vulnerability, Safeguards, Events) identifying interrelationships between these 5 information domains, identifying Geospatial, connectivity and logical inter-relationships, normalizing these inter-relationships, de-conflicting these inter-relationships, consolidating these inter-relationships and writing them to the JNDMS database.

**DID-VED-0**

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.

**DID-VED-4**

Pre-processing Vulnerability and Exploit Data: The JNDMS shall pre-process the acquired Vulnerability and Exploit data sets before storage, to assure formatting and content is suited for subsequent JNDMS analysis functionality. This includes functions such as filtering, aggregating, de-conflicting, and normalizing to the JNDMS data model every data record acquired.

## Use Case: Query - IT Infrastructure affected by new Vulnerability -

**Description:**

The JNDMS IT database is queried to find assets affected by a vulnerability definition (relationships between Vulnerability data and IT Infrastructure data).

| Source | Type | Target |
|---|---|---|
| Query - IT Infrastructure affected by new Vulnerability | precedes | Store Vulnerability Instances |
| Acquire Vulnerability Data | precedes | Query - IT Infrastructure affected by new Vulnerability |
| Query - IT Infrastructure affected by new Vulnerability | | Asset |

**Table 79: Relationships for Query - IT Infrastructure affected by new Vulnerability**

## 4.2.3 Data Warehousing

The data warehousing package includes the use cases related to the storage and queries related to the JNDMS. The data warehouse is the central logical entity where information passes between JNDMS subsystems.

### Use Case: Data Warehousing -

#### Description:

This represents the most general case where the JNDMS database must store data.

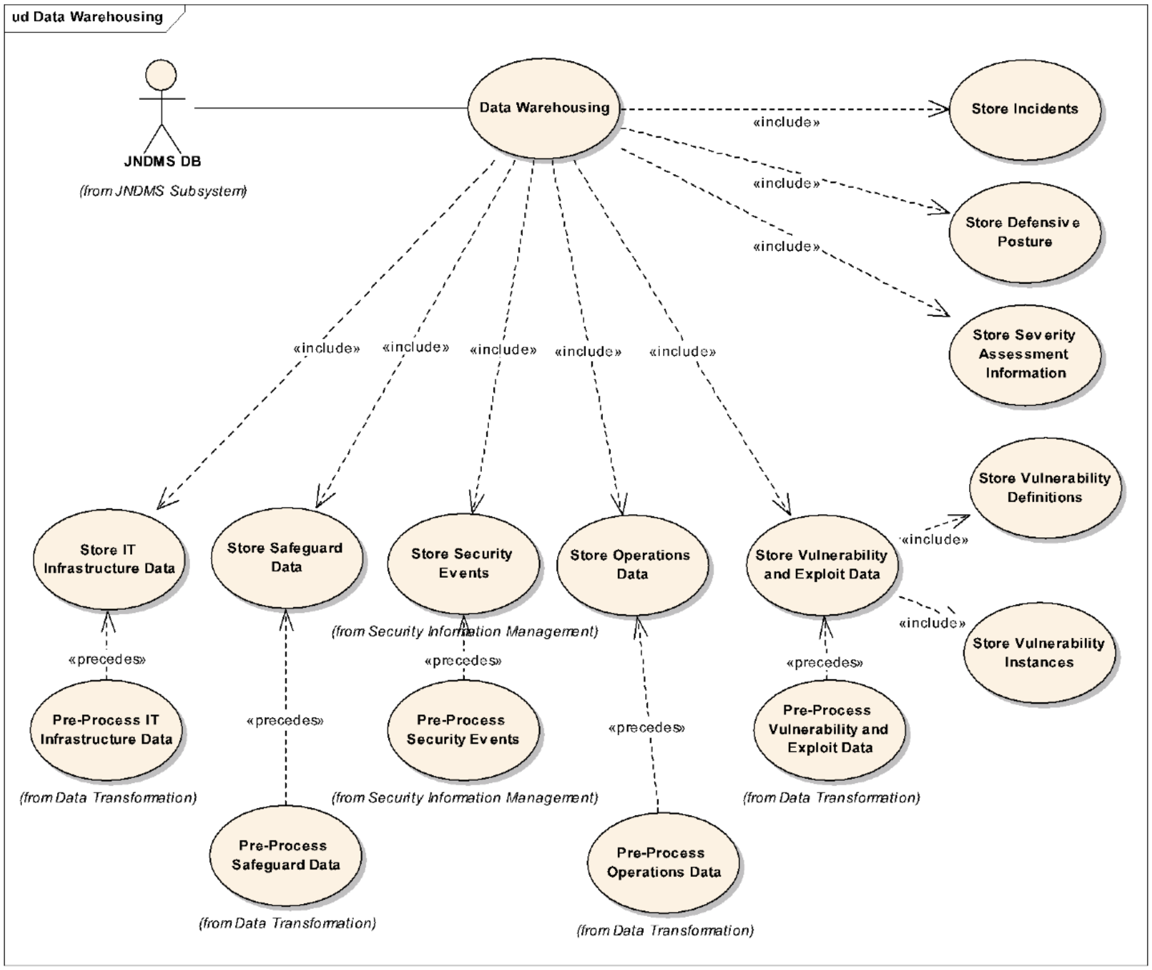

ud Data Warehousing
JNDMS DB
(from JNDMS Subsystem)
Data Warehousing
«include»
Store Incidents
«include»
Store Defensive Posture
«include»
Store Severity Assessment Information
«include»
«include»
«include»
«include»
«include»
Store Vulnerability Definitions
«include»
Store IT Infrastructure Data
Store Safeguard Data
Store Security Events
(from Security Information Management)
Store Operations Data
Store Vulnerability and Exploit Data
«include»
Store Vulnerability Instances
«precedes»
«precedes»
«precedes»
«precedes»
«precedes»
Pre-Process IT Infrastructure Data
(from Data Transformation)
Pre-Process Security Events
(from Security Information Management)
Pre-Process Vulnerability and Exploit Data
(from Data Transformation)
Pre-Process Safeguard Data
(from Data Transformation)
Pre-Process Operations Data
(from Data Transformation)

Figure 17: Data Warehousing

| Source | Type | Target |
|---|---|---|
| JNDMS DB | | Data Warehousing |
| Data Warehousing | | DID-JNDMS-0 |
| Data Warehousing | include | Store IT Infrastructure Data |
| Data Warehousing | include | Store Safeguard Data |
| Data Warehousing | include | Store Security Events |
| Data Warehousing | include | Store Operations Data |
| Data Warehousing | include | Store Vulnerability and Exploit Data |
| Data Warehousing | include | Store Severity Assessment Information |
| Data Warehousing | include | Store Defensive Posture |
| Data Warehousing | include | Store Incidents |

**Table 80: Relationships for Data Warehousing**

**Requirements:**

**DID-JNDMS-0**

The JNDMS shall provide situational awareness (SA) for Computer Network Defence (CND) through the fusion of Military Operations, IT infrastructure, Security events, Vulnerability, and Safeguards data sets. The JNDMS shall capture, store, process, analyze and present data from these five information domains**.**

## Use Case: Store Defensive Posture -

**Description:**

The defensive posture is updated in the data warehouse to reflect the current behaviour of the system.

| Source | Type | Target |
|---|---|---|
| Store Defensive Posture | | DID-DM-0 |
| Store Defensive Posture | | DID-DM-1 |
| Store Defensive Posture | | DID-DM-2 |
| Store Defensive Posture | | DID-DM-3 |
| Store Defensive Posture | | DID-DM-4 |
| Data Warehousing | include | Store Defensive Posture |
| Defensive Posture Assessment | include | Store Defensive Posture |

**Table 81: Relationships for Store Defensive Posture**

**Requirements:**

**DID-DM-0**

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 sub-functions: 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.

**DID-DM-1**

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.

**DID-DM-2**

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 data sets, and point to other data storage systems.

**DID-DM-3**

Temporal Database: The JNDMS shall offer temporal database features including support for temporal queries, precise time stamps of records, and mechanisms preventing the duplication, and loss, of records having conflicting timestamps.

**DID-DM-4**

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.

## Use Case: Store IT Infrastructure Data -

### Description:

Any IT infrastructure data collected that is required by JNDMS will be stored in the data warehouse. The information stored must include the assets, locations, and relationships.

| Source | Type | Target |
|---|---|---|
| Pre-Process IT Infrastructure Data | precedes | Store IT Infrastructure Data |
| Store IT Infrastructure Data | | DID-ITID-5 |
| Store IT Infrastructure Data | | DID-DM-0 |
| Store IT Infrastructure Data | | DID-DM-1 |
| Store IT Infrastructure Data | | DID-DM-2 |
| Store IT Infrastructure Data | | DID-DM-3 |
| Store IT Infrastructure Data | | DID-DM-4 |
| Store IT Infrastructure Data | | DID-ITID-0 |
| Data Warehousing | include | Store IT Infrastructure Data |

**Table 82: Relationships for Store IT Infrastructure Data**

**Requirements:**

**DID-DM-0**

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 sub-functions: 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.

**DID-DM-1**

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**.**

**DID-DM-2**

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 data sets, and point to other data storage systems.

**DID-DM-3**

Temporal Database: The JNDMS shall offer temporal database features including support for temporal queries, precise time stamps of records, and mechanisms preventing the duplication, and loss, of records having conflicting timestamps.

**DID-DM-4**

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.

**DID-ITID-0**

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.

**DID-ITID-5**

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.

## Use Case: Store Incidents -

### Description:

Incidents are stored in the JNDMS database with context information.

| Source | Type | Target |
|---|---|---|
| Store Incidents | | DID-IR-4 |
| Store Incidents | | DID-DM-0 |
| Store Incidents | | DID-DM-1 |
| Store Incidents | | DID-DM-2 |
| Store Incidents | | DID-DM-3 |
| Store Incidents | | DID-DM-4 |
| Data Warehousing | include | Store Incidents |
| Store Incidents | | DID-IR-0 |

**Table 83: Relationships for Store Incidents**

### Requirements:

**DID-DM-0**

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 sub-functions: 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.

**DID-DM-1**

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**.**

**DID-DM-2**

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 data sets, and point to other data storage systems.

**DID-DM-3**

Temporal Database: The JNDMS shall offer temporal database features including support for temporal queries, precise time stamps of records, and mechanisms preventing the duplication, and loss, of records having conflicting timestamps.

**DID-DM-4**

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.

**DID-IR-0**

The JNDMS shall fuse information from the five SA for CND domains (Operations, Infrastructure, Vulnerability, Safeguards, Events) to recognize incidents affecting the IT infrastructure and correlate these incidents together. This function refers to the following sub-functions: identifying incidents through the analysis of data set from the 5 information domains (Operations, Infrastructure, Vulnerability, Safeguards, Events), filtering identified incidents, correlating identified incidents, and writing incidents to the JNDMS database.

**DID-IR-4**

Store Incident Data: The JNDMS shall store incidents in the JNDMS database. The JNDMS shall assure that incident data is stored with accurate timestamp and integrity verification.

## Use Case: Store Operations Data -

### Description:

The operations data collected (generally from J6 ops) must be stored in the database.

| Source | Type | Target |
|---|---|---|
| Pre-Process Operations Data | precedes | Store Operations Data |
| Store Operations Data | | DID-OD-3 |
| Store Operations Data | | DID-DM-0 |
| Store Operations Data | | DID-DM-1 |
| Store Operations Data | | DID-DM-2 |
| Store Operations Data | | DID-DM-3 |
| Store Operations Data | | DID-DM-4 |
| Store Operations Data | | DID-OD-0 |
| Data Warehousing | include | Store Operations Data |

**Table 84: Relationships for Store Operations Data**

### Requirements:

**DID-DM-0**

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 sub-functions: 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.

**DID-DM-1**

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.

**DID-DM-2**

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 data sets, and point to other data storage systems.

**DID-DM-3**

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 timestamps.

**DID-DM-4**

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.

**DID-OD-0**

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.

**DID-OD-3**

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.

## Use Case: Store Safeguard Data -

### Description:

The safeguard data must be stored in such as way as to allow the information to be processed to build the defensive posture.

| Source | Type | Target |
|---|---|---|
| Pre-Process Safeguard Data | precedes | Store Safeguard Data |
| Store Safeguard Data | | DID-SAFD-3 |
| Store Safeguard Data | | DID-DM-0 |
| Store Safeguard Data | | DID-DM-1 |
| Store Safeguard Data | | DID-DM-2 |
| Store Safeguard Data | | DID-DM-3 |
| Store Safeguard Data | | DID-DM-4 |
| Store Safeguard Data | | DID-SAFD-0 |
| Data Warehousing | include | Store Safeguard Data |

**Table 85: Relationships for Store Safeguard Data**

**Requirements:**

**DID-DM-0**

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 sub-functions: 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.

**DID-DM-1**

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**.**

**DID-DM-2**

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 data sets, and point to other data storage systems.

**DID-DM-3**

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 timestamps.

**DID-DM-4**

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.

**DID-SAFD-0**

The JNDMS shall capture IT Infrastructure Safeguards data. This function refers to the following sub-functions: acquiring IT Infrastructure Safeguards data, pre-processing this data, and writing it to the JNDMS database.

**DID-SAFD-3**

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.

## Use Case: Store Severity Assessment Information -

**Description:**

The results of the severity assessment are stored in the JNDMS database.

**Table 86: Relationships for Store Severity Assessment Information**

| Source | Type | Target |
|---|---|---|
| Store Severity Assessment Information | | DID-SA-5 |
| Incident Severity Assessment | include | Store Severity Assessment Information |
| Store Severity Assessment Information | | DID-DM-0 |
| Store Severity Assessment Information | | DID-DM-1 |

| Source | Type | Target |
|---|---|---|
| Store Severity Assessment Information | | DID-DM-2 |
| Store Severity Assessment Information | | DID-DM-3 |
| Store Severity Assessment Information | | DID-DM-4 |
| Data Warehousing | include | Store Severity Assessment Information |
| Store Severity Assessment Information | | DID-SA-0 |

**Requirements:**

**DID-DM-0**

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 sub-functions: 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.

**DID-DM-1**

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**.**

**DID-DM-2**

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 data sets, and point to other data storage systems.

**DID-DM-3**

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 timestamps.

**DID-DM-4**

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.

**DID-SA-0**

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**.**

**DID-SA-5**

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 timestamp and integrity verification. The Severity Assessment Information shall be continuously updated. The JNDMS shall store history of incident severity values and rolled-up values

## Use Case: Store Vulnerability and Exploit Data -

### Description:

The vulnerability and exploit data must be stored to allow for the relationships to the IT assets to be maintained.

**Table 87: Relationships for Store Vulnerability and Exploit Data**

| Source | Type | Target |
|---|---|---|
| Store Vulnerability and Exploit Data | include | Store Vulnerability Definitions |

| Source | Type | Target |
|---|---|---|
| Store Vulnerability and Exploit Data | | DID-VED-5 |
| Store Vulnerability and Exploit Data | | DID-DM-0 |
| Store Vulnerability and Exploit Data | | DID-DM-1 |
| Store Vulnerability and Exploit Data | | DID-DM-2 |
| Store Vulnerability and Exploit Data | | DID-DM-3 |
| Store Vulnerability and Exploit Data | | DID-DM-4 |
| Store Vulnerability and Exploit Data | | DID-VED-0 |
| Data Warehousing | include | Store Vulnerability and Exploit Data |
| Pre-Process Vulnerability and Exploit Data | precedes | Store Vulnerability and Exploit Data |
| Store Vulnerability and Exploit Data | include | Store Vulnerability Instances |
| Store Vulnerability and Exploit Data | | VulnerabilityDefinition |
| Store Vulnerability and Exploit Data | | Exploit |

**Requirements:**

**DID-DM-0**

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 sub-functions: 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.

**DID-DM-1**

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**.**

**DID-DM-2**

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 data sets, and point to other data storage systems.

**DID-DM-3**

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 timestamps.

**DID-DM-4**

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.

**DID-VED-0**

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.

**DID-VED-5**

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.

## Use Case: Store Vulnerability Definitions -

### Description:

This is the JNDMS vulnerability dictionary.

| Source | Type | Target |
|---|---|---|
| Store Vulnerability and Exploit Data | include | Store Vulnerability Definitions |
| Acquire Vulnerability Data | precedes | Store Vulnerability Definitions |
| Acquire Scanners Vulnerability Dictionary | precedes | Store Vulnerability Definitions |
| Store Vulnerability Definitions | | VulnerabilityDefinition |

**Table 88: Relationships for Store Vulnerability Definitions**

### Use Case: Store Vulnerability Instances -

**Description:**

A vulnerability instance is a vulnerability assigned to an Asset. The instance has a Vulnerability Definition parent.

| Source | Type | Target |
|---|---|---|
| Acquire Vulnerability Assessment Scans | precedes | Store Vulnerability Instances |
| Query - IT Infrastructure affected by new Vulnerability | precedes | Store Vulnerability Instances |
| Store Vulnerability Instances | precedes | Vulnerability Severity Assessment |
| Store Vulnerability and Exploit Data | include | Store Vulnerability Instances |
| Store Vulnerability Instances | | VulerabilityInstances |

**Table 89: Relationships for Store Vulnerability Instances**

## 4.2.4 Decision Support System

The decision support system package contains the use cases related to the business logic layer of the JNDMS. The decision support system may be comprised of a set of rules, rule engines or other algorithmic entities that can provide the correlation and decision making support required for JNDMS.

## Use Case: Data Fusion -

### Description:

This represents the most general case where JNDMS will fuse the data collected.

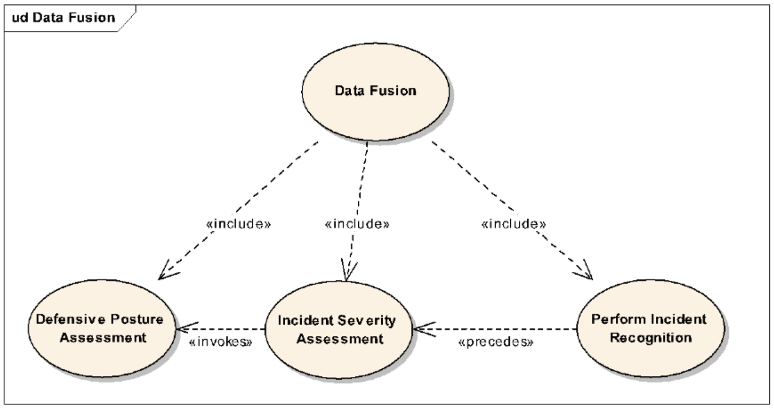

ud Data Fusion
Data Fusion
«include»
«include»
«include»
Defensive Posture Assessment
«invokes»
Incident Severity Assessment
«precedes»
Perform Incident Recognition

**Figure 18: Data Fusion**

| Source | Type | Target |
|---|---|---|
| Data Fusion | include | Perform Incident Recognition |
| Data Fusion | include | Defensive Posture Assessment |
| Data Fusion | include | Incident Severity Assessment |
| Data Fusion | | DID-JNDMS-0 |

**Table 90: Relationships for Data Fusion**

### Requirements:

**DID-JNDMS-0**

The JNDMS shall provide situational awareness (SA) for Computer Network Defence (CND) through the fusion of Military Operations, IT infrastructure, Security events, Vulnerability, and Safeguards data sets. The JNDMS shall capture, store, process, analyze and present data from these five information domains**.**

## Use Case: Real-time Incident Recognition -

### Description:

Incidents are first identified, classified and prioritized in the first layer of JNDMS (the Security Information Manager subsystem, the Enterprise Infrastructure Management subsystem and the Ticketing Tool). The incidents can be from any one of the input domains. JNDMS prioritizes these events and correlates them as referenced in the associated requirements.

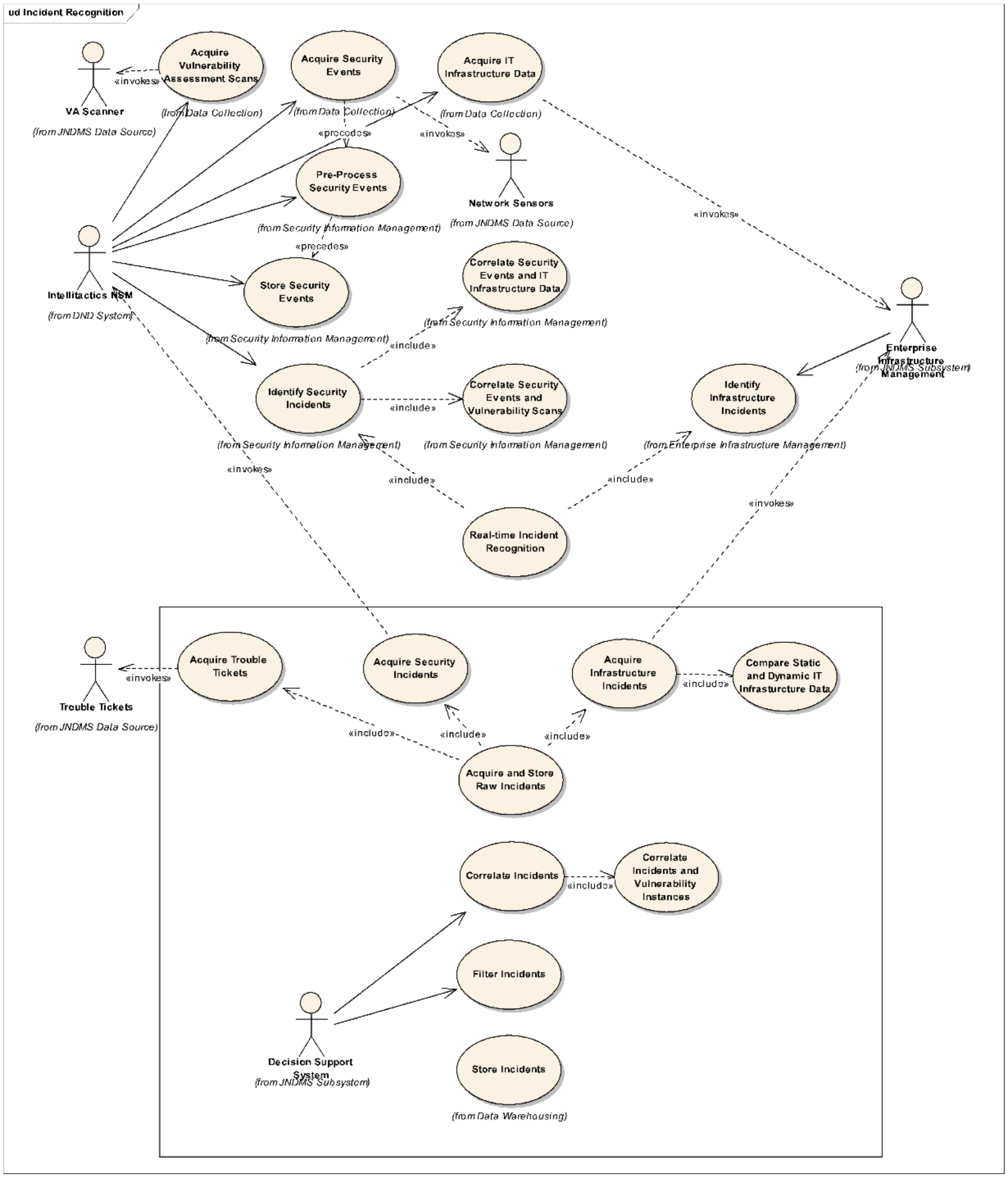

ud Incident Recognition
Acquire Vulnerability Assessment Scans
(from Data Collection)
«invokes»
VA Scanner
(from JNDMS Data Source)
Acquire Security Events
(from Data Collection)
Acquire IT Infrastructure Data
(from Data Collection)
«precedes»
«invokes»
Network Sensors
(from JNDMS Data Source)
Pre-Process Security Events
(from Security Information Management)
«precedes»
Intellitactics NSM
(from DND System)
Store Security Events
(from Security Information Management)
Correlate Security Events and IT Infrastructure Data
(from Security Information Management)
«include»
Identify Security Incidents
(from Security Information Management)
«include»
Correlate Security Events and Vulnerability Scans
(from Security Information Management)
«invokes»
Enterprise Infrastructure Management
(from JNDMS Subsystem)
Identify Infrastructure Incidents
(from Enterprise Infrastructure Management)
«invokes»
«include»
«include»
«invokes»
Real-time Incident Recognition
Trouble Tickets
(from JNDMS Data Source)
«invokes»
Acquire Trouble Tickets
Acquire Security Incidents
Acquire Infrastructure Incidents
«include»
Compare Static and Dynamic IT Infrasturcture Data
«include»
«include»
«include»
Acquire and Store Raw Incidents
Correlate Incidents
«include»
Correlate Incidents and Vulnerability Instances
Filter Incidents
Decision Support System
(from JNDMS Subsystem)
Store Incidents
(from Data Warehousing)

**Figure 19: Incident Recognition**

| Source | Type | Target |
|---|---|---|
| Real-time Incident Recognition | | DID-IR-1 |
| Real-time Incident Recognition | | DID-IR-5 |
| Real-time Incident Recognition | include | Identify Security Incidents |
| Real-time Incident Recognition | include | Identify Infrastructure Incidents |
| Real-time Incident Recognition | | DID-IR-0 |

**Table 91: Relationships for Real-time Incident Recognition**

**Requirements:**

**DID-IR-0**

The JNDMS shall fuse information from the five SA for CND domains (Operations, Infrastructure, Vulnerability, Safeguards, Events) to recognize incidents affecting the IT infrastructure and correlate these incidents together. This function refers to the following sub-functions: identifying incidents through the analysis of data set from the 5 information domains (Operations, Infrastructure, Vulnerability, Safeguards, Events), filtering identified incidents, correlating identified incidents, and writing incidents to the JNDMS database.

**DID-IR-1**

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 meta rules to extend basic rules used by Security Events feeder systems such as IDS.

**DID-IR-5**

Perform near real-time Incident Recognition: The JNDMS shall perform all incident recognition functions in near real-time to support other JNDMS features and functionality. Near real-time performance is discussed in the quality attributes of the JNDMS (section 11).

## Use Case: Acquire and Store Raw Incidents -

**Description:**

The incidents are retrieved from three different sources: the Security Information Management subsystem, for most security incidents, the Enterprise Infrastructure

Management subsystem, for incidents related to the IT infrastructure, and the organisation's Trouble Ticketing tool. These incidents are entered into the JNDMS database and trigger the decision support system.

| Source | Type | Target |
|---|---|---|
| Acquire and Store Raw Incidents | include | Acquire Security Incidents |
| Acquire and Store Raw Incidents | include | Acquire Infrastructure Incidents |
| Acquire and Store Raw Incidents | include | Acquire Trouble Tickets |

**Table 92: Relationships for Acquire and Store Raw Incidents**

## Use Case: Acquire Infrastructure Incidents -

### Description:

The Infrastructure Incidents are incidents that have an impact on the availability of the infrastructure. They are detected with the help of service monitoring tools (EIM, stand alone agents or data collected from network Management Information Bases [MIB]).

| Source | Type | Target |
|---|---|---|
| Acquire Infrastructure Incidents | include | Compare Static and Dynamic IT Infrastructure Data |
| Acquire Infrastructure Incidents | invokes | Enterprise Infrastructure Management |
| Acquire and Store Raw Incidents | include | Acquire Infrastructure Incidents |

**Table 93: Relationships for Acquire Infrastructure Incidents**

## Use Case: Acquire Trouble Tickets -

### Description:

The information from a Trouble Ticketing tool is captured periodically and is used to correlate with other JNDMS incidents.

| Source | Type | Target |
|---|---|---|
| Acquire Trouble Tickets | invokes | Trouble Tickets |
| Acquire and Store Raw Incidents | include | Acquire Trouble Tickets |

**Table 94: Relationships for Acquire Trouble Tickets**

## Use Case: Acquire Security Incidents -

### Description:

JNDMS continuously acquires Security Incidents that have been pre-processed in the Security Information Management Subsystem. These incidents can be one event or a group of related events from sensors.

| Source | Type | Target |
|---|---|---|
| Acquire Security Incidents | invokes | Intellitactics NSM |
| Acquire and Store Raw Incidents | include | Acquire Security Incidents |

**Table 95: Relationships for Acquire Security Incidents**

## Use Case: Compare Static and Dynamic IT Infrastructure Data -

### Description:

The "static" and "dynamic" IT infrastructure data is compared and discrepancies are raised as Incidents.

| Source | Type | Target |
|---|---|---|
| Acquire Infrastructure Incidents | include | Compare Static and Dynamic IT Infrastructure Data |

**Table 96: Relationships for Compare Static and Dynamic IT Infrastructure Data**

## Use Case: Correlate Incidents -

### Description:

Incidents from the three sources (EIM, SIM and TT) are correlated (correlations using asset types or time properties for example). First, it includes associating incidents from the three sources.

| Source | Type | Target |
|---|---|---|
| Correlate Incidents | | DID-IR-2 |
| Decision Support System | | Correlate Incidents |
| Correlate Incidents | | DID-IR-0 |
| Correlate Incidents | include | Correlate Incidents and Vulnerability Instances |

**Table 97: Relationships for Correlate Incidents**

### Requirements:

**DID-IR-0**

The JNDMS shall fuse information from the five SA for CND domains (Operations, Infrastructure, Vulnerability, Safeguards, Events) to recognize incidents affecting the IT infrastructure and correlate these incidents together. This function refers to the following sub-functions: identifying incidents through the analysis of data set from the 5 information domains (Operations, Infrastructure, Vulnerability, Safeguards, Events), filtering identified incidents, correlating identified incidents, and writing incidents to the JNDMS database.

**DID-IR-2**

Correlate Incidents: The JNDMS shall consider new incidents, archived incidents, and shared incidents from other/external organizations 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**.**

## Use Case: Correlate Incidents and Vulnerability Instances -

### Description:

This task correlates any incidents with vulnerability instances.

| Source | Type | Target |
|---|---|---|
| Correlate Incidents | include | Correlate Incidents and Vulnerability Instances |

**Table 98: Relationships for Correlate Incidents and Vulnerability Instances**

## Use Case: Filter Incidents -

### Description:

The correlated incidents are filtered, normalized and de-conflicted. JNDMS filters out incidents, which do not require further processing.

| Source | Type | Target |
|---|---|---|
| Filter Incidents | | DID-IR-3 |
| Decision Support System | | Filter Incidents |
| Filter Incidents | | DID-IR-0 |

**Table 99: Relationships for Filter Incidents**

### Requirements:

**DID-IR-0**

The JNDMS shall fuse information from the five SA for CND domains (Operations, Infrastructure, Vulnerability, Safeguards, Events) to recognize incidents affecting the IT infrastructure and correlate these incidents together. This function refers to the following sub-functions: identifying incidents through the analysis of data set from the 5 information domains (Operations, Infrastructure, Vulnerability, Safeguards, Events), filtering identified incidents, correlating identified incidents, and writing incidents to the JNDMS database.

**DID-IR-3**

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.

## Use Case: Incident Severity Assessment -

### Description:

The overall severity of the incident must be assessed. This is a key event in the Decision Support System and must take into account the full SA to fully evaluate the severity.

JNDMS will generate a severity value for each incident, with supporting evidence. Rolled-up severity values will also be generated for the overall situation.

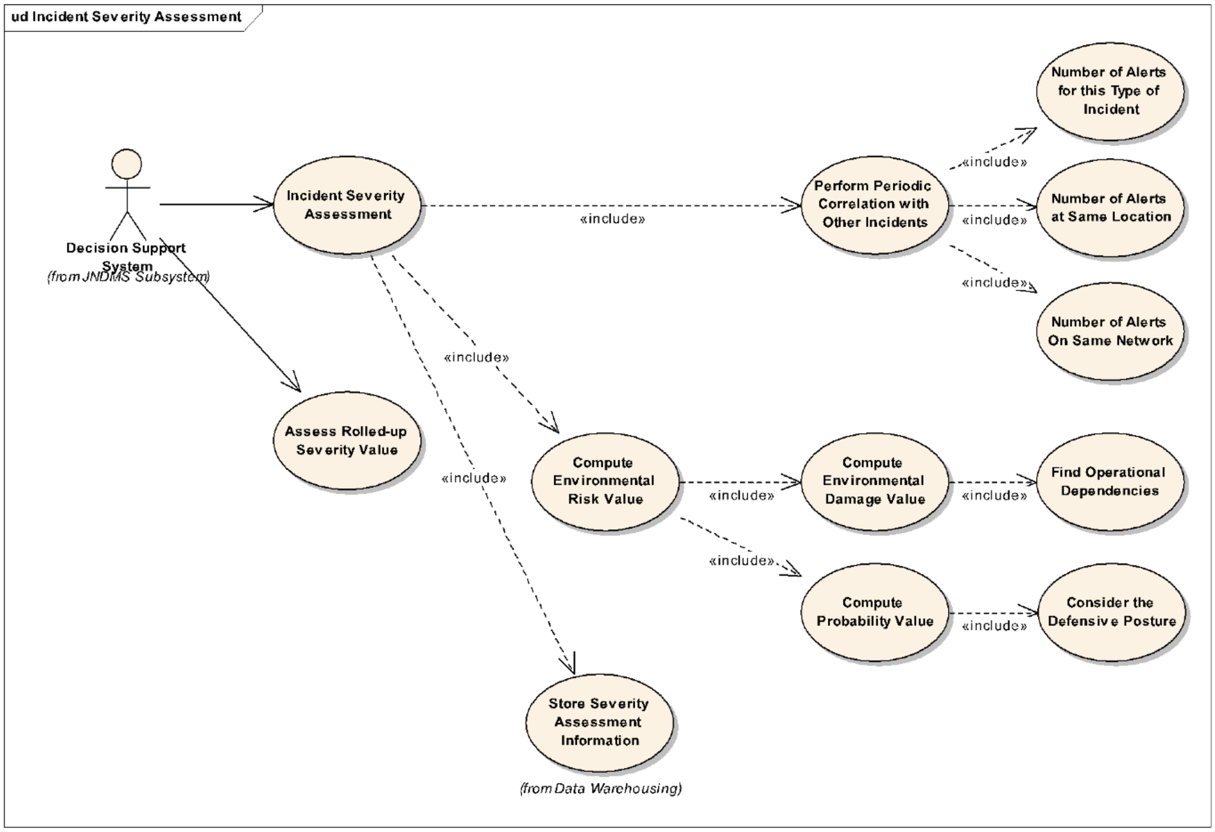

ud Incident Severity Assessment
Decision Support System
(from JNDMS Subsystem)
Incident Severity Assessment
«include»
Perform Periodic Correlation with Other Incidents
«include»
Number of Alerts for this Type of Incident
«include»
Number of Alerts at Same Location
«include»
Number of Alerts On Same Network
Assess Rolled-up Severity Value
«include»
«include»
Compute Environmental Risk Value
«include»
Compute Environmental Damage Value
«include»
Find Operational Dependencies
«include»
Compute Probability Value
«include»
Consider the Defensive Posture
Store Severity Assessment Information
(from Data Warehousing)

**Figure 20: Incident Severity Assessment**

**Table 100: Relationships for Incident Severity Assessment**

| Source | Type | Target |
|---|---|---|
| Perform Incident Recognition | precedes | Incident Severity Assessment |
| Decision Support System | | Incident Severity Assessment |

| Source | Type | Target |
|---|---|---|
| Incident Severity Assessment | include | Perform Periodic Correlation with Other Incidents |
| Incident Severity Assessment | include | Compute Environmental Risk Value |
| Incident Severity Assessment | include | Store Severity Assessment Information |
| Incident Severity Assessment | | DID-SA-3 |
| Incident Severity Assessment | | DID-SA-4 |
| Incident Severity Assessment | | DID-IR-0 |
| Incident Severity Assessment | | DID-SA-0 |
| Incident Severity Assessment | invokes | Defensive Posture Assessment |
| Data Fusion | include | Incident Severity Assessment |

**Requirements:**

**DID-IR-0**

The JNDMS shall fuse information from the five SA for CND domains (Operations, Infrastructure, Vulnerability, Safeguards, Events) to recognize incidents affecting the IT infrastructure and correlate these incidents together. This function refers to the following sub-functions: identifying incidents through the analysis of data set from the 5 information domains (Operations, Infrastructure, Vulnerability, Safeguards, Events), filtering identified incidents, correlating identified incidents, and writing incidents to the JNDMS database.

**DID-SA-0**

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.

**DID-SA-3**

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 data sets. The JNDMS shall make use of a normalized severity scale meaningful to the JNDMS users. The JNDMS shall generate a severity value and supporting evidence statement.

**DID-SA-4**

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.

## Use Case: Assess Rolled-up Severity Value -

**Description:**

This is the rolled-up severity value attributed to the overall situation (for either incidents or vulnerabilities).

| Source | Type | Target |
|---|---|---|
| Decision Support System | | Assess Rolled-up Severity Value |
| Identify Defensive Components | include | Assess Rolled-up Severity Value |

**Table 101: Relationships for Assess Rolled-up Severity Value**

## Use Case: Consider the Defensive Posture -

**Description:**

This is the defensive posture for the targeted asset(s). The defensive posture may influence the probability of damage.

| Source | Type | Target |
|---|---|---|
| Compute Probability Value | include | Consider the Defensive Posture |

**Table 102: Relationships for Consider the Defensive Posture**

## Use Case: Compute Environmental Risk Value -

### Description:

The risk is the probability of realization of the full impact (damage) associated with an incident or vulnerability. The risk can be expressed in the form: Risk = Probability (over time) x Damage (over time).

| Source | Type | Target |
|---|---|---|
| Compute Environmental Risk Value | include | Compute Environmental Damage Value |
| Compute Environmental Risk Value | include | Compute Probability Value |
| Incident Severity Assessment | include | Compute Environmental Risk Value |
| Compute Environmental Risk Value |  | DID-SA-2 |
| Vulnerability Severity Assessment | include | Compute Environmental Risk Value |
| Compute Environmental Risk Value |  | DID-SA-0 |

**Table 103: Relationships for Compute Environmental Risk Value**

### Requirements:

**DID-SA-0**

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**.**

**DID-SA-2**

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 realization 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.

## Use Case: Compute Environmental Damage Value -

### Description:

The Environmental Damage is the summation of the Environment Base Score, the Environmental Damage Value and the Operation Dependency Value.

The Environment Base Score is the value assigned to IT Infrastructure based on Confidentiality, Integrity and Availability (CIA). The score of one asset is the summation of all affected assets (children).

The Environmental Damage Value includes the loss of reputation, financial loss or injury.

The Operation Dependency Value is the IT criticality value based on IT service type, IT value, location priority and operation priority.

| Source | Type | Target |
|---|---|---|
| Compute Environmental Risk Value | include | Compute Environmental Damage Value |
| Compute Environmental Damage Value | include | Find Operational Dependencies |
| Compute Environmental Damage Value | | DID-SA-1 |
| Compute Environmental Damage Value | | DID-SA-0 |

**Table 104: Relationships for Compute Environmental Damage Value**

### Requirements:

**DID-SA-0**

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.

**DID-SA-1**

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.

### Use Case: Compute Probability Value -

#### Description:

The probability changes with time. The time before a preventive action is taken will contribute to increase or decrease the probability of damage. JNDMS may also take into account attributes such as maturity and availability of the exploit to assess the probability of damage. Another factor that may be considered is the characteristics of an attacker.

| Source | Type | Target |
|---|---|---|
| Compute Probability Value | include | Consider the Defensive Posture |
| Compute Environmental Risk Value | include | Compute Probability Value |

**Table 105: Relationships for Compute Probability Value**

### Use Case: Find Operational Dependencies -

#### Description:

Incidents affect IT assets and IT assets are essential for military operations. It is thus essential to consider the IT value for deployed operations while calculating the potential damage of an incident.

| Source | Type | Target |
|---|---|---|
| Compute Environmental Damage Value | include | Find Operational Dependencies |

**Table 106: Relationships for Find Operational Dependencies**

## Use Case: Perform Periodic Correlation with Other Incidents -

### Description:

This kind of correlation is performed periodically as the output may change over time. It provides a sense of damage (or risk) over time.

| Source | Type | Target |
|---|---|---|
| Perform Periodic Correlation with Other Incidents | include | Number of Alerts for this Type of Incident |
| Incident Severity Assessment | include | Perform Periodic Correlation with Other Incidents |
| Perform Periodic Correlation with Other Incidents | include | Number of Alerts at Same Location |
| Perform Periodic Correlation with Other Incidents | include | Number of Alerts On Same Network |

**Table 107: Relationships for Perform Periodic Correlation with Other Incidents**

## Use Case: Number of Alerts On Same Network -

### Description:

This activity will count the number of alerts on the same network and provide this information to requesting modules.

| Source | Type | Target |
|---|---|---|
| Perform Periodic Correlation with Other Incidents | include | Number of Alerts On Same Network |

**Table 108: Relationships for Number of Alerts On Same Network**

## Use Case: Number of Alerts at Same Location -

### Description:

This activity will count the number of alerts at the same location and provide this information to requesting modules. The location will be an input to this activity.

| Source | Type | Target |
|---|---|---|
| Perform Periodic Correlation with Other Incidents | include | Number of Alerts at Same Location |

**Table 109: Relationships for Number of Alerts at Same Location**

## Use Case: Number of Alerts for this Type of Incident -

### Description:

For one particular incident, count of many alerts are of that same type in the system.

| Source | Type | Target |
|---|---|---|
| Perform Periodic Correlation with Other Incidents | include | Number of Alerts for this Type of Incident |

**Table 110: Relationships for Number of Alerts for this Type of Incident**

## Use Case: Defensive Posture Assessment -

### Description:

The defensive posture of the IT infrastructure is assessed periodically.

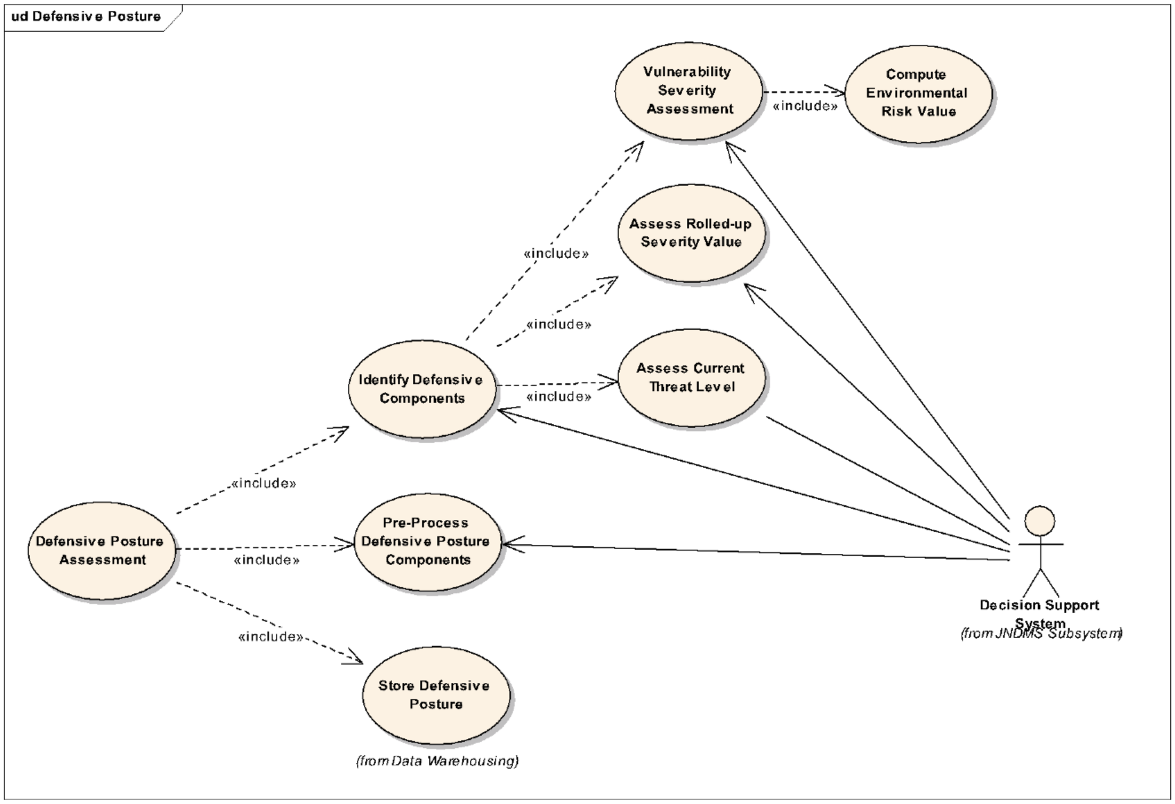

ud Defensive Posture
Vulnerability Severity Assessment
Compute Environmental Risk Value
«include»
Assess Rolled-up Severity Value
«include»
«include»
Identify Defensive Components
Assess Current Threat Level
«include»
«include»
Defensive Posture Assessment
Pre-Process Defensive Posture Components
«include»
«include»
Store Defensive Posture
(from Data Warehousing)
Decision Support System
(from JNDMS Subsystem)

**Figure 21: Defensive Posture**

| Source | Type | Target |
|---|---|---|
| Defensive Posture Assessment | | DID-DPA-0 |
| Defensive Posture Assessment | include | Identify Defensive Components |
| Defensive Posture Assessment | include | Pre-Process Defensive Posture Components |
| Defensive Posture Assessment | include | Store Defensive Posture |
| Incident Severity Assessment | invokes | Defensive Posture Assessment |
| Data Fusion | include | Defensive Posture Assessment |

**Table 111: Relationships for Defensive Posture Assessment**

**Requirements:**

**DID-DPA-0**

The JNDMS shall assess the Defensive Posture of the IT infrastructure. This function refers to the following sub-functions: analyzing the information from data sets, 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**.**

## Use Case: Identify Defensive Components -

**Description:**

JNDMS will look for information in the five CND domains.

| Source | Type | Target |
|---|---|---|
| Identify Defensive Components | include | Assess Current Threat Level |
| Identify Defensive Components | include | Vulnerability Severity Assessment |
| Identify Defensive Components | include | Assess Rolled-up Severity Value |
| Defensive Posture Assessment | include | Identify Defensive Components |
| Decision Support System | | Identify Defensive Components |

**Table 112: Relationships for Identify Defensive Components**

## Use Case: Pre-Process Defensive Posture Components -

**Description:**

The pre-processing stage may include filtering, aggregating, de-conflicting, consolidating and normalization.

| Source | Type | Target |
|---|---|---|
| Defensive Posture Assessment | include | Pre-Process Defensive Posture Components |
| Decision Support System | | Pre-Process Defensive Posture Components |

**Table 113: Relationships for Pre-Process Defensive Posture Components**

## Use Case: Vulnerability Severity Assessment -

### Description:

This is the severity assessment for each vulnerability instances.

| Source | Type | Target |
|---|---|---|
| Decision Support System | | Vulnerability Severity Assessment |
| Vulnerability Severity Assessment | include | Compute Environmental Risk Value |
| Identify Defensive Components | include | Vulnerability Severity Assessment |
| Store Vulnerability Instances | precedes | Vulnerability Severity Assessment |

**Table 114: Relationships for Vulnerability Severity Assessment**

## Use Case: Assess Current Threat Level -

### Description:

The level of threat can be assessed by looking at successful attacks and attempted attacks over time.

| Source | Type | Target |
|---|---|---|
| Identify Defensive Components | include | Assess Current Threat Level |
| Decision Support System | | Assess Current Threat Level |

**Table 115: Relationships for Assess Current Threat Level**

## Use Case: Perform Incident Recognition -

### Description:

This activity represents the complex behaviour required to recognize a particular incident.

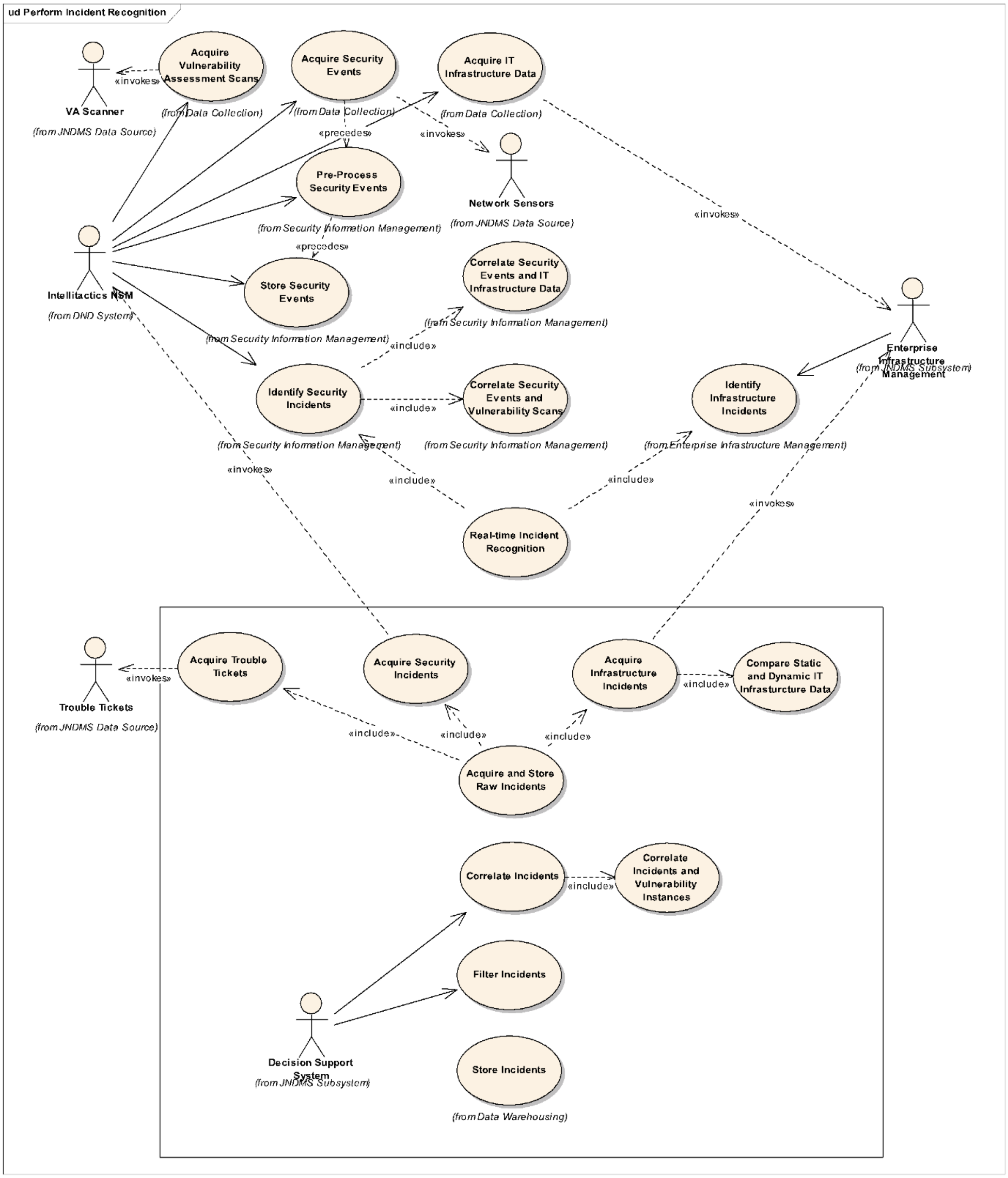

ud Perform Incident Recognition
VA Scanner
(from JNDMS Data Source)
«invokes»
Acquire Vulnerability Assessment Scans
(from Data Collection)
Acquire Security Events
(from Data Collection)
Acquire IT Infrastructure Data
(from Data Collection)
«precedes»
«invokes»
Network Sensors
(from JNDMS Data Source)
Pre-Process Security Events
(from Security Information Management)
«precedes»
«invokes»
Intellitactics NSM
(from DND System)
Store Security Events
(from Security Information Management)
Correlate Security Events and IT Infrastructure Data
(from Security Information Management)
«include»
Enterprise Infrastructure Management
(from JNDMS Subsystem)
Identify Security Incidents
(from Security Information Management)
«include»
Correlate Security Events and Vulnerability Scans
(from Security Information Management)
Identify Infrastructure Incidents
(from Enterprise Infrastructure Management)
«invokes»
«include»
«include»
«invokes»
Real-time Incident Recognition
Trouble Tickets
(from JNDMS Data Source)
«invokes»
Acquire Trouble Tickets
Acquire Security Incidents
Acquire Infrastructure Incidents
«include»
Compare Static and Dynamic IT Infrasturcture Data
«include»
«include»
«include»
Acquire and Store Raw Incidents
Correlate Incidents
«include»
Correlate Incidents and Vulnerability Instances
Filter Incidents
Decision Support System
(from JNDMS Subsystem)
Store Incidents
(from Data Warehousing)

**Figure 22: Perform Incident Recognition**

| Source | Type | Target |
|---|---|---|
| Data Fusion | include | Perform Incident Recognition |
| Perform Incident Recognition | precedes | Incident Severity Assessment |

**Table 116: Relationships for Perform Incident Recognition**

## 4.2.5 Enterprise Infrastructure Management

The enterprise infrastructure management package contains the use cases required for the collection and management of the IT assets. This includes correlation of events related to these assets as well as the dependencies between them. As a whole, EIM identifies the incidents related to the IT infrastructure, including network traffic anomalies.

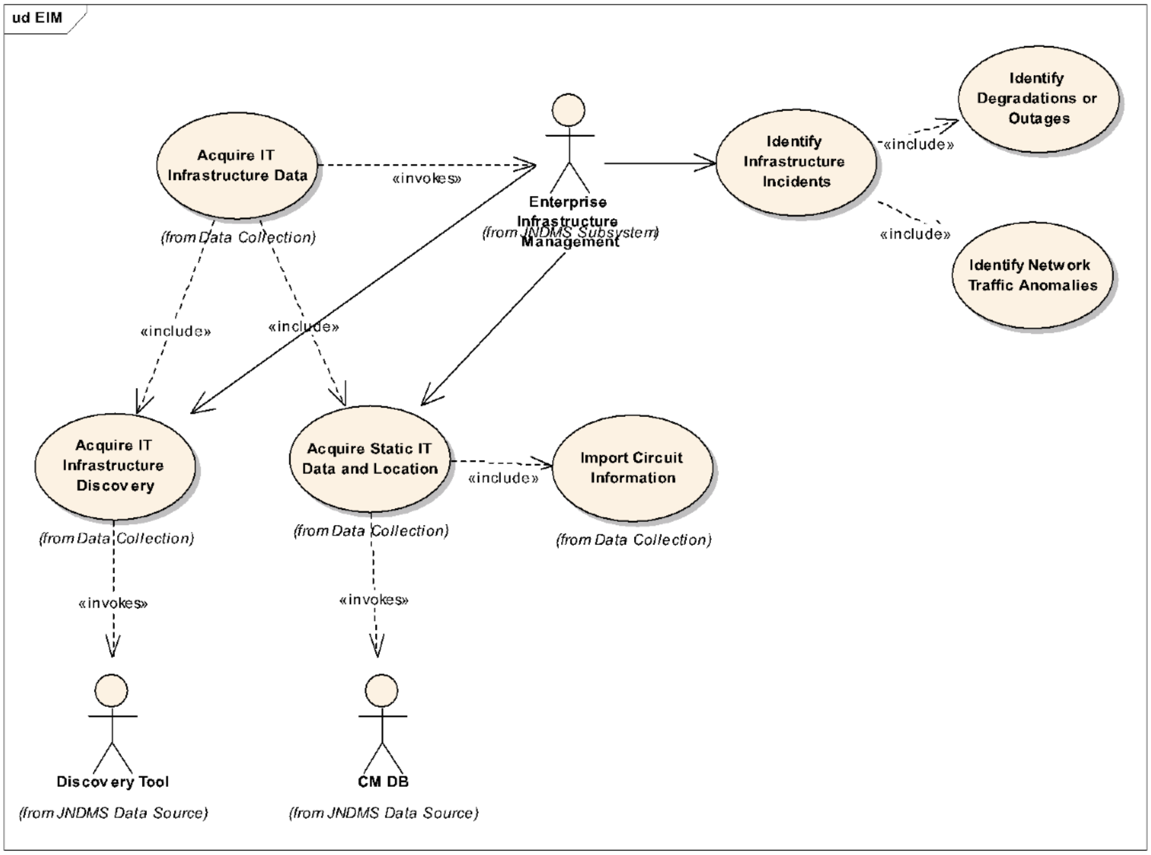

ud EIM
Acquire IT Infrastructure Data
(from Data Collection)
«invokes»
Enterprise Infrastructure Management
(from JNDMS Subsystem)
Identify Infrastructure Incidents
«include»
Identify Degradations or Outages
«include»
Identify Network Traffic Anomalies
«include»
«include»
Acquire IT Infrastructure Discovery
(from Data Collection)
Acquire Static IT Data and Location
(from Data Collection)
«include»
Import Circuit Information
(from Data Collection)
«invokes»
«invokes»
Discovery Tool
(from JNDMS Data Source)
CM DB
(from JNDMS Data Source)

**Figure 23: EIM**

## Use Case: Identify Degradations or Outages -

### Description:

EIM monitors the IT environment and raises alarms when assets are non-responsive.

| Source | Type | Target |
|---|---|---|
| Identify Infrastructure Incidents | include | Identify Degradations or Outages |

Table 117: Relationships for Identify Degradations or Outages

## Use Case: Identify Infrastructure Incidents -

### Description:

EIM monitors the infrastructure and detects Infrastructure incidents that affect the availability of an asset or service. Those incidents are pushed to the JNDMS Database.

| Source | Type | Target |
|---|---|---|
| Identify Infrastructure Incidents | include | Identify Degradations or Outages |
| Identify Infrastructure Incidents | include | Identify Network Traffic Anomalies |
| Real-time Incident Recognition | include | Identify Infrastructure Incidents |
| Enterprise Infrastructure Management |  | Identify Infrastructure Incidents |

Table 118: Relationships for Identify Infrastructure Incidents

## Use Case: Identify Network Traffic Anomalies -

### Description:

EIM monitors the network traffic and raises alarms when anomalies are detected.

| Source | Type | Target |
|---|---|---|
| Identify Infrastructure Incidents | include | Identify Network Traffic Anomalies |

**Table 119: Relationships for Identify Network Traffic Anomalies**

## 4.2.6 External To System

The contents of this package represent items that interface with the JNDMS, however are not directly part of the JNDMS. These are modeled so that the workflow and system interfaces can be described.

### Use Case: Clean Infection and Secure Server -

**Description:**

This is an action to clean infection on a server.

| Source | Type | Target |
|---|---|---|
| CIRT Analyst | | Clean Infection and Secure Server |

**Table 120: Relationships for Clean Infection and Secure Server**

### Use Case: Close Trouble Ticket -

**Description:**

A trouble ticket is closed.

| Source | Type | Target |
|---|---|---|
| Close Trouble Ticket | | Trouble Tickets |
| CFNOC Service Desk Agent | | Close Trouble Ticket |

**Table 121: Relationships for Close Trouble Ticket**

## Use Case: Contact "Point of Contacts" -

### Description:

The POC database is used to contact the required person.

| Source | Type | Target |
|---|---|---|
| Regional System Administrator | | Contact "Point of Contacts" |

**Table 122: Relationships for Contact "Point of Contacts"**

## Use Case: Contact CFNOC and Make Recommendations -

### Description:

A regional DND staff contacts CFNOC and make recommendations.

| Source | Type | Target |
|---|---|---|
| Information Security Services Officer | | Contact CFNOC and Make Recommendations |
| Contact CFNOC and Make Recommendations | | CFNOC Service Desk Agent |

**Table 123: Relationships for Contact CFNOC and Make Recommendations**

## Use Case: Disable Equipment -

### Description:

Equipment is disabled.

| Source | Type | Target |
|---|---|---|
| Regional System Administrator | | Disable Equipment |

**Table 124: Relationships for Disable Equipment**

## Use Case: Enable Equipment -

### Description:

The equipment is enabled.

| Source | Type | Target |
|---|---|---|
| Regional System Administrator | | Enable Equipment |

**Table 125: Relationships for Enable Equipment**

## Use Case: Examine External Sources of Exploit and Vulnerability Information -

### Description:

External sources of vulnerability and exploit data are explored to determine if the DND network is affected or can be affected.

| Source | Type | Target |
|---|---|---|
| CIRT Analyst | | Examine External Sources of Exploit and Vulnerability Information |
| NVAT Analyst | | Examine External Sources of Exploit and Vulnerability Information |

**Table 126: Relationships for Examine External Sources of Exploit and Vulnerability Information**

## Use Case: Identify Network Outage Options -

### Description:

Identify network outage options that are acceptable to DND (no impact on operations).

| Source | Type | Target |
|---|---|---|
| Identify Network Outage Options | | 6-Staff - Signal/Telecommunication Officers |
| Service Interruption Coordinator | | Identify Network Outage Options |

**Table 127: Relationships for Identify Network Outage Options**

## Use Case: Investigate Potential Vulnerability -

### Description:

Once a potential vulnerability is discovered, NVAT must determine if the CND environment is affected.

| Source | Type | Target |
|---|---|---|
| Investigate Potential Vulnerability | include | Enter Potential Vulnerability in IAT |
| NVAT Analyst | | Investigate Potential Vulnerability |

**Table 128: Relationships for Investigate Potential Vulnerability**

## Use Case: Enter Potential Vulnerability in IAT -

### Description:

This activity represents the user, or other system, entering a vulnerability within IAT.

| Source | Type | Target |
|---|---|---|
| Investigate Potential Vulnerability | include | Enter Potential Vulnerability in IAT |
| Enter Potential Vulnerability in IAT | invokes | Impact Assessment Tool |

**Table 129: Relationships for Enter Potential Vulnerability in IAT**

## Use Case: Isolate/Reconnect Subset of Network -

### Description:

A network subnet is isolated or reconnected.

| Source | Type | Target |
|---|---|---|
| Network Operations Management Staff | | Isolate/Reconnect Subset of Network |

**Table 130: Relationships for Isolate/Reconnect Subset of Network**

## Use Case: Issue Corrective Procedures -

### Description:

Corrective procedures are issued to appropriate resource to address a problem.

| Source | Type | Target |
|---|---|---|
| Issue Corrective Procedures | invokes | Information Security Services Officer |
| CIRT Analyst | | Issue Corrective Procedures |

**Table 131: Relationships for Issue Corrective Procedures**

## Use Case: Issue Maintenance Request -

### Description:

The Service Provider informs the NOC that a major upgrade is required.

| Source | Type | Target |
|---|---|---|
| Telco Provider | | Issue Maintenance Request |
| Issue Maintenance Request | | Service Interruption Coordinator |

**Table 132: Relationships for Issue Maintenance Request**

## Use Case: Log Trouble Ticket -

### Description:

A trouble ticket is logged using the trouble ticket system.

| Source | Type | Target |
|---|---|---|
| Service Interruption Coordinator | | Log Trouble Ticket |
| Log Trouble Ticket | | Trouble Tickets |
| Regional Service Desk Agent | | Log Trouble Ticket |

**Table 133: Relationships for Log Trouble Ticket**

## Use Case: Make Decision to Isolate/Reconnect a Domain -

### Description:

CFNOC makes the decision to isolate or reconnect a domain.

| Source | Type | Target |
|---|---|---|
| Watch Officer | | Make Decision to Isolate/Reconnect a Domain |

**Table 134: Relationships for Make Decision to Isolate/Reconnect a Domain**

## Use Case: Plan and Request Appropriate Risk Mitigation -

### Description:

The Vulnerability Assessment Analyst plans appropriate countermeasure.

| Source | Type | Target |
|---|---|---|
| Plan and Request Appropriate Risk Mitigation | invokes | Regional System Administrator |
| NVAT Analyst | | Plan and Request Appropriate Risk Mitigation |

**Table 135: Relationships for Plan and Request Appropriate Risk Mitigation**

## Use Case: Prioritize the Response to Incidents -

### Description:

The severity value helps the Security Analyst prioritize the response to incidents.

| Source | Type | Target |
|---|---|---|
| CIRT Analyst | | Prioritize the Response to Incidents |

Table 136: Relationships for Prioritize the Response to Incidents

## Use Case: Provide Outage Options to Service Provider -

### Description:

Provide feedback to the service provider on network outage preferences.

| Source | Type | Target |
|---|---|---|
| Provide Outage Options to Service Provider | | Telco Provider |
| Service Interruption Coordinator | | Provide Outage Options to Service Provider |

Table 137: Relationships for Provide Outage Options to Service Provider

## Use Case: Reject Service Outage -

### Description:

The coordinator informs the service provider whether the interruption is acceptable or not.

| Source | Type | Target |
|---|---|---|
| Service Interruption Coordinator | | Reject Service Outage |

Table 138: Relationships for Reject Service Outage

### Use Case: Update Vulnerability Status once the Mitigation is Validated -

**Description:**

The status of the vulnerability is updated once it can be confirmed that the asset is mitigated.

| Source | Type | Target |
|---|---|---|
| NVAT Analyst | | Update Vulnerability Status once the Mitigation is Validated |
| Update Vulnerability Status once the Mitigation is Validated | invokes | Impact Assessment Tool |

**Table 139: Relationships for Update Vulnerability Status once the Mitigation is Validated**

## 4.2.7 Presentation Visualization Alerting

This package stores use cases related to the presentation, visualization, alerting and reporting of the JNDMS data. The central theme of this package is to build the 'situational awareness' required for the users of the JNDMS.

This package has also been subdivided into views required by different roles.

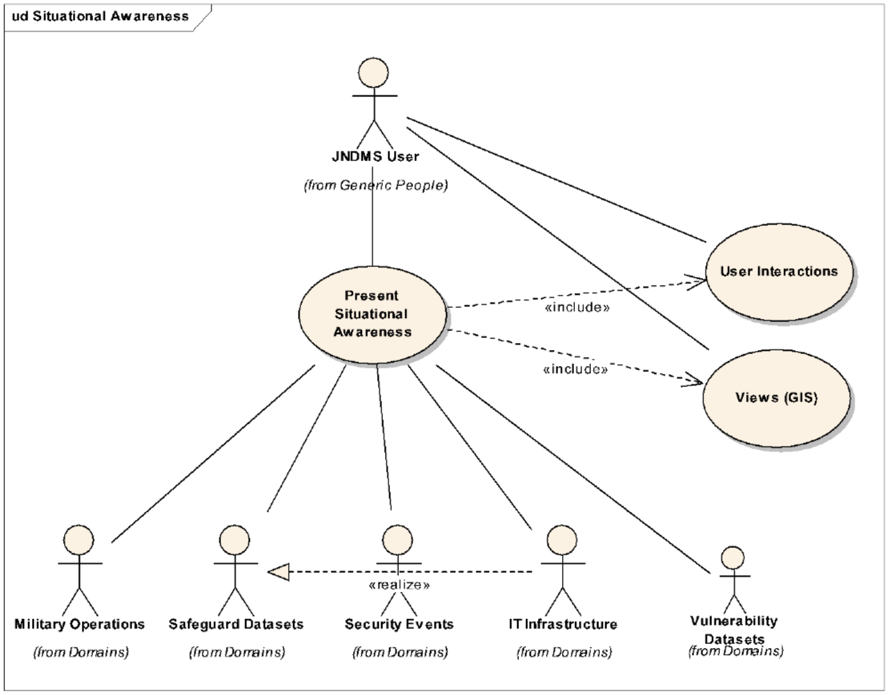


**Figure 24: Situational Awareness**

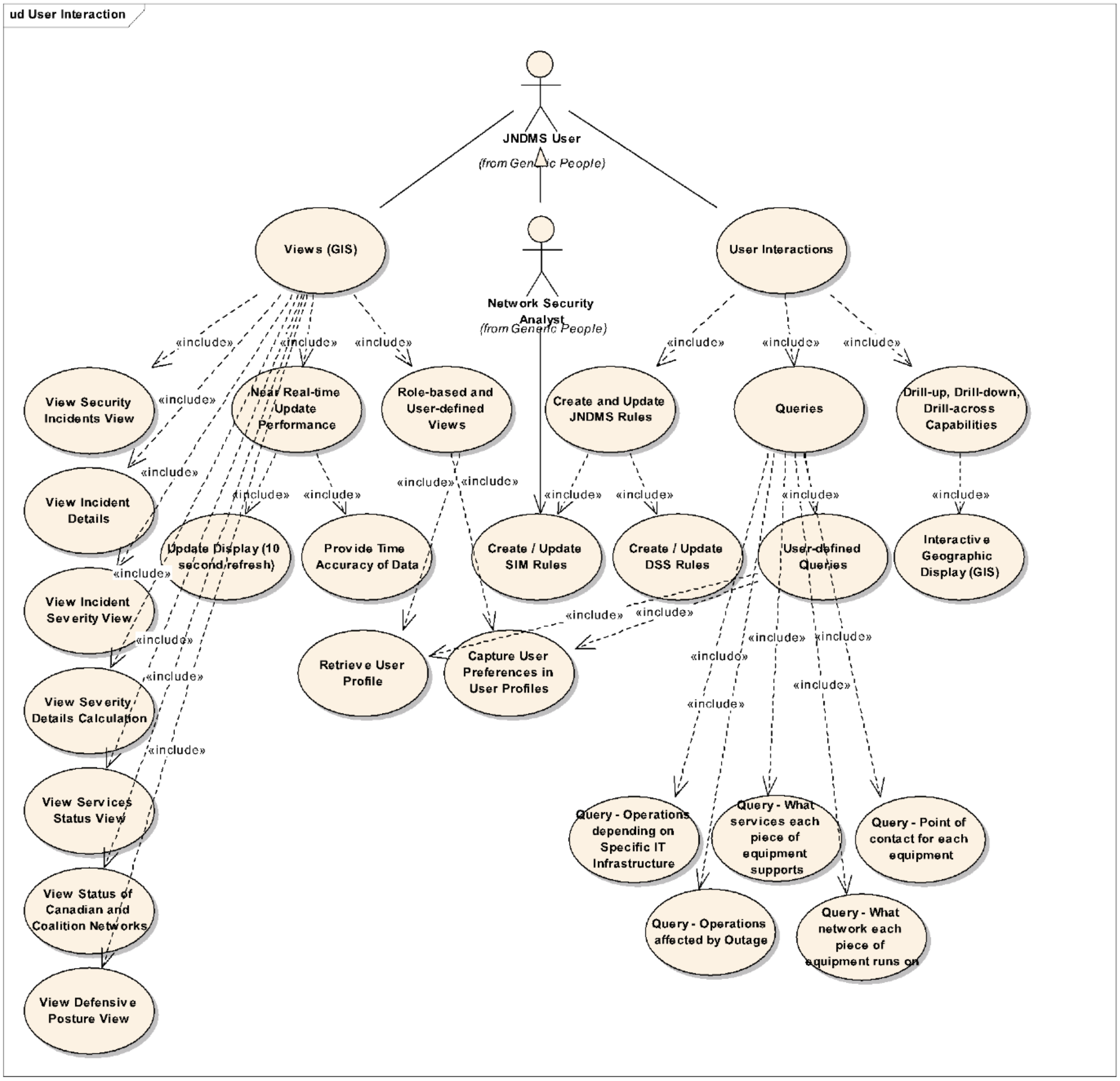

ud User Interaction
JNDMS User
(from Generic People)
Network Security Analyst
(from Generic People)
Views (GIS)
User Interactions
«include»
View Security Incidents View
Near Real-time Update Performance
Role-based and User-defined Views
Create and Update JNDMS Rules
Queries
Drill-up, Drill-down, Drill-across Capabilities
View Incident Details
Update Display (10 second refresh)
Provide Time Accuracy of Data
Create / Update SIM Rules
Create / Update DSS Rules
User-defined Queries
Interactive Geographic Display (GIS)
View Incident Severity View
Retrieve User Profile
Capture User Preferences in User Profiles
View Severity Details Calculation
View Services Status View
View Status of Canadian and Coalition Networks
View Defensive Posture View
Query - Operations depending on Specific IT Infrastructure
Query - What services each piece of equipment supports
Query - Point of contact for each equipment
Query - Operations affected by Outage
Query - What network each piece of equipment runs on

**Figure 25: User Interaction**

## Use Case: Present Situational Awareness -

### Description:

The overall situational awareness is a central theme in JNDMS. The views required to create this situational awareness will be one of the focuses of this project.

The situational awareness is the result of the fusion of military operations data, IT infrastructure information, security events, vulnerability data sets and safeguards.

| Source | Type | Target |
|---|---|---|
| JNDMS User | | Present Situational Awareness |
| Present Situational Awareness | | Military Operations |
| Present Situational Awareness | | Safeguard Datasets |
| Present Situational Awareness | | Security Events |
| Present Situational Awareness | | IT Infrastructure |
| Present Situational Awareness | | Vulnerability Datasets |
| Present Situational Awareness | | DID-JNDMS-0 |
| Present Situational Awareness | include | User Interactions |
| Present Situational Awareness | include | Views (GIS) |

**Table 140: Relationships for Present Situational Awareness**

**Requirements:**

**DID-JNDMS-0**

The JNDMS shall provide situational awareness (SA) for Computer Network Defence (CND) through the fusion of Military Operations, IT infrastructure, Security events, Vulnerability, and Safeguards data sets. The JNDMS shall capture, store, process, analyze and present data from these five information domains**.**

## Use Case: User Interactions -

**Description:**

This use case represents the most generic case of interactions between the user and the JNDMS.

**Table 141: Relationships for User Interactions**

| Source | Type | Target |
|---|---|---|
| JNDMS User | | User Interactions |
| User Interactions | include | Queries |
| User Interactions | include | Drill-up, Drill-down, Drill-across Capabilities |

| Source | Type | Target |
|---|---|---|
| User Interactions | include | Create and Update JNDMS Rules |
| User Interactions | | DID-DP-4 |
| Present Situational Awareness | include | User Interactions |

**Requirements:**

**DID-DP-4**

User Interaction: The JNDMS shall allow the user to 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**.**

## Use Case: Capture User Preferences in User Profiles -

**Description:**

The user will use the JNDMS to set preferences. These preferences will be stored in a user profile to be applied to the given user.

| Source | Type | Target |
|---|---|---|
| Role-based and User-defined Views | include | Capture User Preferences in User Profiles |
| User-defined Queries | include | Capture User Preferences in User Profiles |

**Table 142: Relationships for Capture User Preferences in User Profiles**

## Use Case: Logoff -

### Description:

The user logs off of the system.

| Source | Type | Target |
|---|---|---|
| Headquarters staff checks network status | include | Logoff |

Table 143: Relationships for Logoff

## Use Case: Create and Update JNDMS Rules -

### Description:

The rules within JNDMS are updated based on new information

| Source | Type | Target |
|---|---|---|
| Create and Update JNDMS Rules | include | Create / Update SIM Rules |
| User Interactions | include | Create and Update JNDMS Rules |
| Create and Update JNDMS Rules | include | Create / Update DSS Rules |
| Create and Update JNDMS Rules | | JNDMSRules |

Table 144: Relationships for Create and Update JNDMS Rules

## Use Case: Create / Update DSS Rules -

### Description:

The JNDMS user updates the Decision Support System (DSS) rules.  This is normally done during administration or maintenance cycles.

| Source | Type | Target |
|---|---|---|
| Create and Update JNDMS Rules | include | Create / Update DSS Rules |

Table 145: Relationships for Create / Update DSS Rules

## Use Case: Create / Update SIM Rules -

### Description:

The Network Security Analyst is responsible for maintaining SIM's rules. These rules are created to prioritize and filter security events acquired by SIM.

| Source | Type | Target |
|---|---|---|
| Network Security Analyst |  | Create / Update SIM Rules |
| Create / Update SIM Rules | include | Update SIM Rules |
| Create and Update JNDMS Rules | include | Create / Update SIM Rules |

**Table 146: Relationships for Create / Update SIM Rules**

## Use Case: Logon -

### Description:

RFP 10.1 Step 2 - The JNDMS logon screen appears along with an icon indicating that a change in the network status has occurred. The JNDMS can be configured based on the user profile to take an action such as beep at the workstation or display an icon if a change happens. A change could be, for example, the occurrence of a security incident.

| Source | Type | Target |
|---|---|---|
| Headquarters staff checks network status | include | Logon |

**Table 147: Relationships for Logon**

## Use Case: Drill-up, Drill-down, Drill-across Capabilities -

### Description:

The user will access details through drill-up drill-down, drill-across navigation capabilities.

| Source | Type | Target |
|---|---|---|
| User Interactions | include | Drill-up, Drill-down, Drill-across Capabilities |
| Drill-up, Drill-down, Drill-across Capabilities | include | Interactive Geographic Display (GIS) |

**Table 148: Relationships for Drill-up, Drill-down, Drill-across Capabilities**

## Use Case: Interactive Geographic Display (GIS) -

### Description:

The users of the JNDMS will be able to manipulate a view on the system based on a geographic display.

| Source | Type | Target |
|---|---|---|
| Drill-up, Drill-down, Drill-across Capabilities | include | Interactive Geographic Display (GIS) |

**Table 149: Relationships for Interactive Geographic Display (GIS)**

## Use Case: Queries -

### Description:

This use case is the generic interface of queries into the JNDMS.

**Table 150: Relationships for Queries**

| Source | Type | Target |
|---|---|---|
| Queries | include | User-defined Queries |
| User Interactions | include | Queries |
| Queries | include | Query - Operations depending on Specific IT Infrastructure |
| Queries | include | Query - What network each piece of equipment runs on |
| Queries | include | Query - What services each piece of equipment supports |

| Source | Type | Target |
|---|---|---|
| Queries | include | Query - Point of contact for each equipment |
| Queries | include | Query - Operations affected by Outage |

## Use Case: Query - Operations affected by Outage -

### Description:

The user enters a list of circuits and the forecasted maintenance date. The user is presented with a list of operations, locations and services affected by the outage.

| Source | Type | Target |
|---|---|---|
| Service Interruption Coordinator |  | Query - Operations affected by Outage |
| Queries | include | Query - Operations affected by Outage |

**Table 151: Relationships for Query - Operations affected by Outage**

## Use Case: Query - Operations depending on Specific IT Infrastructure -

### Description:

The user is presented with a list of operations depending on IT infrastructure.

| Source | Type | Target |
|---|---|---|
| Regional System Administrator |  | Query - Operations depending on Specific IT Infrastructure |
| Information Security Services Officer |  | Query - Operations depending on Specific IT Infrastructure |
| CIRT Analyst |  | Query - Operations depending on Specific IT Infrastructure |
| Queries | include | Query - Operations depending on Specific IT Infrastructure |

**Table 152: Relationships for Query - Operations depending on Specific IT Infrastructure**

## Use Case: Query - Point of contact for each equipment -

### Description:

The points of contact are shown for a given piece of equipment.

| Source | Type | Target |
|---|---|---|
| Regional System Administrator | | Query - Point of contact for each equipment |
| Queries | include | Query - Point of contact for each equipment |

**Table 153: Relationships for Query - Point of contact for each equipment**

## Use Case: Query - What network each piece of equipment runs on -

### Description:

The user is shown what network the piece of equipment runs on.

| Source | Type | Target |
|---|---|---|
| Regional System Administrator | | Query - What network each piece of equipment runs on |
| Queries | include | Query - What network each piece of equipment runs on |

**Table 154: Relationships for Query - What network each piece of equipment runs on**

## Use Case: Query - What services each piece of equipment supports -

### Description:

The user is shown which services each piece of equipment supports.

| Source | Type | Target |
|---|---|---|
| Regional System Administrator | | Query - What services each piece of equipment supports |
| Queries | include | Query - What services each piece of equipment supports |

**Table 155: Relationships for Query - What services each piece of equipment supports**

## Use Case: User-defined Queries -

### Description:

The JNDMS supports the creation of user-defined queries.

| Source | Type | Target |
|---|---|---|
| Queries | include | User-defined Queries |
| User-defined Queries | include | Capture User Preferences in User Profiles |
| User-defined Queries | | DID-DP-2 |
| User-defined Queries | include | Retrieve User Profile |

**Table 156: Relationships for User-defined Queries**

### Requirements:

**DID-DP-2**

User-defined Views and Queries: The JNDMS shall support the creation of user defined 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 to create tailored data queries, such as spatial and temporal queries and re-use these queries as required.

## Use Case: Views (GIS) -

### Description:

GIS views are selected to optimize situational awareness: defensive posture, severity assessment, integration of IT, incidents and operations over GIS.

| Source | Type | Target |
|---|---|---|
| Views (GIS) | include | View Security Incidents View |
| Views (GIS) | include | View Services Status View |
| Views (GIS) | include | Near Real-time Update Performance |
| Views (GIS) | include | Role-based and User-defined Views |
| JNDMS User | | Views (GIS) |
| Views (GIS) | include | View Incident Details |
| Views (GIS) | include | View Defensive Posture View |
| Views (GIS) | include | View Incident Severity View |
| Views (GIS) | include | View Status of Canadian and Coalition Networks |
| Views (GIS) | include | View Severity Details Calculation |
| Views (GIS) | | DID-DP-0 |
| Views (GIS) | | DID-DP-3 |
| Present Situational Awareness | include | Views (GIS) |

**Table 157: Relationships for Views (GIS)**

**Requirements:**

**DID-DP-0**

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 visualization 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, de-conflicting data views, decluttering data views, layering data views, exporting data views to different formats and projecting data views to the user.

**DID-DP-3**

Visual Correlation: The JNDMS shall provide through its user interface a mean to visually correlate complex data sets from the five SA for CND 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".

## Use Case: View Defensive Posture View -

### Description:

This will show the current defensive posture.

| Source | Type | Target |
|---|---|---|
| CIRT Analyst | | View Defensive Posture View |
| Views (GIS) | include | View Defensive Posture View |
| NVAT Analyst | | View Defensive Posture View |

**Table 158: Relationships for View Defensive Posture View**

## Use Case: View Risk Assessment View -

### Description:

The user of the JNDMS will be able to view a presentation of the current risk assessment.

| Source | Type | Target |
|---|---|---|
| NVAT Analyst | | View Risk Assessment View |

**Table 159: Relationships for View Risk Assessment View**

## Use Case: View Risk Assessment Details -

### Description:

The user of the JNDMS will be able to drill down into the risk assessment to view the details of the assessment.

| Source | Type | Target |
|---|---|---|
| NVAT Analyst | | View Risk Assessment Details |

Table 160: Relationships for View Risk Assessment Details

## Use Case: View Security Incidents View -

### Description:

This will show security related incidents.

| Source | Type | Target |
|---|---|---|
| Views (GIS) | include | View Security Incidents View |
| Information Security Services Officer | | View Security Incidents View |
| CIRT Analyst | | View Security Incidents View |

Table 161: Relationships for View Security Incidents View

## Use Case: View Incident Details -

### Description:

The details of a given alert (incident) are shown. The details should describe how this alert entered into the JNDMS and any information stored in the alert.

| Source | Type | Target |
|---|---|---|
| Information Security Services Officer | | View Incident Details |
| CIRT Analyst | | View Incident Details |
| Views (GIS) | include | View Incident Details |

Table 162: Relationships for View Incident Details

## Use Case: View Incident Severity View -

### Description:

This view shows the locations of sites with their severity value on a geographic background.

| Source | Type | Target |
|---|---|---|
| CIRT Analyst | | View Incident Severity View |
| Views (GIS) | include | View Incident Severity View |

**Table 163: Relationships for View Incident Severity View**

## Use Case: View Severity Details Calculation -

### Description:

This will show how the severity was derived.

| Source | Type | Target |
|---|---|---|
| CIRT Analyst | | View Severity Details Calculation |
| Views (GIS) | include | View Severity Details Calculation |

**Table 164: Relationships for View Severity Details Calculation**

## Use Case: View Services Status View -

### Description:

This will show the status of any given services.

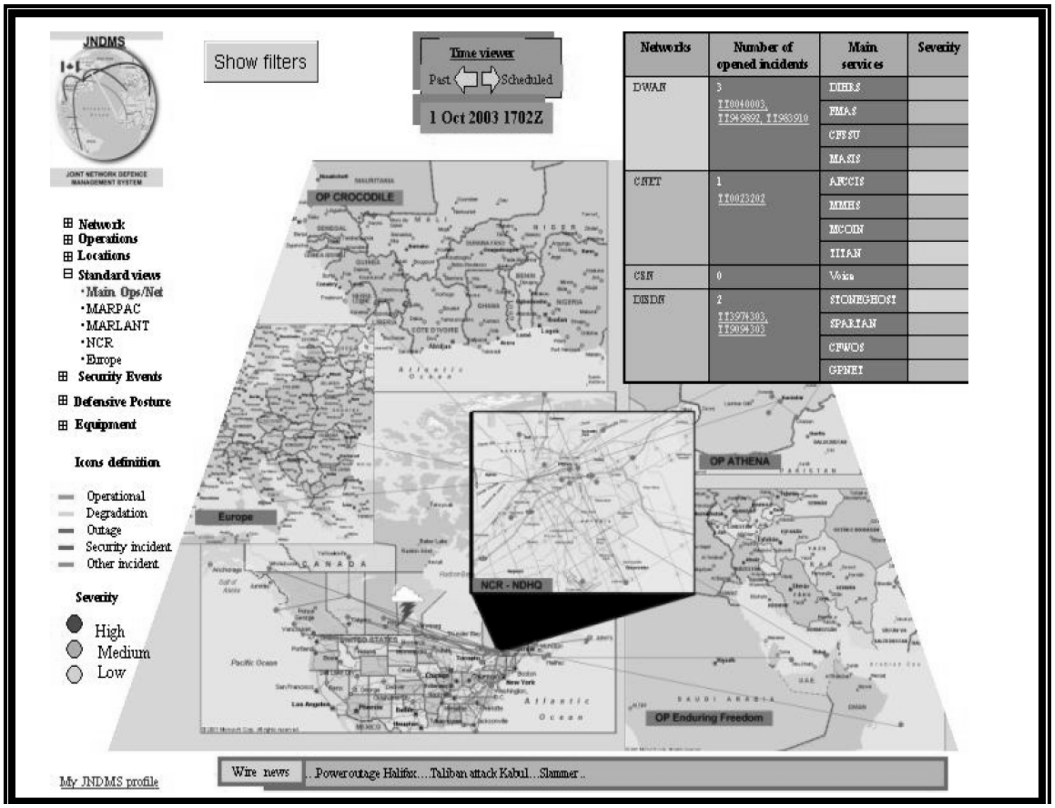
| Source | Type | Target |
|---|---|---|
| Views (GIS) | include | View Services Status View |
| Information Security Services Officer | | View Services Status View |
| CIRT Analyst | | View Services Status View |

**Table 165: Relationships for View Services Status View**

## Use Case: Render Initial Display -

### Description:

RFP 10.1 Step 4 - The initial view consists of three windows that have a geographical map background and network nodes and links as the foreground. The networks displayed are those that provide support for the Colonel's operation. The number of map windows, the map boundaries, and the window sizes and positions, were initially selected by the JNDMS based on the operation chosen by the Colonel. The user can adjust this view. For example, any number of map windows can be shown.



| Networks | Number of opened incidents | Main services | Severity |
|---|---|---|---|
| DWAN | 3<br>TT0040003,<br>TT949892, TT983910 | DIHRS | |
| | | FMAS | |
| | | CFSSU | |
| | | MASIS | |
| CNET | 1<br>TT0023202 | ARCCIS | |
| | | MMHS | |
| | | MCOIN | |
| | | TITAN | |
| CSN | 0 | Voice | |
| DISDN | 2<br>TT3974303,<br>TT9094303 | STONEGHOST | |
| | | SPARTAN | |
| | | CFWOS | |
| | | GPNET | |

.. Power outage Halifax.... Taliban attack Kabul... Slammer ..

**Figure 26: Commander's Profile Proposed Initial View**

| Source | Type | Target |
|---|---|---|
| Headquarters staff checks network status | include | Render Initial Display |

Table 166: Relationships for Render Initial Display

## Use Case: Render Login Screen - COM0010

### Description:

The initial login screen is shown.

| Source | Type | Target |
|---|---|---|
| Headquarters staff checks network status | include | Render Login Screen |

Table 167: Relationships for Render Login Screen

## Use Case: Retrieve User Profile -

### Description:

RFP 10.1 Step 3 - The Colonel types a user identifier and a password in the logon screen of JNDMS and presses the Enter key. This logs the user in and causes JNDMS to bring up its initial display as specified in the user profile. The user can specify what this initial view will be.

| Source | Type | Target |
|---|---|---|
| Headquarters staff checks network status | include | Retrieve User Profile |
| Role-based and User-defined Views | include | Retrieve User Profile |
| User-defined Queries | include | Retrieve User Profile |

Table 168: Relationships for Retrieve User Profile

## Use Case: View Status of Canadian and Coalition Networks -

### Description:

This will show the status of Canadian and Coalition Networks as reported to JNDMS.

| Source | Type | Target |
|---|---|---|
| CIRT Analyst | | View Status of Canadian and Coalition Networks |
| Views (GIS) | include | View Status of Canadian and Coalition Networks |

**Table 169: Relationships for View Status of Canadian and Coalition Networks**

## Use Case: Near Real-time Update Performance -

### Description:

The presentation engine will signal a periodic update to show near real time information. As per RFP section 11.4.

| Source | Type | Target |
|---|---|---|
| Views (GIS) | include | Near Real-time Update Performance |
| Near Real-time Update Performance | include | Update Display (10 second refresh) |
| Near Real-time Update Performance | | DID-DP-1 |
| Near Real-time Update Performance | include | Provide Time Accuracy of Data |

**Table 170: Relationships for Near Real-time Update Performance**

### Requirements:

**DID-DP-1**

Performance: The JNDMS views shall be updated in a near-real time fashion. Different levels 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.

## Use Case: Provide Time Accuracy of Data -

### Description:

JNDMS will provide clues to indicate time accuracy of the data being displayed. A timestamp will be used as well when appropriate.

| Source | Type | Target |
|---|---|---|
| Near Real-time Update Performance | include | Provide Time Accuracy of Data |

**Table 171: Relationships for Provide Time Accuracy of Data**

## Use Case: Update Display (10 second refresh) -

### Description:

The display must update periodically to allow current information to be shown.  An appropriate refresh rate of 10 seconds is estimated.

| Source | Type | Target |
|---|---|---|
| Headquarters staff checks network status | include | Update Display (10 second refresh) |
| Near Real-time Update Performance | include | Update Display (10 second refresh) |

**Table 172: Relationships for Update Display (10 second refresh)**

## Use Case: Role-based and User-defined Views -

### Description:

The users of the JNDMS will have their presentation customized based on their user profile and on their current roles.

**Table 173: Relationships for Role-based and User-defined Views**

| Source | Type | Target |
|---|---|---|
| Views (GIS) | include | Role-based and User-defined Views |
| Role-based and User-defined Views | include | Capture User Preferences in User Profiles |

| Source | Type | Target |
|---|---|---|
| Role-based and User-defined Views | | DID-DP-2 |
| Role-based and User-defined Views | include | Retrieve User Profile |

**Requirements:**

**DID-DP-2**

User-defined Views and Queries: The JNDMS shall support the creation of user defined 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 to create tailored data queries, such as spatial and temporal queries and re-use these queries as required.

### 4.2.7.1 JNDMS User Views

This package contains the use cases required for different views.

### Use Case: Maintenance Impacts Users -

**Description:**

Overview: Bell Nexxia informs the NOC that a major upgrade is required on all FALCATE multiplexing equipment over the entire Bell Nexxia infrastructure. This implies that major public and private clients of Bell including banks, police, and governments will be affected. The proposed date for this maintenance is 30 days in the future.

Flow of Events:

1. A request is received by the NOC Service Interruption Coordinator from Bell Nexxia. The request includes a list of several hundred circuit numbers, the maintenance date, a four hour window for the actual work, and an anticipated outage of 30 minutes within this window.

2. Using JNDMS the Service Interruption Coordinator copies the circuit list into a query table and obtains a report of the services using these circuits, the locations affected, and the operations using those services now, and scheduled to be using them in 30 days. The Service Interruption Coordinator observes that a critical system required for a scheduled operation will be affected. The Service Interruption Coordinator contacts Bell Nexxia and requests that the maintenance be scheduled for another time period.

3. Bell Nexxia escalates the need for this maintenance to occur at the initially proposed time due to the number of people involved and the impossibility of finding another time that will accommodate everyone. The cost of changing the maintenance time is estimated at several million dollars.

4. The Service Interruption Coordinator informs the chain of command about this dilemma. The decision is escalated to J6 who decides after confirming the JNDMS information with the Command Centre that the operational requirement for the systems cannot be changed and that DND cannot accept, regardless of the cost, the proposed maintenance time.

5. Using JNDMS to forecast periods when the operational impact will be minimized, the Service Interruption Coordinator provides a list of alternate time intervals. Bell Nexxia presents this list to its other clients and one of the intervals on the list is accepted.

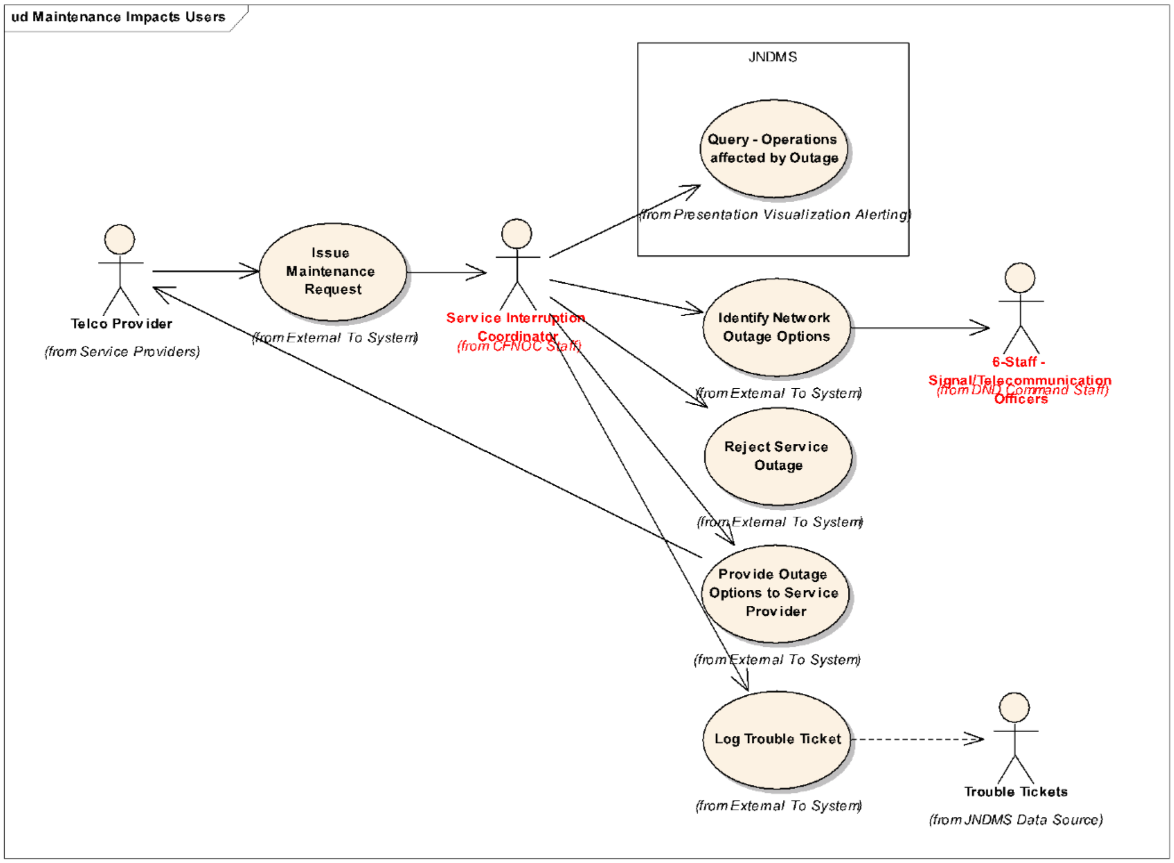

ud Maintenance Impacts Users
JNDMS
Query - Operations affected by Outage
(from Presentation Visualization Alerting)
Telco Provider
(from Service Providers)
Issue Maintenance Request
(from External To System)
Service Interruption Coordinator
(from CFNOC Staff)
Identify Network Outage Options
(from External To System)
6-Staff - Signal/Telecommunication Officers
(from DND Command Staff)
Reject Service Outage
(from External To System)
Provide Outage Options to Service Provider
(from External To System)
Log Trouble Ticket
(from External To System)
Trouble Tickets
(from JNDMS Data Source)

Figure 27: Maintenance Impacts Users

## Use Case: Physical Damage -

### Description:

Overview: Physical damage at a specific location has an impact on many services and operations. The JNDMS ability to reveal these impacts quickly is important for mitigating the impact of physical damage during an emergency.

Flow of Events:

1. Water damage begins in a room that contains several pieces of equipment used by various networks and services. Initially it is clear that all the equipment in this room will have to be shut down, but the order in which this will take place is not clear. The System Administration staff want to make this disruption as graceful as possible.

2. The System Administrator uses the JNDMS central database to find out which equipment pieces are in the damaged room. The JNDMS supports queries that return the equipment located at specific locations. The information retrieved includes: what network each piece of equipment runs on, what services each piece of equipment supports, and the point of contact for each piece of equipment.

3. Based on the services that will be disrupted, the System Administration person begins contacting the "point of contact" staff for the most critical services first. With their involvement a plan is put into effect for mitigating the problems.

4. The JNDMS supports queries that return the operations and services depending on specific networks and pieces of equipment. This type of querying is crucial for mitigating the impact of physical damage. The operations that will be affected by these disruptions are notified by the System Administration staff involved in mitigating the problems. Given this warning, steps are taken within each operation to adjust its activities until the services are restored.

5. The water damage continues and all the equipment in the room is lost.

6. As a short term solution each damaged piece of equipment is replaced by a backup item. This restores all services, but in a degraded mode, since the network is not backed up now.

7. The original room and its equipment are restored. Services are put into full operation again. Operations are warned and make adjustments to minimize the impact of these switchovers to full service.

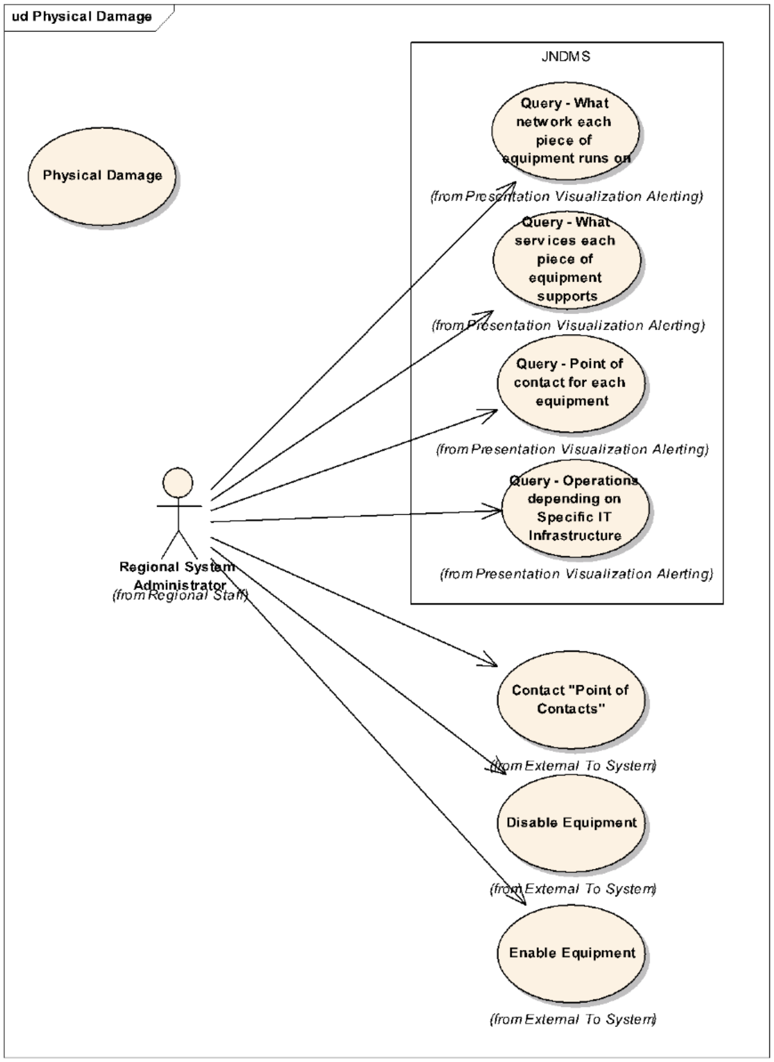

ud Physical Damage
Physical Damage
JNDMS
Query - What network each piece of equipment runs on
(from Presentation Visualization Alerting)
Query - What services each piece of equipment supports
(from Presentation Visualization Alerting)
Query - Point of contact for each equipment
(from Presentation Visualization Alerting)
Query - Operations depending on Specific IT Infrastructure
(from Presentation Visualization Alerting)
Regional System Administrator
(from Regional Staff)
Contact "Point of Contacts"
(from External To System)
Disable Equipment
(from External To System)
Enable Equipment
(from External To System)

**Figure 28: Physical Damage**

### 4.2.7.1.1 Commander Views

This package contains the use cases for the presentation of data to the commander role.

## Use Case: Headquarters staff checks network status -

**Description:**

This use case was initially in the RFP as use case 10.1.

Overview: A Colonel watches the JNDMS tool for thirty seconds to confirm that the IT infrastructure for an operation is back to normal.

Flow of Events:

1. A Colonel in Headquarters who is responsible for an operation decides to check the current status of the networks supporting the operation. The Colonel invokes the JNDMS tool. The expectation is that the user will invoke JNDMS to view the information that it is processing. In this example, the Colonel could have been verbally prompted to invoke the JNDMS tool by a member of the 6-staff.

2. The JNDMS logon screen appears along with an icon indicating that a change in the network status has occurred. The JNDMS can be configured based on the user profile to take an action such as beep at the workstation or display an icon if a change happens. A change could be, for example, the occurrence of a security incident.

3. The Colonel types a user identifier and a password in the logon screen of JNDMS and presses the Enter key. This logs the user in and causes JNDMS to bring up its initial display as specified in the user profile. The user can specify what this initial view will be.

4. The initial view consists of three windows that have a geographical map background and network nodes and links as the foreground. The networks displayed are those that provide support for the Colonel's operation. The number of map windows, the map boundaries, and the window sizes and positions, were initially selected by the JNDMS based on the operation chosen by the Colonel. The user can adjust this view. For example, any number of map windows can be shown.

5. In this case, all of the network nodes and links are coloured green indicating that the network is operating within the rule limits configured by the System Administration staff, since the legend selection is “availability status”. Selecting a security view would show colours that reflect rules configured by the security analysts. The Colonel sees that the entire network is operational.

6. The information presented by the JNDMS is dynamically updated every ten seconds (approximation depending on bandwidth requirements and availability). Each map window updates its information independently by polling the JNDMS server. The Colonel watches the screen for thirty seconds, knowing that the lack of change implies that the network status is not changing. Each map window indicates that it is being refreshed as the polling steps complete so the user is confident that the tool is running as expected.

7. A menu with a hierarchical list of options is on the side of the user's screen. The default selection on this menu is stored in the user's profile. The user can make other selections by clicking on them. The selected option is always highlighted. The selected option and the legend on the display tell the user how to interpret the symbols and colours on the map windows.

8. The Colonel, satisfied that the network is back to normal, clicks the Exit button to end this session. JNDMS does not log user actions, so no record is kept of this session.

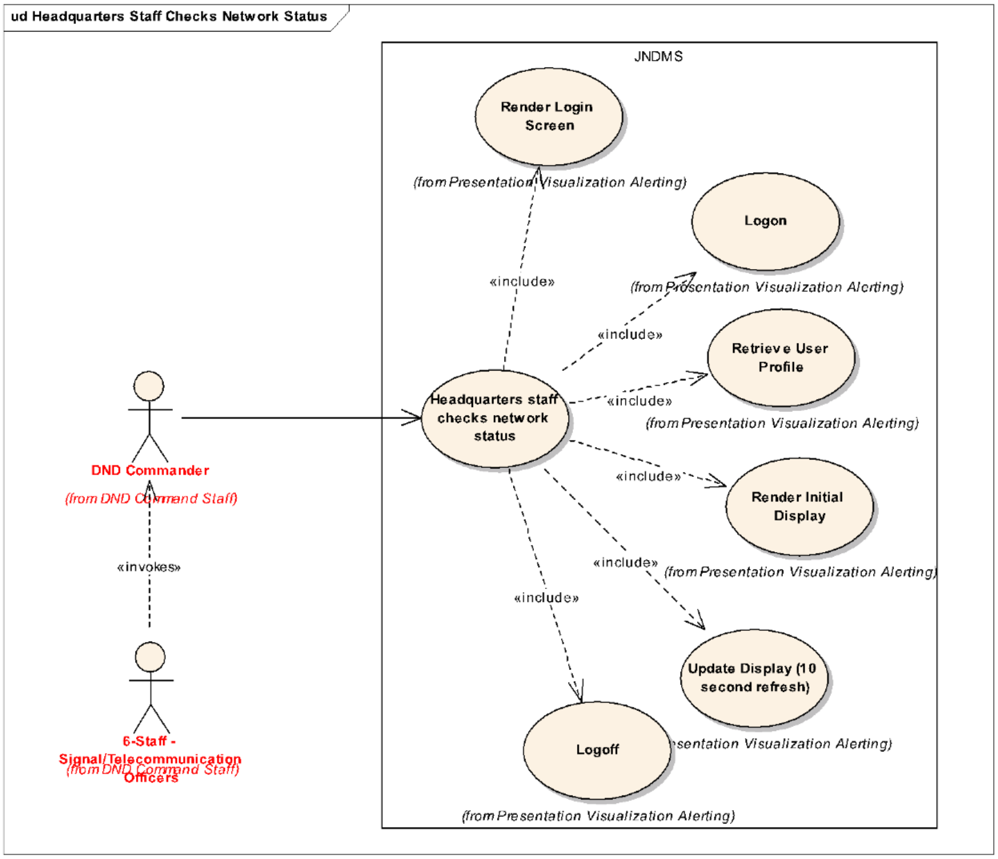

ud Headquarters Staff Checks Network Status
JNDMS
Render Login Screen
(from Presentation Visualization Alerting)
Logon
(from Presentation Visualization Alerting)
Retrieve User Profile
(from Presentation Visualization Alerting)
Render Initial Display
(from Presentation Visualization Alerting)
Update Display (10 second refresh)
Logoff
(from Presentation Visualization Alerting)
Headquarters staff checks network status
«include»
«invokes»
DND Commander
(from DND Command Staff)
6-Staff - Signal/Telecommunication Officers
(from DND Command Staff)

**Figure 29: Headquarters Staff Checks Network Status**

| Source | Type | Target |
|---|---|---|
| Headquarters staff checks network status | include | Render Login Screen |
| Headquarters staff checks network status | include | Logon |
| Headquarters staff checks network status | include | Retrieve User Profile |
| Headquarters staff checks network status | include | Render Initial Display |
| Headquarters staff checks network status | include | Update Display (10 second refresh) |
| Headquarters staff checks network status | include | Logoff |
| DND Commander | | Headquarters staff checks network status |

**Table 174: Relationships for Headquarters staff checks network status**

### 4.2.7.1.2 Security Analyst Views

This package contains the views required for the security analysts.

### Use Case: Isolation of a Local Domain -

**Description:**

Overview: A security analyst responsible for a Metropolitan Area Network suspects that some malicious code has been placed on the network, and it is causing the loss of services on many hosts. Using JNDMS, the cause of the problem is revealed and the problem is resolved without disrupting users who were not affected by the problem.

Flow of Events:

1. Initially all domains that constitute this network are running without any incidents. Active network information gathering components are running in each domain (i.e., A, B, and C) and at the NOC. The data that the domains collect is pushed to their own JNDMS database and to the JNDMS database at the NOC. These components have been set-up to probe for the existence of two services on every machine in their domain, namely: Login, and VirusScan. The components collect this data and send it on periodically, e.g., every ten seconds.

2. At 10:04 hours, the System Administration person in "A" Domain runs a script that incorrectly removes the Login and VirusScan services from most of the machines in the domain. The System Administration person is not aware of this error and the fact that running the script caused a problem.

3. The System Administration person continues to work and notices that login is not possible on some machines. This is unexpected, and the System Administration person cannot login anywhere to check further or make corrections. The System Administration person telephones the “A” Domain Helpdesk and causes an “A” Domain trouble ticket to be raised. The existence of a trouble ticket is a monitored item for the JNDMS, so the local JNDMS database and the JNDMS database at the NOC receive this data.

4. The System Administration person contacts the local Security Analyst who is using a machine that is always logged in and is not affected by the current problem. The Security Analyst is currently running JNDMS and has the “Security Events” view selected. The Security Analyst has received several alerts about unexpected changes on “A” Domain.

5. In the “Security Events” view, the host sites for which an alert has been raised are coloured red. The Security Analyst clicks on one red host site and sees an alert summary. It indicates that the Login and VirusScan services have not been running since 10:05 hours. The Security Analyst then adds the "services status" view with columns indicating which services are running. Login and VirusScan are not running on hosts where alerts were raised. The Security Analyst steps this view back and sees that these services were running correctly on all hosts at 10:03 hours.

6. The Security Analyst returns to the general monitoring view for alerts, and selects a view that displays all the domains and the primary network. This information indicates that the missing service problem is restricted to “A” Domain.

7. The Security Analyst then queries the Operations and Infrastructure dependencies database and determines that no operations are dependent on “A” Domain. It can be isolated without operational impact.

8. The Security Analyst telephones the NOC to report that the situation is suspicious, but apparently localized. This data is added to the “A” Domain trouble ticket. The Security Analyst recommends that “A” Domain be isolated.

9. The NOC uses JNDMS to confirm the Security Analyst's report and reaches the same conclusion. They then isolate the “A” Domain by stopping the connection between “A” Domain and the router. “A” Domain and the NOC are now isolated, and the information held in their instances of JNDMS begins to diverge. At this point, the NOC begins to review external sources, such as CERT, to determine if the observed symptoms correspond with any currently known exploits. No evidence of related problems is found.

10. Meanwhile, the System Administration person discovers the error in the script that caused this problem, and makes the necessary corrections. “A” Domain is now operating as expected. The Security Analyst monitors the local situation using the JNDMS Services view locally to collect evidence that everything is working correctly. The System Administration person telephones the NOC and recommends that “A” Domain be connected to the router.

11. The NOC reconnects “A” Domain and monitors its behaviour closely for a short time. The trouble ticket is closed.

Notes:

The information in the JNDMS database about the operations affected by “A” Domain was essential for deciding to isolate “A” Domain. In the actual incident, this information was difficult to obtain, causing disruptions and delays in putting the isolation into effect.

The JNDMS data revealed a relationship in time concerning the loss of services. This led to an association of the loss of these services with the running of the erroneous script, and consequently led to the timely discovery of the problem and its correction. In the actual incident, this analysis took many hours. Using the JNDMS data, these associations would be apparent and the correction would be made quickly.

The sharing of infrastructure status information between “A” Domain and the central NOC was important for the fast resolution of this problem. The Security Analyst could see that the problem was isolated to “A” Domain (by using a local access to the central view), and the NOC could confirm these conclusions (by using a central access to local view). Even after the isolation of “A” Domain the NOC could continue helping with the problem because they had their copy of the “A” Domain data to help with queries to external agencies, such as CERT.

The availability of historical data that showed when the alerts were raised, when services were running, and when they were no longer running, was essential for determining the cause of the problem – the erroneous script.

Being able to overlap information, such as what services are running where, and what alarms were raised where, was also necessary to solve this problem.

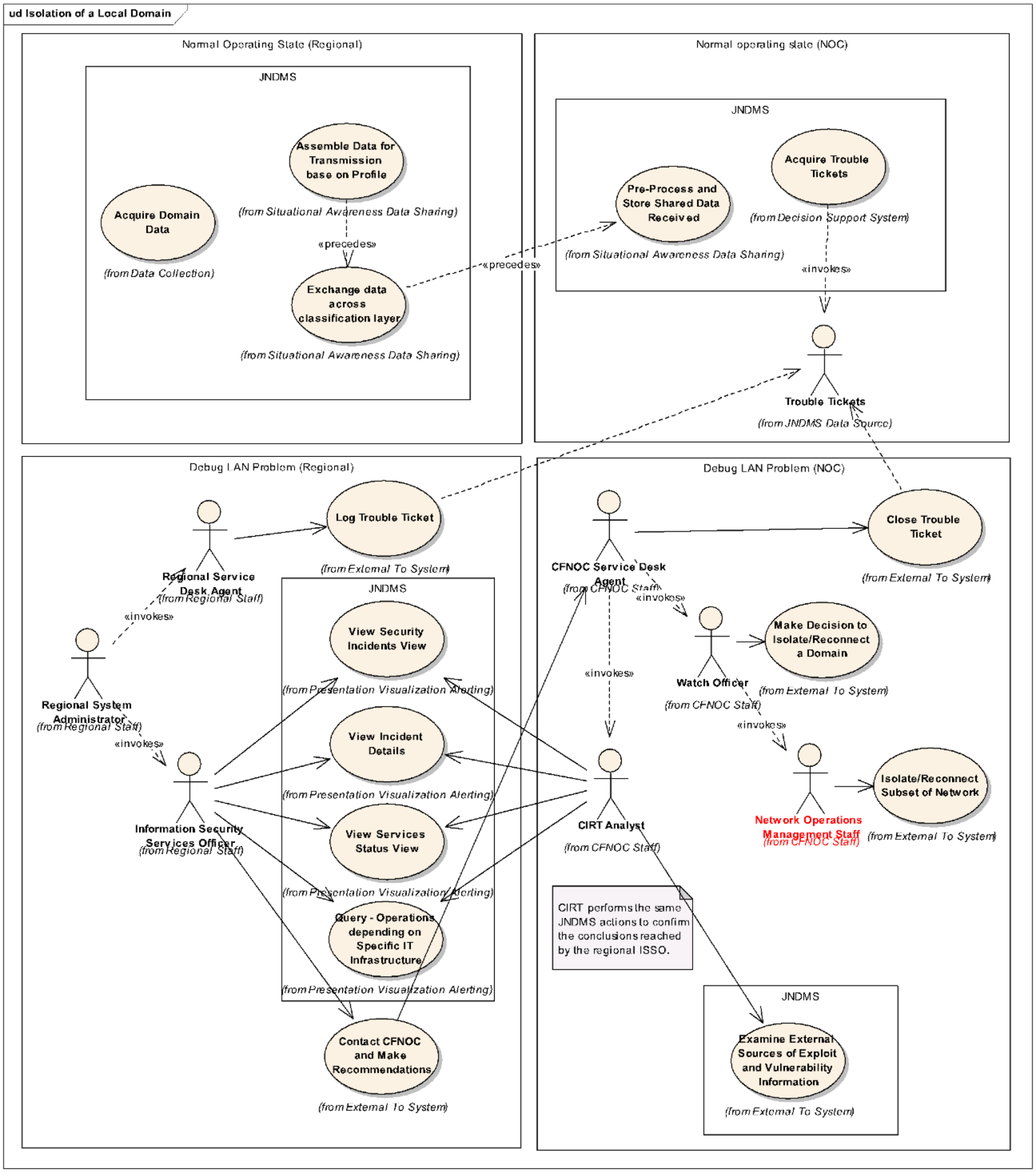

ud Isolation of a Local Domain
Normal Operating State (Regional)
JNDMS
Acquire Domain Data
(from Data Collection)
Assemble Data for Transmission base on Profile
(from Situational Awareness Data Sharing)
«precedes»
Exchange data across classification layer
(from Situational Awareness Data Sharing)
«precedes»
Normal operating state (NOC)
JNDMS
Pre-Process and Store Shared Data Received
(from Situational Awareness Data Sharing)
Acquire Trouble Tickets
(from Decision Support System)
«invokes»
Trouble Tickets
(from JNDMS Data Source)
Debug LAN Problem (Regional)
Regional Service Desk Agent
(from Regional Staff)
Log Trouble Ticket
(from External To System)
«invokes»
Regional System Administrator
(from Regional Staff)
«invokes»
Information Security Services Officer
(from Regional Staff)
JNDMS
View Security Incidents View
(from Presentation Visualization Alerting)
View Incident Details
(from Presentation Visualization Alerting)
View Services Status View
(from Presentation Visualization Alerting)
Query - Operations depending on Specific IT Infrastructure
(from Presentation Visualization Alerting)
Contact CFNOC and Make Recommendations
(from External To System)
Debug LAN Problem (NOC)
CFNOC Service Desk Agent
(from CFNOC Staff)
Close Trouble Ticket
(from External To System)
«invokes»
«invokes»
Watch Officer
(from CFNOC Staff)
Make Decision to Isolate/Reconnect a Domain
(from External To System)
«invokes»
Network Operations Management Staff
(from CFNOC Staff)
Isolate/Reconnect Subset of Network
(from External To System)
CIRT Analyst
(from CFNOC Staff)
CIRT performs the same JNDMS actions to confirm the conclusions reached by the regional ISSO.
JNDMS
Examine External Sources of Exploit and Vulnerability Information
(from External To System)

**Figure 30: Isolation of a Local Domain**

## Use Case: Response based on Severity of Incidents -

### Description:

Overview:

The network extends to four locations:

1. Router A is in DND Headquarters in Ottawa.

2. Router B is in Montreal.

3. Router C is on a deployed ship.

4. The NOC is in Ottawa.

A security incident affects all the workstations on the network. The Security Analyst is able to decide which workstations to correct first using the severity calculation provided by JNDMS.

Flow of Events:

1. Six workstations at three sites, DND Headquarters in Ottawa, the Montreal Armoury, and HMCS Iroquois, generate identical alerts indicating that they are compromised by a Trojan program. The Trojan program is transmitting data from each workstation. The traffic created by this transmission has a signature pattern that JNDMS data analyzer components have detected on the local subnetwork. The detection of this traffic pattern raised alerts at the NOC.

2. A Security Analyst at the NOC is looking at the JNDMS incident severity view. This view shows the locations of sites on a geographic background. The icon for DND Headquarters (i.e., Router A and its workstation) is red and shows a severity value of 17. The icon for HMCS Iroquois (i.e., Router C and its workstations) is red and shows a severity value of 18. The icon for the Montreal Armoury (i.e., Router B and its workstations) is yellow and shows a severity value of 11.

3. The Security Analyst clicks on the red icon for HMCS Iroquois (i.e., Router C) since this icon shows the highest severity value. This click brings into view a table of alert details, listing all the alerts raised at this site.

4. The Security Analyst clicks on one of the lines in this table to see the details about the severity calculation. In this case, all the alerts are the same, so clicking on any line brings up this table.

5. The Security Analyst clicks on the red icon for DND Headquarters (i.e., Router A) since this icon shows the next highest severity value. This click brings into view a table of alert details, listing all the alerts raised at this site.

6. The Security Analyst clicks on the line in this table to see the details about the severity calculation.

7. The Security Analyst observes that the assets that have been compromised at DND Headquarters and at HMCS Iroquois are all associated with the same operation, Operation Apollo. It appears that the network is being used to compromise this operation. The Security Analyst contacts the System Administration staff at HMCS Iroquois first, since this is where the incident is having the most significant impact. The Security Analyst provides the information needed to start the procedure for correcting this problem at HMCS Iroquois.

8. When the Security Analyst is available to address the next problem, the Security Analyst then telephones the System Administration staff at DND Headquarters and provides the information needed to start the procedure for correcting the problem there.

9. When the Security Analyst is available to address the next problem, the Security Analyst clicks on the icon for the Montreal Armoury since this icon shows the next highest severity value. This click brings into view a table of alert details, listing all the alerts raised at this site.

10. The Security Analyst clicks on one of the lines in this table to see the details about the severity calculation. In this case, all the alerts are the same, so clicking on any line brings up this table.

11. The Security Analyst emails the System Administration staff at the Montreal Armoury to begin the procedure for correcting the problem there.

Notes:

The severity value that depends on operations asset value helped the Security Analyst prioritize the response to incidents.

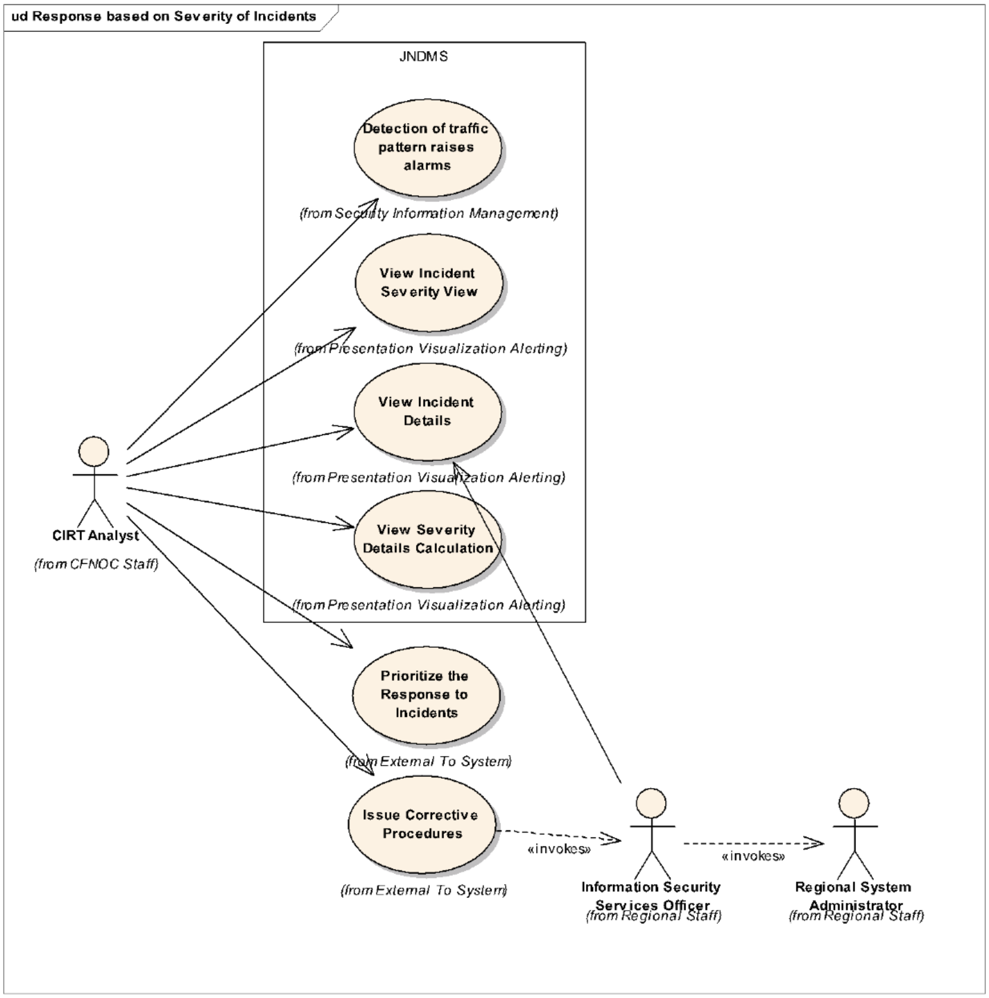

ud Response based on Severity of Incidents
JNDMS
Detection of traffic pattern raises alarms
(from Security Information Management)
View Incident Severity View
(from Presentation Visualization Alerting)
View Incident Details
(from Presentation Visualization Alerting)
View Severity Details Calculation
(from Presentation Visualization Alerting)
CIRT Analyst
(from CFNOC Staff)
Prioritize the Response to Incidents
(from External To System)
Issue Corrective Procedures
(from External To System)
«invokes»
Information Security Services Officer
(from Regional Staff)
«invokes»
Regional System Administrator
(from Regional Staff)

**Figure 31: Response based on Severity of Incidents**

### 4.2.7.1.3 Vulnerability Analyst Views

This package contains the views required for the vulnerability assessment analysts.

## Use Case: NVAT is Informed of a New Vulnerability -

**Description:**

Once the NVAT is informed of a new vulnerability the NVAT analyst must interact with the JNDMS to input the required information, then use the JNDMS to perform their vulnerability and risk assessment.

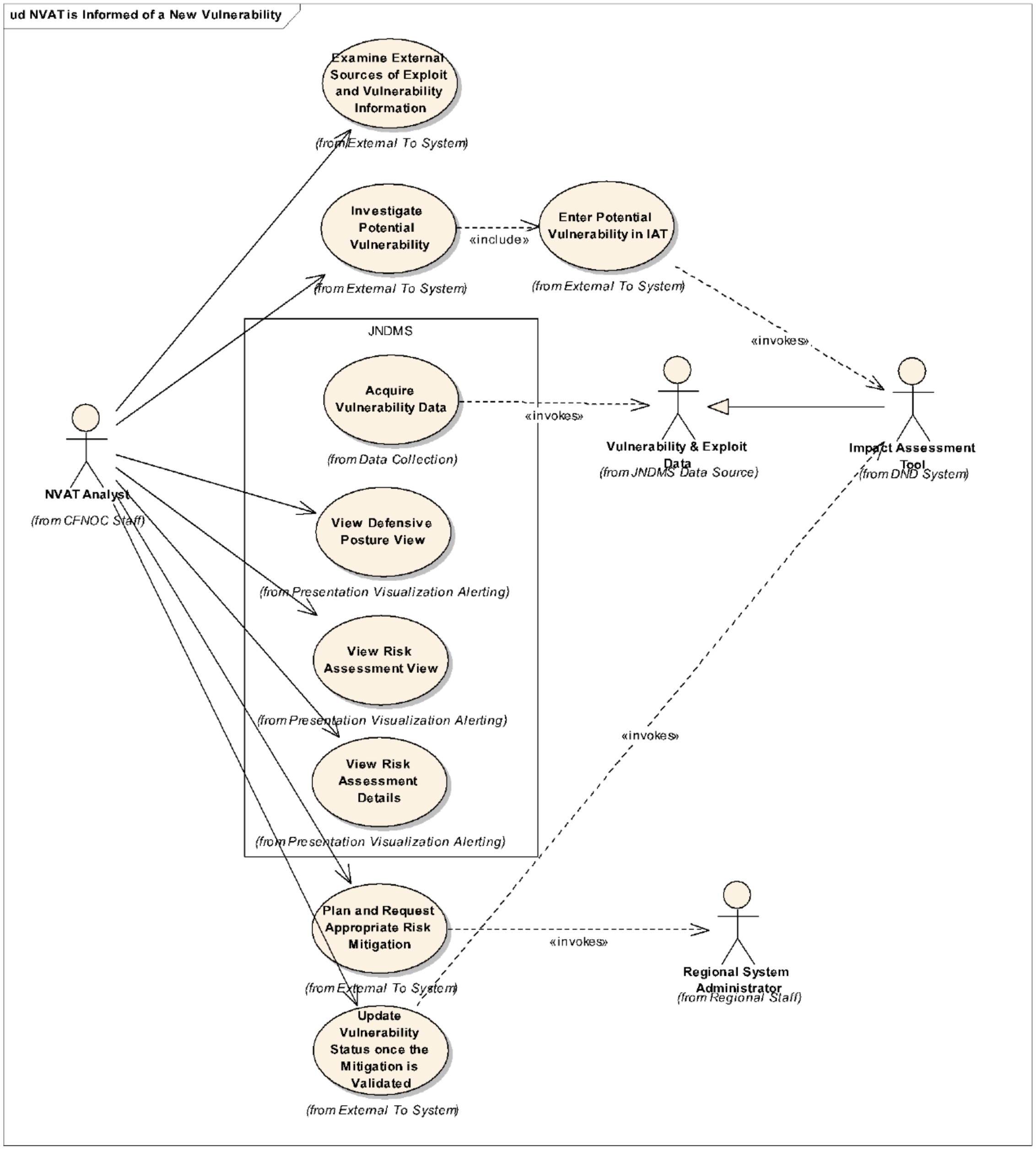

ud NVAT is Informed of a New Vulnerability
Examine External Sources of Exploit and Vulnerability Information
(from External To System)
Investigate Potential Vulnerability
(from External To System)
«include»
Enter Potential Vulnerability in IAT
(from External To System)
«invokes»
JNDMS
Acquire Vulnerability Data
(from Data Collection)
«invokes»
Vulnerability & Exploit Data
(from JNDMS Data Source)
Impact Assessment Tool
(from DND System)
NVAT Analyst
(from CFNOC Staff)
View Defensive Posture View
(from Presentation Visualization Alerting)
View Risk Assessment View
(from Presentation Visualization Alerting)
«invokes»
View Risk Assessment Details
(from Presentation Visualization Alerting)
Plan and Request Appropriate Risk Mitigation
(from External To System)
«invokes»
Regional System Administrator
(from Regional Staff)
Update Vulnerability Status once the Mitigation is Validated
(from External To System)

**Figure 32: NVAT is Informed of a New Vulnerability**

### 4.2.8 Security Information Management

This package contains the use cases related to the management of security information and events.

#### Use Case: Correlate Security Events and IT Infrastructure Data -

**Description:**

This task correlates the security events and the IT infrastructure data. The use of the Internet Protocol (IP) address and the IP port are key factors to correlate the events to the infrastructure.

| Source | Type | Target |
|---|---|---|
| Identify Security Incidents | include | Correlate Security Events and IT Infrastructure Data |

**Table 175: Relationships for Correlate Security Events and IT Infrastructure Data**

#### Use Case: Correlate Security Events and Vulnerability Scans -

**Description:**

This task correlates any security events with vulnerability scans.

| Source | Type | Target |
|---|---|---|
| Identify Security Incidents | include | Correlate Security Events and Vulnerability Scans |
| Correlate Security Events and Vulnerability Scans | | Incident |
| Correlate Security Events and Vulnerability Scans | | VulerabilityInstances |
| Correlate Security Events and Vulnerability Scans | | VulnerabilityDefinition |

**Table 176: Relationships for Correlate Security Events and Vulnerability Scans**

## Use Case: Detection of traffic pattern raises alarms -

### Description:

An anomaly in traffic patterns is noted by the network security analyst or by the SIM subsystem. This information triggers an alert within JNDMS.

| Source | Type | Target |
|---|---|---|
| CIRT Analyst | | Detection of traffic pattern raises alarms |
| Detection of traffic pattern raises alarms | | Incident |

**Table 177: Relationships for Detection of traffic pattern raises alarms**

## Use Case: Identify Security Incidents -

### Description:

Intellitactics Network Security Manager (NSM) correlates and prioritizes security events using a set of based rules. These rules can also be further extended to satisfy JNDMS requirements. Some of the rules include prioritizing based on IP, port, vulnerability assessment scans, etc).

A subset of these incidents (the higher priority events) is pushed to the JNDMS Database.

| Source | Type | Target |
|---|---|---|
| Intellitactics NSM | | Identify Security Incidents |
| Real-time Incident Recognition | include | Identify Security Incidents |
| Identify Security Incidents | include | Correlate Security Events and Vulnerability Scans |
| Identify Security Incidents | include | Correlate Security Events and IT Infrastructure Data |

**Table 178: Relationships for Identify Security Incidents**

## Use Case: Pre-Process Security Events -

### Description:

Intellitactics NSM normalizes and aggregates security event data to a common, complete and consistent format.

| Source | Type | Target |
|---|---|---|
| Pre-Process Security Events | precedes | Store Security Events |
| Intellitactics NSM | | Pre-Process Security Events |
| Pre-Process Security Events | | DID-IRELD-0 |
| Acquire Security Events | precedes | Pre-Process Security Events |
| Pre-Process Security Events | | DID-SED-2 |
| Pre-Process Security Events | | DID-SED-0 |
| Data Transformation | include | Pre-Process Security Events |
| Pre-Process Security Events | | VulerabilityInstances |

**Table 179: Relationships for Pre-Process Security Events**

### Requirements:

**DID-IRELD-0**

The JNDMS shall capture inter-relationships between Security Events, Military Operations, IT Infrastructure, Vulnerabilities and safeguards. This function refers to the following sub-functions: analyzing data sets from the 5 information domains (Operations, Infrastructure, Vulnerability, Safeguards, Events) identifying interrelationships between these 5 information domains, identifying Geospatial, connectivity and logical inter-relationships, normalizing these inter-relationships, de-conflicting these inter-relationships, consolidating these inter-relationships and writing them to the JNDMS database.

**DID-SED-0**

The JNDMS shall capture Security Events Data. This function refers to the following sub-functions: acquiring, pre-processing and storing security events data.

**DID-SED-2**

Pre-processing security events data: The JNDMS shall pre-process security events data so that only “clean” data sets 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.

### Use Case: Store Security Events -

**Description:**

SIM stores security events into a tiered Security Data Warehouse (SDW).

| Source | Type | Target |
|---|---|---|
| Pre-Process Security Events | precedes | Store Security Events |
| Intellitactics NSM | | Store Security Events |
| Store Security Events | | DID-SED-0 |
| Store Security Events | | DID-SED-3 |
| Data Warehousing | include | Store Security Events |

**Table 180: Relationships for Store Security Events**

**Requirements:**

**DID-SED-0**

The JNDMS shall capture Security Events Data. This function refers to the following sub-functions: acquiring, pre-processing and storing security events data.

**DID-SED-3**

Storing the security events data: The JNDMS shall write the security events data to the JNDMS database for storage and analysis by subsequent processing functionality. The data shall be stored with proper association to source and context within the JNDMS data model.

### Use Case: Update SIM Rules -

**Description:**

The Security Information Management (SIM) rules are updated.

| Source | Type | Target |
|---|---|---|
| Create / Update SIM Rules | include | Update SIM Rules |

**Table 181: Relationships for Update SIM Rules**

## 4.2.9 Situational Awareness Data Sharing

This package contains use cases used in the export of information from JNDMS.

### Use Case: Data Sharing -

**Description:**

This represents the most general case where JNDMS will share Situation Awareness data.

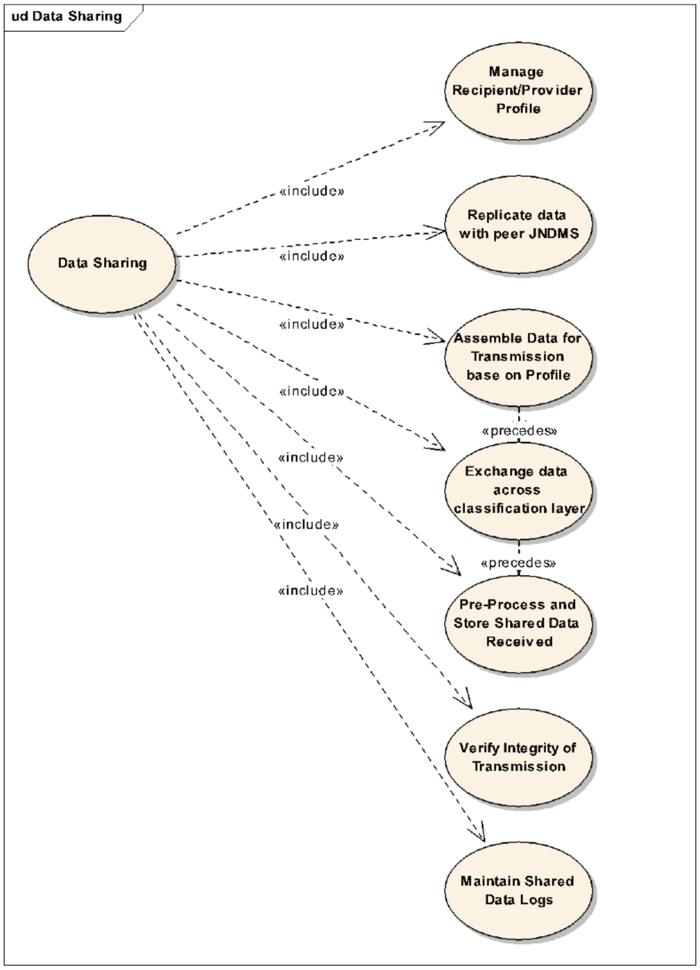

ud Data Sharing
Data Sharing
Manage Recipient/Provider Profile
Replicate data with peer JNDMS
Assemble Data for Transmission base on Profile
Exchange data across classification layer
Pre-Process and Store Shared Data Received
Verify Integrity of Transmission
Maintain Shared Data Logs
«include»
«include»
«include»
«include»
«include»
«include»
«include»
«precedes»
«precedes»

**Figure 33: Data Sharing**

**Table 182: Relationships for Data Sharing**

| Source | Type | Target |
|---|---|---|
| Data Sharing | include | Replicate data with peer JNDMS |
| Data Sharing | include | Exchange data across classification layer |
| Data Sharing | include | Assemble Data for Transmission base on Profile |
| Data Sharing | include | Manage Recipient/Provider Profile |
| Data Sharing | | DID-JNDMS-0 |
| Data Sharing | | DID-DS-0 |

| Source | Type | Target |
|---|---|---|
| Data Sharing | | DID-DM-3 |
| Data Sharing | include | Pre-Process and Store Shared Data Received |
| Data Sharing | include | Verify Integrity of Transmission |
| Data Sharing | include | Maintain Shared Data Logs |

**Requirements:**

**DID-DM-3**

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 timestamps.

**DID-DS-0**

The JNDMS shall allow for sharing of Situation Awareness Data. This function includes the following sub-function: managing the SA data recipient/provider permissions, assembling data sets for transmission, interpreting and storing received data sets, verifying transmission integrity, maintaining shared data logs with time, classification, content and recipient/provider information for each shared record set.

**DID-JNDMS-0**

The JNDMS shall provide situational awareness (SA) for Computer Network Defence (CND) through the fusion of Military Operations, IT infrastructure, Security events, Vulnerability, and Safeguards data sets. The JNDMS shall capture, store, process, analyze and present data from these five information domains**.**

## Use Case: Working with a Coalition Partner -

**Description:**

Overview: In response to a terrorist threat to the east coast of North America, Canada and the US have joined forces for the surveillance of the east coast. Computer networks belonging to both Canada and the US are critical assets for this operation. These networks are to be managed, monitored, and defended by the coalition team located in both countries. The JNDMS is interoperable with multinational tools to provide network operational status. The JNDMS provides network defence SA information for the Canadian portion of the networks used in this operation.

1. A JNDMS station located at the central NOC is connected to a multinational network. Information collected by the JNDMS is filtered through a guard and securely shared with

allies. All nations share an “agreed upon” set of network defence SA information. The CIA Common Operating Procedure (COP) is designed to handle caveat separation so that individual nations can choose with whom they wish to share information.

2. For this operation, Canada and the US (having dealt with the appropriate foreign disclosure agreements) have agreed to share a more complete set of network defence SA information but only for the underlying network assets supporting the operation. The JNDMS is configured to filter information related to the Canadian networks supporting the operation and to push this information to coalition partners. Equivalent information from the US networks is fed to the JNDMS so that the Canadian Computer Network Defence (C-CND) team can view the status of the entire Canadian-US network.

3. A security event occurs on the US network. A web server has been compromised and is being used to covertly steal information using a variant of “HTTP Tunnel” through port 80.

4. A Canadian intrusion analyst is checking the status of the Canadian networks using their JNDMS console. The analyst sees a map of the Canadian networks, as well as a high level view of US networks. The analyst notices a red flashing dot at one of the network nodes located on a US base. In this case, the red dot signifies that a severe event has occurred at that location.

5. The analyst clicks on the red flashing dot to see details of the event. A screen pops up providing the event summary. In this case, the network event is security-related and involves a web server. Meanwhile, US analysts, alerted by their IDS, are investigating this event.

6. One Canadian analyst clicks on the “security alerts” option of the JNDMS console and is able to read details of the nature of the security event. The analyst then clicks on the “applications” option and sees that a Canadian web-based C2 tool depends on the compromised US server. The confidentiality and integrity of the C2 information may have been compromised.

7. The analyst selects the “defensive posture” view highlighting all the security features of the web server. Immediately, the analyst finds out that the C2 tool was designed with built-in security features. All files related to the C2 tool are encrypted. Also, the analyst notices that the attacker cannot access Canadian hosts from the compromised web server.

8. Rather than immediately isolate the web server, which would disrupt the operation, the CND team takes extra time to remove the malicious code and secure the web server, such that the attacker can no long steal information.

Notes:

In this example, the CND team could immediately see that the confidentiality of the information obtained from the web server was not compromised even if the intruder had access to the web server. To deal with the security breach, it wasn't necessary to isolate the web server and disrupt operations.

This use case demonstrates the usefulness of automatically sharing network defence SA information in support of a coalition operation.

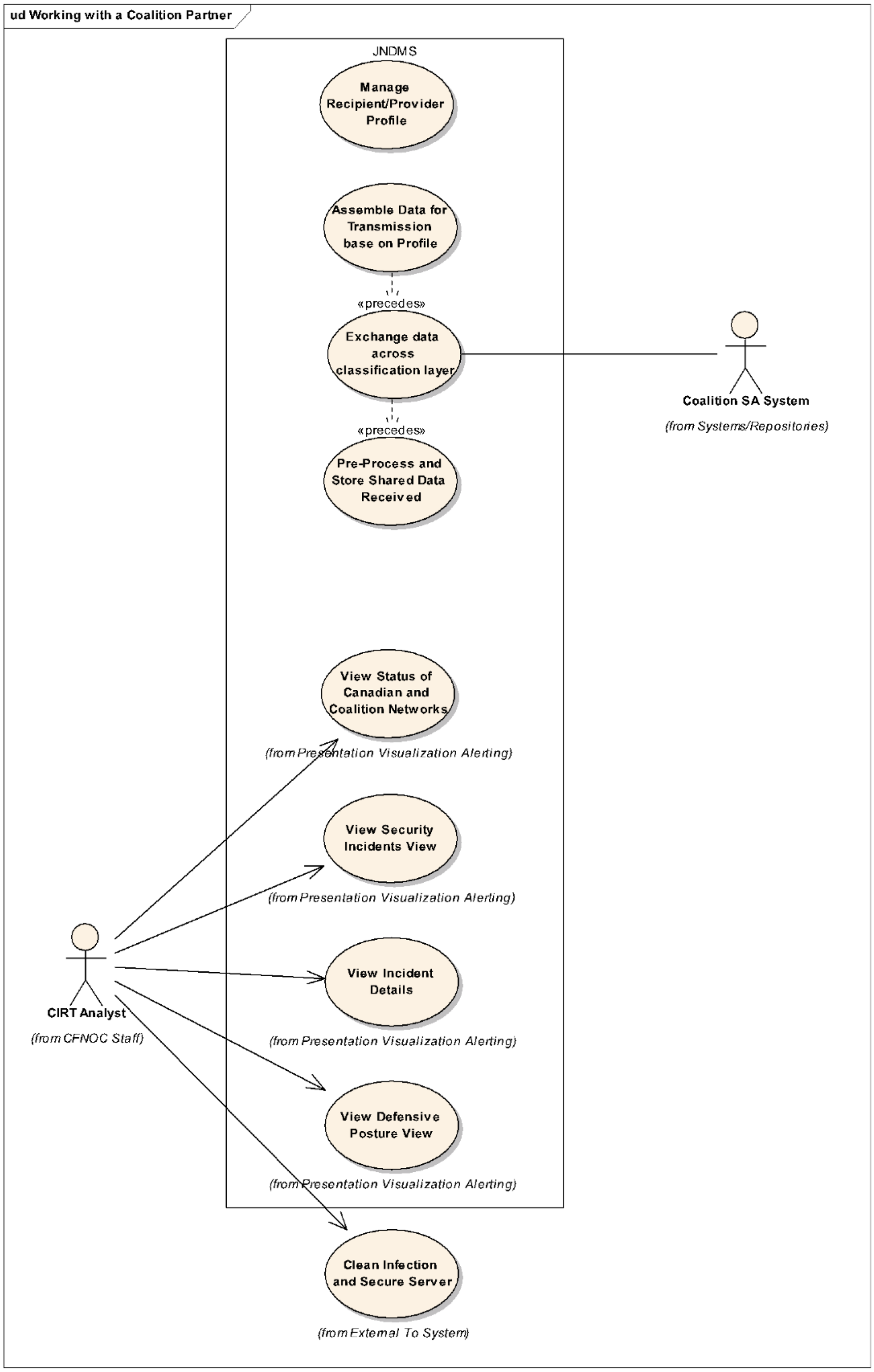

ud Working with a Coalition Partner
JNDMS
Manage Recipient/Provider Profile
Assemble Data for Transmission base on Profile
«precedes»
Exchange data across classification layer
«precedes»
Pre-Process and Store Shared Data Received
Coalition SA System
(from Systems/Repositories)
View Status of Canadian and Coalition Networks
(from Presentation Visualization Alerting)
View Security Incidents View
(from Presentation Visualization Alerting)
View Incident Details
(from Presentation Visualization Alerting)
View Defensive Posture View
(from Presentation Visualization Alerting)
CIRT Analyst
(from CFNOC Staff)
Clean Infection and Secure Server
(from External To System)

**Figure 34: Working with a Coalition Partner**

| Source | Type | Target |
|---|---|---|
| Working with a Coalition Partner | | C2IEDMPeer |

**Table 183: Relationships for Working with a Coalition Partner**

### Use Case: Maintain Shared Data Logs -

#### Description:

Logs will record time, classification, content and recipient/provider information for each transmission.

| Source | Type | Target |
|---|---|---|
| Data Sharing | include | Maintain Shared Data Logs |

**Table 184: Relationships for Maintain Shared Data Logs**

### Use Case: Manage Recipient/Provider Profile -

#### Description:

Remote JNDMS instances or other stakeholders' systems will connect and provide a data sharing profile. This profile will specify the parameters for partial situational awareness data sharing. This also includes managing permissions.

| Source | Type | Target |
|---|---|---|
| Data Sharing | include | Manage Recipient/Provider Profile |
| Manage Recipient/Provider Profile | | DID-DM-4 |

**Table 185: Relationships for Manage Recipient/Provider Profile**

#### Requirements:

**DID-DM-4**

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.

## Use Case: Pre-Process and Store Shared Data Received -

### Description:

JNDMS interprets the SA data received using the provider's profile and stores the data in the database.

| Source | Type | Target |
|---|---|---|
| Exchange data across classification layer | precedes | Pre-Process and Store Shared Data Received |
| Data Sharing | include | Pre-Process and Store Shared Data Received |

**Table 186: Relationships for Pre-Process and Store Shared Data Received**

## Use Case: Verify Integrity of Transmission -

### Description:

JNDMS will perform data transmission integrity checks.

| Source | Type | Target |
|---|---|---|
| Data Sharing | include | Verify Integrity of Transmission |

**Table 187: Relationships for Verify Integrity of Transmission**

## Use Case: Assemble Data for Transmission base on Profile -

### Description:

The data is assembled based on data attributes and the user profile.

| Source | Type | Target |
|---|---|---|
| Assemble Data for Transmission base on Profile | precedes | Exchange data across classification layer |
| Data Sharing | include | Assemble Data for Transmission base on Profile |
| Assemble Data for Transmission base on Profile | | DID-DS-3 |

**Table 188: Relationships for Assemble Data for Transmission base on Profile**

**Requirements:**

**DID-DS-3**

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.

## Use Case: Replicate data with peer JNDMS -

**Description:**

This is a complete replication of data between two JNDMS instances residing at the same level of classification.

| Source | Type | Target |
|---|---|---|
| Replicate data with peer JNDMS | | DID-DS-1 |
| Data Sharing | include | Replicate data with peer JNDMS |
| Replicate data with peer JNDMS | | DID-DM-4 |
| Replicate data with peer JNDMS | | JNDMSPeer |

**Table 189: Relationships for Replicate data with peer JNDMS**

**Requirements:**

**DID-DM-4**

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.

**DID-DS-1**

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.

## Use Case: Exchange data across classification layer -

**Description:**

Two JNDMS instances are running on different classification layers. The lower level domain will connect to the higher level and push the data through a one way information flow.

| Source | Type | Target |
|---|---|---|
| Exchange data across classification layer | | DID-DS-1 |
| Assemble Data for Transmission base on Profile | precedes | Exchange data across classification layer |
| Exchange data across classification layer | | DID-DS-2 |
| Exchange data across classification layer | precedes | Pre-Process and Store Shared Data Received |
| Data Sharing | include | Exchange data across classification layer |
| Exchange data across classification layer | | Coalition SA System |
| Exchange data across classification layer | | Inbox |

**Table 190: Relationships for Exchange data across classification layer**

**Requirements:**

**DID-DS-1**

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.

**DID-DS-2**

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.

# ANNEX A – USE CASE TRACEABILITY

| Package | Use Case Name | Requirement ID |
|---|---|---|
| Data Collection | Acquire Domain Data | DID-JNDMS-0 |
| Data Transformation | Data Transformation | DID-JNDMS-0 |
| Data Transformation | Pre-Process IT Infrastructure Data | DID-IRELD-0<br>DID-ITID-0<br>DID-ITID-4 |
| Data Transformation | Pre-Process Operations Data | DID-IRELD-0<br>DID-OD-0<br>DID-OD-2 |
| Data Transformation | Pre-Process Safeguard Data | DID-IRELD-0<br>DID-SAFD-0<br>DID-SAFD-2 |
| Data Transformation | Pre-Process Vulnerability and Exploit Data | DID-IRELD-0<br>DID-VED-0<br>DID-VED-4 |
| Data Warehousing | Data Warehousing | DID-JNDMS-0 |
| Data Warehousing | Store Defensive Posture | DID-DM-0<br>DID-DM-1<br>DID-DM-2<br>DID-DM-3<br>DID-DM-4 |
| Data Warehousing | Store Incidents | DID-DM-0<br>DID-DM-1<br>DID-DM-2<br>DID-DM-3<br>DID-DM-4<br>DID-IR-0<br>DID-IR-4 |

| Package | Use Case Name | Requirement ID |
|---|---|---|
| Data Warehousing | Store IT Infrastructure Data | DID-DM-0<br>DID-DM-1<br>DID-DM-2<br>DID-DM-3<br>DID-DM-4<br>DID-ITID-0<br>DID-ITID-5 |
| Data Warehousing | Store Operations Data | DID-DM-0<br>DID-DM-1<br>DID-DM-2<br>DID-DM-3<br>DID-DM-4<br>DID-OD-0<br>DID-OD-3 |
| Data Warehousing | Store Safeguard Data | DID-DM-0<br>DID-DM-1<br>DID-DM-2<br>DID-DM-3<br>DID-DM-4<br>DID-SAFD-0<br>DID-SAFD-3 |
| Data Warehousing | Store Severity Assessment Information | DID-DM-0<br>DID-DM-1<br>DID-DM-2<br>DID-DM-3<br>DID-DM-4<br>DID-SA-0<br>DID-SA-5 |

| Package | Use Case Name | Requirement ID |
|---|---|---|
| Data Warehousing | Store Vulnerability and Exploit Data | DID-DM-0<br>DID-DM-1<br>DID-DM-2<br>DID-DM-3<br>DID-DM-4<br>DID-VED-0<br>DID-VED-5 |
| Decision Support System | Data Fusion | DID-JNDMS-0 |
| Decision Support System | Defensive Posture Assessment | DID-DPA-0 |
| Decision Support System | Incident Severity Assessment | DID-IR-0<br>DID-SA-0<br>DID-SA-3<br>DID-SA-4 |
| Decision Support System | Real-time Incident Recognition | DID-IR-0<br>DID-IR-1<br>DID-IR-5 |
| Presentation Visualization Alerting | Present Situational Awareness | DID-JNDMS-0 |
| Presentation Visualization Alerting | User Interactions | DID-DP-4 |
| Presentation Visualization Alerting | Views (GIS) | DID-DP-0<br>DID-DP-3 |
| Security Information Management | Pre-Process Security Events | DID-IRELD-0<br>DID-SED-0<br>DID-SED-2 |
| Security Information Management | Store Security Events | DID-SED-0<br>DID-SED-3 |
| Situational Awareness Data Sharing | Assemble Data for Transmission base on Profile | DID-DS-3 |

| Package | Use Case Name | Requirement ID |
|---|---|---|
| Situational Awareness Data Sharing | Data Sharing | DID-DM-3<br>DID-DS-0<br>DID-JNDMS-0 |
| Situational Awareness Data Sharing | Exchange data across classification layer | DID-DS-1<br>DID-DS-2 |
| Situational Awareness Data Sharing | Manage Recipient/Provider Profile | DID-DM-4 |
| Situational Awareness Data Sharing | Replicate data with peer JNDMS | DID-DM-4<br>DID-DS-1 |

# ANNEX B – FUNCTIONAL REQUIREMENTS

| DID Description | CDRL ID | DID | Requirement |
|---|---|---|---|
| Provide SA for CND | 1 | DID-JNDMS-0 | The JNDMS shall provide situational awareness (SA) for Computer Network Defence (CND) through the fusion of Military Operations, IT infrastructure, Security events, Vulnerability, and Safeguards datasets. The JNDMS shall capture, store, process, analyze and present data from these five information domains |
| Capture Security Events Data | 2 | DID-SED-0 | The JNDMS shall capture Security Events Data. This function refers to the following sub-functions: acquiring, pre-processing and storing security events data. |
| | 3 | DID-SED-1 | 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 equipment, tools and repositories such as firewalls, IDS/IPS, virus scanner, incident ticketing tools, intelligence community reports and other contextual information reports |
| | 4 | DID-SED-2 | 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 | DID-SED-3 | 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. |
| Capture Operations Data | 6 | DID-OD-0 | 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. |
| | 7 | DID-OD-1 | 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. |

| DID Description | CDRL ID | DID | Requirement |
|---|---|---|---|
| Capture Operations Data | 8 | DID-OD-2 | 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 record imported from the operational databases or other sources. |
| | 9 | DID-OD-3 | 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. |
| Capture IT Infrastructure Data | 10 | DID-ITID-0 | 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. |
| | 11 | DID-ITID-1 | 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). |
| | 12 | DID-ITID-2 | 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. |
| | 13 | DID-ITID-3 | 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. |

| DID Description | CDRL ID | DID | Requirement |
|---|---|---|---|
| Capture IT Infrastructure Data | 14 | DID-ITID-4 | 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 record acquired. |
|  | 15 | DID-ITID-5 | 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. |
| Capture Vulnerability and Exploit Data | 16 | DID-VED-0 | 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. |
|  | 17 | DID-VED-1 | 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. |
|  | 18 | DID-VED-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. |
| Capture Vulnerability and Exploit Data | 19 | DID-VED-3 | 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. |

| DID Description | CDRL ID | DID | Requirement |
|---|---|---|---|
| | 20 | DID-VED-4 | 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 record acquired. |
| | 21 | DID-VED-5 | 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. |
| Capture Safeguard data | 22 | DID-SAFD-0 | The JNDMS shall capture IT Infrastructure Safeguards data. This function refers to the following sub-functions: acquiring IT Infrastructure Safeguards data, pre-processing this data, and writing it to the JNDMS database. |
| | 23 | DID-SAFD-1 | 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. |
| | 24 | DID-SAFD-2 | 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 record acquired. |
| | 25 | DID-SAFD-3 | 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. |
| Capture the interrelationships data | 26 | DID-IRELD-0 | The JNDMS shall capture inter-relationships between Security Events, Military Operations, IT Infrastructure, Vulnerabilities and safeguards. This function refers to the following sub-functions: analyzing 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, normalizing these inter-relationships, deconflicting these inter-relationships, consolidating these inter-relationships and writing them to the JNDMS database. |

| DID Description | CDRL ID | DID | Requirement |
|---|---|---|---|
| Data fusion to perform Defensive Posture Assessment | 27 | DID-DPA-0 | The JNDMS shall assess the Defensive Posture of the IT infrastructure. This function refers to the following sub-functions: analyzing 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. |
| Data fusion to recognize incidents | 28 | DID-IR-0 | The JNDMS shall fuse information from the five SA for CND domains (Operations, Infrastructure, Vulnerability, Safeguards, Events) to recognize incidents 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. |
|  | 29 | DID-IR-1 | 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. |
|  | 30 | DID-IR-2 | Correlate Incidents: The JNDMS shall consider new incidents, archived incidents, and shared incidents from other/external organizations 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. |
| Data fusion to recognize incidents | 31 | DID-IR-3 | 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. |
|  | 32 | DID-IR-4 | Store Incident Data: The JNDMS shall store incidents in the JNDMS database. The JNDMS shall assure that incident data is stored with accurate timestamp and integrity verification. |
|  | 33 | DID-IR-5 | Perform near real-time Incident Recognition: The JNDMS shall perform 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). |

| DID Description | CDRL ID | DID | Requirement |
|---|---|---|---|
| Data fusion to perform Severity Assessment | 34 | DID-SA-0 | 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. |
|  | 35 | DID-SA-1 | 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. |
|  | 36 | DID-SA-2 | 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 realization 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. |
| Data fusion to perform Severity Assessment | 37 | DID-SA-3 | 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 normalized severity scale meaningful to the JNDMS users. The JNDMS shall generate a severity value and supporting evidence statement. |
|  | 38 | DID-SA-4 | 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. |
|  | 39 | DID-SA-5 | 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. |

| DID Description | CDRL ID | DID | Requirement |
|---|---|---|---|
| Store and manage SA for CND data | 40 | DID-DM-0 | 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 sub-functions: 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. |
| | 41 | DID-DM-1 | 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. |
| Store and manage SA for CND data | 42 | DID-DM-2 | 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. |
| | 43 | DID-DM-3 | 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 timestamps. |
| | 44 | DID-DM-4 | 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. |
| Present Situational Awareness data | 45 | DID-DP-0 | 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. |

| DID Description | CDRL ID | DID | Requirement |
|---|---|---|---|
| | 46 | DID-DP-1 | Performance: The JNDMS views shall be updated in a near-real time fashion. Different levels 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. |
| | 47 | DID-DP-2 | User-defined Views and Queries: The JNDMS shall support the creation of user defined 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 to create tailored data queries, such as spatial and temporal queries and re-use these queries as required. |
| Present Situational Awareness data | 48 | DID-DP-3 | Visual Correlation: The JNDMS shall provide through its user interface a mean to visually correlate complex datasets from the five SA for CND 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”. |
| | 49 | DID-DP-4 | 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. |
| Share Situational Awareness data | 50 | DID-DS-0 | The JNDMS shall allow for sharing of Situation Awareness Data. This function includes 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. |
| | 51 | DID-DS-1 | 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. |

| DID Description | CDRL ID | DID | Requirement |
|---|---|---|---|
| | 52 | DID-DS-2 | 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. |
| Share Situational Awareness data | 53 | DID-DS-3 | 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. |

# ANNEX C – ASSOCIATED REQUIREMENT TRACEABILITY

| Requirement Traceability | |
|---|---|
| **1 Purpose** | **Comments** |
| The purpose of this document is to specify the Joint Network Defence and Management System (JNDMS) requirements. This document consists in a modified version of the IEEE 830-1998 standard for software requirements specification. | context |
| **2 Introduction** | |
| Military forces are becoming increasingly reliant on communications and computer-based networks to perform their operations. This is true for all phases of an operation, from strategic intelligence gathering and dissemination, operational planning, logistics support, command and control, to time-critical tactical sensing and decision-making in the field. Because networks underlie so many military activities, understanding the state of the required networks and maintaining their health is extremely important, particularly as the networks themselves become targets of potential adversaries. The network environment is being viewed today as another battlespace that must be controlled and defended. | context |
| As seen in Figure 1, the cyber domain can be presented as a battlefield using common military symbology. In this abstraction of the cyber-battlefield, the Computer Network Exploitation (CNE) and Computer Network Defence rectangles represent operational units, analogous to reconnaissance patrols and defensive position observation posts in traditional warfare. The protected regions are presented as cyber domains, but may also include physical network assets. The casualties suffered in this battlespace can undoubtedly translate into decreased operational capabilities for the entire defence organisation. | context |
| In order to provide Computer Network Defence (CND) in this modern battlespace, one must maintain situational awareness, analogously to other Command and Control activities in the land, air/space and sea elements. Situational Awareness (SA) for Computer Network Defence (CND) can be seen as a process by which one perceives its network environment, as well as understands and continuously predicts the risk and its evolution in time and space. The primary purpose of SA for CND is the efficient defence of the Information Technology (IT) Infrastructure and Services, in support of military operations. | context |
| This implies that the information requirements for SA ought to include military operations and their dependencies on IT services. However, bringing SA for CND in the Military Operation context is a significant challenge which must be addressed so that CND decisions take operational risk into consideration. As shown in Table 1, information requirements for SA for CND can be grouped into five information domains: Military Operations, IT Infrastructure and Services, Vulnerabilities and Exploits, Safeguards and Security Events. The integration and analysis of these domains provide decision makers with knowledge about the defensive posture of the networks and the severity assessment of network incidents. | context |

| Requirement Traceability | |
|---|---|
| The provision of SA for CND to the decision maker also involves the continuous processing of a very large volume of data which is generated at a fast rate. In an organisation such as the Department of National Defence (DND), there are a number of people and departments, both internal and external, involved in the capture and processing of the data relevant to SA for CND. This complexity adds to the challenge of building a system to provide SA for CND. | context |
| The JNDMS Technology Demonstration Project (TDP) is an initiative of the Network Information Operations (NIO) Section at Defence R&D Canada - Ottawa (DRDC Ottawa) whose objective is to provide SA for CND. | context |
| **3 Scope** | |
| This document forms the technical foundation for development of the JNDMS TD, which addresses the expressed needs of the Canadian Forces (CF) and the operational units involved in CND. The JNDMS is an integration, analysis and monitoring system that will provide SA for CND. The JNDMS is focused on bringing to decision makers the right network information at the right time. | context |
| The JNDMS' goals are to :<br>a) Provide commanders, network controllers and security analysts with an integrated computer network defence situational awareness picture of the computer networks being used for military operations;<br>b) Support operation-centric computer network defence and network management; and<br>c) Support sharing of network information among CF and international coalition partners to enhance the CF ability to identify network threats and support network defence within coalition operations. | context (goals) (addressed in CDRL #1 - 53) |
| The JNDMS TDP will provide a fundamental step toward a comprehensive, near real-time, decision support system for integrated computer network defence and management. | context |
| **4 Needs and Proposed Changes** | |
| The following section lists the needs of the CF units involved in CND. Those needs represent actual challenges which will be addressed by the JNDMS TDP in order to enhance SA for CND. | context (intro to 7 challenges) |
| **4.1 Data integration** | |
| The CND operational community requires an integrated system to monitor, manage and defend the IT infrastructure. | context |

| Requirement Traceability | |
|---|---|
| The CND operational community requires a means to collect and integrate information including the five information domains defined in table 1 (Security Events, Safeguards, IT infrastructure, Vulnerability, Operations) to provide integrated SA for CND. This information is currently distributed over several repositories and available in different formats. Moreover, this information resides on different networks, which have different levels of classification. The CND operational community needs a means to facilitate access to this data for more complete awareness and more effective response to network incidents. The data collection needs to be automated to deal with the volume of information and to keep this information up-to-date in near real-time. The CND operational community must be assured that everyone requiring SA for CND information has consistent information. The information required to achieve SA for CND must be accessible by anyone responsible for the maintenance and security of the DND IT infrastructure. It must also be accessible by command staff requiring information about the IT infrastructure supporting their operations. | Addressed in CDRL #2, 6, 10, 16, 22 |
| The JNDMS approach to providing SA for CND is to automate as much as possible the gathering of Security Events, Operations, Vulnerability, Safeguards and IT Infrastructure data and to store this data in a database. The JNDMS will use information exchange standards and a comprehensive data model to integrate this data. This database will be geographically distributed/replicated and accessible by all authorized users. | Addressed in CDRL #2, 6, 10, 16, 22, 40-44, 50-53 |
| **4.2 Operation-centric defence** | |
| The CND operational community requires a clear understanding of the interdependencies between Security Events, Safeguards, Vulnerabilities and IT Infrastructure assets and services with military Operations. | Addressed in CDRL #26, 45 |
| It is assumed that Operations drive the need for supporting IT Infrastructure. However, tracking of the operational relevance of given IT assets, once deployed, is challenging due to the interconnections, fusions and integrations occurring at the different layers of the OSI model. | context |
| When responding to network incidents, the CND operational community requires that actions take place with minimal impact to DND/CF's ability to monitor, manage and direct ongoing operations. To help determine the effect of the network incident on operations, the CND operational community requires a detailed mapping of the dependency of Military Operations on the IT infrastructure. This dependency is also required by the command staff to be aware of the status of IT assets supporting their operations. The command staff also requires this information to help determine the impact of network incidents on operations and to understand the consequences of taking proposed actions. | Addressed in CDRL #26, 45 |
| The JNDMS will use its global database of SA for CND information to provide the relationship between IT assets and operations. The user will be able to query for operations depending on particular networks, IT services or physical devices. The user will also be able to highlight the IT assets supporting particular operations. This will allow the JNDMS user to relate network incident to Military Operations, and ultimately, perform accurate impact/risk analysis. | CDRL #49 |

| Requirement Traceability | |
|---|---|
| **4.3 Visualization** | |
| The CND operational community requires a clear picture of the IT infrastructure, and its threats and vulnerabilities. | Addressed in CDRL #45 - 49 |
| Network defence situational awareness information is required by a variety of users such as network administrators, security analysts and command staff. Consequently, the visual presentation of this information must be intuitive to many users with differing responsibilities, skills, and depth of IT knowledge. | Addressed in CDRL #45 - 49 |
| Much like the battlemaps used by the Environments (Army, Navy, and Air Force) the CND operational community requires a network battlemap to view the status of IT infrastructure activities and assets, and their role in supporting operations. This view of the network battlespace must be compatible with those of the other Environments so that it can be integrated into a joint command and control system. | CDRL #47 |
| To address these requirements, the JNDMS will enable the efficient aggregation of complete and comprehensive information via a visually rich interface. The database's content will be presented according to the user-specific preferences within a Geographic Information System (GIS) framework. The GIS framework will allow users to overlap layers of information, including military operations, for visual correlation. When appropriate, SA for CND information will be displayed on a network map. The user will choose the portion of the network to be displayed and the type of information to be mapped onto the network. The SA for CND information will be available at various levels of detail as required by the several levels of command. | Addressed in CDRL #45 - 49<br>The user will choose the portion of the network to be displayed and the type of information to be mapped onto the network. |
| A key element of the JNDMS will be the visual correlation of geographic and network information achieved by presenting the network information with a map background. This will allow users to view the correlation between network information or events and geo-location. This will also provide a geospatial view of the IT infrastructure more closely related to the battlemaps of the physical environments. | Addressed in CDRL #48 |
| **4.4 Severity assessment** | |
| The CND operational community requires a measure to help prioritize response to network incidents. | Addressed in CDRL #34 - 39 |
| The CND operational community needs an automated capability to recognize network incidents. The CND operational community also requires a severity computation capability which will enable prioritization of identified incidents and provide command staff with decision enabling information for resource allocation. | Addressed in CDRL #28 - 33, 34 - 39 |
| Intrusion alerts and events logs provide limited contextual information and require intense manual work to review and extract relevant clues and incidents. In order for the JNDMS to automate this process, the fusion of various sensors and information layers is required. | Addressed in CDRL #28 - 33, 34 - 39 |

| Requirement Traceability | |
|---|---|
| The improved data integration provided by JNDMS will make new capabilities possible, including the introduction of a means to calculate network incident severity taking operational requirements into account. The user will be able to query the global database to correlate incidents and estimate their effect on operations. This will be accomplished by providing a severity assessment capability that calculates the severity of each incident using computed operational impact and risk assessment values. The module will use incident information such as the type, the systems, applications and network affected, the locations involved, the existing incidents, redundancies, the current threats, vulnerabilities and safeguards, the IT service value and the duration to assess how significant the incident is. These severity assessment values, provided along with their supporting statements and hypothesis, can then be considered by the watch staff when deciding the order for handling concurrent incidents. As well, these values can be rolled-up to provide an overall corporate security status. | Addressed in CDRL #34 - 39 |
| **4.5 Interoperability** | |
| The CND operational community requires a means to share automatically network situational awareness information among its operational and support organizations as well as with its allies. | Addressed in CDRL #50 - 53 |
| The CND operational community requires a means to coordinate dynamic sharing with networks of coalition partners. This will enable the CND operational community to share computer network defence situational awareness information with coalition partners developing their own computer network defence situational awareness capabilities. | Addressed in CDRL #50 - 53 |
| To achieve interoperability, the JNDMS requires a common data model and database accessible by coalition partners and other DND Common Operating Picture projects through open APIs and replication mechanisms. Using a coalition-sharing gateway, situational awareness data pertinent to given operations will be shared dynamically with other systems. | Addressed in CDRL #50 - 53<br>Common data model and database |
| **4.6 Common Operating Environment** | |
| DND requires a common operating environment to monitor, manage and defend the IT infrastructure. | Addressed in CDRL #1 |
| Network defence and management leads to excessive training and preparation costs due to the large variety of tools and approaches currently used. To deal with this issue, DND requires a unified network defence environment. | Addressed in CDRL #1 |
| The JNDMS will provide one operating environment for all computer network defence situational awareness activities. The user interface of JNDMS will reflect the used asset hierarchy and allow process-based navigation. This will enhance the intuitive use of the tool and help unify terminology throughout the department. The presentation of the IT infrastructure database on a GIS will also provide a more comprehensive decision environment. This general outlook will decrease dependence on specific tools and allow a reduced set of tools to be used to achieve the same result. | Addressed in CDRL #1 |
| **4.7 Defensive Posture** | |
| DND requires a means to evaluate its departmental and threat-specific defensive posture. | context |

| **Requirement Traceability** | |
|---|---|
| There is a need for understanding the level of protection of IT infrastructure assets and IT services, taking into consideration both physical and cyber-domain potential threats and specific vulnerabilities. These vulnerabilities may, or may not, be exposed to threat agents by existing avenues of approach (refer to figure 1). The JNDMS needs to clearly relate potential threats with known vulnerabilities, avenues of approach and safeguards. The JNDMS will dynamically assess the defensive posture by automatically evaluating the relevance of the deployed safeguards and their ability to mitigate the risk, or the exposure to given threat events. | Addressed in CDRL #16, 22, 26, 27 |
| **5 System features** | |
| In order to address the needs of the operational community, the JNDMS will define, develop and demonstrate capabilities allowing:<br>- Demonstrating the value of Network Situational Awareness information;<br>- Establishing the benefits of having a real-time mapping of the dependencies of military operations onto cyber assets;<br>- Investigating network information visualization systems, including Geographic Information System (GIS), as potential candidates for the Network Battlemap;<br>- Demonstrating integration of SA for CND information from different classification domains;<br>- Exploring the benefits of sharing information between international, national and local CND stakeholders, such as Network Operation Centres (NOCs); and<br>- Determining the advantages of sharing information (with different levels of detail) between various levels of command. | context (system features)<br>(addressed in CDRL #1-53) |
| **The features of the JNDMS shall include:** | |
| **1. Integrating, distributing, and fusing IT infrastructure information.** | |
| The IT infrastructure status data will be widely distributed and replicated, allowing many different centres to use it as they respond to incidents. This makes the total response diverse and robust since analysis can continue following the defensive isolation of a domain. The result will be faster defensive actions and improved decision accuracy based on more up to date information. | Addressed in CDRL #10-15, 50-53 |
| **2. Mapping the dependencies of operations on the IT infrastructure.** | |
| The dependence of operations on services provided by the IT infrastructure will be explicitly recorded in the JNDMS database. This will allow the importance of a service for an operation to be queried, as well as the importance of a device which impacts a service to be queried. This information will lead to more complete SA for CND for operational command staff if there is a loss of some components of the IT infrastructure. It will also lead to less disruptive scheduling of maintenance activities. | Addressed in CDRL #26 |
| **3. Using physical location to display IT infrastructure information.** | |

| Requirement Traceability | |
|---|---|
| A network diagram is the most intuitive representation of the IT infrastructure. It shows the data flow paths between infrastructure elements using various definitions of data flow, and it allows details to be retrieved for specific elements through user selection on the display screen. This kind of display is referred to as a logical representation of the infrastructure because it shows how elements are connected without any consideration of their physical location. For JNDMS the physical location will also be used, and the network topology information will be overlayed on a geographical background using GIS technology. This will provide a much better means to assess the infrastructure status since queries by location will be supported and the consequences of a problem at a specific location will be obtainable for an operation. Also, for mobile infrastructure elements, this geographical display of the infrastructure status will convey useful visual correlations of incident and location information to the operation command staff. | Addressed in CDRL #12, 45 |
| **4. Having a Network Battlemap as a component of the Common Operating Picture.** | |
| The JNDMS geographically organized display will convey IT infrastructure status directly, along with visually correlated information about assets and operations. This will provide better background information as a basis for operational command decisions. These views, shared between the various levels of command, will facilitate understanding of the current situation, making the organization's total response quicker and more effective. | Addressed in CDRL #45 |
| **5. Automating the support for decisions about incident severity.** | |
| The globally available data about the IT infrastructure, operations, and incidents will be used by a severity assessment module to calculate a severity value for each incident. This value will help decision makers when they are prioritizing their responses to several concurrent incidents. The severity assessment will make use of operations data to estimate the impact of the incident on current operations. Decision makers will be able to rely on this assessment as a comprehensive and consistent indicator that applies known and well defined rules. This will lead to better decisions concerning resource use for network defence in a fast paced operational context. | Addressed in CDRL #34 |
| 6. Establishing basic capabilities needed to join coalition networks for integrated international operations. | |
| The JNDMS addresses some of the issues involved in coalition participation: network defence situational awareness, and the capability for automated visualization of infrastructure incidents that affect the other partners in a coalition. | Addressed in CDRL #50-53 |
| 7. Providing a common approach for improved staff effectiveness and training. | |

| Requirement Traceability | |
|---|---|
| Given the proliferation of different though equivalent tools, incomplete data sets, and the fast rate of change in IT infrastructure capabilities, assessing the state of the network is currently more complex than necessary. All this will be improved through the JNDMS initiative, which will evolve toward the use of the most effective tools, full integration when new tools are introduced, and automated and dynamic data generation that will result in more complete data being available. Training will be simplified, and the ability of different centres to collaborate will be improved as a result of this data integration. | Addressed in CDRL #10 (capturing IT data) |
| 8. Having historical, current and future/predictive views of the IT infrastructure status. | |
| The JNDMS database can be checkpointed at regular intervals to capture what was in effect at those times. This data will provide trend indicators that will be useful for future planning. For example, trends in the number of internationally deployed hosts would be apparent. The data can also be used for short term planning, in particular for maintenance activities, since the dependence of an operation on the availability of a specific device will be available as a result of a query. This will improve the DND ability to plan maintenance so that it minimizes operational impacts. Finally, the historical data will assist security incident investigations by providing trusted, accurate, and complete forensic evidence. | Addressed in CDRL #10 (capturing IT data) |
| **6 User characteristics** | |
| JNDMS is designed to provide CND stakeholders with situational awareness. Some of JNDMS users are:<br>- Head Quarters and Commanding Staff;<br>- Staff – Signal Officers;<br>- Watch staff at Network Operations Centers;<br>- Network Security Analysts;<br>- System Administrators, Service desk agent; and<br>- Network operation management staff. | context |
| They each perform various functions and support different processes. | context |
| JNDMS does not differentiate between user classes, with the exception of specific system administration functions. Views will be defined by the users who set their own profiles. All users having access to JNDMS will have full visibility over the data, with the exception of the groups accessing JNDMS through the sharing module used for coalitions. For these groups, privileges will be defined in sharing profiles and managed centrally by JNDMS administrator. | Addressed in CDRL #47, 53 |
| JNDMS is a monitoring tool. The user views the available data, and then takes action using other systems and tools. Support for direct interactions between JNDMS users are not specify in this document, but future work could look into collaborative environment features integration. | context |
| **7 Constraints** | |

| **Requirement Traceability** | |
|---|---|
| The following section lists the constraints that the JNDMS Contractor will have to consider in the development of the JNDMS solution. These constraints are not exclusive. The Contractor is encouraged to balance these constraints with other pertinent benefits to the TD Program, including additional capabilities, innovativeness, overall development risk, deployment and in-support cost, etc., for the design of the proposed solution. | context |
| **Transition Constraints** | |
| **7.1 Operating System and networking environment** | |
| DND has identified the Windows operating system as its platform of choice for servers and workstations. The user workstations have a software baseline including common MS Office suite products and MS Internet Explorer as browser. DND has deployed Microsoft MOM and SMS. | |
| **7.2 Protocols and Middleware** | |
| All Application Program Interface (API) and interactions between system components shall be based on open technologies and standards. The contractor shall not use “mobile code” in the final solution. For example, the use of ActiveX and Java applets in the context of Web based application is only permitted if the code is statically put on the workstation using a standard installation process. | |
| **7.3 Security** | |
| The JNDMS is intended to support Command and Control activities. As such, using configuration based on Common Criteria (www.commoncriteria.org) security specification is recommended. Other configurations (not Common Criteria compliant or accredited) may be proposed as part of the JNDMS architecture as long as it is for the purpose of demonstrating technological breakthrough, innovation, or new pertinent features in the context of situational awareness for CND otherwise not demonstrable. The JNDMS design must not prohibit successful certification and accreditation security audits by using poor security practices and architecture. | |
| The JNDMS will be a multi-network system which will acquire data from networks having different classification levels. Due to the fact that no “trusted” technical solution exists to move information in a bi-directional fashion between networks of different classifications, the Contractor’s solution should make use of a hierarchical architecture to support multi-level data integration and fusion. This proposed approach makes use of one-way data feeds. This asynchronous data exchange approach (push) is proposed for interoperability between coalition partners as well as the integration of information between JNDMS instances residing on networks of different classifications. Figure 2 provides an example of such architecture. | Addressed in CDRL #52 |
| **Development Risk Mitigation Constraints** | |
| **7.4 Use of international data standards wherever possible** | |

| Requirement Traceability | |
|---|---|
| The JNDMS must be able to share network defence information with other organizations and allies. The solution developed by the contractor shall make use of already accepted standards. Some standards to be considered are Common Information Model (CIM) and Management Information Base (MIB) for network discovery, Incident Object Description and Exchange Format (IODEF) / Intrusion Detection Message Exchange format (IDMEF) for incidents, Information Technology Infrastructure Library (ITIL) for processes, SNML, CVSS and VulnXML for threats, MIL-STD-2525 for symbology, Multilateral Interoperability Project (MIP) Command and Control Information Exchange Data Model (C2IEDM) for the data model, and Open GIS Consortium standards for GIS, etc. In the absence of international standards, JNDMS shall use common, Industry Standard, non-vendor specific, formats (definitions, incident reporting, raw data, etc.) in order to facilitate information sharing with clients and partners. | CDRL #50 |
| **7.5 Commercial Off-the-Shelf (COTS)** | |
| The prototype developed shall be as close as possible to a fully supported and operational system. Hence, incorporating already commercialized and supported modules and sub-systems is preferred over custom-developed solutions as long as development flexibility, functionalities and future deployment ease are not restricted by the COTS software selected. The cost of deployment of the operational solution based on the JNDMS TDP should also not be prohibitive and be comparable to similar systems in terms of roll-out and life-cycling costs. | Context |
| Product families which can be considered to provide partial functionality include:<br>- Enterprise Security Management suites;<br>- Enterprise Network Management suites;<br>- Network Discovery products;<br>- Geospatial Information Systems (GIS);<br>- Network Information Integration, Display and Computation products. | Context |
| Software installed on JNDMS devices shall be obtained from the provider on physical media. Beta Releases should not be considered for use unless on a temporary trial basis. | Context |
| **7.6 Open Source** | |
| Some of the JNDMS features may be implemented using Open Source software. This approach is acceptable as long as the chosen Open Source software packages have demonstrated security features, are provided by trusted sources, and are widely supported. This approach does not alleviate the need for documenting and associating modules with described functionalities. The contractor shall consider maintenance cost and support of the open source product in the context of an eventual DND-wide implementation of the JNDMS. | context |
| **7.7 Passive and active data collection** | |

| Requirement Traceability | |
|---|---|
| For the purpose of monitoring networks and network dependant activities, passive and active techniques can be used. JNDMS should make use of both approaches for data gathering functions. The DND already makes use of Intrusion Detection Sensors (IDS), which can be used as passive data gathering tools, or “sniffers”. Host based agents, such as SNMP agents, could be considered to provide additional and more complete data. However, many active host-based components are subjected to security vulnerabilities and should therefore be thoroughly assessed prior to integrating them into the system design. | context |
| **8 Dependencies and Assumptions** | |
| **8.1 Feeder systems** | |
| The JNDMS shall have the capability to integrate data from various data sources under various formats. Standard data formats used by feeder systems such as network management and security tools shall be considered for the JNDMS solution. The main network management and security COTS used in DND that are pertinent to the project are:<br>- Microsoft SMS;<br>- Microsoft MOM;<br>- Intellitactics Network Security Manager (NSM);<br>- Alcatel 5620; | Context |
| DND also makes use of several commonly used NMS. The ability of the JNDMS design to integrate or leverage these COTS will improve transition potential. | Context |
| **8.2 Dynamic IT software market environment** | |
| Due to the dynamic nature of the IT security and operation management tool market, the JNDMS shall be adaptable. For this purpose, the JNDMS shall be as modular as possible, using common interfacing standards. This feature would enable the integration of new solutions within the JNDMS architecture (ex: simulation capability could be added at a later date), or the replacement of an existing component with a more recent version, or completely different software. | context |
| **8.3 Automated network control and course of actions** | |
| The JNDMS will not be developed to perform network control through suggested courses of action and automated responses. However, the design of JNDMS should not prevent such capabilities from being added at a later date. | context |