INTERFACE CONTROL DOCUMENT (ICD) FOR PROGNOS KNOWLEDGE EXCHANGE MODULE

2 MAY 2010

TOTAL NUMBER OF PAGES: **26**

Version Modification Table

Version	Date	By	Comments
0	04/18/10	Richard Rockweiler	Initial Outline
1	04/25/10	Richard Rockweiler	Draft
2	04/29/10	Nhan Nguyen	Format and other minor edits

Table of Contents

Table of Figures

Table of Tables

1 INTRODUCTION

1.1 Purpose

The purpose of this Interface Control Document (ICD) is to define the external interfaces of the PROGNOS Knowledge Exchange module.

1.2 Scope

The scope of this document is limited to United States Navy's FORCENet systems. The document has been additionally de-scoped by focusing on the Navy's FORCENet Intelligence, Surveillance, and Reconnaissance (ISR) system which is the Distributed Common Ground Station – Navy (DCGS-N) and the Navy's future Command and Control (C2) system which will be based on Network Enabled Command and Control (NECC). It is assumed that NECC will be the replacement for Global Command and Control System – Maritime (GCCS-M), the United States Navy's current command and control system.

1.3 Overview

1.3.1 FORCEnet

FORCEnet is the US Navy/US Marine Corps alignment and integration effort for three major elements: (1) Department of Navy Transformation, Joint Interoperability, and Network Centric Warfare; (2) Innovation, demonstration, testing, and assessment to achieve Chief of Naval Operations' (CNO) goal of "Speed to Capability"; (3) Operational requirements, architectures, standards, compliance, and oversight of Naval programs to achieve Joint War-fighting capability. FORCEnet is an operational construct composed of multiple different automation systems, network infrastructure systems, and telecommunications systems provided by multiple Navy program offices and contractors. It is not a homogenous network or program; rather it serves as a framework to define the Navy tactical network and to define the policies to support standards development, compliance, and interoperability. FORCEnet connects diverse automation systems that support multiple battlespace functions to include Intelligence, Surveillance, and Reconnaissance (ISR); operational Command and Control (C2); and logistical functions. These systems are connected via multiple transmission systems to include satellite, Line of Sight (LOS) radio systems, and fixed telecommunication infrastructure. The automation systems, network infrastructure, and transmission systems are supported by multiple Navy programs that were acquired and planned in a disjointed fashion resulting in "stovepipes" systems, custom designed for a specific purpose. The systems serve their defined purpose; however, since they were developed in a divergent fashion, sharing data between these systems is a significant technical challenge due to incompatible message formats and protocols.

1.3.2 PROGNOS

PROGNOS, a system for Predictive Naval Situation Awareness currently being developed at George Mason University's C4I Center, is a project to improve situation awareness for the U.S. Navy and to "enable predictive analysis with principled hypothesis management"[1]. "PROGNOS will integrate four state-of-the-art enabling technologies into a distributed system architecture that represents domain knowledge as a modular collection of probabilistic ontologies, combine these

---

[1] Costa, Laskey, Chang. PROGNOS: Applying Probabilistic Ontologies to Distributed Predictive Situation Assessment in Naval Operations.

"knowledge nuggets" dynamically into complex situation models, and apply theoretically sound, computationally efficient hypothesis management and inference to combine evidence and background knowledge to reason about the current situation. PROGNOS will also interoperate with other FORCEnet systems by interacting via semantically enabled services."[2] Figure 1 illustrates the system overview diagram that depicts the modules and components of FORCENet and PROGNOS.

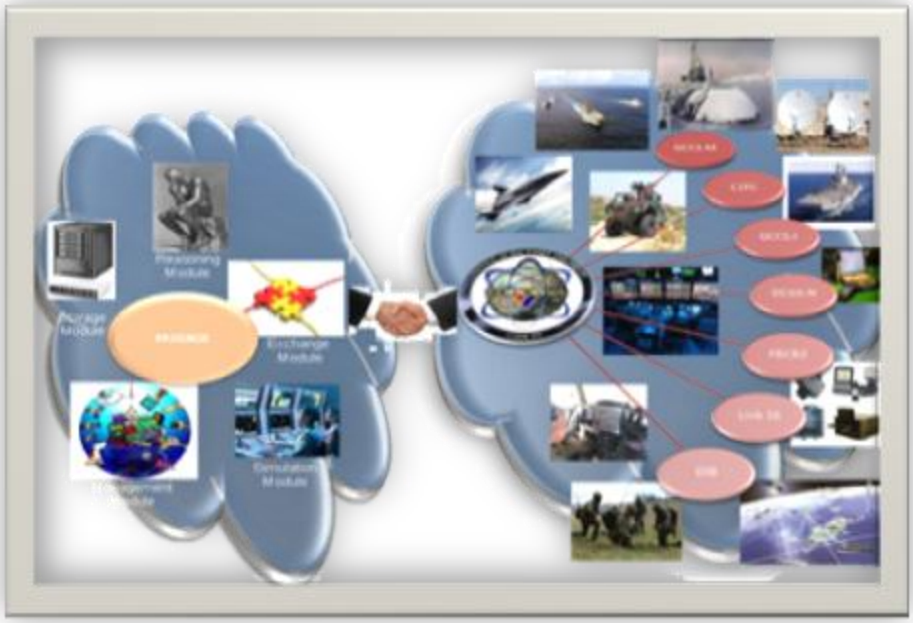


Figure 1. External System Diagram

The PROGNOS system consists of five modules as shown in Figure 2: Knowledge Storage module, the Reasoning module, Knowledge Management module, Knowledge Exchange module, and the Simulation module. The Knowledge Storage Module is responsible for storing the ontological information.

[2] Ibid.

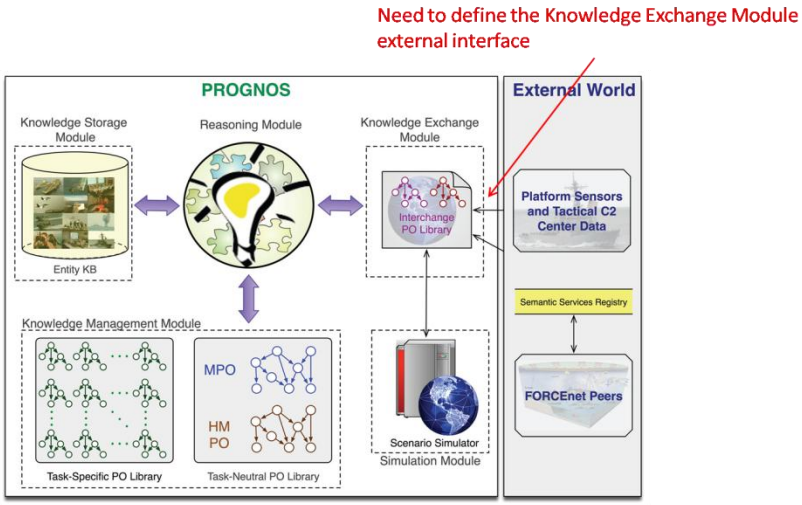


Figure 2. PROGNOS Modules

The Reasoning Module is the heart of the PROGNOS System. "It is composed of a Multi-Entity Bayesian Network (MEBN) reasoner that interacts with the other modules and coordinates the execution of Situation-Specific Bayesian Network (SSBN) construction, which includes interleaved hypothesis management and inference…"[3]

The Knowledge Storage Module stores the entities and attributes necessary to implement the PROGNOS probabilistic ontology. ".. every track and its respective data are stored within a schema based on and dynamically linked to the PROGNOS system's MPO (Main Probabilistic Ontology)."[4]

The Knowledge Exchange Module is responsible for interfacing with the external FORCEnet ISR and C2 system such as DCGS-N and NECC. The red arrow in figure 2 defines the interface that this document will describe.

The Knowledge Management Module is the brains of the PROGNOS System. The Knowledge Manage Module ".. is responsible for understanding the situation at hand and defining how to proceed in face of a situation."[5] "The module contains a set of probabilistic ontologies that capture domain knowledge..."[6] The Knowledge Management Module is comprises of two libraries – a Task-Specific Probabilistic Ontology and a Task-Neutral Probabilistic Ontology. The Task-Neutral Probabilistic Ontology contains knowledge applicable to any task. The Task-Specific Probability Ontology contains knowledge specific to a particular task.

The Simulation Module supports computerized military exercises, operation simulation, and "what-if" scenario planning. . The simulation module ".. sends geographical data (coordinates, known or probable) and status (friend, foe, unknown, etc.) of fictitious entities that are going to be used to evaluate the system's response"[7].

---

[3] Ibid, page 6.

[4] Ibid, page 6.

[5] Ibid, page 7.

[6] Ibid, page 7.

[7] Ibid, page 7.

The Knowledge Exchange Module is responsible for exchanging data with external Navy FORCEnet systems. The original scope as defined in the "PROGNOS: Applying Probabilistic Ontologies to Distributed Predictive Situation Assessment in Naval Operations" dissertation is the following: "…exchanges knowledge with the platform's sensors and tactical C2 system, the Simulation Module, FORCEnet peers, and other networked systems."[8] However, there is not a need to directly connect to platform sensors since the sensors are networked into existing C2 and ISR systems such as GCCS-M (will be replaced by NECC) and DCGS-N. The Knowledge Exchange Module only needs to interface with Navy FORCENet C2 and ISR systems.

1.3.3 System Description

The PROGNOS Knowledge Exchange Module is responsible for exchanging data (legacy systems) and knowledge (next generation ontology based systems). Figure 3 shows at a high level the interaction between multiple systems. In Figure 3, PROGNOS is communicating with DCGS-N and via DCGS-N receiving information from a Unmanned Aerial Vehicle (UAV) and satellites. PROGNOS is also communicating with GCCS-M (will be replaced by NECC) and via GCCS-M is receiving Position Location Information (PLI) via Link-16 for fighter aircraft and ground and surface tracks via the Blue Force Tracking (BFT) application.

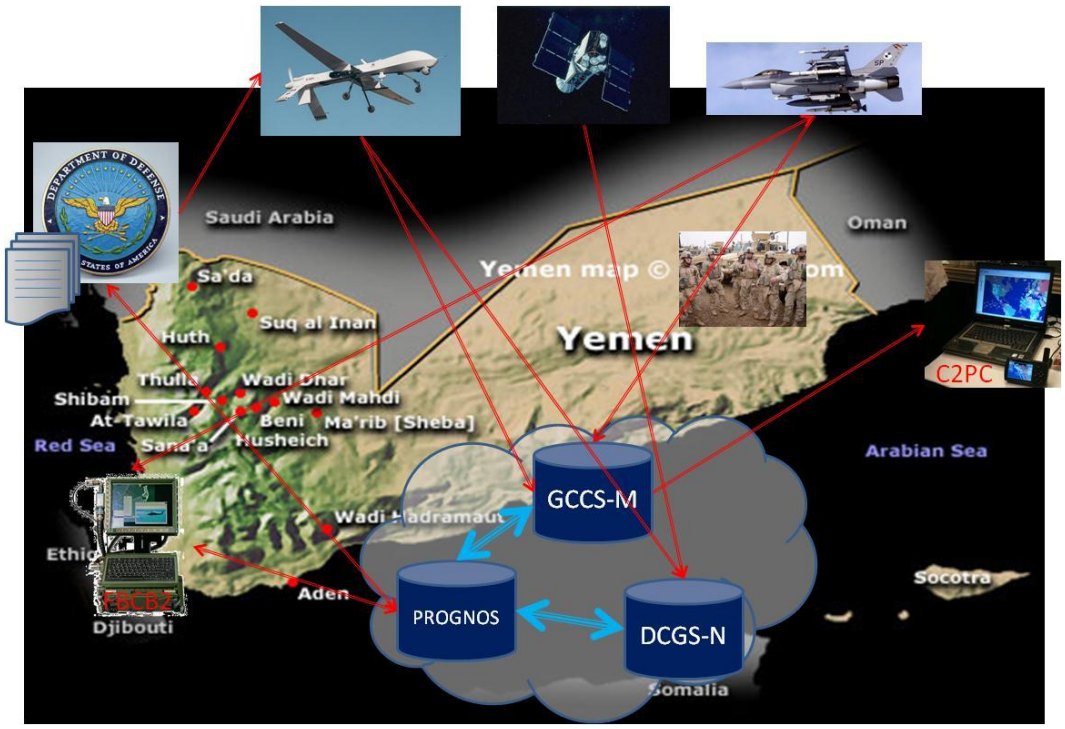


Figure 3. PROGNOS Context Diagram

The PROGNOS Knowledge Exchange Module needs to communicate with five primary system based on message types as shown in Figure 4.

[8] Ibid, page 7.

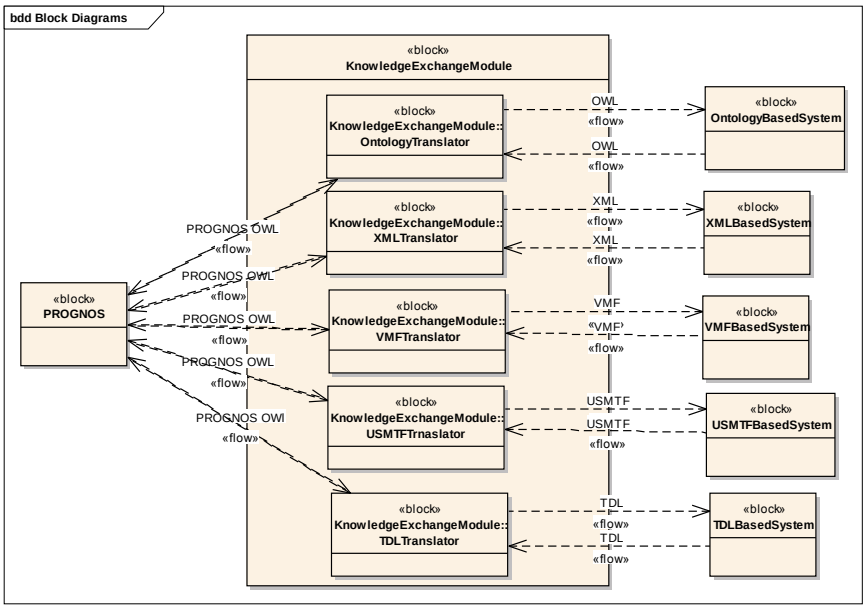


Figure 4. Summary of Interfaces by Message Types

Ontology Based Systems

The Knowledge Exchange Module must communicate with next generation systems that will be ontology based. Ontology Based Systems will be XML communication based; however, the XML data exchange will be further refined by the Resource Definition Framework (RDF) and the Web Ontology Language (OWL).

Non-Ontology XML Based Systems

The Knowledge Exchange Module must communicate with non-ontology based XML systems such as next generation Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM) North Atlantic Treaty Organization (NATO) systems. XML based systems will use Simple Object Access Protocol (SOAP). SOAP uses XML as its message format and HTTP or HTTPS as its transport mechanism. If it is too complex to communicate with an ontology based system via OWL due to lack of information or organization issues, an ontology based system can fall back to non-OWL XML/SOAP/HTTPS approach.

Joint Variable Message Format (JVMF) Systems

The Knowledge Exchange module will need to communicate with Joint Variable Message Format systems such as FBCB2 and Advanced Field Artillery Tactical Data System (AFATDS). These systems used a binary encoded message format defined by MIL-STD-6017. The PROGNOS Knowledge Exchange Module needs to support JVMF to receive the ground BFT picture and fire support information for the United States Marine Corps.

United Stated Message Text Format (USMTF) Systems

The Knowledge Exchange Module will need to communicate with USMTF based systems. Most of the official correspondence in the military is in a USMTF format. The USMTF format is defined by MIL-STD-6040. In order to parse intelligence reports and summaries, the Knowledge Exchange Module must be able to parse USMTF messages.

1.3.4 Distributed Common Ground System – Navy (DCGS-N)

The DCGS-N is the fleet variant of the Department of Defense (DoD) DCGS Family of Systems that provides integration of ISR support capabilities previously accessed from a variety of stand-alone systems.

It is developed for the following:

- Increase interoperability
- Ease of use with regard to C4I products
- Share actionable intelligence needed to identify and destroy targets

The DCGS-N system was designed to leverage commercial-off-the-shelf and mature government off-the-shelf software, tools and standards to provide a scalable, modular and extensible multi-source capability that operates at the General Service and Sensitive Compartmented Information security levels. DCGS-N uses an ashore Enterprise Point of Presence, accessible to all users via a Web interface, to facilitate sharing and receiving information with mission partners in a web-enabled, network-centric, joint-interoperable enterprise. This improvement also significantly reduces the stress on already limited bandwidth in the DCGS-N afloat configuration.

The DoD DCGS Family of Systems (FoS) access data from spaceborne, airborne, and afloat ISR collection assets, intelligence databases and intelligence producers. The data is shared across the Joint Enterprise using DCGS Integration Backbone and Net-Centric Enterprise Services standards to optimize timeliness, quality, and multi-service integration of ISR information.

The DCGS-N is designed to serve across several echelons, or tiers, in the Navy. Tier 1 capabilities are shore- or command-ship-based systems serving as reach-back nodes for theater operations. Units fielding Tier 2 systems include carrier, strike and expeditionary task forces, with the main nodes installed on aircraft carriers and large-deck amphibious ships. The final category is Tier 3, which is tailored for individual ships.

1.3.5 Net-Enabled Command Capability (NECC)

Net-Enabled Command Capability (NECC) is the future web-enabled Command and Control system for the United States Department of Defense. "In Increment 1, NECC will produce net-centric capabilities that replace the Global Command and Control System (GCCS) Family of Systems (FoS) as its first priority."[9]

The objective of the previous GCCS-M system that NECC will replace is to satisfy Fleet C4I requirements through the rapid and efficient development and fielding of C4I capability. GCCS-M enhances the operational commander's war-fighting capability and aids in the decision-making process by receiving, retrieving, and displaying information relative to the current tactical situation. GCCS-M receives, processes, displays, and manages data on the readiness of neutral, friendly, and hostile forces in order to execute the full range of Navy missions (e.g., strategic deterrence, sea control, power projection, etc.) in near-real-time via external communication channels, local area networks (LANs) and direct interfaces with other systems links. NECC will need to satisfy these same high level requirements in additional to the command and control requirements for the other military services and at the joint level.

---

[9] Net-Enabled Command Capability GCCS FAMILY OF SYSTEMS TO NECC FUNCTIONALITY TRANSITION PLAN (FTP) Version 1.5, Net-Enabled Command Capability Joint Program Management Office (JPMO), 12 March 2009, page v.

The overall intent of NECC (figure 5) is to evolve from individual stove-piped Global Command and Control Systems oriented towards each military service to a common system based on standards based enterprise services and capability modules. The move from a producer center to a user centric approach will enable greater information sharing between the services and at the joint level. To enable this interoperability, the Defense Information Systems Agency (DISA) is evolving the GCCS Family of Systems (FoS) to Service Oriented Architecture (SOA) ontology based system using UCore as the foundation.

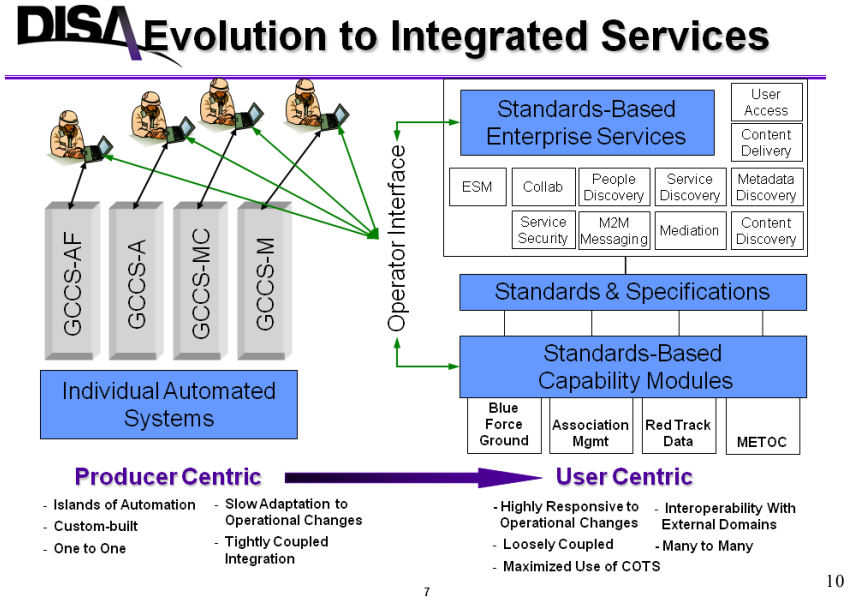


Figure 5. NECC Evolution to Integrated Services

[10] NECC/NCES Program Interaction, Defense Information Systems Agency, 14 APR 2008, slide 7.

2 APPLICABLE DOCUMENTS

2.1 Government Documents

DODD 8230.02, Data Sharing in a Net-Centric Department of Defense

DoD 8320.02-G, Guidance for Implementing Net-Centric Data Sharing

NECC/NCES Program Interaction, Defense Information Systems Agency, 14 APR 2008

CECOM Life Cycle Management Command Software Engineering Center, "Army Net-Centric Data Strategy Center of Excellence Semantic Technology Studies Ontology Languages Analysis Report"

National Geospatial-Intelligence Agency, "NGA-DCGS ISR Metadata Harmonization Ontology Guide", Version 1, 30 September 2009

NECC Increment #1 Architecture Review, Mark Kuzma, November 2007

Net-Enabled Command Capability (NECC) Architecture Overview AFCEA NECC/GCCS-J Course, Defense Information Systems Agency, 4 April 2008

Net-Enabled Command Capability NECC INCREMENT I DATA ARCHITECTURE, 12 May 2009

3 DCGS-N INTERFACES

3.1 DCGS-N Interface Overview

The message format between DCGS-N will be an XML based format and will be transported via the HTTPS protocol. Information on the DCGS-N is limited since it has undergone very limited fielding and is undergoing an upgrade acquisition process. For the purposes of PROGNOS, it is assumed that DCGS-N message interface will be similar to the National Geospatial Agency NGA-DCGS system which is also in the DCGS Family of Systems (FoS).

3.2 DCGS-N Interface Design

DCGS-N will likely use a Service Oriented Architecture (SOA) Semantic Web Activity based architecture as shown below.

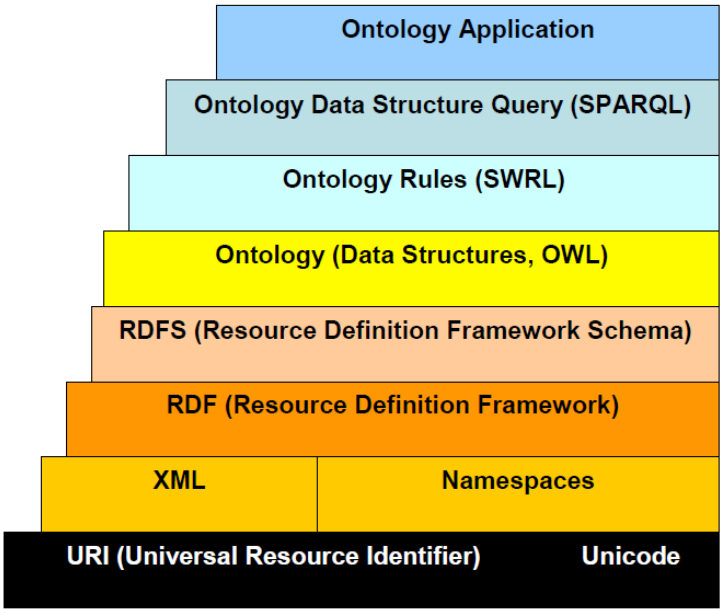


Figure 6. Semantic Web Activity Layered Approach[11]

The Semantic Web is based off of legacy HTML tagging approach to display web pages. However, instead of the legacy HTML tagging which is used largely for formatting, XML metadata tagging is used to meaningfully categorize the data. However, XML metadata tagging alone is insufficient to delineate the data sufficiently for computer systems. XML needs to be further structured through XML schema. But even XML schema is insufficient. The web based data must be further structured by the Resource Definition Framework (RDF) which serves a function similar to a class diagram in UML. RDF defines the entities and entity attributes. Much as XML schema limits XML, the RDF schema further limits RDF and formally defines classes. The Web Ontology Language (OWL) "adds more vocabulary for describing properties and classes: among others, relations between classes (e.g. disjointness), cardinality (e.g. "exactly one"), equality, richer typing of properties, characteristics of properties (e.g. symmetry), and

[11] CECOM Life Cycle Management Command Software Engineering Center, "Army Net-Centric Data Strategy Center of Excellence Semantic Technology Studies Ontology Languages Analysis Report", page 8.

enumerated classes."[12] SPARQL a RDF based ontology query language used to query web semantic based ontologies.

The Semantic Web Activity is a multiple layer approach. The bottom lay is the Universal Resource Identifier (URI). However, to support the URI layer multiple protocols are required. URI is typically HyperText Transfer Protocol (HTTP) or HyperText Transfer Protocol Secure (HTTPS) based. To support HTTP an HTTP, an IP infrastructure with Domain Name Servers (DNS) and HTTP and HTTPS web servers are required.

"eXtensible Markup Language (XML) is a set of rules for encoding documents electronically."[13] XML schema can be extended to markup almost any type of data. It is frequently used for metadata, or data to describe data, purposes. Metadata is a key initiative by the Department of Defense. Operation cells, intelligence analysts and commanders are overwhelmed by the sheer amount of data available in the battlespace and need a means to categorize the data. There is a large repository of standardized XML based metadata stored at the DoD MetaData Registry (MDR) to include BFT and ISR Community of Interest (COI) XSD schemas.

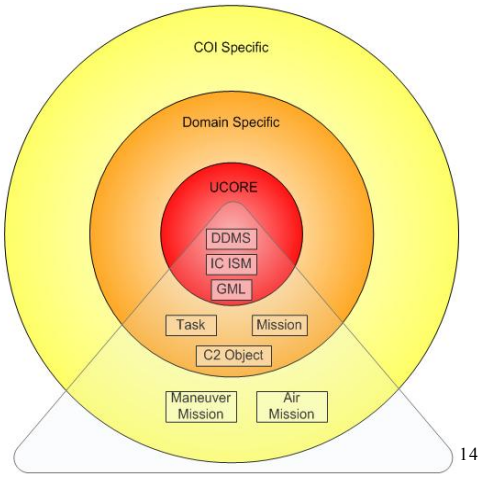


Figure 7. DoD Semantic Web Layered Approach

DoD is using a layered approach to their Service Oriented Architecture Semantic Web implementation. The core of the approach is UCore. Universal Core (UCore) is a federal information sharing initiative that supports the National Information Sharing Strategy and all associated Departmental / Agency strategies. UCore enables information sharing by defining an implementable specification (XML Schema) containing agreed upon representations for the most commonly shared and universally understood concepts of who, what, when, and where.

Ucore is based on three primary standards – the DoD Discovery Metadata Specification, the Intelligence Community Information Security Marking (IC-ISM), and the Geographical Markup Language (GML). DDMS provides enterprise level data discover. The IC ISM provides security related metadata for trusted net-centric accessibility. Geography Markup Language (GML) is the XML grammar defined by the Open Geospatial Consortium (OGC) to express geographical features. GML serves as a modeling language for geographic systems as well as an open interchange format for geographic transactions on the Internet.

---

[12] http://en.wikipedia.org/wiki/Web_Ontology_Language, accessed 7 APR 2010

[13] http://en.wikipedia.org/wiki/XML, accessed 5 APR 2010

[14] NECC/NCES Program Interaction, Defense Information Systems Agency, 14 APR 2008.

The Task, Mission, and C2 Object are domain and military specific and is defined my military doctrine such as the Universal Joint Task List (UJTL) and MIL-STD-2525 which defines military symbology.

The outer most layer is Community of Interest (COI) specific. The repository for the COI XML schema is the DoD Metadata Registry. There are multiple COI schemas – blue force tracking, ISR, air mission, and more.

DoD publication 8320.2-G provides extensive guidance on the purpose, formation, management, and responsibilities of COIs. "COIs are organizing constructs created to assist in implementing net-centric information sharing. Their members are responsible for making information visible, accessible, understandable, and promoting trust – all of which contribute to the data interoperability necessary for effective information sharing[3]… The focus for COIs is to gain semantic and structural agreement on shared information."[4]

3.2.1 DCGS-N Interface Diagram

Figure 8 shows a DoDAF SV-2 diagram that represents that DCGS-N to PROGNOS connectivity on a naval vessel.

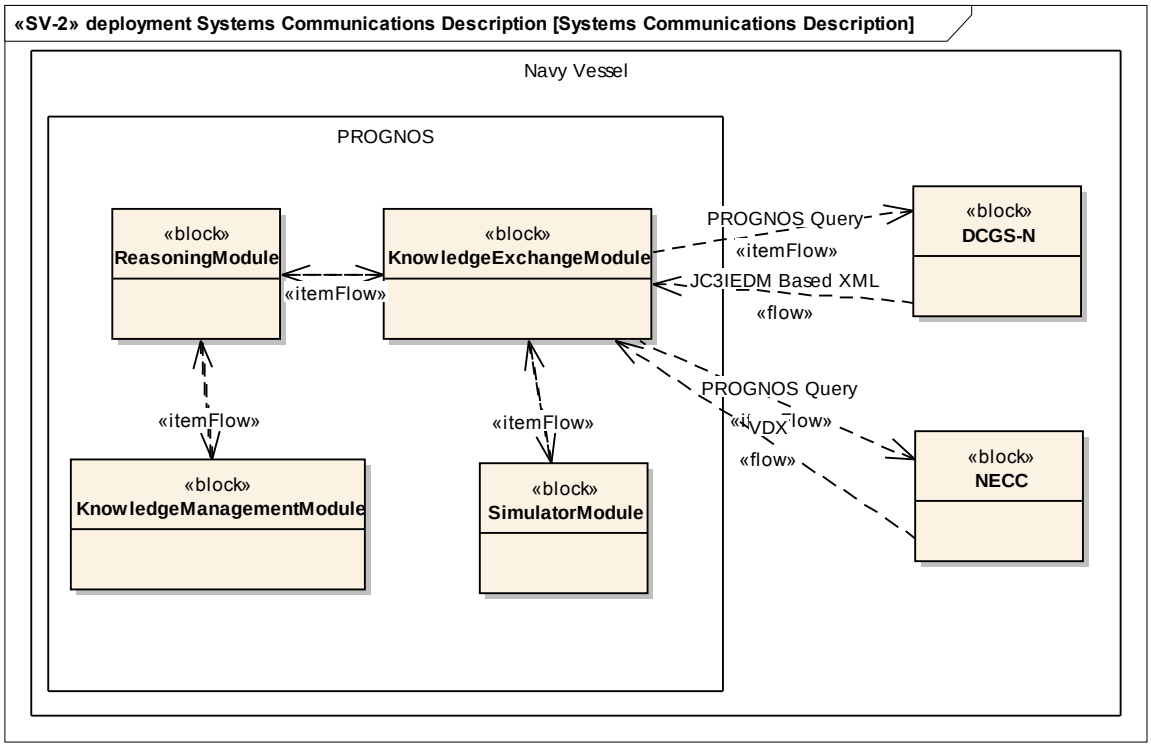


Figure 8. DCGS-N System View 2

3.2.2 DCGS-N Interface Physical Interconnection

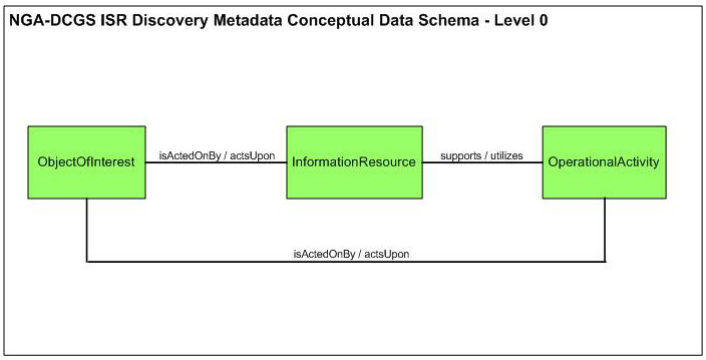
DCGS-N and PROGNOS will be co-located on the same platform as shown in Figure 8. The physical connectivity between the PROGNOS Knowledge Exchange module and DCGS-N will be Ethernet and IP based via the Consolidated Afloat Networks and Enterprises Services (CANES) on-board ship infrastructure. The Knowledge Exchange module will connect to DCGS-N via a 1000BaseT, IEEE 802.3ab electrically compatible interface. It is anticipated that DCGS-N and PROGNOS will be co-located on the same platform; however, the two systems will not be directly connected. The connection will be via the ISNS/CANES shipboard infrastruction.

3.3 DCGS-N Interface Messages

DCGS-N uses a Service Oriented Approach (SOA) approach with SOAP, HTTPS and PKI to transport the OWL-based ontology messaging .

3.3.1 DCGS-N Taxonomy

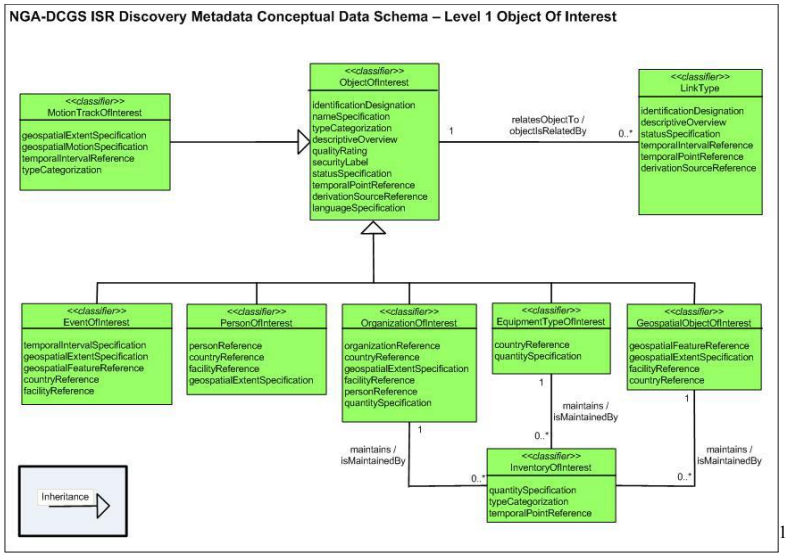
All NGA-DCGS data can be represented using either the ObjectofInterest, InformationResouce, or OperationalActivity three data classes shown in the following figure. ObjectofInterest represents an event, person, organization, equipment, or area of interest that may need to be monitored by Intelligence, Surveillance, or Reconnaissance (ISR) assets. InformationResource is also considered a DataAsset and is composed of controlled vocabulary, images, intelligence production assets, information access services, and metacards. An Operational Asset consists of staff members, organizational elements, and equipment assets.



[15]

Figure 9. NGA-DCGS Level 0 Metadata Schema

The following diagram represents a decomposition of the ObjectofInterest.



[16]

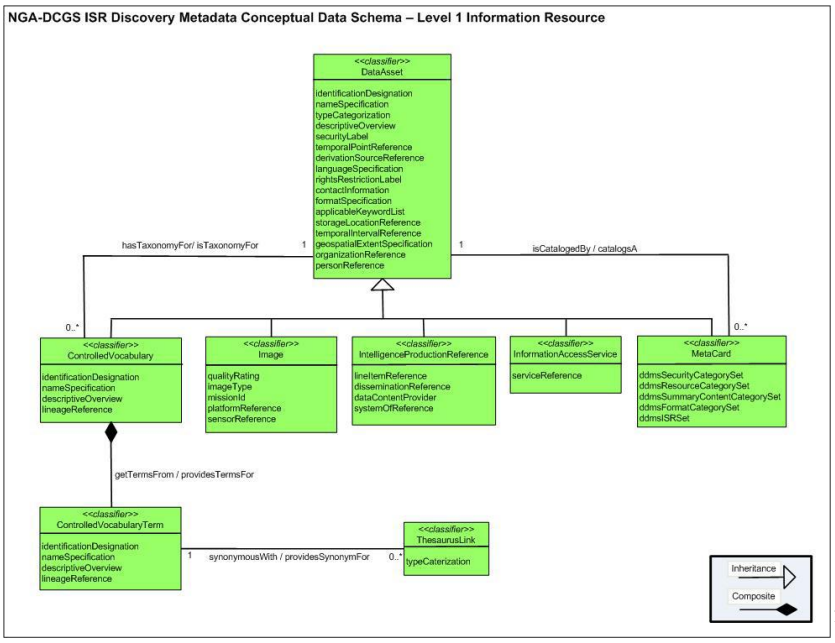
---

[15] National Geospatial-Intelligence Agency, "NGA-DCGS ISR Metadata Harmonization Ontology Guide", Version 1, 30 September 2009

[16] National Geospatial-Intelligence Agency, "NGA-DCGS ISR Metadata Harmonization Ontology Guide", Version 1, 30 September 2009

Figure 10. NGA-DCGS Level 1 Object of Interest

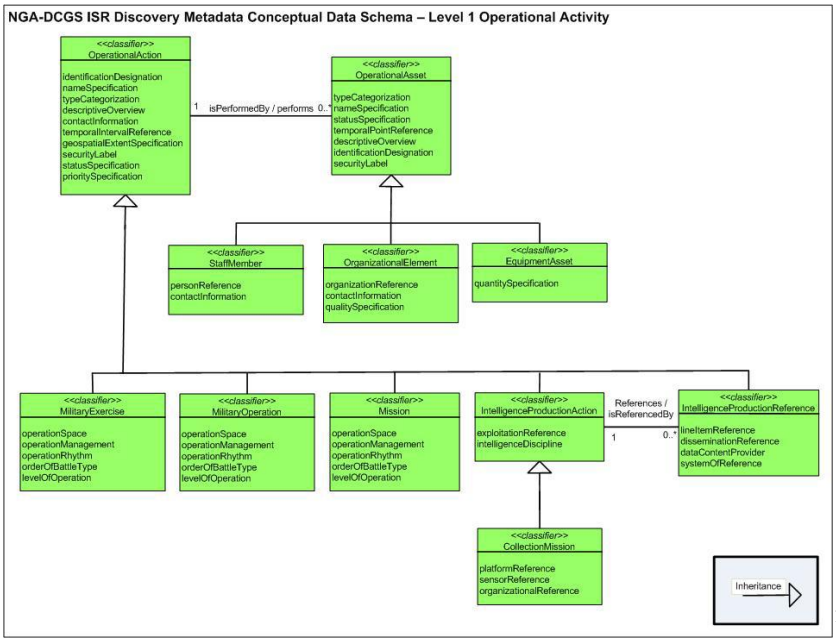
The following represents a decomposition of DataAsset.



[17]

Figure 11. NGA-DCGS Level 1 Information Resource

The following is a decomposition of OperationalAsset.



[18]

[17] National Geospatial-Intelligence Agency, "NGA-DCGS ISR Metadata Harmonization Ontology Guide", Version 1, 30 September 2009

Figure 12. NGA-DCGS Level 1 Operational Activity

3.4 DCGS-N Interface Message Protocols

DCGS-N will need to support a range of web based protocols to transport the XML/OWL information. The XML information will use the SOAP protocol as a transport the structured XML/RDF/OWL information. HTTPS, in turn, will serve as a transport for the SOAP protocol. HTTPS is supported by the Transport Layer Security (TLS) which will provide Advanced Encryption Standard 128 bit level or better encryption. To support authenticated communication, the DoD's X.509v3 Public Key Infrastructure (PKI) certificates will be incorporated. Both the PROGNOS Knowledge Exchange Module and DCGS-N will authenticate all communication based on DoD X.509v3 PKI certificates.

---

[18] National Geospatial-Intelligence Agency, "NGA-DCGS ISR Metadata Harmonization Ontology Guide", Version 1, 30 September 2009

4 NET-ENABLED COMMAND CAPABILITY (NECC) INTERFACES

NECC is a distributed web Service Oriented Architecture (SOA) system and the servers will be distributed strategically throughout the globe at Global Information Grid (GIG) Computing Nodes as shown in Figure 13.

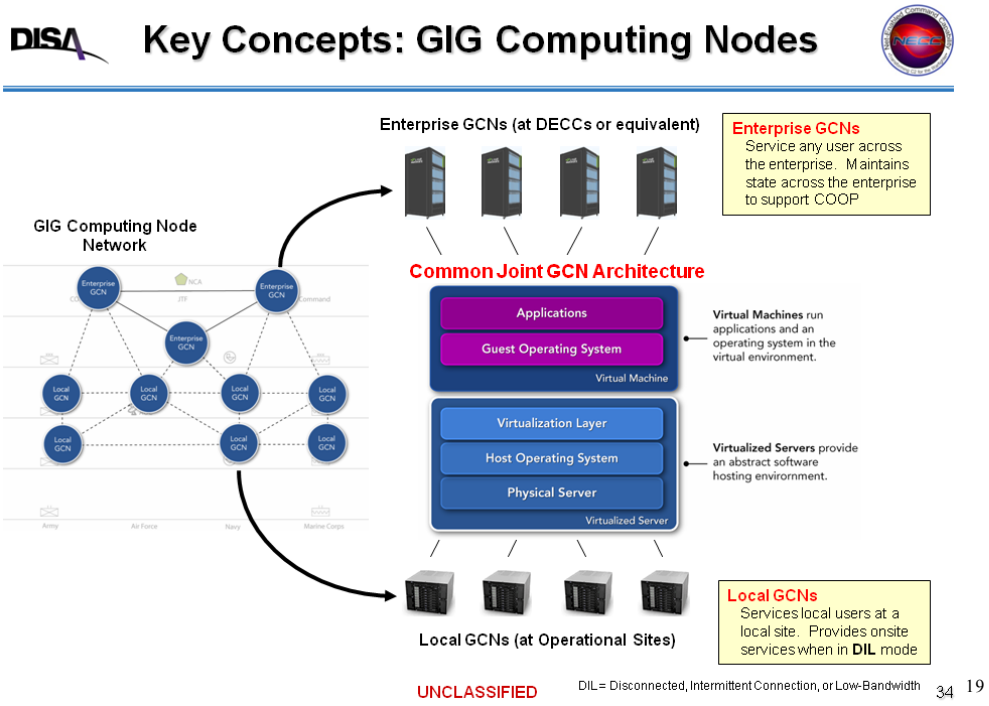
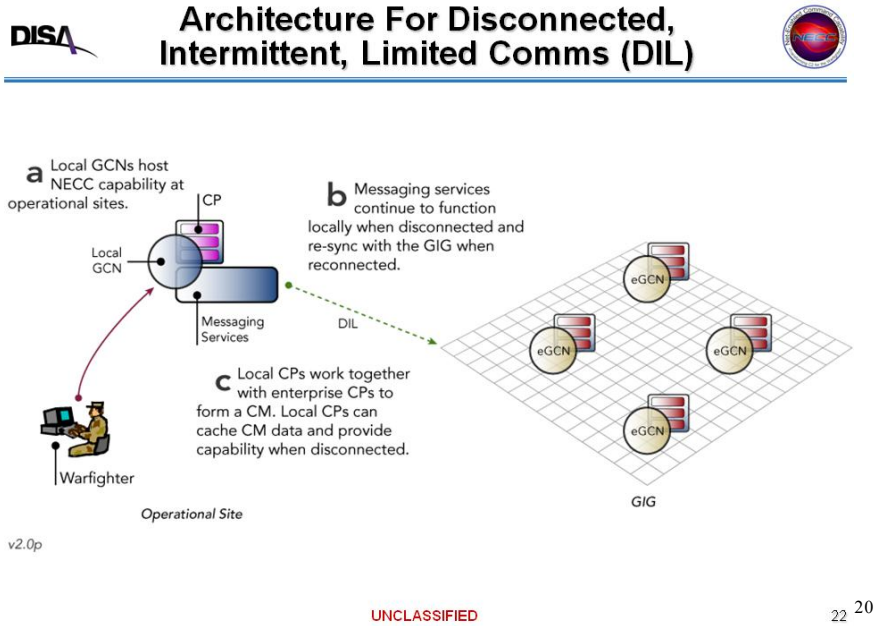


Figure 13. NECC GIG Computing Nodes

To compensate for Disconnected, Intermittent Connection, or Low-Bandwidth (DIL) communications, GCNs will need to be co-located on naval platforms. Figure 14 shows how communications will work on warfighting platforms. Several Capability Packages will form a Capability Module.

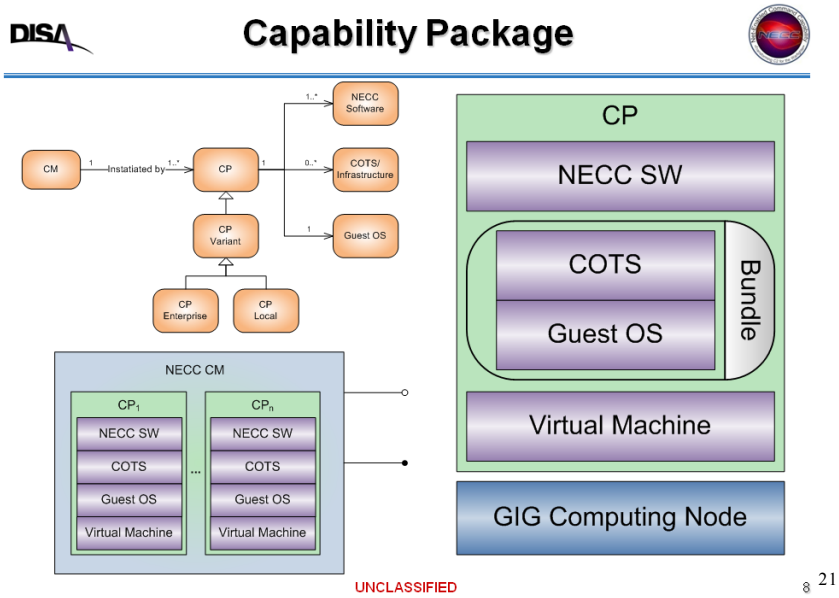
[19] NECC Increment #1 Architecture Review, Mark Kuzma, November 2007, slide 24.



[20]

Figure 14. Architecture for Disconnected, Intermittent, Limited Communications

A Capability Package is a hardware/software set supporting a virtual machine, an operating system, and the NECC web based software as shown in Figure 15.



[21]

Figure 15. Capability Package

---

[20] NECC Increment #1 Architecture Review, Mark Kuzma, November 2007, slide 22.

[21] Net-Enabled Command Capability (NECC) Architecture Overview AFCEA NECC/GCCS-J Course, Defense Information Systems Agency, 4 April 2008, slide 8.

A Capability Module (CM) is "is a set of software components that implements a set of logically grouped services".[22] As shown by Figure 11, a Capability Module can be implemented by one or more Capability Packages. Figure 16, shows how the Capability Modules is implemented by multiple Capability Packages, some with Disconnected, Intermittent, or Limited (DIL) communications. It also shows how legacy applications such as FBCB2 will be implemented in a Back Office implementation at an enterprise site.

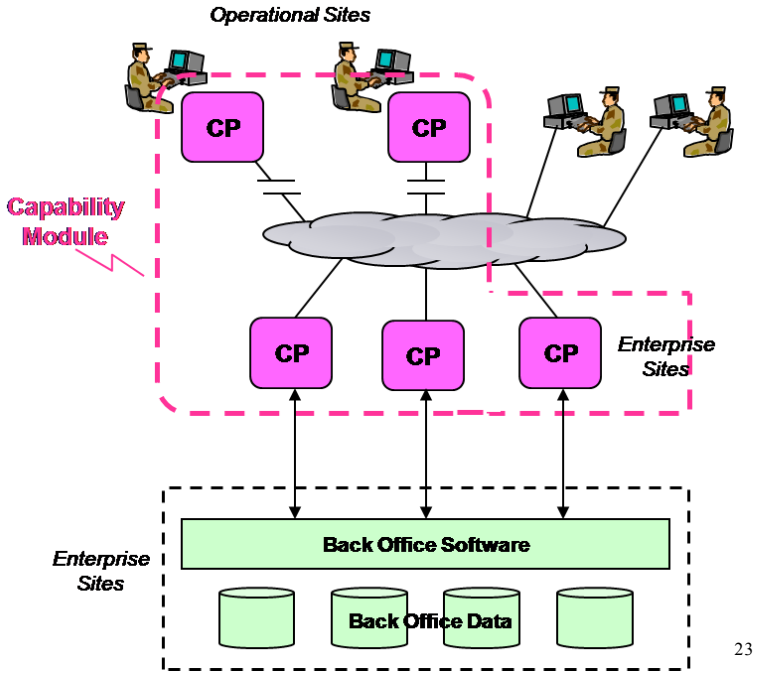


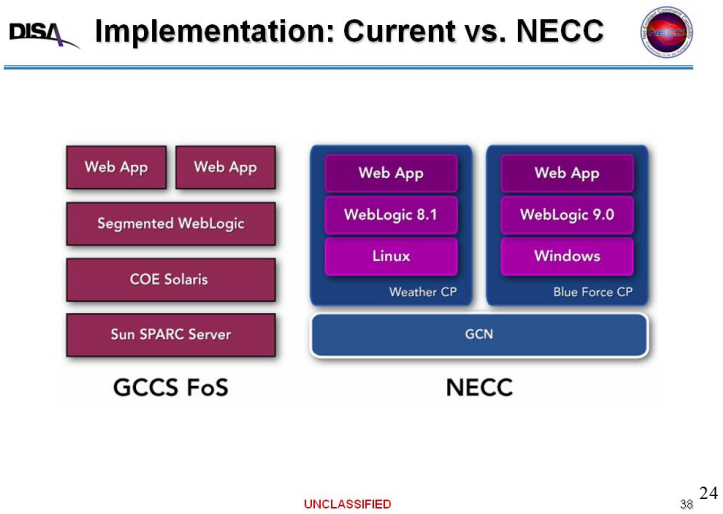
Figure 16. Capability Module

4.1 NECC Interface Overview

The message format between NECC and will be an XML based format and will be transported via the HTTPS protocol. As can be seen by figure 17, BEA (now Oracle) WebLogic provides the HTTPS web interface.

[22] Matthews, Smiley. "Net-Enabled Command Capability (NECC) Architecture Overview", 4 APR 2008, slide 6.

[23] Net-Enabled Command Capability (NECC) Architecture Overview AFCEA NECC/GCCS-J Course, Defense Information Systems Agency, 4 April 2008, slide 9.



[24]

Figure 17. NECC Software Architecture

4.2 NECC Interface Design

4.2.1 NECC Interface Diagram

Figure 18 is a DoDAF SV-2 diagram that represents the NECC to PROGNOS connectivity on a naval vessel.

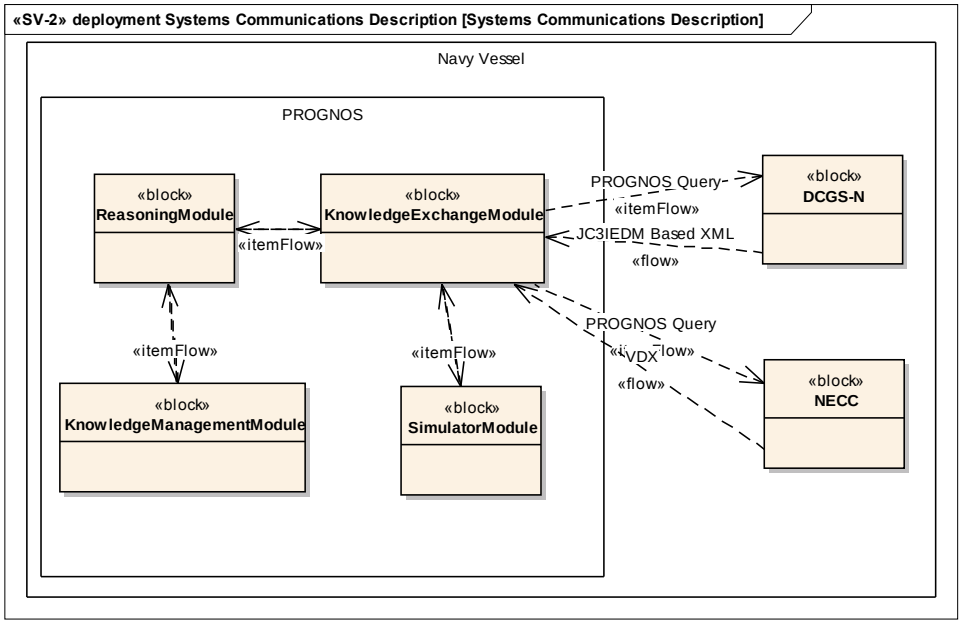


Figure 18. NECC System View 2

4.2.2 NECC Interface Physical Interconnection

The physical connectivity between the PROGNOS Knowledge Exchange module and NECC will be Ethernet and IP based via the CANES on-board ship infrastructure. The Knowledge Exchange

[24] NECC Increment #1 Architecture Review, Mark Kuzma, November 2007, slide 38.

module will connect to DCGS-N via a 1000BaseT, IEEE 802.3ab electrically compatible interface.

4.3 NECC Interface Messages

The NECC interface message type is defined by the DoD Metadata Registry (MDR). NECC will use the following messages

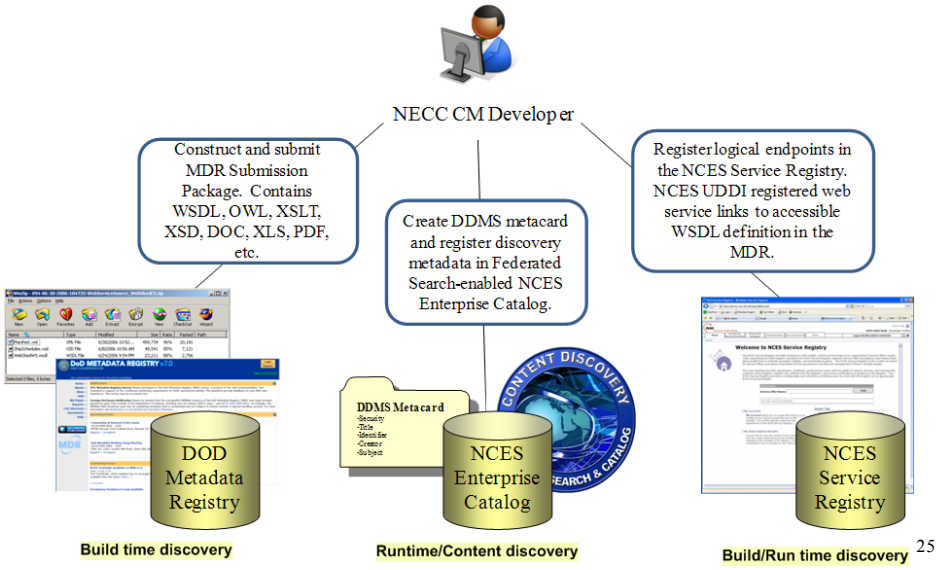
NECC will need to support the following key web based protocols.

STANDARD	PURPOSE
XML Schema	Encoding XML content.
XML Path Language	Accessing an XML document.
XQuery Language	Query an XML data source.
Geography Markup Language	XML encoding geography and temporal entities.
DoD Discovery Metadata Specification	XML encoding of discovery metadata.
IC ISM	XML encoding of security metadata.
SSATF	Space Shared Situational Awareness Framework
UCore	Universal Core

Table 1. NECC Key Standards

4.4 NECC Interface Message Protocols

NECC is dependent on two DoD web based repositories – the DoD MetaData Registry (MDR) and the Net-Centric Enterprise Services (NCES). The MDR defines the schema of the knowledge and the DDMS metacard. The NCES serves as a repository for the DDMS metacards and a registry of the logical endpoints as shown in figure 15.

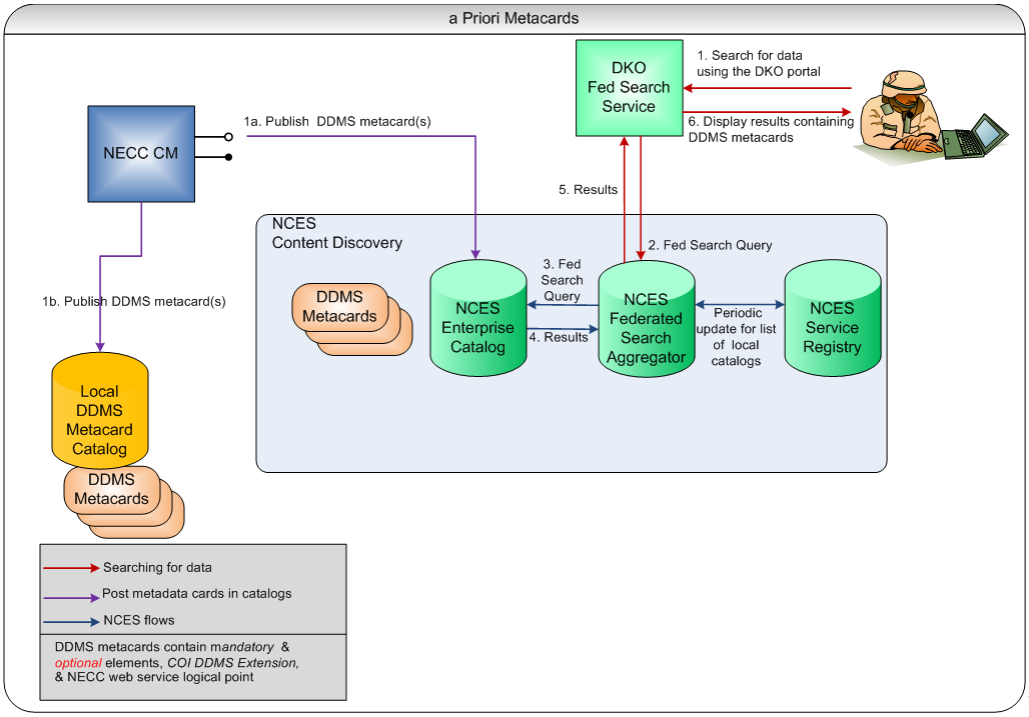


[25]

Figure 19. Metadata Registry and NCES Relationship

[25] Net-Enabled Command Capability NECC INCREMENT I DATA ARCHITECTURE, 12 May 2009, page 22.

In figure 16, DDMS metacards are published to both the NCES Enterprise and a Local DDMS Metacard Catalog. A user needs to query the information remotely. In this case, the user queries the Defense Knowledge Online (DKO) federated search service. The DKO federated search service, then queries the NCES Federated Search Aggregator which in turn queries the NCES Enterprise Catalog which has the complete DoD catalog of DDMS metacards. The NCES enterprise catalog returns the results back to the warfighter via the NCES Federated Search Aggregator and DKO Federal Search Service. The result indicates the endpoint that will have the needed information. However, to determine the endpoint, a Universal Description Discovery and Integration (UDDI) query is needed against the NCES Service Registry. UDDI returns the endpoint the warfighter receives the needed information.



[26]

Figure 20. A Priori Metacards

NECC will need to support a range of web based protocols to transport the XML/OWL information. The XML information will use the SOAP protocol as a transport the structured XML/RDF/OWL information. HTTPS, in turn, will serve as a transport for the SOAP protocol. HTTPS is supported by the Transport Layer Security (TLS) which will provide Advanced Encryption Standard 128 bit level or better encryption. To support authenticated communication, the DoD's X.509v3 Public Key Infrastructure (PKI) certificates will be incorporated. Both the PROGNOS Knowledge Exchange Module and NECC will authenticate all communication based on DoD X.509v3 PKI certificates.

[26] Net-Enabled Command Capability NECC INCREMENT I DATA ARCHITECTURE, 12 May 2009, page 22.

5 NOTES

5.1 Acronyms and Abbreviations

Acronym	Definition
AFATDS	Advanced Field Artillery Tactical Data System
BFT	Blue Force Tracking
C2	Command and Control
C2PC	Command and Control Personal Computer
C4I	Command, Control, Communications, Computers, and Intelligence
COI	Community Of Interest
DCGS-N	Distributed Common Ground Station -- Navy
DDMS	DoD Discovery Metadata Specification
DISA	Defense Information Systems Agency
FBCB2	Force XXI Brigade and Below Command and Control
FoS	Family of Systems
GCCS-M	Global Command and Control System -- Maritime
GML	Geography Markup Language
ICD	Interface Control Document
IC-ISM	Intelligence Community Information Security Marking
ISR	Intelligence, Surveillance, Reconnaissance
JC3IEDM	Joint Consultation, Command and Control Information Exchange Data Model
LAN	Local Area Network
KEM	Knowledge Exchange Module
HTML	Hyper Text Markup Language
JVMF	Joint Variable Message Format
LOS	Line of Sight

NATO	North Atlantic Treaty Organization
NECC	Net-Enabled Command Capability
NGA-DCGS	National Geospatial Agency – Distributed Common Ground Station
OPLAN	Operational Plan
OPORD	Operational Order
OWL	Web Ontology Language
PLI	Position Location Information
RDF	Resource Definition Framework
SOA	Service Oriented Architecture
UCore	Universal Core
UAV	Unmanned Aerial Vehicle
USMTF	United States Message Text Format
XML	eXtensible Markup Language