2006 CCRTS

The State of the Art and the State of the Practice

FORCEnet Net Centric Architecture – A Standards View

Fred M. (Mike) Stewart

Space and Naval Warfare Systems Command

4301 Pacific Highway, San Diego, CA 92110-3127

(619) 524-7230

fred.stewart@navy.mil

Abstract

As the operational construct and architectural framework for naval warfare, FORCEnet is the Navy and Marine Corps initiative to achieve Netcentric Warfare (NCW) and Joint Transformation by providing robust information sharing and collaboration across the naval force. FORCEnet is defined as the operational construct and architectural framework for naval warfare in the information age that integrates warriors, sensors, networks, command and control, platforms, and weapons into a networked, distributed combat force that is scalable across all levels of conflict from seabed to space and sea and land. The FORCEnet enterprise architecture provides the naval Netcentric framework. Part of the architecture is a list of standards to provide the entire Naval community with a source of standards to ensure Naval, joint, and allied coalition interoperability in support of the netcentric objective. The information technology standards to implement a Netcentric capability are a key element to build the FORCEnet capability. The main focus of this paper will be the technical standards.

Background

During the fall of 2005, riots erupted in France caused by ethnic, social, and economic tensions in a segment of the populace that felt disenfranchised and ignored by the government - and to a larger extent - by French society. A few people in this disenfranchised segment of the population expressed their frustration by destroying property and attacking people in the towns and the suburbs. For several days there was wave after wave of attacks springing up in 274 towns.[1] Just as the authorities would deal with one area, another incident would flare up. The French authorities were surprised and had a difficult time dealing with the widespread riots. The government deployed 1,500 gendarmes and 8,000 troops to deal with the crisis. There appeared to be almost a pattern or plan to the riots. And in a way there was. There was no single mastermind but there was coordination. This coordination was accomplished by groups of individuals around the area using blogs and text messages to convey information such as where the next criminal disturbance was to take place.[2] In this way information was disseminated to a large number of individuals using the existing network infrastructure available from Internet service providers and cellular companies.

Introduction

There are two terms that are sometimes used synomously; Network Warfare and NCW. Initially there was some confusion that this type of warfare only concerned a group of computer servers sitting someplace. The term NCW attempts to remove that perception. Part of the definition of Network Centric Warfare defined in Alberts, Garska, Stein's book; Network Centric Warfare, is characterized by ability of geographically dispersed forces to create a high level of shared battle space awareness that can be exploited by self synchronization and other network centric operations to achieve commanders intent.[3] Of course these concepts are not unique to US Navy and Marine Corp, US Army, US Air Force, congress, industry through forums such as National Defense Industrial Association (NDIA), Armed Forces Communications and Electronics Association (AFCEA), etc. have pointed out the importance of the U.S. defense agencies adopting this type of 'thinking' - to adopt a netcentric approach to dealing with and using data and information.

For the riots mentioned previously, even though there was no single mastermind, a group of people in France with a common goal were conducting a form of NCW. They were separated in different towns yet information was shared among various people and were able to roughly synchronize and coordinate where a riot was to take place. While there was no plan in this instance, what it does demonstrate is how powerful this type of networking interaction can be.

NCW and FORCEnet

FORCEnet is the Navy's instantiation of the Department of Defense Global Information Grid (GIG). As the operational construct and architectural framework for naval warfare in the Information Age, FORCEnet is the Navy and Marine Corps initiative to achieve Net-Centric Warfare (NCW) and Joint Transformation by providing robust information sharing and collaboration capabilities across the Naval force. It is the centerpiece of Sea Power 21, Naval Power 21 and the Naval Operating Concept for Joint Operations and the Department of the Navy's (DON) Naval Transformation Roadmap. As a result, FORCEnet provides the foundation for Sea Basing, Sea Shield, Sea Strike, Sea Warrior and Expeditionary Maneuver. In addition to the instantiation of the GIG, FORCEnet is the Naval initiative for migrating toward Joint Vision 2010 and Joint Vision 2020.

Principles

Some of the fundamental principles for FORCEnet are interconnectivity, interoperability, information sharing, and information assurance across all major domains (sea, undersea, air, space, ashore) and is the foundation for interoperability with the other service branches. Net-Centric Operations/NCW – allow the use of computers and communications to link people through information flow that depend on the interoperability of systems to enable an agile warfighting-centric organization characterized by distributed command and control (C2) and network enabled operations. Using a Service Oriented Architecture (SOA) approach which is fundamentally about sharing and reuse of functionality across diverse applications. Service-oriented design focuses on composeability, the ability of computing platform independent publish/subscribe services that connect service providers with service users and are seamless, ubiquitous, and discoverable. Or in other words, create a netcentric environment that has the following characteristics:

- Distributed/Web Services - A Web Service is application or business logic that is accessible using standard Internet protocols. Web Services combine the best aspects of component-based development and the World Wide Web. Like components, Web Services represent "black-box" functionality that can be used and reused without regard to how the service is implemented.

- Extensible Markup Language - The Extensible Markup Language (XML) is at the core of the World Wide Web Consortium vision for the Web. Many of the services that will be available through FORCEnet will use XML to define, describe, store, exchange, and use information. The DON XML Naming and Design Rules will be used to ensure consistency and an enterprise approach in developing all FORCEnet XML.

- Data-Oriented Services – Metadata, data tagging, registration, and management are key to FORCEnet and related architectures. FORCEnet will require that programs follow the guidelines of SECNAVINST 5000.36 for data engineering, the DON's implementation of the DOD Net-centric data strategy for data engineering. FORCEnet will also require adherence to key International Organization for Standardization (ISO) data standards 11179 and 15000-5.
- Real-time systems support – For combat and weapons systems that require a stringent quality of service for information flow.
- Human Systems Integration (HSI) – FORCEnet requires warrior-centric capabilities and the use of DOD approved Human Engineering standards and practices.
- Information Assurance - Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

FORCEnet Architecture

The Chief of Naval Operation's Strategic Studies Group XXI[4] has defined FORCEnet as "the operational construct and architectural framework for Naval Warfare in the Information Age, integrating warriors, sensors, networks, Command and Control (C2), platforms, and weapons into a networked, distributed combat force, scalable across the spectrum of conflict from seabed to space and sea to land." This definition is consistent with the vision described in the FORCEnet Functional Concept document. To achieve this net-centric, distributed combat force requires an enterprise-wide architecture with the flexibility to dynamically adapt to rapidly changing requirements. The FORCEnet architecture is modeled using a framework that defines services that can be combined in adaptable ways to deliver functional capabilities. The DOD Architecture Framework (DODAF) is used as well as SOA approach in defining and documenting the FORCEnet services definition of the operational, system and technical views. The architecture products that are produced and approved by the Navy are registered and reside in the DOD Architecture Repository (DARS).

The DODAF architecture guidance lists three products;

Operational View (OV) – This is a description of the tasks activities, operational elements, and information. It contains graphical and textual depictions identify the operational nodes and elements, assigned operational tasks, and information flow between nodes or elements. It defines the type of information exchanged, the frequency of exchange, which tasks and activities are supported by the information exchanges and the nature of the exchanges.

System View (SV) – This is a graphical and textual depiction that describes systems and interconnections. It associates systems to the OV. These systems support the operational activities and facilitate the exchange of information among operational nodes.

Technical View (TV) – This is the set of rules that govern the arrangement, interaction, and interdependence of system parts and elements. Its purpose is to ensure that a system satisfies a specified set of operational requirements. It provides the technical systems implementation guidelines upon which engineering speciation are written, systems developed, and products lines produced. It includes a collection of the technical standards, options, rules, and criteria organized into profiles that relates to specific systems and system elements,

Standards

The FORCEnet TVs or list of standards will be the main topic of this paper. The TV-1 contains the current standards and the TV-2 contains the emerging Information Technology (IT) and netcentric standards which include commercial standards, military standards, and international standards to ensure service, joint, government, and allied/coalition interoperability.

The TVs were compiled by an ad hoc working group as part of the FORCEnet architecture effort and drew expertise from the Navy and Marine Corp, the Departmen of Defense (DOD), other services and industry. Key items defined early on by the ad hoc working group were the need for a standards repository and a method to compile lists of standards. The Joint Technical Architecture (JTA) was the first attempt to create a list of joint interoperability standards but the Defense Information Systems Agency (DISA) was developed a replacement for the JTA called the Defense Information Standards Registry (DISR) which is both a repository and a tool to create a list of standards. In addition, DISR also had the capability to create a database of services specific standards called an Organization Unique Standards (OUS) database for each service. This allows the Navy to use the core list of DISR standards plus the Navy unique standards to provide complete profiles that are compliant with the FORCEnet architecture. This creates one tool that has not only has a capability to build lists or profiles of standards but also includes the Navy standards needed to complete the FORCEnet TV's. It should be noted that the FORCEnet TV's integration with DISR provides one Navy repository that will achieve both JCIDS and FORCEnet compliance using a single repository under configuration management control.

The FORCEnet TVs are the collections of technical standards that provide the technical system guidelines to build a system as well as support voice, video and data communications and a SOA. They provide the system developer and integrator with the IT and netcentric standards to implement the Naval part of NCW called FORCEnet. The Navy needs to provide this information to industry, so that all companies have the capacity to use consistent standards. With universal standards, individual vendors don't have to guess what the Fn standards may be.

The TVs are approximately 80% commercial standards from Institute of Electrical and Electronic Engineers (IEEE), Internet Engineering Task Force (IETF), International Standardization Organization (ISO), American National Standards Institute (ANSI) and other industry bodies. An important aspect is to establish the relationship between the FORCEnet efforts, in this case standards, to industry practices. In this regard, a notional FORCEnet

reference model was developed that describes the basic model of FORCEnet. This notional reference model can be cross-referenced to the ISO Open System Interconnection (OSI) industry model to show where the blocks are common and therefore where the standards are common.

Notional FORCEnet Reference Model

Figure 1 shows how the FORCEnet Reference Model illustrates the components of the FORCEnet Architecture and the relationship to industry and DOD models. The FORCEnet Reference Model uses a layered architectural style to describe functionality, with each layer rolling up the details of the layer below. This hierarchy supports the concept of small services that are composed by sequencing and grouping into functional capabilities. Real-time and time-shared warrior net-centric applications are supported by a foundation of Communications and Networks and Enterprise Services. Quality of Service (QoS), Information Assurance (IA), and HSI are the supporting disciplines present at every layer.

The key objectives of the FORCEnet Reference Model are to:

- Identify the major components of the FORCEnet architecture;
- Provide a framework that contributes the ability to reuse technology by specifying components that can be easily coupled to provide new war-fighting capabilities;
- Guide development and acquisition toward a service oriented model;
- Ensure interoperability among FORCEnet systems;
- Provide the basis for assessing architectural compliance for technical solutions;
- Identify as-is and to-be attributes for FORCEnet architectural elements.

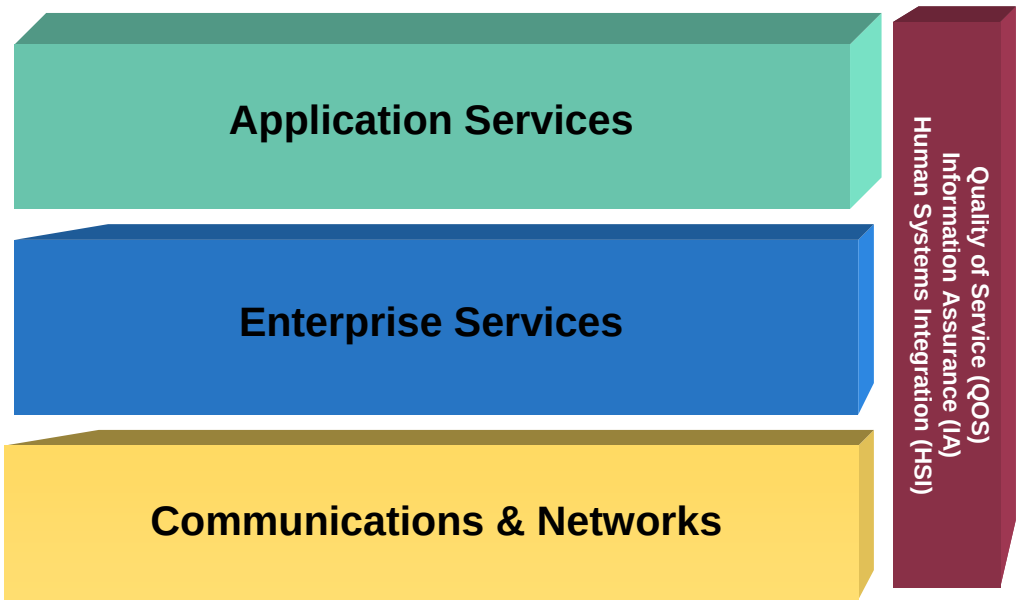

Figure 1 The Notional FORCEnet* Reference *Model, Level 0

Communications and Networks

The Communications and Networks component of the model provides for dynamic, interoperable connectivity through provisioning of a secure backplane of communications systems. Elements of the communications component include satellite communications, tactical data links, common data links, land entry points, terrestrial backbones or long haul services, wireless communications, and circuit management systems. Voice, video and data networks and information systems form a global Naval information grid that will be fully integrated with the other services and into the GIG. This Naval grid is envisioned as a ubiquitous Internet Protocol (IP)-based network that provides a host of services with high availability, reliability, and survivability across the Naval enterprise in airborne, afloat, undersea and ashore domains. Communications services are provided to support distributed applications requiring data access and applications interoperability in networked environments to support user applications. These services are the functions and interfaces that reside on the underlying communications system protocol software.

This component includes all the services that enable communication among distributed devices. It provides the IP network services needed to communicate among DON organizational units, other federal organizations, and mobile users. Elements of the networks component include wide area and metropolitan area networks, Command Control Communications Computers Intelligence Surveillance reconnaissance (C4ISR) networks, combat weapons networks, Hull, Mechanical and Electrical (HM&E) networks, and support and business IT networks. Also included here are Network Management Services. Network Management Services provide the capability to manage networks, systems, and information services. This includes controlling the network's topology, dynamically segmenting the network into multiple logical domains, maintaining network routing tables, monitoring the network load, and making routing adjustments to optimize throughput. Additionally, Network Management Services enable the capability to review and publish addresses of network and system objects, monitor the status of objects, start, restart, reconfigure, or terminate network or system services, and detect loss of network or system objects to support automated fault recovery.

Enterprise Services

Services are key functions to the FORCEnet SOA infrastructure that enables systems to function more effectively and efficiently than the same services maintained individually. Services such as email, user interface services and web-based services are examples of services that no longer need to be supplied in specific node systems. Effective use of services streamlines systems and lowers development and deployment costs along with facilitating interoperability.

The Enterprise Services (ES) component is the infrastructure on which the applications rely. Currently, systems utilize the Defense Information Infrastructure (DII) Common Operating Environment (COE) services. The COE approach with tightly coupled software components focused on integration will migrate to a loosely coupled, services orientation of the enterprise

services environment. These ES include a wide range of services such as web-based services, data management services, data interchange services, and eBusiness.

Enterprise Services are modeled after the GIG-ES Core Enterprise Services (CES). These services have been specified in the GIG ES Capstone Requirements Document (CRD) that defines Net-Centric Enterprise Services (NCES) as that set of services required providing a general set of functionality to the widest range of organizational tasks in an optimal manner. The nine CES elements are Enterprise Service Management, Messaging, Application, Discovery, Mediation, Collaboration, Storage, Security and User Assistance. These core enterprise services make information and applications accessible across the information environment and provide users the means to take full advantage of the capabilities of the environment. FORCEnet distributed services will subscribe to GIG Enterprise Services (GIG-ES) and implement Navy unique services only where operationally required.

FORCEnet and the GIG ES are being developed in parallel. As a result, FORCEnet may be required to deploy capability before GIG-ES can provide a common service. In this case, FORCEnet will deploy an interim solution in coordination with DISA with a plan to transition to the GIG ES when it becomes available.

Applications

The Applications component of the FORCEnet Reference Model includes such applications as combat and weapons systems, command and control systems and business systems that can be classified as either real-time or time-shared. Applications are supported by and share data through the foundational components. As shown in the model, both real-time and time-shared application systems ride on the framework of enterprise services.

Overarching Disciplines

As shown in Figure 1, there are 3 overarching disciplines that apply to all three layers of the reference model:

Quality of Service : Services provided to applications are governed by QoS requirements. Providing better service to designated applications or selected network traffic may include dedicating bandwidth, controlling latency, setting IP precedence, and managing congestion. QoS is defined by programs under service level agreements (SLA's).

Information Assurance : The reference model reflects DOD's Defense-in-Depth strategy. Information Assurance is embedded in every FORCEnet component of the reference model. The implementation of FORCEnet standards assures the security of information and data while being processed or during transmission through DON information systems and network infrastructures.

Human Systems Integration : HSI standards must be considered in all layers of the FORCEnet Reference Model as a key component. Warrior-centric system-of-systems result from using HSI standards and procedures – that is how Warfighters, teams, and organizations use FORCEnet capabilities to accomplish the mission in an operational environment. HSI, as an

element of systems engineering, should be implemented IAW ISO/IEC 15228 systems Life Cycle Processes.

Automation and optimization of selected human functions on ships has been identified as a critical factor in achieving necessary cost reductions as well as improving the speed of command. This desired automation and optimization of functions both automated and manual must be carefully planned and evaluated throughout the system development process. Nominally, a warfighter performs a variety of tasks under varying operational conditions. The automation of warfighter tasks is not simply replacing man with machine. Instead, it is a complex process of trading-off between man and machine, man and man (e.g., enhanced training to provide improved operator performance), and many other issues (e.g., distributed organizations, considerations of reliability and availability for a machine versus an operator, relationship in system-of-systems).

The OSI and the Notional FORCEnet Reference Model

The ISO OSI 7-layer model[5] provides an abstract conceptualization for communications and computer-network protocol design—the OSI model protocols are applicable to the Navy's shipboard and communications networks such as FORCEnet. Figure 2 illustrates the inherent relationship between the 7-Layer OSI model and the notional FORCEnet reference model.

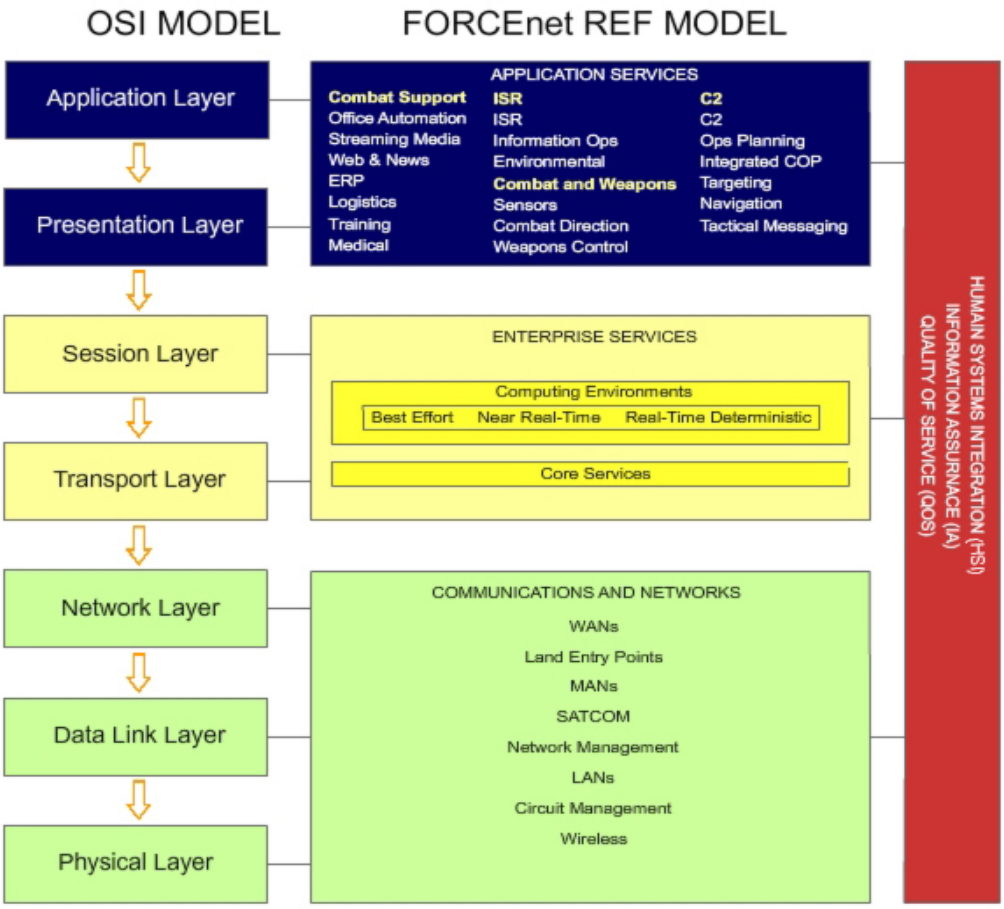

Figure 2 OSI and FORCEnet Integration

The Layers

- **The Physical Layer.** This layer has standards and protocols to control the transmission of data or information over a particular medium. For example, signal durations and frequencies that a communication system operates at would be described at this layer.

- **Data Link Layer.** Standards and protocols that specify how a system access and share the transmission medium would be described in this layer.

- **Network Layer**. Standards and protocols that specify how the network connection, routing, relays and connections between nodes are specified in this layer.

- **Transport Layer.** Standards and protocols for data transfer completion; error recovery, data flow and other related areas are specified in this layer.

- **Session Layer.** Standards and protocols to manage communication between computers are specified in this layer.

- **Presentation Layer.** Standards and protocols to control incoming and outgoing data from on format to another are specified in this layer.

- **Application Layer.** Standards and protocols that specify services for an application such as authentication are in this particular layer.

There are FORCEnet standards and protocols that apply to multiple layers under this model, which is not duplication but an extension of the goal of interoperability. If the same standard is used in the particular layer this will ensure there is interoperability between the layers. For example, HTTP is a protocol used at layers 6 and 7; therefore want to ensure that the developers working on the applications are using the same HTTP standards as the developers at the presentation layer. WiFi is another example that is cited in the physical and data layers.

Conclusions

By mapping the FORCEnet reference model to the OSI ISO model, the standards that have been listed in the FORCEnet TVs can be cross referenced to the OSI ISO model thereby showing what commercial standards apply to the FORCEnet architecture products (the SVs then to the OVs). For example, the commercial as well as the international and military standards to support netcentric operations for a weapon system could be identified and listed.

The list of standards for FORCEnet has been developed and documented. It is not a list of just military unique standards and specifications. The majority of the standards are commercial standards. And a potential industry partner or company does not have to try to determine the Navy's net centric standards if we share this information with industry. This would also provide some relief to the government program managers, who have the unenviable job of ensuring the standards proposed for their system are consistent with every other program in the Navy and DOD. Rather than using whether or not a vendor chooses the correct standards as trade space to get a "better" product. Use that trade space to get a better capability using the standards as the common denominator. Lets share that list with industry.

Bibliography

Alberts, David S, Garstka, John J., and Stein, Fredrick P. “Network Centric Warfare Developing and Leveraging Information Superiority,” CCRP February 2000

Rheingold, Howard. “Smart Mobs Transforming Cultures and Communities in the Age of Instant Access” Perseus Publishing 2002

Office of the FORCEnet Chief Engineer Office, Department of Navy. “ Architecture and Standards Vol II Technical View”. Department of Navy 31 December 2004

Rackley, Steve. “Networking in Easy Steps” Barnes and Noble Books New York 2004

Stewart, Mike. “FORCEnet: Networking the Naval Combat Force.” Defense Standardization Journal October/December 2004

“France Imposes Curfews” US News and World Report Novemebr 8, 2005

Crampton, Thomas. “Blogs and Text Messages Spread Call to Violence.” International Herald Tribune November 9, 2005

Department of Defense. “DOD Architecture Framework Version 1.0, Volume II Product Descriptions.” DOD 30 August 2003

“Naval Power 21…A Naval Vision” Gordon England Secretary of the Navy, Vern Clark, Admiral USN, Chief of Naval Operations, James L/ Jones, General USMC, Commandant of the Marine Corps

“FORCEnet A Functional Concept for the 21 st Century.” Vern Clark, Admiral UASN, Chief of Naval Operations, Michael W. Hagee, General USMC, Commandant of the Marine Corps

Footnotes

1. France Imposes Curfews US News and World Report 11/8 2005 and
2. Blogs and Text Messages spread call to violence International Herald Tribune Nov 9, 2005
3. Page 88, Network Centric Warfare
4. CNO's Strategic Study Group - XXI definition from 22 July 02 CNO Briefing
5. ISO OSI Website www.iso.ch

Acronyms

American National Standards Institute (ANSI)
Armed Forces Communications and Electronics Association (AFCEA)
Command and Control (C2)
Command Control Communications Computers Intelligence Surveillance reconnaissance (C4ISR)
Common Operating Environment (COE)
Defense Information Infrastructure (DII)
Defense Information Standards Registry (DISR)
Defense Information Systems Agency (DISA)
DOD Architecture Framework (DODAF)
DOD Architecture Repository (DARS)
Enterprise Services (ES)
Extensible Markup Language (XML)
GIG Enterprise Services (GIG-ES)
Global Information Grid (GIG)
Hull, Mechanical and Electrical (HM&E)
Human Systems Integration (HSI)
Information Assurance (IA)
Institute of Electrical and Electronic Engineers (IEEE)
International Organization for Standardization (ISO)
Internet Engineering Task Force (IETF)
Internet Protocol (IP)
Joint Technical Architecture (JTA)
National Defense Industrial Association (NDIA)
Netcentric Warfare (NCW)
Open System Interconnection (OSI)
Operational View (OV)
Organization Unique Standards (OUS)
Quality of Service (QoS)
service level agreements (SLA)
Service Oriented Architecture (SOA)
System View (SV)
Technical View (TV)