

D R A F T

**OPEN ARCHITECTURE
COMPUTING ENVIRONMENT
TECHNOLOGIES AND STANDARDS**

Version 1.0 (Pre-release 1)

04 September 2003

This document is a pre-release copy intended for final review prior to its signature and release as an Open Architecture initiative guidance document. The document is available for review on NSWCDD ViewNet and final commentary for a period of one week, beginning 4 September and concluding 12 September. Comments should be addressed to David T. Marlow, MarlowDT@nswc.navy.mil.

D R A F T

(This page intentionally left blank)

FOREWORD

The Assistant Secretary of the Navy for Research, Development and Acquisition (ASN (RD&A)) assigned responsibility for coordinating the introduction of Open Architecture (OA) into the Navy's warfighting systems to the Program Executive Office for Integrated Warfare Systems (PEO IWS). As part of the OA tasking, and based on significant research and testing, the PEO IWS Open Architecture technical team has developed a number of supporting documents relevant to Open Architecture. These documents describe the process and technical characteristics of and standards applicable to functional capabilities and computing system technologies in support of OA-based warfighting systems. In accord with the Joint Technical Architecture (JTA), the OA initiative encompasses both system architecture and technical architecture. (Operational architecture is not expected to initially change as a result of OA and so is not currently documented.) The technical architecture, or unified standards-based set of computing resources, is called the Open Architecture Computing Environment (OACE). These documents provide significant insight into OA capabilities and requirements. They have been through a formal review cycle within the Navy as well as an industry comment phase.

Computing technology is a key part of the OA effort. This document, *Open Architecture Computing Environment Technologies and Standards Version 1.0* of ___ September 2003, provides a core set of technologies and standards that apply to the OACE technology base. In cases where standards are still under development, preliminary product selection guidance is provided. A companion document, *Open Architecture Computing Environment Design Guidance, Version 1.0*, provides guidance concerning design aspects of the standards-based computing environment that is to be used in OA warfighting systems. The scope of OA is intended to encompass warfighting systems for ships, submarines and aircraft – including their sensor systems, weapon systems, combat direction systems and other mission critical support systems. Initial review indicates that the technologies and standards cited as written has applicability in both the warfighting system domain as well as the command, control and communication domains. Therefore, selected C4ISR systems are also included, the specifics of which are still under discussion. Therefore this document is intended to provide technologies and standards for the design and implementation of warfighting-capable software which, when coupled with OACE, will meet warfighting mission requirements for systems across the range of deployments listed above.

This document contains three major technical sections. The first, Section 4, OACE Technology Base, discusses the OACE Technologies by technology area emphasizing issues that impact standards for that technology area. The second, Section 5, Standards and OACE Compliance, enumerates mandated and emerging standards by technology area, providing in cases where standards are still under development additional interim product selection guidance. The third, Section 6, OACE Compliance Assessment, describes how to document OACE compliance claims.

Open Architecture Computing Environment Technologies and Standards

The OA Technical Architecture team has developed the information contained within this document for Program Executive Office for Integrated Warfare Systems (PEO IWS). The information contained will be updated on a periodic basis by PEO IWS according to a formal process (currently being defined) that is closely aligned with changes in the commercial market as well as according to a cycle that meet the needs of Programs of Record adhering to the OA technologies and standards. Because of the ongoing nature of this effort, comments on the document or the material contained herein are always in order. As input to this process, program managers, industry sources and system developers are requested by the OACE Technical Architecture (TA IPT) team to provide inputs concerning their computing requirements according to the particulars described in the next paragraph. Inputs will be incorporated into a new issue of this document and the design guidance document as appropriate.

Comments and recommended changes should reference a specific page or paragraph whenever possible and should provide supporting rationale describing the anticipated utility and implementation implications of the change. In addition, each responding organization should identify a single point of contact for discussion of proposed changes. Inputs may be provided at any time but will be considered for incorporation only at scheduled (approximately annual) updates. The next update is scheduled for September 2004. To provide inputs, or for further information concerning Open Architecture and the applicability of this document, contact the OA Project Officer, CAPT Thomas J. Strei, PEO IWS Code 1S at StreiTJ@navsea.navy.mil or (202) 781-1160. For further information concerning technical content and/or to provide recommended changes to this document, contact lead editor David T. Marlow, NAVSEA Dahlgren, Code B35 at (540) 653-1675, or via email at MarlowDT@nswc.navy.mil.

Open Architecture Computing Environment Technologies and Standards

Contents

1	Purpose	2
1.1	Open Architecture Goals	2
1.1.1	Common Warfighting Functions	2
1.1.2	Open Architecture Computing	2
1.2	Scope	3
1.2.1	Warfighting Function Commonality	3
1.2.2	Warfighting Function Applicability	4
1.2.3	Computational Domain Applicability	4
1.3	Technical Approach	5
1.3.1	Open Systems	6
1.3.2	Computing Standards	6
1.3.3	Product Selection	7
1.3.4	Federated vs. Integrated	7
1.4	OACE Change Management	8
1.5	Document Overview	8
2	Applicable Documents	8
3	Technology Overview	9
3.1	OACE Technologies	9
3.2	Reference Architecture	10
3.3	Sources of Standards	11
3.4	OACE Compliance Categories	11
3.5	Pools of Processing	13
4	OACE Technology Base	15
4.1	Physical Media	15
4.2	Enclosures	16
4.3	Information Transfer	17
4.4	Computing Resources	17
4.5	Operating Systems	18
4.5.1	Real-time Support	19
4.6	Peripherals	20
4.7	Adaptive Middleware	20
4.8	Distribution Middleware	21
4.8.1	Distributed Objects	21
4.8.2	Publish-Subscribe	22
4.8.3	Group Ordered Communication	22
4.8.4	Data Parallel	23
4.8.5	Multiple Distribution Middleware Standards and Families	24
4.9	Frameworks	26
4.10	Information Management	27
4.11	Resource Management	28
4.12	Security Services	29
4.12.1	DoD Policy Constraints	29
4.12.2	Commercial Best Practice	29
4.12.3	Data Separation	30

Open Architecture Computing Environment Technologies and Standards

4.13	Time Synchronization	30
4.14	Programming Languages	30
5	Standards and OACE Compliance Statements	31
5.1	Physical Media	33
5.2	Enclosures.....	45
5.3	Information Transfer	45
5.4	Computing Resources	54
5.5	Operating Systems	54
5.6	Peripherals	59
5.7	Adaptive Middleware	59
5.8	Distribution Middleware	59
5.8.1	Distributed Objects	59
5.8.2	Publish-Subscribe	59
5.8.3	Group Ordered Communications	60
5.8.4	Message Passing Interface for Data Parallel Applications	60
5.9	Frameworks.....	66
5.10	Information Management.....	66
5.11	Resource Management	69
5.12	Security Services.....	69
5.13	Time Synchronization.....	73
5.14	Programming Languages	75
6	OACE Compliance Assessment	77
6.1	OACE System Compliance Assessment	77
6.2	OACE Application Program Compliance Assessment.....	77
6.3	OACE Infrastructure Compliance Assessment.....	77
6.4	Documenting OACE Compliance Assessment Claims	78
6.5	OACE Infrastructure Components	78

Figures

Figure 1. Open Architecture Layered Approach	5
Figure 2. OACE Reference Architecture.....	10
Figure 3. OACE Compliance Categories	12
Figure 4. Notional Pools of Computing Aboard a Tactical Platform	14
Figure 5. Families of Distribution Middleware	25

Tables

Table 1. Sources of OACE Standards	11
Table 2. POSIX 1003.13 Profiles.....	20
Table 3. Standards Bridging Technologies.....	26
Table 4. Technology Area OACE Compliance	32

(This page intentionally left blank)

Open Architecture Computing Environment Technologies and Standards

1 Purpose

The purpose of this document is to define the computing technology base and standards that are to be used in Open Architecture (OA) warfighting systems. The overall set of computing resources used in OA systems is called the Open Architecture Computing Environment (OACE). This document describes the OACE technologies, identifies the standards used in defining the OACE and defines compliance assessment to these OACE standards. A companion document, *Open Architecture Computing Environment Design Guidance, Version 1.0* [1], provides interim guidance concerning design aspects of the standards-based computing environment that is to be used in OA warfighting systems.

1.1 Open Architecture Goals

The goals of OA include 1) reducing total ownership cost; 2) making system change and upgrade easier and faster; 3) lowering the impact of commercial off-the-shelf (COTS) computing technology refreshes; and 4) reducing compatibility and interoperability problems. The OA initiative accomplishes this by evolving Navy surface ship warfighting systems from the current status quo – many warfighting systems and ship classes developed over time and under less than fully coordinated acquisition strategies – toward a unified Navy warfighting system product line.

The unified product line approach is based on two major implementation concepts: 1) a common set of warfighting functions, built to a single functional architecture and shared across many ship classes, and 2) a layered, standards-based computing environment (the OACE) applicable, with variations, to all warfighting systems. This goal applies directly to future construction, and it may in cases apply to backfit as well.

1.1.1 Common Warfighting Functions

Common warfighting components are being developed under the auspices of the OA initiative, either directly or through leveraged contracting arrangements. These common components must be matched to and integrated with the unique warfighting components associated with a particular ship class or backfit upgrade. While some shipboard components must inevitably be unique to mission and function, applying the principle of commonality and reuse wherever possible is seen as a major mechanism for cost control in future Navy warfighting systems.

1.1.2 Open Architecture Computing

Achieving commonality of warfighting components across ship classes places a corresponding requirement for application computer program portability across potentially differing equipment and support software bases. The rapidly changing

nature of COTS also levies portability requirements on application software as an enabler of low-cost COTS technology refreshes.

To that end, the OA initiative includes a coherent computing technology strategy based on the widely employed commercial practice called *open systems* – that is, standards-based systems that are easy to upgrade and change over time. This strategy is based on maximum use of a compatible set of layered, standards-based computing technologies, many of them real-time capable – the OACE. Within this layered approach, various forms of adaptive and service-based third party software, collectively called *middleware*, provides additional isolation mechanisms between applications and equipment that contribute to application portability.

1.2 Scope

This document applies to the computing implementation of the functional capabilities embodied in naval warfare systems, including but not limited the ship classes shown below. These ship classes are covered under the scope of the OA program, and therefore under the guidelines of the OACE. The OACE standards information contained herein applies to all new constructions and, selectively, to backfit. Schedule information will be provided in separate documentation.

- Aegis-equipped cruisers and destroyers (DDG new construction and CG/DDG backfit)
- SSDS-equipped carriers and large deck amphibious assault ships, e.g. LPDs, LHAs, LHDs, etc. (new construction and backfit)
- Submarines (new construction and backfit)
- DD(X) land attack destroyer (future construction)
- Littoral Combat Ship (LCS) (future construction)

1.2.1 Warfighting Function Commonality

Commonality of warfighting functions is a primary goal for OA. The following list represents a partial enumeration of candidate common warfighting functions. This list should be interpreted as illustrative rather than definitive.

- Mission Planning
- Track Formation
- Tactical Information Mgmt
- Identification
- Doctrine Management
- Threat Evaluation
- Damage Control
- Mission Evaluation
- Readiness Control
- Readiness Assessment
- Training

Open Architecture Computing Environment Technologies and Standards

- Display
- Time
- Navigation
- Data Extract / Record
- Ship Control
- UV Control

1.2.2 Warfighting Function Applicability

OACE computing capabilities are intended to serve the requirements of not only the common functions listed above but also other warfighting functions as well. Extending and generalizing the list of supporting common functions contained in Section 1.2.1, the following list of application domain functional categories is considered within scope of OACE guidance.

- Sensor control
- Signal processing (only where requirements permit)
- Local sensor fusion and track formation
- Remote sensor fusion, gridlock, data registration, etc.
- External Communications
- Combat Direction
- Weapon control
- Fire control
- Navigation
- Readiness, damage control, etc.
- Tactical Training
- Tactical display
- Tactical support services and frameworks

1.2.3 Computational Domain Applicability

The scope to which OACE capabilities apply encompasses most but not all combat system and support system application areas. Included are 1) real-time tactical computation requirements that can be met by mainstream commercial products; 2) physically embedded computational requirements that can be met by well-accepted niche market products; 3) tactical display and decision support requirements that can be met by mainstream COTS; and 4) high security requirements that can be met by appropriate commercial technology, albeit niche market.

Not included within the present scope of OACE are performance domains for which custom designed special purpose devices are required to meet performance requirements. Also not included are decision support resources with little or no real-time requirements and other systems such as:

- Extremely high performance domains such as some signal processing

Open Architecture Computing Environment Technologies and Standards

- Low-level embedded devices such as those that implement machinery control or other Hull, Mechanical and Electrical (HM&E) functions
- Command support functions such as those associated with Information Technology – 21st Century (IT-21)
- Administrative or personal computing support, e.g. personal laptops

In the case of IT-21, further examination is required to determine the degree of overlap between IT-21 and OACE. In any case, interconnect and bridging technologies for interfacing components of the above types to OACE-based systems are included.

1.3 Technical Approach

OACE computing infrastructure components provide the computational framework upon which both common and unique warfighting and support applications are to be built under the guidelines of the OA functional architecture. The overall scope of OACE includes technical architecture, standards and products. Conceptually, OACE provides isolation of warfighting applications and services by means of a standards-based, layered approach, see Figure 1.

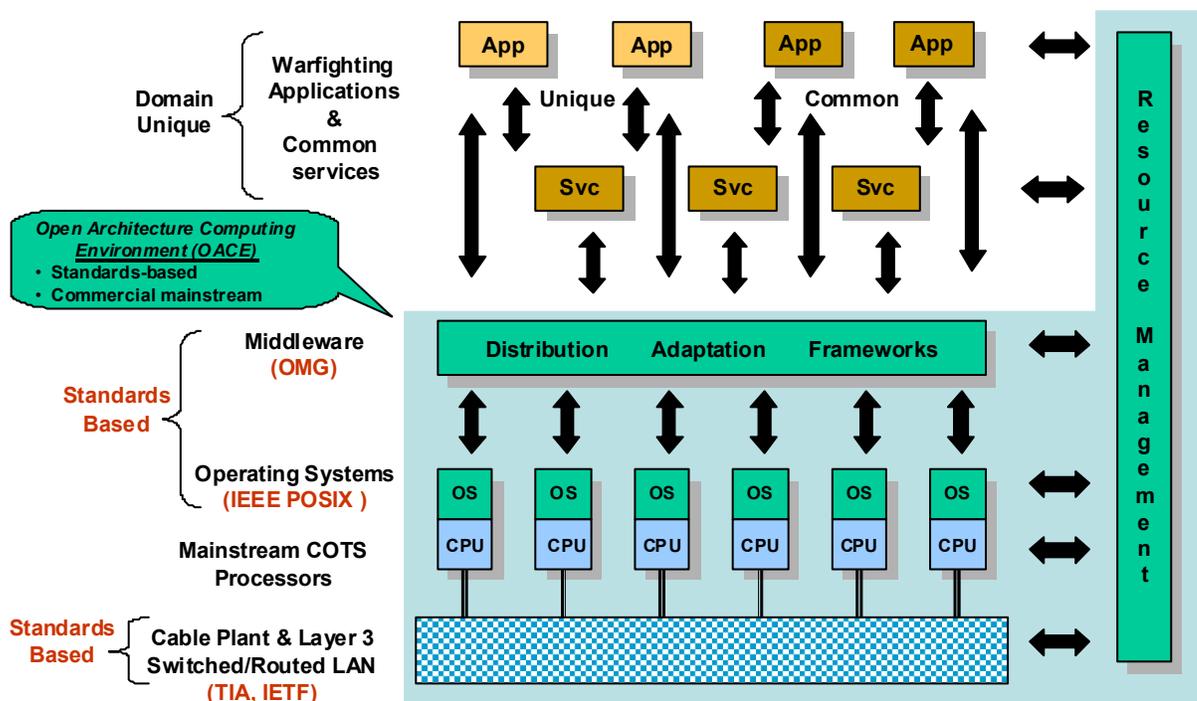


Figure 1. Open Architecture Layered Approach

The description of the OACE technology set is based on a reference architecture that is applicable to mission critical distributed systems. The reference architecture, discussed in section 3.2, is a representation of the key technologies (and their interrelationships) known to be suitable for successful development and fielding of Navy surface ship warfighting systems. Requirements encompass various aspects of real-

time computation as well as various support requirements, e.g. display, decision support, security, etc.

This document describes each of the OACE technologies and identifies the standards that they are based on. Where standards do not yet exist the approach for implementing the functions of the OACE technology is provided.

1.3.1 Open Systems

The OA initiative and its computing environment, the OACE, are based on the widespread commercial practice called open systems. The open approach has been widely adopted because open systems convey certain benefits in terms of reduced life-cycle cost, reduced time-to-market, increased ability to inter-operate and cooperate with others, reduced personnel training, etc. A number of open systems definitions exist within the literature. From a process and business strategy point of view, this document adopts the definition provided by the Open Systems Joint Task Force (OSJTF), which operates at the level of the Office of the Secretary of Defense:

“An Open Systems Approach is an integrated business and technical strategy that employs a modular design and, where appropriate, defines key interfaces using widely supported, consensus-based standards that are published and maintained by a recognized industrial standards organization.” [2]

A number of technical definitions for open systems are available. Given the selection of standards for OA, perhaps one of the most relevant is the definition adopted for the POSIX operating system standard by IEEE.

Open system: *“A system that implements sufficient open specifications or standards for interfaces, services, and supporting formats to enable properly engineered application software*

- *To be ported with minimal changes across a wide range of systems from one or more suppliers*
- *To interoperate with other applications on local and remote systems*
- *To interact with people in a style that facilitates user portability” [3]*

1.3.2 Computing Standards

A major goal of the open approach to computing chosen for OA is to enable the development of applications that are portable across multiple brands and generations of COTS computing products. This portability is fostered primarily through 1) choice of computing products that conform to widely accepted commercial standards (wherever possible), and 2) through the use of middleware for communications, abstraction of services, and application programmer interfaces (APIs). Thus, standards are a cornerstone of the open systems approach.

Open Architecture Computing Environment Technologies and Standards

The standards chosen for use in OA are described in this document. They are drawn from a number of widely respected standards communities, see below, and are compatible with the standards invoked in the JTA [4] as described in Section 5.

- Telecommunications Industry Association (TIA) – physical media, e.g. fiber
- Internet Engineering Task Force (IETF) – networks and protocols
- IEEE Portable Operating System Interface (POSIX) – operating systems
- Object Management Group (OMG) – distribution middleware, e.g. CORBA
- International Standards Organization (ISO) – Ada programming language (the use of which shall be restricted to legacy applications), Structured Query Language (SQL) information management
- American National Standards Organization (ANSI) – C, C++ languages
- Java Community Process – Java programming language and infrastructure, Java Data Objects (JDO) and Java Database Connectivity (JDBC) information management

1.3.3 Product Selection

In furtherance of the goal of compatibility and commonality, the OA initiative provides guidance concerning computing product selections as well as standards. Based on past experience, standards tend to evolve more slowly than computing products. Therefore product selection guidance will be documented separately from *this document except for the case where no standard is available for a needed technology.*

For maximum flexibility in leveraging the commercial computing marketplace, the philosophy employed in OACE product selection is to provide selections of product classes and families while empowering individual Navy acquisition programs to select specific products (manufacturers, version numbers, configuration options, etc.) according to their unique warfighting needs and acquisition plans and shipbuilding or overhaul schedules. This approach is discussed in section 1.3.4.

1.3.4 Federated vs. Integrated

It should be acknowledged that the OA goal of commonality is, to some degree, in tension with the goal of providing maximum flexibility of choice to acquisition managers. The term “integrated” is used to describe the commonality approach, and the term “federated” is used to describe a contrasting approach where choice is unrestricted.

The integrated approach enables mission flexibility and enhanced failure recovery through a high degree of redundancy delivered via operational resource sharing. It may also engender economies of scale in procurement, although this is less important in an era of very low cost COTS processors. The federated approach allows maximum flexibility to meet stressing or system-unique requirements through selection of leading edge technologies. It also places fewer requirements on programs to align their schedules with factors outside their immediate programs.

One of the means by which commonality is encouraged is the availability of on-line management of computing resources. This capability, similar to the *total ship computing* (not to be confused with OACE Level 5, Total Ship Computing described in Section 3.4) utilized in the DD-21 Operational Requirements Document [5], permits resource sharing, mission optimization and failure recovery on a ship-wide basis across all compatible computing resources. This service is available to all systems that are able to participate in the integrated approach, but it does not preclude employment of the federated approach for systems that have requirements that justify a different approach.

1.4 OACE Change Management

Current mainstream COTS computing technology meets many, but not all warfighting computing requirements. However, the pace of computing technology innovation has been very rapid for decades and shows little signs of slackening. Thus, mainstream products may in the future meet many requirements that are currently met only by special purpose solutions. Because of this rapid evolution, the boundaries between what is within OACE scope and what is not will require periodic reconsideration.

For this reason, an OACE change management process will be formally documented. This document, when released in the near future, will define a formal process that provides for periodic review of the standards contained in this document. This change process, cyclic in nature, will include mechanisms for incorporating the requirements of each program manager as well as inputs from industry.

1.5 Document Overview

Section 2 provides applicable documents identified within the main body of this document (excluding the Standards Listings). Section 3 provides a list of the OACE Technology Areas, an introduction to the OACE Reference Architecture, identifies the primary standards bodies for the OACE Technology Areas, describes the OACE Compliance Categories and describes processor pooling. Section 4 discusses the OACE Technologies by Technology Area emphasizing issues that impact standards for each area. Section 5 provides the compliance statements of mandated and emerging standards by Technology Area, providing in cases where standards are still under development additional product selection guidance. Section 6 discusses OACE compliance assessments.

2 Applicable Documents

1. Open Architecture Computing Environment Design Guidance, Version 1.0, dated _____ 2003.
2. An Open System Approach to Weapon System Acquisition, Version 1.0, Working Draft, http://www.acq.osd.mil/osjtf/approach/approach_os.html

3. IEEE Std 1003.0-1995. IEEE Guide to the POSIX Open System Environment (OSE)
4. DoD Joint Technical Architecture, Version 4.0, dated 17 July 2002.
5. DD-21 Operation Requirements Document (ORD).
6. IEEE Std 1003.1-2001. Base Definitions, Issue 6, 1003.1 Standard for Information technology - Portable Operating System Interface (POSIX)
7. IEEE Std 1003.13-1998. IEEE Standard for Information Technology - Standardized Application Environment Profile - POSIX® Realtime Application Support
8. Document -- ptc/03-07-07 (Updated Data Distribution Service Final Adopted specification), dated 7 July 2003, <http://www.omg.org/docs/ptc/03-07-07.pdf>
9. Department of Defense DIRECTIVE NUMBER 8500.1, October 24, 2002 http://www.dtic.mil/whs/directives/corres/pdf/d85001_102402/d85001p.pdf
10. Navy Recommended Fiber Optic Components Parts List, 21 May 2003.

3 Technology Overview

The OACE technology base consists of a number of computing technologies. In aggregate, these technologies largely reflect the current state of the practice as it applies to real-time systems and other associated systems of a shipboard nature. Wide ranges of computing technologies are available in addition to those listed herein. However, only those technologies currently deemed to be capable of delivering reliable real-time or near-real-time performance are included in the OACE technology base.

Other technology domains, such as those applicable to business or web applications are briefly discussed but not included in this version of this document. If deemed appropriate, they may be discussed in a future version. Individual technologies will be reviewed periodically, by a process under development (described in 1.4), for possible future inclusion as their apparent viability merits.

3.1 OACE Technologies

The following list constitutes the set of technologies considered under the scope of OACE.

- Physical Media
- Enclosures
- Information Transfer
- Computing Resources
- Operating Systems
 - General Purpose
 - Real Time
- Peripherals
- Adaptive Middleware

- Distribution Middleware
 - Distributed Object Computing
 - Publish-Subscribe Protocols
 - Group Ordered Communication Protocols
 - Data Parallel
- Frameworks
- Information Management
- Resource Management
- Security Services
 - Commercial Best Practice
 - Data Separation
- Time Synchronization
- Programming Languages

3.2 Reference Architecture

Figure 2 provides an abstracted view of a number of the technology base components and their interrelationships. This diagram contains the OACE reference architecture. The diagram is notional in nature and does not necessarily imply a particular design or implementation. For example, three of the classes of Distribution Middleware listed in Section 3.1 (i.e. Distributed Objects, Group Ordered, and Publish-Subscribe) appear as separate components in the reference architecture. However, the future evolution of the OMG distributed computing standards is in the direction of providing the three key distribution middleware protocols within a single product family.

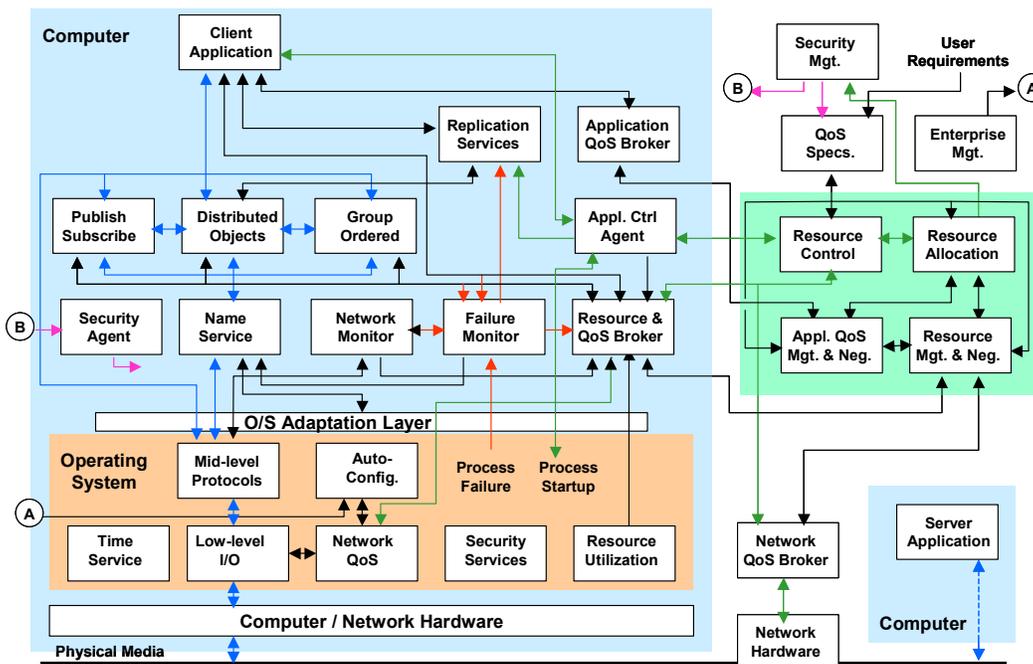


Figure 2. OACE Reference Architecture

3.3 Sources of Standards

Table 1 below provides initial information as to the source of standards for those components for which standards have been selected.

Table 1. Sources of OACE Standards

Technology Component	Source of Standard
Physical Media	MIL standards, Commercial Item Description (CID), Electronics Industry Association/Telecommunications Industry Association (EIA/TIA)
Enclosures	None at present
Information Transfer	Internet Engineering Task Force (IETF), Institute for Electrical and Electronics Engineers (IEEE), Joint Technical Architecture (JTA)
Computing Resources	Commercial products of various types
Operating Systems	IEEE Portable Operating System Interface (POSIX) standard, JTA
Peripherals	Various
Adaptive Middleware	POSIX-based
Distribution Middleware	Object Management Group (OMG) standard for Common Object Request Broker Architecture (CORBA), Message Passing Interface (MPI) Forum, World Wide Web Consortium (W3C)
Frameworks	None at present
Information Management	International Organization for Standardization (ISO), Java Community Process (JCP)
Resource Management	None at present
Security Services	National Institute of Standards and Technology (NIST), IETF, JTA
Time Synchronization	Inter-Range Instrumentation Group (IRIG), IETF Network Time Protocol (NTP), JTA
Programming Languages	ISO, JCP

3.4 OACE Compliance Categories

There are five approaches identified for tactical systems to work with/within an OACE infrastructure. Figure 3 shows the five approaches. OACE compliance is defined for three of these categories; these three are defined as the Fully OACE Compliant categories. OACE migration is defined as the moving a tactical system into one of the Fully OACE Compliant categories. OACE compliance assessments

referenced against this document are required to identify a particular Fully OACE Compliant compliance category.

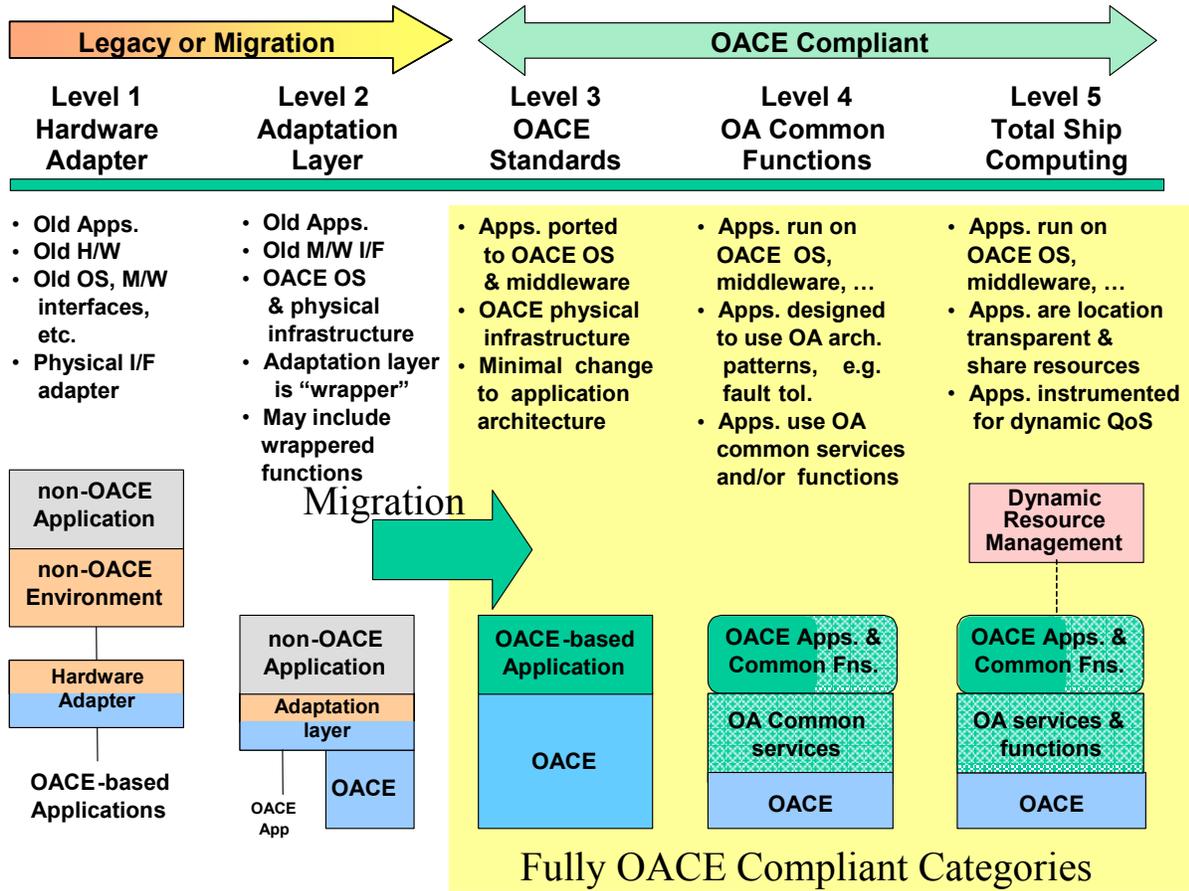


Figure 3. OACE Compliance Categories

A Hardware Adapter OACE (Level 1) approach uses a system, not built to the OACE Standards (typically a legacy system), interfaced to OACE-based Applications via a Hardware Adapter that is compliant with the OACE Standards identified in this document. The only compliance issues are with the Hardware Adapter and not with the legacy system. OACE compliance assessments are not used with this approach.

An Adaptation Layer (Level 2) approach uses OACE compliant hardware and operating system with an Adaptation Layer that isolates a non-OACE application (typically a legacy application) from the underlying platform. The Adaptation Layer should provide OS wrapper functions, design pattern components, and system interfaces for use by non-OACE applications running within the OACE. OACE compliance assessments are not used to describe a component or system built with this approach.

Open Architecture Computing Environment Technologies and Standards

An OACE Standards (Level 3) approach uses an OACE compliant infrastructure but does not use OA Common Services and OA Common Functions. For this approach typically legacy applications are ported to OACE infrastructures. In such a port, minimal changes are made to the application architecture. Any OACE compliance assessments referenced against this document for a system or component must specifically identify any exceptions to OACE compliance requirements listed within this document.

An OA Common Functions (Level 4) approach uses an OACE compliant infrastructure for which an application has been designed to use the OA architectural patterns/frameworks (e.g. OA fault tolerance pattern). Such applications must use the OA Common Services (e.g. time synchronization, navigation, DX/DR, etc.) and OA Common Functions versus different (e.g. legacy) approaches for such services and functions when these are needed. Such applications need to be developed with planned periodical upgrades as new OA infrastructure capabilities, OA Common Services and OA Common Functions become available. Any OACE compliance assessments referenced against this document for a system or component must specifically identify any exceptions to OACE compliance requirements listed within this document.

A Total Ship Computing (Level 5) approach includes all the requirements for OA Common Functions (Level 4) compliance with the addition of a dynamic resource management capability that provides for application location transparency and the ability to share the infrastructure resources via an integrated software approach. To achieve the Total Ship Computing (Level 5) category's dynamic QoS capability, the application must be instrumented to provide Resource Management with timely status of its resource requirements. Any OACE compliance assessments referenced against this document for a system or component must specifically identify any exceptions to OACE compliance requirements listed within this document.

3.5 Pools of Processing

As previously described, one of the focus areas for the OACE infrastructure is to support an integrated software approach. In such an approach, a system would deliver a module of application software (using the OA Common Services and Functions) instead of delivering a unique set of hardware and infrastructure software bundled with a system's unique application software. In the integrated software approach, the module of application software delivered would run with a variety of other applications on a common pool of processors within an OACE infrastructure. Aboard a platform there may be a number of such pools of processors, as shown in Figure 4. Each pool would host a number of integrated software applications with compatible security requirements and operating characteristics.

The OACE Fully OACE Compliant compliance categories all support running application software upon a pool of processors. A Hardware Adapter OACE approach uses a hardware adapter to isolate a legacy system from an OACE pool (or pools) of processors. The Total Ship Computing (Level 5) approach is intended to meet a

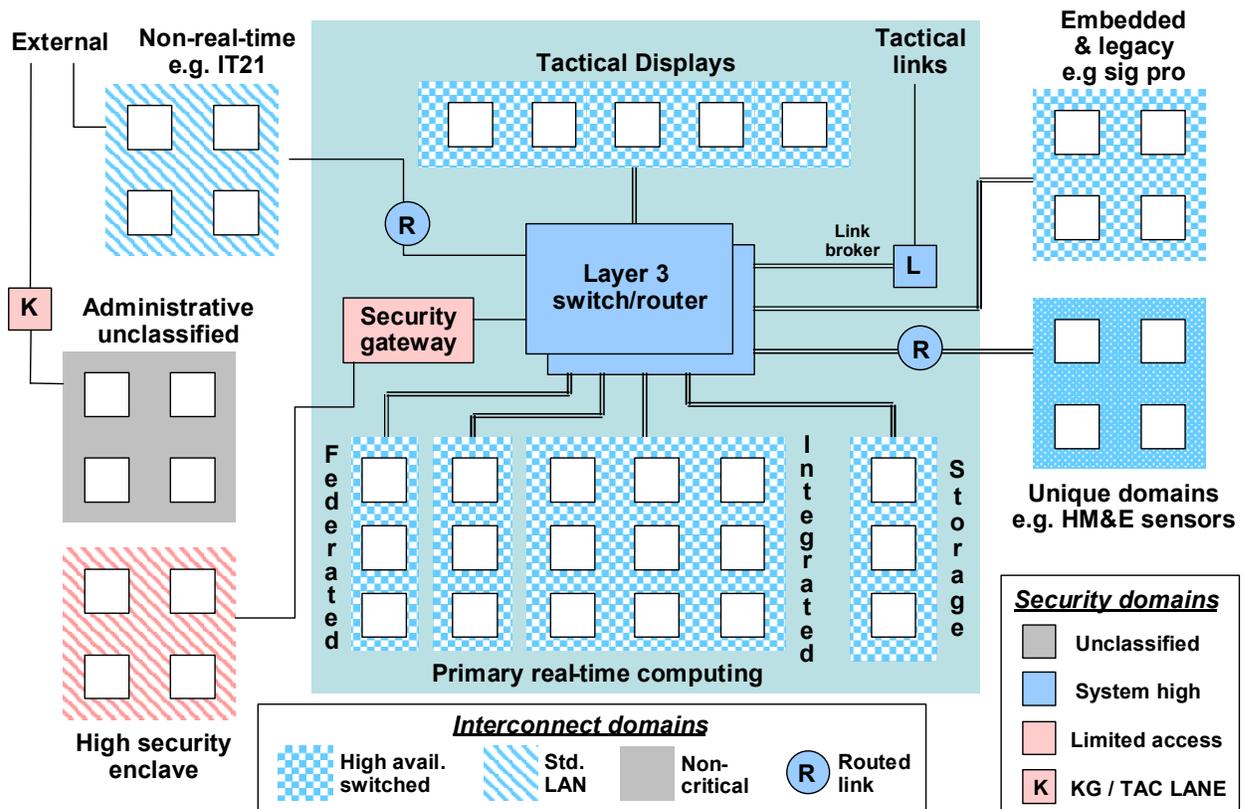


Figure 4. Notional Pools of Computing Aboard a Tactical Platform

primary objective of OA: the dynamic assignment of resources to applications depending upon the situation that the tactical platform finds itself in. Thus, as new threats are identified, the pool of processors may increase the resources provided to meet the AAW threats. Later when the situation changes, this same pool of processors can adapt to meet an increased ASW threat. This allows a flexible approach responsive to changing tactical situation and resource failures versus the current stovepipe approach where a fixed inflexible set of hardware and infrastructure software is pre-allocated to a specific tactical application.

OACE compliance statements provided within this document can be tied to the characteristics of the pools of processors provided for the applications. For example, a compliance statement may allow a pool of processors to utilize a choice of one of two Publish-Subscribe Distribution Middleware alternatives identified.

4 OACE Technology Base

4.1 Physical Media

Physical media products/components are used to develop the cable topology installed aboard naval platforms. The OA Physical Media standards and specifications provide for design and installation standards as well as both Military unique and commodity COTS based product specifications. Military performance specifications are developed for Navy unique products used in applications where environmental or safety requirements (e.g. low-smoke, zero halogens) shall be met. Commercial Item Descriptions (CIDs) are developed for commodity COTS based products to ensure interoperability among products. These standards and specifications are used to reduce the long-term risk of the shipboard cable topology.

There are many Military and Commercial physical media technologies available that will address the Navy's physical media goals of Open Architecture. These technologies can be placed in several categories:

Optical Fiber – A filament-shaped waveguide, made of dielectric material such as glass or plastic, that guides light. It usually consists of single discrete optically-transparent transmission element consisting at least of a cylindrical core with cladding on the outside.

Multimode fiber – An optical fiber that will allow more than one mode to propagate at a given wavelength. The number of modes will depend on the core diameter, the numerical aperture, and the wavelength.

Single Mode fiber- An optical fiber in which only one bound mode can propagate at a given wavelength and numerical aperture.

Optical Fiber Cable – A cable in which one or more optical fibers are used as the propagation medium.

Blown Optical Fiber (BOF) cable - A cable that contains one or more BOF tubes through which optical fibers or optical fiber bundles are blown.

Conventional optical fiber cable - An optical fiber cable in which the optical fiber is an integral part of the cable and is installed during the cable manufacturing process.

Single Terminus Connectors – In fiber optics, a connector that is designed and intended from use inside of an interconnection box (distribution box) or cabinet.

Multi-Terminus Heavy Duty Connectors - In fiber optics, a connector that is designed and intended from use outside of an interconnection box (distribution box) or cabinet.

Optical Fiber Terminus – A device used to terminate an optical fiber, that provides a means of locating and holding the fiber within a connector.

Open Architecture Computing Environment Technologies and Standards

Interconnection Box – A housing for holding fiber optic splices, connectors, couplers, and Blown Optical Fiber (BOF) tubes used to distribute signals on incoming cables to outgoing cables by means of connections.

Blown Optical Fiber (BOF) Components – Components used for installing, interconnecting, and terminating BOF tubes and fibers.

Twisted Pair Cable - Electrical cable with 100 ohm twisted pair (TP) and an optimized braided shield and outer jacket, used for Local Area Networks (LANs).

Twisted Pair Connectors – A device used to terminate Twisted Pair cable, that provides a means of locating and holding the electrical conductors.

Baseline specifications for these products are currently in place.

The physical media products must meet the specific shipboard environmental requirements and the installation applications for which they are targeted. There are multiple vendors across these product lines that have been qualified or approved to the Navy specifications, and these products are currently being used in the Fleet. However, the physical media technology is an ever-changing market, and new vendors and new product offerings are ongoing. There are new products for which specifications are being developed and new products that are at various levels of maturity.

4.2 Enclosures

Enclosures are used to mount COTS equipment aboard naval platforms. The standard for many years has been the 19" (wide) rack. COTS products to be mounted in enclosures include computers, peripherals and Network switches. Example Products include a large number of commercial racks without environmental isolation, as well as the Q70 EPS rack and the Aegis MCE cabinet.

COTS equipment enclosures (19" racks) are readily obtainable in a variety of heights and depths. The key issue is whether the enclosure itself provides any environmental isolation (e.g. shock, vibration...) for the COTS equipment or whether this isolation is provided via other means.

If a programmatic decision is made to use a common set of enclosures, then following issues will need to be addressed:

- Specify the enclosure environmental isolation required.
- How will equipment suites be tested for environmental isolation?
- Will changing equipment in the enclosure require re-testing?

4.3 Information Transfer

The Information Transfer Technologies and Standards fall into three broad categories: Connectivity Protocols, Transfer Protocols, and Support Protocols. These protocols are used in varying combinations as required in specific OACE products. Examples of OACE products that will require Information Transfer Standards include computers (network interface cards), operating systems (the IP Protocol Suite), Enterprise Class Layer 3 switches, Access Routers, Enterprise Network Management, and Wireless Access Points.

The Connectivity Protocols are the lower layer protocols that are included in the International Organization for Standardization (ISO) Open System Interconnection (OSI) Reference Model's Physical and Data Link layers. They provide basic physical and logical connectivity between communicating devices. The most common family of standards in this category is the IEEE 802 Local Area Network Standards including various types of Ethernet.

The Transfer Protocols are the middle layer protocols that are included in the ISO OSI Reference Model's Network and Transport layers. They provide end-to-end data transfer over potentially multiple types of network connectivity protocols. The Internet Protocol (IP) is the single common denominator for providing end-to-end interoperability. All of the protocols required to provide this end-to-end transfer are included here including routing protocols and basic quality-of-service functionality.

Finally, the Support Protocols are the upper layer protocols that are included in the ISO OSI Reference Model's Session, Presentation, and Application layers. This group of protocols provides common communication services including file transfer and email transfer. There are wide ranges of protocols in this category representing a wealth of functionality.

4.4 Computing Resources

Computing resources as described here include all general purpose or dynamically reconfigurable computing devices required to support the OACE with the one exception of tactical display processors (which will come from the current programs such as the Q70 or future Navy defined display processing efforts). Examples include personal computers (PCs); common commercial UNIX workstations such as those manufactured by Sun Microsystems, Hewlett-Packard, Silicon Graphics, and others; symmetric multiprocessor servers such as those manufactured by Sun, Dell and others, and a wide variety of single board computers, many of them designed for the VME backplane chassis standard.

Middleware techniques are viewed as isolating the application software from changes at the computer hardware (and operating system) technology level; but the following are factors to minimize the number of types of computers within OACE:

1. Performance qualification of computing hardware can be a cost driver. Many different items are often bundled with the computing hardware (e.g. operating

systems, time synchronization software, network interfaces,...). Performance can typically only be measured given specific hardware and software. Thus, if OA has a large set of critical performance measures (e.g. time synchronization capabilities of **X** microseconds), then qualifying a computer to all of the performance requirements may be expensive. Selecting a common set of computing hardware may reduce duplicative qualification efforts and thus reduce costs.

2. Environmental qualification of computers may be a cost driver. A common set of computers may minimize such testing.
3. Life cycle costing and logistic/maintenance issues may force the number of processor types down to a minimum.

Although it would be easier to manage the entire set of computing resources on a platform as homogeneous computing resources, two factors make it an unreasonable expectation:

1. Different applications require a different mix of hardware support—some are I/O intensive, some are compute intensive, some are memory intensive—which indicates that a heterogeneous mix of computing resources might better support the computational needs of the ship.
2. Some applications require real-time support. A requirement for homogeneity will force all applications to run in a real-time environment. This places a heavy burden on software developers because real-time systems tend to be less portable and, due to a much smaller market share, lag the development of the wider software development world.

A goal is to support heterogeneity *transparently* through a layered architecture and an adaptive resource management capability. This will allow each individual tactical computing environment to continually evolve (through small, incremental, discrete purchasing decisions) as the applications themselves evolve to better support the needs of the tactical environment.

4.5 Operating Systems

In today's computing systems it is becoming increasingly important to design software with operating systems that are based on widely recognized industry standards. This is even more important for systems designed for longevity, where the hardware and software infrastructure will change during the system's life cycle. Standards are pervasive in today's systems; and new standards are constantly being defined to address the rapidly changing state of technology.

To be effective a standard must be based on established technology and widely accepted by industry. The Portable Operating System Interface for Computing Environments (POSIX) family of standards includes over 30 individual standards. First

published in 1990, POSIX defines a standard for application portability across different operating system platforms. The original POSIX 1003.1a defines standard interfaces to such core functions as: file operations, process management, signals and devices. Later releases have been defined to address such topics as real time extensions (1003.1b, d, j and 1003.21) and threading (1003.1c).

Functions defined in the original real-time extension standard 1003.1b are supported across a wider number of operating systems than the other two specifications. Specific features defined in POSIX 1003.1b include:

- Periodic timers
- Priority scheduling: fixed priority preemptive scheduling with a minimum of 32 priority levels
- Real-time signals with multiple levels of priority
- Semaphores: named and memory counting semaphores
- Memory queues: message passing using named queues
- Shared memory: named memory regions shared between multiple processes
- Memory locking: functions to prevent swapping of physical pages

Commercial support for POSIX varies. To be POSIX *conformant* requires certification testing of the operating system and hardware platform to a suite of tests. POSIX is established as a set of optional features, this allows vendors to implement portions of the POSIX standards and still be *compliant* to POSIX. Compliance only requires vendors to state which options are not implemented.

The core of the Open Group Single UNIX Specification, Version 3 is also IEEE Std 1003.1-2001. IEEE Std 1003.1-2001 [6] is a major revision and incorporates IEEE Std 1003.1-1990 (POSIX.1) and its subsequent amendments, and IEEE Std 1003.2-1992 (POSIX.2) and its subsequent amendments, combined with the core volumes of the Single UNIX Specification, Version 2. It is technically identical to The Open Group, Base Specifications, Issue 6; they are one and the same documents, the front cover having both designations.

4.5.1 Real-time Support

An operating system is just one component of any system that includes hardware, application software, other system software (e.g. middleware) and possibly a network or interconnection infrastructure. In a system with real-time requirements the insertion of a real-time operating system only addresses one element in a complex system. A real-time operating system (RTOS) alone cannot compensate in any large measure for insufficient determinism in the remaining system elements.

The POSIX standard promotes portability of applications; historically however, in real-time systems predictability and low overhead are important. Portability has often been sacrificed. Embedded real-time systems usually have space and resource restrictions that may make full compliance to all aspects of POSIX inappropriate. The POSIX 1003.13 profile standard [7] establishes profiles for systems based on intended functionality. Table 2 provides current POSIX profiles:

Table 2. POSIX 1003.13 Profiles

Profile	Number of Processes	Threads	File Systems
54	Multiple	Yes	Yes
53	Multiple	Yes	No
52	Single	Yes	Yes
51	Single	Yes	No

4.6 Peripherals

The OA peripherals will include both Man Machine Interface peripherals and Input/Output peripherals. The list of peripherals identified for OA is:

Man Machine Interface Peripherals

- Keyboard
- Mouse
- Cathode Ray Tube (CRT) Display
- Liquid Crystal Display (LCD)
- Plasma Display

Input/Output Peripherals

- Hard Drive
- Compact Disk
- DVD Read Write
- Printer
- Raid Mass Storage Device
- Network Attached Storage (NAS) peripherals
- Storage Area Network (SAN)
- Digital Linear Tape Backup Storage/Retrieval Devices

4.7 Adaptive Middleware

Adaptive middleware technology isolates applications from the differences in operating systems and compilers, thus increasing portability. Although standards for both operating system (e.g. POSIX) and compilers (e.g. C++) exist, in practice varying degrees of compliance with specific versions of the standards can affect the ability to readily port software between products produced by different vendors.

Adaptive middleware is available via widely used open source products (e.g. ACE), commercial vendors (e.g. RogueWave), and through products developed by DoD contractors (e.g. DSR middleware). Adaptive middleware products are targeted for a particular language, such as C++. Although there are no specific standards for adaptive middleware, products are generally based on the POSIX family of operating system

standards. The use of adaptive middleware is understood to be a long-term undertaking on the part of OA.

Unfortunately, the different adaptation middleware implementations are not fully interchangeable. Thus, a decision to use a particular adaptive middleware product would thereafter preclude the use of another without (possibly extensive) source code porting. For this reason, if an adaptive middleware product is selected for use, it is preferable that the product isolate and encapsulate the necessary operating system functionality and provide wide usage across multiple platforms.

As an alternative to adaptive middleware, it is possible to obtain complete adaptive environments, such as the commercially available MKS Nutcracker, which allows a Microsoft environment to appear like a standards-compliant Unix environment. There are few vendors of these products available, however, and little support for real-time applications by these products.

4.8 Distribution Middleware

Four types of distribution middleware are discussed, including distributed objects, publish-subscribe protocols, group ordered communication protocols and message passing middleware for data parallel applications. Additionally, as it is recognized that occasionally, the need may exist to have interactions between components developed using different middleware standards and/or products, bridging between middleware products is discussed.

4.8.1 Distributed Objects

Multiple different distributed object protocols are currently in use. These protocols allow the exchange of information by invoking methods on objects that may reside at some other location on a network. The most widely used examples of distributed object protocols include the Common Object Request Broker Architecture (CORBA), Microsoft DCOM, and Java Remote Method Invocation (RMI). Of these, only CORBA is a formal standard that is platform neutral, has interfaces available across multiple computer languages, and is supported by a vendor neutral industry consortium. Although a standards process supports Java RMI, it is specific to the Java language. Microsoft DCOM is specific to Microsoft platforms.

The CORBA standard is managed by an active industry standards group of approximately 800 members - the Object Management Group (OMG). Extensions to the core standard provide for interoperability of products from different vendors, real-time support, fault tolerance, transactions, object registration and discovery, event notification, and many other features.

The OMG also manages other important technology standards such as the Unified Modeling Language (UML) and the emerging Model Driven Architecture (MDA) standard. Since MDA is intended to support the concept of automatic code generation from UML models, the potential for substantial software productivity and reliability gains is high.

CORBA products that support the major languages of interest to OA, including C++, Java, and Ada, are available. Multiple products are available that are compliant with the CORBA real-time specification, including TAO, an open source, commercially supported Object Request Broker (ORB). The commercially available real-time ORBs include Objective Interface System's OrbExpress, Borland's Highlander, and PrismTech's E-ORB.

4.8.2 Publish-Subscribe.

Publish/subscribe middleware provides an important middleware capability by supporting the distribution of potentially high-volume, low latency data from anonymous servers to anonymous clients. Publish/subscribe middleware is widely used to support the development of systems that are highly extensible. Data distributed by a publish/subscribe middleware can be accessed by any application that declares itself a subscriber, thus making it easy to add new functionality without requiring the addition of new interfaces.

Although there are currently no widely accepted standards, some commercial products are available, including those that support real-time mission-critical applications. The OMG recently adopted the specification for the real-time Data Distribution Service (DDS), which is now publicly available for review [8]. Presently, the OMG is in the process of finalizing DDS as a formal publish-subscribe standard that is scheduled for release by early 2004.

4.8.3 Group Ordered Communication

Middleware support for building replicated, distributed applications is critical for an OACE. Group communications middleware provides effective support for building such applications. This is accomplished by providing higher levels of delivery guarantees, ordering of messages to help with maintaining consistency of state between replicated applications, and detection and handling of communications failures that are ordered with respect to the message flows. The latter feature enables applications to determine which communications activities were completed prior to a failure event or the start up of a new replica.

The most widely used group communications product is arguably Ensemble, developed by Cornell University. The Totem group communications middleware comprises a part of the CORBA-compliant Eternal fault tolerance product. Other group communications middleware products include RTCast (University of Michigan), Cactus (University of Arizona), and Spread (Johns Hopkins University).

No standards exist for group communications. No commercially produced products are available, either. The group communications products that are currently obtainable are generally open source, experimental products, developed by university researchers and maintained by dedicated developers, researchers, and/or users.

However, this class of middleware products is very important to building systems that provide seamless fault tolerance via application replication. The alternative to using a group communications middleware product is to build this essential but complex functionality into every state data-critical interface of a replicated application. Not only is this process labor-intensive, but it is prone to introducing defects into the application code as well. Thus, there is ample motivation to solve this specialized problem for the real-time community.

OMG is working to address this situation within the CORBA community. The OMG Fault Tolerant CORBA specification defines a fault tolerance capability that works in conjunction with the CORBA distributed object standard. This specification clearly states that group communications middleware is required as an underlying communications protocol if state-consistency of replicated objects is to be achieved. Recently, OMG has issued a Request for Proposals (RFP) for the development of a reliable ordered multicast communication protocol standard. Although this standard, when complete, will likely not fully replace a group ordered communications middleware, it will provide much of the critical functionality in a way that allows interoperability between implementations.

In view of the importance of this class of middleware in building reliable real-time systems that are fault tolerant and scalable, effort should be invested in assuring that this capability is available for use in the design and development of OACE. This may be accomplished via one or more of the following approaches.

- Work within the OMG community to encourage group ordered communication standardization within the CORBA envelope
- Develop an alternative strategy such as a higher level framework providing group ordered communication functionality on top of another middleware protocol class, e.g. CORBA or publish-subscribe
- Develop or adapt a Navy middleware solution that incorporates group ordered communication functionality

These three alternatives are listed in order of preference. Least preferred is the last one, the development of a custom solution for Navy use. However, this class of protocol is sufficiently important to justify selection of the third alternative if neither of the first two approaches proves to be viable.

4.8.4 Data Parallel

This class of distribution middleware is used primarily in parallel processing applications, such as signal processing. Products of this class are primarily intended for communication across the backplane of a massively parallel processor, although many products allow for communication across a network. Two standards exist, including Message Passing Interface (MPI) and Message Passing Interface - Real-Time (MPI-RT). Of these, MPI is clearly the most widely used.

Many implementations of MPI are available, including multiple open source products and commercially obtainable products from IBM, Hewlett-Packard, Critical Software, and MPI Software Technology. MPI-RT is not as mature as MPI and does not have a significant number of implementations. Also, a substantial niche of researchers in the parallel processing domain uses a data parallel software package, Parallel Virtual Machine (PVM), which is not compliant with either the MPI or MPI-RT standards.

The OMG has recently adopted a specification for Data Parallel CORBA, which is undergoing finalization. This specification is based on the most commonly used features of MPI. Implementations of Data Parallel CORBA are expected to be available in the next year.

4.8.5 Multiple Distribution Middleware Standards and Families

Computing technology innovation continues at a rapid pace. Thus, while standards exist within the overall computing community, the rapid pace of innovation means that standards themselves will evolve, albeit at a slower pace than the technologies they address. Furthermore, new standards appear and old standards disappear. For this reason, it is important to define a framework within which standards-based products may evolve and change over time. This phenomenon is a significant driver in devising systematic approaches to legacy capture and transition.

In addition, many widely divergent communities use computing products, ranging from business automation to real-time control systems. Because of this situation, multiple families of standards exist, and for each one there is a recognized domain of applicability. For this reason, it is necessary in selecting standards to specify to what problem space a particular standard is applied.

In the area of distribution middleware, several families of standards have evolved to meet the needs of a wide variety of user domains. Depending on use, each has a greater or lesser domain of applicability and therefore an inherent market share. Among the more likely families of standards for distribution middleware, both *de jure* (formal international standards body) and *de facto* (dominant vendor and/or large market share), the following distributed object models stand out as possibilities for OA application.

- DCOM - large market share distributed object technology driven almost exclusively by Microsoft; serves as *de facto* standard for business and non-real time decision analysis such as those that might be associated with mission planning.
- Java/RMI - large market share distributed object technology driven primarily by Sun Microsystems but maintained by a separate standards organization; broadly applicable to soft real-time display, human systems integration and decision aids as well as to business and other non-real-time applications.

Open Architecture Computing Environment Technologies and Standards

- CORBA – formal distributed object standard maintained by Object Management Group; suitable for soft real-time command and control, and hard real-time sensor control and weapons control.
- DDS – emerging real-time, data-centric, publish-subscribe standard for data distribution developed and driven by the Object Management Group; highly applicable for periodic transmission of hard real-time sensory and weapons data, as well as soft real-time command and control data.
- MPI - formal message-oriented standard for low latency message-based communication narrowly used for signal processing and other extremely low latency data parallel processes.

These product families and their most prominent domains of applicability are represented graphically in Figure 5.

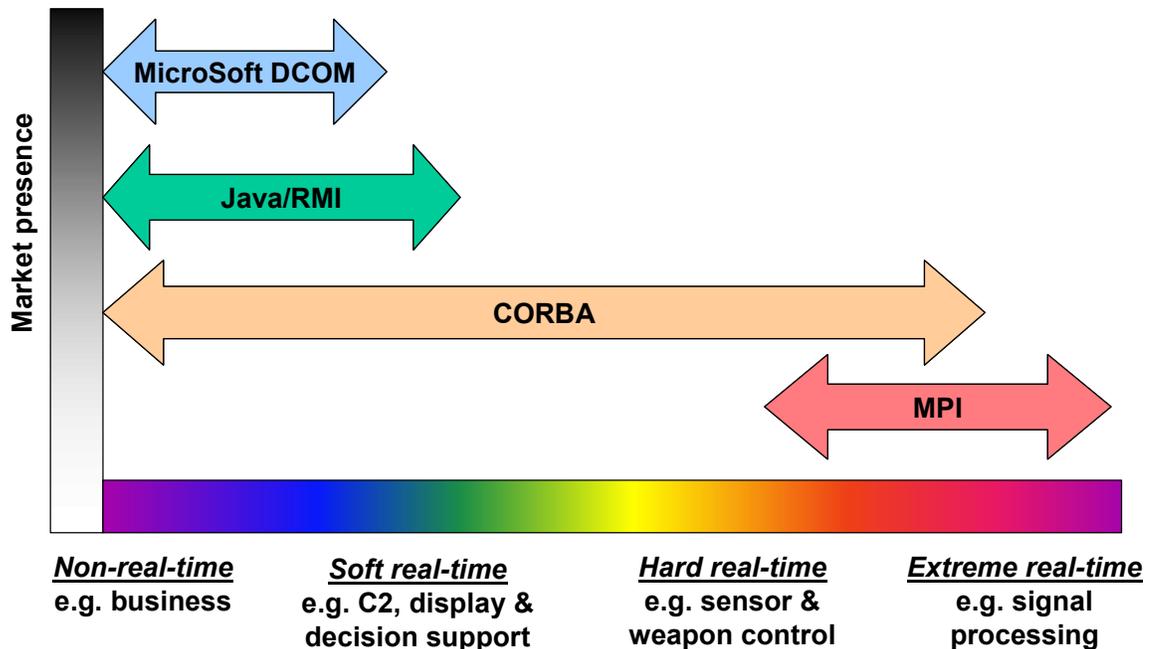


Figure 5. Families of Distribution Middleware

Given the likelihood that products adhering to multiple families of standards may appear in OA systems, and that the standards themselves may change over time, it is important to identify methods by which these differences may be systematically addressed and appropriate standards identified within the evolving versions of this OACE standards document. One such method is the use of bridges between products, a method that is widely used in some standards communities.

A key factor in making this strategy work is the selection of standards families that serve as integration technologies (i.e. those that support integration of disparate products) rather than those that are "displacement technologies" (i.e. those that displace other products). Products of the latter type force everything in a system to

conform to their model, an approach that is far too restrictive to serve as the basis for a program as broad as OA.

For the four families of products given above, Table 3 provides information concerning the current state of the art in bridging between these product families.

Table 3. Standards Bridging Technologies

	DCOM	Java/RMI	CORBA	MPI
DCOM	DCOM			
Java/RMI	Limited products available (i.e. J-Integra).	RMI		
CORBA	Multiple products available (e.g. IONA, Visual Edge).	Supported by OMG CORBA-Java Language Mapping Spec. Multiple products available (e.g. BEA, OMEX). Also, RMI over IIOP support in J2SE v1.3	Internet Inter-ORB Protocol (IIOP) – OMG Standard.	
MPI	No products available. Not likely to be required.	No products available. Not likely to be required.	No products available – OMG CORBA Data Parallel Spec may obviate need.	MPI messages

4.9 Frameworks

A framework is a reusable, tailor-able design in the form of code for all or part of a software system. For example, a user interface framework provides a design and code for the user interface of a system. A framework generally is an object-oriented design. It doesn't have to be implemented in an object-oriented language, though it usually is. Large-scale reuse of object-oriented libraries requires frameworks. The framework provides a context for the components in the library to be reused.

A framework middleware is a software implementation that provides some generic functionality to other applications through some means of instantiation or definition of application specific data and/or processing. Currently framework middleware technology support for mission critical and real-time applications is very limited. Examples of framework capabilities include event handling, scheduling, concurrency, and container support. Additionally, some languages (e.g. C++ STL and

Java) supply libraries that provide very rudimentary capabilities, such as containers and graphics interface support.

The current state of the practice in DoD is for contractors to develop framework middleware specifically targeted to a given tactical system's requirements and configuration. Framework products to support required capabilities of an OACE, such as fault tolerance, resource management, and security are not currently available. No standards for frameworks exist.

4.10 Information Management

Data management services facilitate sharing persistent data/objects across applications. Data management services to manage the lifecycle of data/objects include creation, reading, updating and deletion (CRUD). Data management services to manage the concurrent access to data/objects by multiple applications include transaction management, locking, versioning, and checkpointing. Collectively, these services are referred to as a database management system (DBMS).

There are currently three published DBMS standards supported by existing commercial and open source products that are applicable to the OACE: the ISO Structured Query Language (SQL) Object/Relational DBMS standards family and the Sun Java Community Process Java Data Objects (JDO) and Java Database Connectivity (JDBC) standards.

Early versions of SQL concerned only relational DBMSs with data organized into two-dimensional tables with rows of attributes of standard data types. SQL has evolved to include object-oriented capabilities such as user defined data types with object behavior provided by user-defined methods bound to those data types.

SQL also provides bindings to a large selection of programming languages and extensions that cover a wide variety of application areas.

JDO grew out of work started by the Object Database Management Group (ODMG) Java language binding. The ODMG standard addressed both C++ and Java bindings but wide industry acceptance and consistent implementations of the C++ bindings was not achieved for the C++ binding. The ODMG decided to cease work on the C++ binding and transfer its work on the Java binding to the Sun Java Community process where it was the starting point for the JDO standard.

JDO provides persistence of Java objects to either object-oriented or SQL-based datastores via an identical application program interface. JDO's transparent persistence mechanism (where persistent and transient objects are consistently manipulated with standard Java language constructs rather than using SQL for persistent objects and Java for transient objects) can reduce the complexity and code size for applications requiring object-oriented access to legacy relational databases. JDO is therefore complementary to SQL but limited to OA applications utilizing the Java programming language/environment.

JDBC provides a widely accepted standard interface to relational databases from the Java programming language/environment. JDBC may be preferable to JDO for OA applications that have less complicated data models than may warrant JDO or are leveraging COTS products, such as application servers, that utilize JDBC.

4.11 Resource Management

The resource management (RM) technology products can be separated into two distinct categories, static RM and dynamic RM. Static resource management provides for the manual and/or predefined startup, shutdown, allocation, and reallocation of software processes. Dynamic resource management provides for the automatic startup, shutdown, allocation, and reallocation of software processes based on some detected change (policy, performance, failure, etc.) in the system.

At present, there are no standards defined for either static or dynamic resource management technologies. There are several standards organizations working on business-oriented resource management-related standards, many of which are potentially applicable for niche areas within the scope of Open Architecture resource management. However, there are currently no encompassing resource management standards. Standards bodies currently involved with resource management-related standards include W3C (World Wide Web Consortium), DMTF (Distributed Management Task Force), and the IETF (Internet Engineering Task Force).

As examples, XML (eXtensible Markup Language), CIM (Common Information Model), and SNMP (Simple Network Management Protocol) are potentially applicable within various resource management sub-areas. In addition, there is ongoing work in the Java community, primarily J2EE (Java 2 Enterprise Edition), on standards for web and business application monitoring, fault recovery, and scalability; the applicability of these efforts will need to be periodically reassessed.

While there may be instances where static resource management products may be useful in an open architecture system, the more desirable products would be those that fit into the category of dynamic resource management. It is well to note that any dynamic resource management product will likely have the ability to be used as a static RM product if needed.

A dynamic RM product appropriate for an open architecture system should contain most, if not all, of the following features:

- application/process instrumentation
- operating system instrumentation
- network instrumentation
- system health monitoring
- resource and application control
- system and resource specifications (including structure, capabilities, and requirements)

- fault detection / fault isolation / fault recovery
- dynamic resource allocation

The technology of dynamic resource management is in its infancy. As mentioned previously, there is no single product that is both mature and complete in its coverage of the functions required for Navy real-time systems.

4.12 Security Services

In order to be consistent with commercial industry's current state of practice, the OA security services will be provided using a configuration of "system-high" enclaves of processors that will use accredited guard technologies (e.g., Radiant Mercury) to communicate between enclaves at different security levels. It is an OA goal to ensure that the OA application software is unaware of the security mechanisms used at lower layers to protect data and computing resources. Also, the current state of technology does not support a fully multi level security (MLS) architecture without using proprietary, non-accredited, vendor-specific products. OA will be actively monitoring the progress of the MLS efforts and be opportunistic in using such capabilities where needed (e.g., coalition warfare) as they obtain OA validation and DITSCAP accreditation.

For the purposes of the OACE, technologies that provide the infrastructure's security services have been placed in one of two broad categories: commercial best practice or data separation. The state of industry standards for the technology in each of these categories varies, with a substantial number of technologies having no industry standards.

4.12.1 DoD Policy Constraints

The selection of standards for each of the technologies is constrained by DoD policy. All DoD-owned or controlled information systems that receive, process, store, display or transmit DoD information, regardless of mission assurance category, classification or sensitivity must adhere to DoD Directive 8500.1[9].

DoD Directive 8500.1 "establishes policy and assigns responsibilities under reference (a) to achieve Department of Defense (DoD) information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare." DoD Directive 8500.1 does not apply to weapons systems, but it does apply to the interconnection of a weapons system to an external network.

4.12.2 Commercial Best Practice

Commercial best practice information security technologies are those that commercial industry has pursued and deployed to protect commercial assets. Examples of commercial best practice technology include firewalls, anti-virus software packages, and intrusion detection systems (IDS). There are no industry standards available for commercial best practice products. It is anticipated that

there will be OA guidance provided in the future for selecting commercial best practice products.

4.12.3 Data Separation

Data separation technologies provide a method to separate data with differing classification levels. Examples of data separation technologies include IP security; encryption algorithms implemented in hardware and/or software, and hardened or trusted operating systems. There is not a comprehensive set of standards that fully cover the data separation category. For example, there are no industry standards for a trusted operating system. However, there are a number of standards for cryptographic algorithms that are mandated by the OACE.

The classification level of the information to be protected will dictate the standard to be used. For classified information, it is DoD policy to acquire and use devices that implement Type 1 encryption. The vendors that provide these components are approved and certified by the National Security Agency. There are no standards available for Type 1 encryption algorithms.

4.13 Time Synchronization

Time synchronization for OACE is provided in accordance with a Common Time Reference Architecture. The requirement is to synchronize all time sources to UTC (USNO). OACE assumes the existence of a Common Time Reference that is synchronized to UTC (USNO) presumably via GPS with disciplined oscillators. The Network Time Protocol (NTP) and IRIG are the time standards used for the distribution and synchronization of time information within the platform. Three initial categories of products have been identified in the time synchronization area: NTP Servers, NTP client software and IRIG Time Interfaces.

4.14 Programming Languages

While numerous higher-level programming languages exist in industry and academia today, OA has selected two to provide the basis for all new development. These languages are Java and C++.

Java, developed by Sun Microsystems, has become so pervasive as to qualify as a *de facto* open standard. The Java standards evolve through the Java Community Process, where membership is open to anyone, but the characteristics of the language are defined in the reference identified in section 5.14 below. In order to legally qualify as Java (the *Java* trademark is owned by Sun), a vendor's product must conform to Sun's specification of the language, as well as to the Sun Java Virtual Machine (JVM).

C++, originally created by Bjarne Stroustrup and now defined in the C++ standard identified in section 5.14 below, added object-oriented programming features to the powerful and popular C programming language, of which it is a superset (therefore C++ compilers are capable of compiling C programs). While early C++

compilers often left much to be desired in terms of speed of the generated executable, modern compilers are capable of producing code whose performance rivals that from C compilers.

If C++ is used, compilers and libraries shall be used which conform to the listed specification.

Ada 95 is included in section 5.14 below, to support recent legacy use of software developed in Ada.

5 Standards and OACE Compliance Statements

It is the intention of the Navy that all OACE products be standards-based to the maximum extent possible. In order to help influence the industry in a standards direction contributory to meeting Navy requirements in technology areas critical to OA, OA should be an active participant in standards organizations. This document provides the computing standards required by OA. A primary source for the OACE standards is the JTA (Joint Technical Architecture). To the maximum extent possible, the OACE standards are to be the standards mandated by the JTA. In any case where a mandated JTA standard is inadequate for OACE, OA personnel will work with the JTA Development Group (JTADG) to resolve the issue. Such situations are therefore anticipated to be temporary conditions. In other cases, the JTA mandates standards not in the scope of OA and this document identifies technologies and standards out of the JTA scope (e.g. dynamic resource management, Publish-Subscribe middleware, physical media, ...). In these cases, the JTA and this document will differ.

Following the conventions established by the Open System Joint Task Force, if appropriate standards-based products are not available - and likewise if products in the process of standardization are not available - the next preference is given products with a widespread base of commercial support. Exceptions to this rule are considered appropriate when no standards based product is capable of providing needed performance.

OA identifies three types of standards "Mandatory", "Emerging" and "Guidance". The designations "Mandatory" and "Emerging" are derived from the JTA and have the same meaning in defining the status of OACE standards as these designations do in the JTA. These two designations are defined in JTA v4.0 section 1.6, which states:

"The mandatory standards in the JTA must be implemented or used by systems that have a need for the corresponding service areas. A standard is mandatory in the sense that if a service/interface is going to be implemented, it shall be implemented in accordance with the associated standard. If a required service can be obtained by implementing more than one standard (e.g., operating system standards), the appropriate standard should be selected based on system requirements."

And in JTA v4.0 section 1.4.1:

Open Architecture Computing Environment Technologies and Standards

“Emerging Standards” ... “description of standards that are candidates for possible addition to the JTA mandates.” ... “The purpose of listing these candidates is to help the program manager determine those areas likely to change in the near term (within three years) and suggest those areas in which “upgradability” should be a concern. The expectation is that emerging standards will be elevated to mandatory status when implementations of the standards mature. Emerging standards may be implemented, but shall not be used in lieu of a mandated standard.”

Standards with an OACE status of “Guidance” provide information that should be followed. Taking an approach different than that described within a referenced document with an OACE status of “Guidance” does not affect the OACE compliance of system, application or infrastructure. It is recommended that such exceptions be documented as a part of that provided during the system’s or component’s development.

The OACE compliance statements provided below are directed towards the following tactical developers:

- Infrastructure Component Suppliers
- Platform Infrastructure Integrators
- Tactical Software Developers

Table 4 provides a listing of the OACE Technology Areas that have a compliance statement and those currently without a compliance statement. Only the Technology Areas that have a compliance statement are considered in assessing whether a system has met OACE compliance.

Table 4. Technology Area OACE Compliance

Compliance Statements	No Compliance Statements
Physical Media	Enclosures
Information Transfer	Computing Resources
Operating Systems	Peripherals
Distribution Middleware	Adaptive Middleware
Information Management	Frameworks
Security Services	Resource Management
Time Synchronization	
Programming Languages	

The OACE is providing a common infrastructure for Naval warfighting system development. For this reason, it is critical not to use capabilities (whether from

standards, products, or services) not specified in this document that fall within a Technology Area with a compliance statement.

Within the compliance statements below: “**shall**” statements must be met and “**should**” statements must be met or rationale provided for an exception which needs to include the impact this exception will have on application software developed above the OACE infrastructure.

The standards provided at this time comprise the core of the OACE standards. In cases where standards are still under development, product selection is provided.. A change management process is being put in place for further developing the OACE Standards Set.

5.1 Physical Media

Shipboard fiber optic system design shall be in accordance with the Fiber Optic System Design Criteria Standard MIL-STD-2052 listed below.

The Fiber Optic Cable Topology (FOCT) should be developed and designed using the Fiber Optic Shipboard Cable Topology Design Guidance MIL-HDBK-2051 listed below.

The Fiber Optic Cable Topology (FOCT) shall be installed and tested in accordance with the Fiber Optic Cable Topology Installation Standard Methods For Naval Ships MIL-STD-2042 listed below.

All fiber optic physical media products/components used shall be in accordance with the OA physical media specifications listed below and those products/components listed in the “Navy Recommended Fiber Optic Components Parts List” 21 May 2003 [10] or latest version. All other physical media products/components shall be in accordance with the OA physical media specifications listed below.

All military or commercial fiber optic single terminus connectors used for equipment connections shall be housed within that equipment or interconnection box.

Copper cable shields shall be grounded by approved 360-degree grounding connectors at terminating equipment and enclosures, connection or junction boxes and at points of penetration into topside areas.

Physical Media Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
Fiber Optic System Design						
Fiber Optic System Design	Shipboard Fiber Optic System Design Requirements	MIL-STD-2052	Mandatory	NAVSEA	Published	No
Fiber Optic Topology Design Guidance						
Fiber Optic Shipboard Cable Topology Design Guidance	Shipboard Cable Plant Design	MIL-HDBK-2051	Guidance	NAVSEA	Published	No
Fiber Optic Topology Installation and Test Standards						
Fiber Optic Cable Topology Installation Standard Methods For Naval Ships	Shipboard Fiber Optic Installation Methods	MIL-STD-2042	Mandatory	NAVSEA	Published	No
Fiber Optic Cable Topology Installation Standard Methods For Naval Ships (Cables)	Shipboard Fiber Optic Cable Installation Methods	MIL-STD-2042-1	Mandatory	NAVSEA	Published	No
Fiber Optic Cable Topology Installation Standard Methods For Naval Ships (Equipment)	Shipboard Fiber Optic Equipment Installation Methods	MIL-STD-2042-2	Mandatory	NAVSEA	Published	No
Fiber Optic Cable Topology Installation Standard Methods For Naval Ships (Cable Penetrations)	Shipboard Fiber Optic Penetration Installation Methods	MIL-STD-2042-3	Mandatory	NAVSEA	Published	No
Fiber Optic Cable Topology Installation Standard Methods For Naval Ships (Cableways)	Shipboard Fiber Optic Cableway Installation Methods	MIL-STD-2042-4	Mandatory	NAVSEA	Published	No

Physical Media Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
Fiber Optic Cable Topology Installation Standard Methods For Naval Ships (Connectors and Interconnections)	Shipboard Fiber Optic Connector Installation Methods	MIL-STD-2042-5	Mandatory	NAVSEA	Published	No
Fiber Optic Cable Topology Installation Standard Methods For Naval Ships (Tests)	Shipboard Fiber Optic Installation Tests	MIL-STD-2042-6	Mandatory	NAVSEA	Published	No
Fiber Optic Cable Topology Installation Standard Methods For Naval Ships (Pierside Connectivity Cable Assemblies and Interconnection Hardware)	Fiber Optic Pierside Connectivity Installation Methods	MIL-STD-2042-7	Mandatory	NAVSEA	Published	No
Optical Fiber						
Fiber, Optical, Type I, Class I, Size IV, Composition A, Wavelength B, Radiation Hardened (Metric)	Multimode 62.5 Micron Optical Fiber	MIL-PRF-49291/6	Mandatory	DoD	Published	No
Fiber, Optical, Type II, Class 5, Size II, Composition A, Wavelength D, Radiation Hardened (Metric)	Singlemode Optical Fiber	MIL-PRF-49291/7	Mandatory	DoD	Published	No
Optical Fiber Cable						
Cable, Fiber Optic, Eight Fibers, Enhanced Performance, Cable Configuration Type 2 (OFCC), Application B (Shipboard), Cable Class SM And MM, (Metric)	Shipboard Eight-Fiber Cable	MIL-PRF-85045/17	Mandatory	DoD	Published	No

Physical Media Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
Cable, Fiber Optic, Four Fibers, Enhanced Performance, Cable Configuration Type 2 (OFCC), Application B (Shipboard), Cable Class SM And MM, (Metric)	Shipboard Four-Fiber Cable	MIL-PRF-85045/18	Mandatory	DoD	Published	No
Cable, Fiber Optic, Twenty Four, Thirty Three, And Thirty Six Fibers, Enhanced Performance, Cable Configuration Type 2 (OFCC), Application B (Shipboard), Cable Class SM And MM, (Metric)	Shipboard Thirty-Six Fiber Cable	MIL-PRF-85045/20	Mandatory	DoD	Published	No
Cable, Fiber Optic, Seven Tube, Blown Optical Fiber, Standard and Enhanced Performance, Cable Configuration Type 5 (Tube), Application B (Shipboard), Cable Class SM And MM, (Metric)	Shipboard Seven-Tube BOF Cable	MIL-PRF-85045/25	Mandatory	DoD	Published	No
Cable, Fiber Optic, One Tube, Blown Optical Fiber, Standard and Enhanced Performance, Cable Configuration Type 5 (Tube), Application B (Shipboard), Cable Class SM And MM, (Metric)	Shipboard Single-Tube BOF Cable	MIL-PRF-85045/26	Mandatory	DoD	Published	No

Physical Media Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
Cable, Fiber Optic, Six-Fiber Bundle, Blown Optical Fiber, Cable Configuration Type 1 (Buffered Fiber), Application B (Shipboard), Cable Class SM And MM, (Metric)	Shipboard Six-Fiber BOF Bundle	MIL-PRF-85045/27	Mandatory	DoD	Published	No
Cable, Fiber Optic, Nineteen Tube, Blown Optical Fiber, Standard and Enhanced Performance, Cable Configuration Type 5 (Tube), Application B (Shipboard), Cable Class SM and MM, (Metric)	Shipboard Nineteen-Tube BOF Cable	MIL-PRF-85045/28	Emerging	DoD	Draft	No
Single Terminus Connectors						
Connector, Fiber Optic, Single Terminus, Plug, Adapter Style, 2.5 Millimeters Bayonet Coupling, Epoxy	Shipboard Light Duty ST Single-Fiber Connector	MIL-C-83522/16	Mandatory	DoD	Published	No
Connector, Fiber Optic, Single Terminus, Adapter, Bayonet Coupling (ST Style), 2.5 Millimeter Diameter Ferrule, Bulkhead Panel Mount	Shipboard Light Duty ST Single-Fiber Connector Adapter	MIL-C-83522/17	Mandatory	DoD	Published	No
Commercial Intermateability Standards						
Fiber Optic Connector Intermateability Standard	COTS ST Dimensional Standard	TIA/EIA-604-2	Mandatory	Telecommunications Industry Association	Published	No

Physical Media Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
Fiber Optic Connector Intermateability Standard Type SC	COTS SC Dimensional Standard	TIA/EIA-604-3	Mandatory	Telecommunications Industry Association	Published	No
Fiber Optic Connector Intermateability Standard	COTS LC Dimensional Standard	TIA/EIA-604-10	Mandatory	Telecommunications Industry Association	Published	No
Multi Terminus, Heavy Duty Connectors						
Connectors, Fiber Optic, Circular, Plug and Receptacle Style, Multiple Removable Termini, General Specification For	Shipboard Heavy Duty Multifiber Fiber Optic Equipment Connectors	MIL-PRF-28876	Mandatory	DoD	Published	No
Connectors, Fiber Optic, Circular, Receptacle Style, Multiple Removable Termini, Screw Threads, Wall Mounting, Without Strain Relief, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Equipment Receptacle Connectors	MIL-PRF-28876/1	Mandatory	DoD	Published	No
Connectors, Fiber Optic, Circular, Plug Style, Multiple Removable Termini, Screw Threads, Without Strain Relief, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Cable Plug Connectors	MIL-PRF-28876/6	Mandatory	DoD	Published	No
Connectors, Fiber Optic, Circular, Plug Style, Multiple Removable Termini, Screw Threads, With Straight Strain Relief, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Cable Plug Connectors	MIL-PRF-28876/7	Mandatory	DoD	Published	No

Physical Media Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
Connectors, Fiber Optic, Circular, Plug Style, Multiple Removable Termini, Screw Threads, With 45 Deg. Strain Relief, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Cable Plug Connectors	MIL-PRF-28876/8	Mandatory	DoD	Published	No
Connectors, Fiber Optic, Circular, Plug Style, Multiple Removable Termini, Screw Threads, With 90 Deg. Strain Relief, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Cable Plug Connectors	MIL-PRF-28876/9	Mandatory	DoD	Published	No
Connectors, Fiber Optic, Circular, Plug Style, Multiple Removable Termini, Dust Cover, Screw Threads, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Cable Plug Dust Cover	MIL-PRF-28876/10	Mandatory	DoD	Published	No
Connectors, Fiber Optic, Circular, Receptacle Style, Multiple Removable Termini, Screw Threads, Jamnut Mounting, Without Strain Relief, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Equipment Receptacle Connectors	MIL-PRF-28876/11	Mandatory	DoD	Published	No
Connectors, Fiber Optic, Circular, Receptacle Style, Multiple Removable Termini, Dust Cover, Screw Threads, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Equipment Receptacle Dust Cover	MIL-PRF-28876/15	Mandatory	DoD	Published	No

Physical Media Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
Connectors, Fiber Optic, Circular, Plug And Receptacle Style, Multiple Removable Termini, Screw Threads, Straight Backshell, Strain Relief, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Connector Backshells	MIL-PRF-28876/27	Mandatory	DoD	Published	No
Connectors, Fiber Optic, Circular, Plug And Receptacle Style, Multiple Removable Termini, 45 Deg. Backshell, Screw Threads, With Strain Relief, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Connector Backshells	MIL-PRF-28876/28	Mandatory	DoD	Published	No
Connectors, Fiber Optic, Circular, Plug And Receptacle Style, Multiple Removable Termini, 90 Deg. Backshell, Screw Threads, With Strain Relief, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Connector Backshells	MIL-PRF-28876/29	Mandatory	DoD	Published	No
Connectors, Fiber Optic, Circular, Receptacle Style, Multiple Removable Termini, Screw Threads, Light Duty Backshell, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Equipment Receptacle Backshells	MIL-PRF-28876/30	Emerging	DoD	Draft	No
Connectors, Fiber Optic, Circular, Receptacle Style, Multiple Removable Termini, Screw Threads, EMI Retention Nut	Shipboard Heavy Duty Multifiber Fiber Optic Equipment Receptacle EMI Backshell	MIL-PRF-28876/31	Emerging	DoD	Draft	No
Optical Fiber Termini						

Physical Media Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
Termini, Fiber Optic, Connector, Removable, Environment Resisting, Class 5, Type II, Style A, Pin Terminus, Front Release, Ceramic Guide Bushing	Pin Termini for MIL-PRF-28876 Connectors	MIL-PRF-29504/14	Mandatory	DoD	Published	No
Termini, Fiber Optic, Connector, Removable, Environment Resisting, Class 5, Type II, Style A, Socket Terminus, Front Release, Ceramic Guide Bushing	Socket Termini for MIL-PRF-28876 Connectors	MIL-PRF-29504/15	Mandatory	DoD	Published	No
Boxes						
Interconnection Box, Fiber Optic, Metric, General Specification for	Shipboard Fiber Optic Interconnection Boxes	MIL-I-24728	Mandatory	DoD	Published	No
Interconnection Box, Fiber Optic, Submersible, 354 x 330 MM	One-Module Shipboard Fiber Optic Interconnection Box	MIL-I-24728/1	Mandatory	DoD	Published	No
Interconnection Box, Fiber Optic, Submersible, 308.4 X 609.6 MM	Two-Module Shipboard Fiber Optic Interconnection Box	MIL-I-24728/2	Mandatory	DoD	Published	No
Interconnection Box, Fiber Optic, Submersible, 406.4 X 863.6 MM	Three-Module Shipboard Fiber Optic Interconnection Box	MIL-I-24728/3	Mandatory	DoD	Published	No

Physical Media Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
Interconnection Box, Fiber Optic, Submersible, 101.6 X 177.8 MM	Small Shipboard Fiber Optic Interconnection Box	MIL-I-24728/4	Mandatory	DoD	Published	No
Interconnection Box, Fiber Optic, Submersible, 152.4 X 228.6 MM	Small Shipboard Fiber Optic Interconnection Box	MIL-I-24728/5	Mandatory	DoD	Published	No
Interconnection Box, Fiber Optic, Connector Patch Panel Module	ST Patch Panel for Shipboard One, Two, and Three Module Fiber Optic Interconnection Boxes	MIL-I-24728/6	Mandatory	DoD	Published	No
Enclosures for Electrical Fittings and Fixtures	General Purpose Tube Routing Boxes for BOF Cables	MIL-E-24142	Mandatory	DoD	Published	No
Blown Optical Fiber Components						
Plug, Tube Fitting, Blown Optical Fiber	Tube Fitting Plugs for BOF Tube Fittings	A-A-59728	Mandatory	DoD	Published	No
Furcation Units, Tube, Blown Optical Fiber	Furcation Units for BOF Tubes	A-A-59729	Mandatory	DoD	Published	No
Plugs, Tapered Tube, Blown Optical Fiber	Tube Plugs for BOF Tubes	A-A-59730	Mandatory	DoD	Published	No
Tube Fittings, Blown Optical Fiber	Tube Fittings/ Connectors for BOF Tubes	A-A-59731	Mandatory	DoD	Published	No
Copper Cable Topology Installation and Test Standards						

Physical Media Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
Electrical Plant Installation Standard Methods For Surface Ship And Submarines	Shipboard Copper Cable Installation Methods	DOD-STD-2003	Mandatory	DoD	Published	No
Shipboard Electrical/Electronic/Fiber Optic Cable; Remove, Relocate, Repair, And Install	Shipboard Installation and Test for Copper/Fiber Optic Cable	NAVSEA Standard Item Number 009-73	Mandatory	NAVSEA	Published	No
Commercial Building Telecommunications Cabling Standard, Part 2: Balanced Twisted Pair Cabling Components	Installation Testing For Category 5E Electrical Connectors/Cable	TIA/EIA-568B.2	Mandatory	Telecommunications Industry Association	Published	TBD
Copper Cable, Twisted Pair						
Cables, Light-Weight, Electric, Low Smoke, For Shipboard Use, General Specification For	General Specification for Shipboard Copper/Electrical Cable	MIL-C-24640	Mandatory	NAVSEA	Published	No
Cables And Cords, Electric, Low Smoke, For Shipboard Use, General Specification For	General Specification for Shipboard Copper/Electrical Cable	MIL-C-24643	Mandatory	NAVSEA	Published	No
Cable, Electrical, Type LSC5OS	Shipboard Category 5E Twisted Pair Cable	MIL-C-24643/59	Emerging	NAVSEA	Draft	No
Cable, Electrical, Local Area Network	Light Duty Commercial Category 5E Twisted Pair Cable	A-A-XXXXX	Emerging	NAVSEA	Draft	TBD
Connectors, Twisted Pair						

Physical Media Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
Connectors, Electrical, Circular, Screw Threads, High Shock, High Density, Crimp Contacts Receptacle, Jam Mounting, Class D and DS	Heavy Duty Shipboard Circular Electrical Connector	MIL-C-28840/14	Mandatory	DoD	Published	No
Connectors, Electrical, Circular, Screw Threads, High Density, High Shock, Shipboard, Crimp Contacts Plug, Class D and DS	Heavy Duty Shipboard Circular Electrical Connector Plug	MIL-C-28840/16	Mandatory	DoD	Published	No
Commercial Building Telecommunications Cabling Standard, Part 2: Balanced Twisted Pair Cabling Components	Light Duty Commercial RJ-45 Category 5E Electrical Connectors	TIA/EIA-568B.2	Mandatory	Telecommunications Industry Association	Published	TBD

5.2 Enclosures

There are no OA standards identified at the time for Enclosures. However, OA guidance, at this time, is to utilize the industry standard 19" (wide) rack mounting for installing COTS equipment aboard naval platforms. COTS products to be mounted in enclosures include computers, peripherals and Network switches. There are no vertical spacing requirements or recommendations provided at this time.

5.3 Information Transfer

All OACE components will require an information transfer capability. An information transfer capability is composed of numerous sub-components depending on the functionality required. Functionality choices include connectivity type (e.g. Gigabit Ethernet), basic and specialized transfers (e.g. SCTP), and support services required (e.g. FTP, telnet). Each sub-component capability shall be implemented in accordance with the applicable standards listed below. As a result, a individual instance of OACE will include a selected subset of the standards listed below based on the sub-component capabilities chosen.

Note: The Department of Defense has issued a directive regarding migration to IPv6. Some of the base specifications for IPv6 are included as emerging systems in the table below. Later editions of this document will more fully address the use of IPv6 in OACE based systems.

Information Transfer Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
Connectivity (Lower Layer) Protocols						
Fast Ethernet	100 Mbps half & full duplex over twisted pairs and optical fiber cables	IEEE Std 802.3-2002	Mandatory	IEEE 802	Standard	Yes, 3.2.2.2.1
Gigabit Ethernet	1,000 Mbps full duplex over twisted pairs and optical fiber cables	IEEE Std 802.3-2002 (originally IEEE 802.3z-1998)	Mandatory	IEEE 802	Standard	Yes, 3.2.2.2.6
10 Gigabit Ethernet	10,000 Mbps full duplex over optical fiber cables	IEEE 802.3ae-2002	Emerging	IEEE 802	Standard	
Aggregation of Multiple Link Segments	Provides for increased link availability and bandwidth by providing mechanisms for parallel link segment aggregation.	IEEE Std 802.3-2002 (originally IEEE 802.3ad-2000)	Mandatory	IEEE 802	Standard	No
Media Access Control Bridges	MAC Bridging, includes Spanning Tree Algorithm & Protocol	IEEE Std 802.1D, 1998 Edition (with amendment IEEE 802.1t-2001)	Mandatory	IEEE 802	Standard	Yes, 3.3.2.3
Traffic Class Expediting and Dynamic Multicast Filtering	This supplement, incorporated into IEEE 802.1D, 1998 Edition, defines additional capabilities for traffic class expediting and dynamic multicast address filtering.	IEEE Std 802.1D, 1998 Edition (originally IEEE 802.1p)	Mandatory	IEEE 802	Standard	Yes, 3.3.2.3
Virtual Bridged Local Area Networks	Defines the operation of Virtual LAN (VLAN) Bridges that permit the definition, operation and administration of Virtual LAN topologies within a Bridged LAN infrastructure.	IEEE 802.1Q-2003 (including IEEE 802.1u-2001, IEEE 802.1v-2001, IEEE 802.1s)	Mandatory	IEEE 802	Standard	Yes, 3.3.2.3

Information Transfer Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
Port-Based Network Access Control	A supplement to IEEE Std 802.1D, 1998 Edition. Defines the changes necessary to the operation of a MAC Bridge in order to provide Port based network access control	IEEE 802.1X-2001	Emerging	IEEE 802	Standard	No
Rapid Reconfiguration	A supplement to IEEE Std 802.1D, 1998 Edition. Defines the changes necessary to the operation of a MAC Bridge in order to provide rapid reconfiguration capability.	IEEE 802.1w-2001	Emerging	IEEE 802	Standard	No

Information Transfer Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
802.11b, WiFi	Wireless, local area networks in 2.4 GHz band.	(originally IEEE Std. 802.11b-1999)	Emerging	IEEE 802	Standard	Yes, 3.3.2.1
802.11a	Wireless, local area networks in newly allocated UNII, 5 GHz, band	(originally IEEE Std. 802.11a-1999)	Emerging	IEEE 802	Standard	Yes, 3.3.2.1
802.11g	Wireless, local area networks with higher speed(s) PHY extension to the IEEE 802.11b standard.	IEEE 802.11g	Emerging	IEEE 802	Standard	No
802.11i	Enhance the 802.11 Medium Access Control (MAC) to enhance security and authentication mechanisms.	IEEE 802.11i	Emerging	IEEE 802	Draft	No
Bluetooth RPR	Wireless Personal Area Networks	IEEE 802.15.1-2002 (Bluetooth v1.1)	Emerging	IEEE 802 and Bluetooth SIG	Standard	No
	Resilient Packet Ring	IEEE 802.17	Emerging	IEEE 802	Draft	No
Fibre Channel	High performance serial link supporting its own, as well as other, protocols at various speeds.	ANSI X3.230-1994 / AM 2-1996	Mandatory	ANSI, Fibre Channel Industry Association (FCIA)	Standard	Yes, C4ISR.3.2.2.1.1
SCSI	Small Computer System Interconnect, multiple versions	Numerous standards (including ANSI x3.131)	Mandatory	ANSI / NCITS T10 USB Implementers Forum	Standard	Yes, WS.GV.3.5.2, WS.MS.3.5.3, WS.MUS.3.5.2
USB	Universal Serial Bus, multiple versions	USB 2.0	Mandatory	USB Implementers Forum		No
Firewire	High performance serial bus communications	IEEE 1394-1995	Emerging	IEEE	Standard	Yes, C4ISR.3.2.2.1.2

Information Transfer Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
InfiniBand	Channel-based, switched fabric, interconnect architecture for servers.	InfiniBand 1.0.a	Emerging	InfiniBand Trade Association		No

Information Transfer Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
Transfer (Middle Layer) Protocols						
IP, also IPv4	Internet Protocol, version 4	RFCs 791, 950, 919, 922, 1112, 3168 (STD 5)	Mandatory	IETF	Standard	Yes, 3.2.1.2.2.1.3, 3.2.2.1.1
ICMP	Internet Control Message Protocol	RFCs 792, 950 (STD 5)	Mandatory	IETF	Standard	Yes, 3.2.1.2.2.1.3, 3.2.2.1.1
ARP	Address Resolution Protocol	RFC 826 (STD 37)	Mandatory	IETF	Standard	Yes, 3.2.2.2.1
IGMPv3	IGMP, version 3	RFC 3376	Mandatory	IETF	Proposed Standard	Yes, 3.2.1.2.2.1.3, 3.2.2.1.1
IP over Ethernet	Transmission of IP Datagrams over Ethernet Networks	RFC 894 (STD 41)	Mandatory	IETF	Standard	Yes, 3.2.2.2.1
RIPv2	Routing Information Protocol, version 2	RFC 2453 (STD 56)	Mandatory	IETF	Standard	No
TCP	Transmission Control Protocol	RFCs 793, 3168 (STD 7)	Mandatory	IETF	Standard	Yes, 3.2.1.2.2.1.1
UDP	User Datagram Protocol	RFC 768 (STD 6)	Mandatory	IETF	Standard	Yes, 3.2.1.2.2.1.2
OSPFv2	Open Shortest Path First, version 2	RFC 2328 (STD 54)	Mandatory	IETF	Standard	Yes, 3.2.2.1.2.1
BGP4	Border Gateway Protocol, version 4	RFCs 1771, 1772	Mandatory	IETF	Draft Standard	Yes, 3.2.2.1.2.2
PPP	Point to Point Protocol	RFCs 1661, 1662 (STD 51)	Mandatory	IETF	Standard	Yes, 3.2.2.2.2
VRRP	VRRP	RFC 2338	Emerging	IETF	Proposed Standard	No
MPLS	Multi-Protocol Label Switching	RFC 3031	Emerging	IETF	Proposed Standard	No
DVMRP	Distance Vector Multicast Routing Protocol	RFC 1075	Emerging	IETF	Experimental	No

Information Transfer Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
PIM - Sparse Mode	Protocol Independent Multicast - Sparse Mode	RFC 2362	Emerging	IETF	Experimental	No
PIM - Dense Mode	Protocol Independent Multicast - Dense Mode	IETF Draft	Emerging	IETF		No
RTP	Transport Protocol for Real-Time Applications	RFC 3550	Emerging	IETF	Draft Standard	Yes, 3.3.1.1
RARP	Reverse ARP	RFC 907 (STD 40)	Mandatory	IETF	Standard	No
IPv6	Internet Protocol, version 6	RFC 2460	Emerging	IETF	Draft Standard	Yes, 3.4.1.11
ICMPv6	ICMP, version 6	RFC 2463	Emerging	IETF	Draft Standard	Yes, 3.4.1.11
ND for IPv6	Neighbor Discovery for IPv6 (IPv6)	RFC 2461	Emerging	IETF	Draft Standard	Yes, 3.4.1.11
IPv6 Autoconfiguration	IPv6 Stateless Address Autoconfiguration	RFC 2462	Emerging	IETF	Draft Standard	Yes, 3.4.1.11
Addressing Architecture	Internet Protocol, Version 6 (IPv6) Addressing Architecture	RFC 3513	Emerging	IETF	Draft Standard	Yes, 3.4.1.11
Address Format	An IPv6 Aggregate Global Unicast Address Format	RFC 2374	Emerging	IETF	Draft Standard	Yes, 3.4.1.11

Information Transfer Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
Support (Upper Layer) Protocols						
DHCP	Dynamic Host Configuration Protocol	RFC 2131	Mandatory	IETF	Draft Standard	Yes, 3.2.1.2.1.7
Network Time Protocol (NTP) Version 3	Network Time Protocol (NTP) Version 3, Time Synchronization across a network	RFC 1305	Mandatory	IETF	Draft Standard	Yes 3.2.1.2.1.5
FTP	File Transfer Protocol	RFC 959 (STD 9)	Mandatory	IETF	Standard	Yes, 3.2.1.2.1.3
Telnet	Remote Terminal Protocol	RFCs 854, 855	Mandatory	IETF	Standard	Yes, 3.2.1.2.1.4
SMTP	Simple Mail Transport Protocol	RFCs 821, 1869, 1870	Mandatory	IETF	Standard	Yes, 3.2.1.2.1.1
RSVP	Resource Reservation Protocol	RFCs 2205, 2750	Emerging	IETF	Proposed Standard	Yes, 3.3.1.1
DNS	Domain Name System	RFCs 1034, 1035, 2136 (STD 13)	Mandatory	IETF	Standard	Yes, 3.2.1.2.1.2.3
SIP	Session Initiation Protocol	RFCs 3261, 3262, 3263, 3264, 3265	Emerging	IETF	Proposed Standard	Yes, 3.3.1.1
H.323	Packet-based Multimedia Communications Systems, version 2	ITU-T Recommendation H.323	Emerging	ITU		Yes, 3.3.1.1
Megaco	Gateway Control Protocol, version 1	RFC 3525	Emerging	IETF	Proposed Standard	Yes, 3.3.1.1
SNMP	Simple Network Management Protocol	RFC 1157 (STD 15)	Mandatory	IETF	Historic	Yes, 3.2.4.1
RMON	Remote Network Monitoring MIB, version 1	RFC 2819	Mandatory	IETF	Standard	Yes, 3.2.4.1
RMON2	Remote Network Monitoring MIB, version 2	RFC 2021	Mandatory	IETF	Proposed Standard	Yes, 3.3.5.2
HTTPv1.1	Hypertext Transfer Protocol, version 1.1	RFCs 2616, 2817	Mandatory	IETF	Draft Standard	Yes, 3.2.1.2.1.8.1
LDAPv3	Lightweight Directory Access Protocol, version 3	RFCs 2251, 3377	Mandatory	IETF	Proposed Standard	Yes, 3.3.1.1
RADIUS	Remote Authentication Dial-In User Service	RFCs 2865, 3575	Emerging	IETF	Draft Standard	Yes, 6.3.2.2.2.2

Information Transfer Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
SSHv2	Secure Shell, version 2	IETF Draft	Emerging	IETF		Yes, 6.3.3.2.1, CS.DTS.2.6.3.1
BOOTP	Bootstrap Protocol	RFCs 951, 2132, 1542, 3442	Mandatory	IETF	Draft Standard	Yes, 3.2.1.2.1.6
TFTPv2	Trivial File Transfer Protocol, version 2	RFCs 1350, 2347, 2348, 2349 (STD 33)	Mandatory	IETF	Standard	Yes, 3.2.2.1
DiffServ	Differentiated classes of service for Internet traffic	RFCs 2474, 3168	Emerging	IETF	Proposed Standard	No
SCTP	Stream Control Transmission Protocol	RFCs 2960, 3309	Emerging	IETF	Proposed Standard	No
FCIP	Fibre Channel over TCP/IP	IETF Draft	Emerging	IETF		No
iSCSI	Internet SCSI. Protocol to carry SCSI over IP networks	IETF Draft	Emerging	IETF		No
NFSv4	Network File System, version 4	RFC 3530	Emerging	IETF	Proposed Standard	No
NNTP	Network News Transfer Protocol	RFC 977	Mandatory	IETF	Proposed Standard	No
SNMPv3	Simple Network Management Protocol, version 3	RFCs 3411-3418 (STD 62)	Emerging	IETF	Standard	Yes, 3.3.5.1
MIB-II	Management Information Base for TCP/IP-based internets, MIB- II	RFC 1213 (STD 17)	Mandatory	IETF	Standard	Yes, 3.2.4.1
OSPFv2 MIB	MIB for OSPFv2	RFC 1850	Mandatory	IETF	Draft Standard	Yes, 3.2.4.1
MIB	MIB for Ethernet-like interfaces	RFC 1643 (STD 50)	Mandatory	IETF	Standard	Yes, 3.2.4.1

5.4 Computing Resources

There are no OA standards identified at the time for Computing Resources. However, OA guidance, at this time, is to construct OA systems using pools of commercially available commodity processors (e.g. PC based) able to perform server and/or client processing.

5.5 Operating Systems

Operating System compliance is based on implementing and using the key APIs from IEEE Std 1003.1-2001. When **real time** capabilities (as defined by IEEE Std 1003.13) are required, compliance is based on implementing and using the mandatory features of IEEE Std 1003.13 –1998 Profile 54. This profile selects features specified within IEEE Std 1003.1. As conformance tests are developed for the IEEE Std 1003.1-2001 and sufficient conformant products are available, it is OA's plan to replace the requirement from compliance to conformance to the mandatory features of IEEE Std 1003.13 Profile 54.

A new version of POSIX 1003.13 is presently under development and anticipated for release in 2004. OA will assess replacing the 1998 edition of this standard specified within the OS section with the updated standard when there is broad industry support for this new version.

The OA Operating System standards provide for implementations that utilize either general purpose or real-time operating systems. Below are the OA Operating System standards:

- For the Fully OACE Compliant compliance categories, an Operating System selected for use within a pool of processors shall be compliant with IEEE Std 1003.1-2001 [6]; Standard for Information Technology – Portable Operating System Interface (POSIX) Base Definitions (Issue 6), System Interfaces (Issue 6) and Shells and Utilities (Issue 6). OACE mandatory capabilities shall include the POSIX mandatory core facilities and the facilities to provide:
 - the POSIX Parent/Child Relationship Multiple Processing model (e.g. multiple POSIX processes, fork (), exec (), ...)
 - POSIX Signals
 - POSIX Threads
 - POSIX Timers
 - POSIX Message Queues
 - POSIX Semaphores
 - POSIX Shared Memory
- For the Fully OACE Compliant compliance categories, an Operating System selected for use within a pool of processors to support **real time** application requirements shall comply to the mandatory features of Profile 54 of the IEEE

Std 1003.13 –1998 [7], as applied to IEEE Std 1003.1-2001. In assessing OACE compliance for a particular system, application program, infrastructure or component, if that compliance is based on using this **real time** functionality, it must be called out within any assessment of their OACE compliance (e.g. a system is OACE Standards (Level 3) category, Version 1 compliant using the **real time** functionality).

- While the Operating System industry is presently developing POSIX 1003.1-2001 conforming products, there are not sufficient numbers of available products for OA to mandate this version of POSIX 1003.1. For this reason OACE compliance currently can be met via using an operating system **conformant** to the previous versions of this standard (ISO POSIX-1: 1996 and ISO POSIX –2: 1993). It is the intent of OA to remove this option in the future as the Operating System industry matures its POSIX 1003.1-2001 capabilities.
- For the Fully OACE Compliant compliance categories, Operating System selected should follow the guidance provided within IEEE Std 1003.0-1995; IEEE Guide to the POSIX Open System Environment (OSE).
- For the Fully OACE Compliant compliance categories, OS component suppliers providing additional features (i.e. APIs) beyond those of IEEE Std 1003.1 – 2001 (as described above) and/or POSIX 1003.13 Profile 54 (for **real time** usage) needed to utilize their products (e.g. in IO control and devices) shall be described in open (i.e. distribution unlimited) documentation.
- For the Fully OACE Compliant compliance categories, OS users (e.g. Middleware Developers and Application Developers) shall utilize the capabilities standardized by IEEE Std 1003.1 – 2001, as described above, wherever possible. **Real time** OS users shall utilize the mandatory items of POSIX 1003.13 Profile 54 wherever possible. Where additional functionality is needed (e.g. in IO control and devices) all instances of additional functionality shall be identified within the documentation developed (e.g. flagged within the source code) in order to support future re-use/porting of the software. Inappropriate usage of such additional functionality (e.g. using proprietary APIs where POSIX functionality is available) may result in the OACE non-compliance of the application.
- While the preferred OACE Operating System compliance approach is via the POSIX standards listed within this section, a second alternative is currently acceptable as the Linux community develops true POSIX capabilities. OA shall accept the use of the standard Linux equivalent functionality (e.g. Linux threads vs. POSIX threads, Linux signals vs. POSIX signals, ...) in place of the POSIX functionality. For each “pool of processors” implemented (or used) all processors must use the same functionality (either the POSIX or the Linux functionality). In assessing OACE compliance for a particular system, application program, infrastructure or component, if that compliance is based on using the equivalent

Open Architecture Computing Environment Technologies and Standards

Linux functionality it must be called out within any assessment of their OACE compliance (e.g. a system is OACE Standards (Level 3) category, Version 1 compliant using the Linux Operating System **real time** functionality). No special assessment qualification is required for a particular system, application program or infrastructure that utilize POSIX compliant functionality. It is the intent of OA to remove this option in the future as the Linux community matures its POSIX capabilities.

Operating Systems Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
IEEE Std 1003.1-2001 is a major revision and incorporates IEEE Std 1003.1-1990 (POSIX.1) and its subsequent amendments, and IEEE Std 1003.2-1992 (POSIX.2) and its subsequent amendments. *						
Base Definitions, Issue 6 1003.1Standard for Information technology - Portable Operating System Interface (POSIX)	Mandated Services	IEEE Std 1003.1 - 2001	Mandatory	IEEE	Standard	yes* - 2.3.3 references older version
System Interfaces, Issue 6 1003.1Standard for Information technology - Portable Operating System Interface (POSIX)	Mandated Services	IEEE Std 1003.1 - 2001	Mandatory	IEEE	Standard	yes* - 2.3.3 references older version
Shells and Utilities, Issue 6 1003.1Standard for Information technology - Portable Operating System Interface (POSIX)	Mandated Services	IEEE Std 1003.1 - 2001	Mandatory	IEEE	Standard	yes* - 2.3.3 references older version
Rationale (informative), Issue 6 1003.1Standard for Information technology - Portable Operating System Interface (POSIX)	Guidance	IEEE Std 1003.1 - 2001	Guidance	IEEE	Standard	yes* - 2.3.3 references older version
IEEE Guide to the POSIX Open System Environment (OSE)	Guidance	IEEE Std 1003.0 - 1995	Guidance	IEEE	Standard	No
IEEE Standard for Information Technology - Standardized Application Environment Profile - POSIX® Realtime Application Support	Environment Profiles	IEEE Std 1003.13 - 1998	Mandatory	IEEE	Standard	yes 2.2.2.1.7
IEEE Standard for Information Technology - Standardized Application Environment Profile - POSIX® Realtime Application Support	Environment Profiles	1003.13 - 200X	Emerging	IEEE	Emerging Std	No

Operating Systems Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
IEEE Guide for Developing User Open System Environment (OSE) Profiles	Guidance	IEEE Std 1003.23 - 199	Guidance	IEEE	Approved Publication of IEEE	No
IEEE Guide for defining an application program interface to device drivers.	Guidance	IEEE 1003.26-2003	Guidance	IEEE	Emerging Std	No
ISO POSIX-1: 1996: incorporates ISO/IEC 9945-1: 1996, Information Technology — Portable Operating System Interface (POSIX) — Part 1: System Application Program Interface (API) [C Language] (identical to ANSI/IEEE Std 1003.1-1996). Incorporating ANSI/IEEE Stds 1003.1-1990, 1003.1b-1993, 1003.1c-1995, and 1003.1i-1995.	Mandated Services	IEEE Std 1003.1 - 1996; ISO/IEC 9945-1: 1996	Mandatory (temporary optional alternative to IEEE Std 1003.1 - 2001)	IEEE & ISO/IEC	Standard	yes - 2.2.2.1.7 and 2.3.3
ISO POSIX-2: 1993: ISO/IEC 9945-2: 1993, Information Technology — Portable Operating System Interface (POSIX) — Part 2: Shell and Utilities (identical to ANSI/IEEE Std 1003.2-1992, as amended by ANSI/IEEE Std 1003.2a-1992).	Mandated Services	ISO/IEC 9945-2: 1993	Mandatory (temporary optional alternative to IEEE Std 1003.1 - 2001)	IEEE & ISO/IEC	Standard	yes - 2.2.2.1.7 and 2.3.3

5.6 *Peripherals*

There are no specific OA Peripherals standards identified at this time. ***Adaptive Middleware***

There are no specific OA standards identified at this time for adaptive middleware. However, OA guidance, at this time, is that adaptive middleware products selected for use should be based on the POSIX family of operating system standards. In addition it is preferable that the product allow for wide usage across many different platforms.

5.8 *Distribution Middleware*

Four types of distribution middleware are identified for OA usage: distributed objects, publish-subscribe protocols, group ordered communication protocols and message passing middleware for data parallel applications. At this time, only the distributed objects area has mature standards to identify. Interim approaches are provided for two of the other three areas.

For the Fully OACE Compliant compliance categories, the distribution middleware selected for use within a pool of processors to support application requirements shall meet the requirements provided in the following subsections. All application program message transfer shall be provided by the Distribution Middleware capabilities described below and not by the direct access of capabilities provided by other Technology Areas (e.g. Operating System sockets). Each of the following subsections covers a different functionality, only those functionalities required by a system needs to be implemented/used.

5.8.1 Distributed Objects

For the Fully OACE Compliant compliance categories, if distributed objects middleware is needed, the following are required for OACE compliance:

- The application shall use CORBA distributed objects middleware to meet all distributed objects middleware requirements other than interfaces to legacy systems.
- The application shall use a CORBA product that conforms to the standards specified.
- The application shall not make use of any proprietary (non-standard) features of the selected product(s).
- The application shall not make use of any optional CORBA parts of the CORBA standard, standardized CORBA services or facilities that are not specifically listed below.

5.8.2 Publish-Subscribe

For the Fully OACE Compliant compliance categories, if publish-subscribe middleware is needed, the system developer will select either the Real Time Innovations (RTI) NDDS Version 3.0m product or the Northrup Grumman/Thales

Splice Version 2.7 product.

OA has selected products since there is no mature standard for publish-subscribe distribution middleware. Since there are two mature products currently available that provide publish-subscribe functionality, the system developer may select the product that most closely meets his needs. Note that an implementation based on one product is not interoperable with implementations based on the other product.

As indicated below, there is an emerging standard in this area, Data Distribution Service (DDS), for which a standard is expected to be finalized in early 2004 by the OMG. The vendors developing the products selected have been the leaders in the development of OMG DDS. It is the intent of OA to remove reference to the products identified at this time, as the publish-subscribe community matures its products around the DDS standard.

In stating OACE compliance for a particular system or product, if publish-subscribe middleware is required, the product selected must be called out within any assessment of their OACE compliance (e.g. a system is OA Common Functions (Level 4) category, Version 1 compliant using the RTI NDDS publish-subscribe middleware).

5.8.3 Group Ordered Communications

There are no standards or products selected for Group Ordered Communications distribution middleware. This technology is deemed to be too immature for use in operational systems. As group ordered communications products and standards are developed this situation may change and OA may provide standards or interim products for use.

5.8.4 Message Passing Interface for Data Parallel Applications

If a data parallel application requires message passing interfaces, the following are required for OACE compliance:

- The application shall use middleware product(s) that are MPI/MPI-RT compliant, to the standards listed below, to meet all message passing for data parallelism middleware requirements other than interfaces to legacy systems.
- The application shall not make use of any proprietary (non-standard) features of the selected product.

Once the OMG standardizes a CORBA data parallel standard and commercial products are available, the following are required for OACE compliance:

- The application shall use a CORBA middleware to achieve its data parallelism requirements other than interfaces to legacy systems.
- The application shall use a CORBA product that conforms to the standards listed below.
- The application shall not make use of any proprietary (non-standard) features of the selected product.

Open Architecture Computing Environment Technologies and Standards

The application shall not make use of any optional CORBA parts of the CORBA standard, standardized CORBA services or facilities that are not specifically listed below.

Distribution Middleware Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
<u>DISTRIBUTED OBJECTS:</u>						
Common Object Request Broker Architecture (CORBA)	Interface Repository - chapter 10	formal/02-06-33	Mandatory	OMG	Standard	yes - version-2.3.1
Common Object Request Broker Architecture (CORBA)	CORBA Interoperability - chapter 12	formal/02-06-33	Mandatory	OMG	Standard	yes - version-2.3.1
Common Object Request Broker Architecture (CORBA)	General Inter-ORB Protocol - chapter 15	formal/02-06-33	Mandatory	OMG	Standard	yes - version-2.3.1
Common Object Request Broker Architecture (CORBA)	Portable Interceptors - chapter 21	formal/02-06-33	Mandatory	OMG	Standard	yes - version-2.3.1
Common Object Request Broker Architecture (CORBA)	Messaging - chapter 22	formal/02-06-33	Mandatory	OMG	Standard	yes - version-2.3.1
Common Object Request Broker Architecture (CORBA)	Fault Tolerant CORBA - chapter 23	formal/02-06-33	Mandatory	OMG	Standard	yes - version-2.3.1
Common Object Request Broker Architecture (CORBA)	Common Secure Interoperability - chapter 24	formal/02-06-33	Mandatory	OMG	Standard	yes - version-2.3.1
Real-Time CORBA Spec v1.1	Real-time CORBA	formal/02-08-02	Mandatory	OMG	Standard	yes (emerging)

Distribution Middleware Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
Minimum CORBA Spec v1.0	Minimum CORBA	formal/02-08-01	Mandatory	OMG	Standard	yes (emerging)
CORBA Data Parallel Spec	CORBA Data Parallel Spec	pending formalization	Emerging	OMG	pending formalization	no
CORBA Dynamic Scheduling Spec.	CORBA Dynamic Scheduling	pending formalization	Emerging	OMG	pending formalization	no
CORBA Extensible Transports	CORBA Extensible Transports	pending formalization	Emerging	OMG	pending formalization	no
CORBA Unreliable Multicast Spec	CORBA Unreliable Multicast	pending formalization	Emerging	OMG	pending formalization	no
CORBA Data Distribution	CORBA Data Distribution	in progress	Emerging	OMG	in progress	no
CORBA Reliable Ordered Multicast	CORBA Reliable Ordered Multicast	in progress	Emerging	OMG	in progress	no
<u>CORBA SERVICES:</u>						
Lifecycle Services Spec v2	Lifecycle Services	formal/02-09-01	Mandatory	OMG	Standard	no
Naming Service Spec, V2	Naming Service	formal/02-09-01	Mandatory	OMG	Standard	yes (earlier version v1.0)
Notification Service Spec, V1.0.1, Aug, 2002	Notification Service	formal/02-08-04	Mandatory	OMG	Standard	yes (earlier version v1.0)
Security Service Spec, V1.8, Mar, 2002	Security Service	formal/02-03-11	Mandatory	OMG	Standard	yes (earlier version v1.5)
Persistent State Service Spec, V2.0, Aug 1999	Persistent State Service	formal/02-09-06	Mandatory	OMG	Standard	yes (emerging)

Distribution Middleware Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
CORBA Component Model v3.0, Jun 2002	CORBA Component Model	formal/02-06-65	Mandatory	OMG	Standard	yes (earlier version v2.0)
CORBA FTAM/FTP Interworking Spec, v1.0, March 2002	CORBA FTAM/FTP Interworking	formal/02-03-13	Mandatory	OMG	Standard	no
CORBA Concurrency Service v1.0, Apr 2000	CORBA Concurrency Service	formal/00-06-14	Mandatory	OMG	Standard	no
Time Service Spec v1.1, May 2002	Time Service	formal/02-05-06	Mandatory	OMG	Standard	yes(earlier version v1.0)
Enhanced View of Time Spec, v1.1, May 2002	Time Service	formal/02-05-07	Mandatory	OMG	Standard	yes(earlier version v1.0)
Event Service Spec, v1.1, March 2001	Event Service	formal/01-03-01	Mandatory	OMG	Standard	yes(earlier version v1.0)
Externalization Service Spec, v1.0, May 2000	Externalization Service	formal/00-06-16	Mandatory	OMG	Standard	no
Transaction Service spec, v1.2.1, May 2001	Transaction Service	formal/01-11-13	Mandatory	OMG	Standard	yes(earlier version v1.1)
Trading Object Service Spec, v1.0, June 2000	Trading Object Service	formal/00-06-27	Mandatory	OMG	Standard	yes

PUBLISH
SUBSCRIBE:

Distribution Middleware Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
RT Publish Subscribe Wire Protocol Spec	RT Publish Subscribe Wire Protocol		Emerging	IETF	Draft	no
Data Distribution Specification for Real-Time Systems	CORBA Data Distribution	in progress	Emerging	OMG	in progress	no
<u>GROUP ORDERED COMMS:</u>						
NONE						
<u>MESSAGE PASSING for DATA PARALLEL APPS:</u>						
Extensions to the Message Passing Interface, July 1997	Message Passing Interface	MPI-2	Mandatory	MPI Forum	Standard	no
CORBA Data Parallel Spec	CORBA Data Parallel Spec	pending formalization	Emerging	OMG	pending formalization	no
<u>OTHER MESSAGE-ORIENTED MIDDLEWARE:</u>						
Extensible Markup Language (XML)	XML	XML 1.0 (Second Edition)	Mandatory	W3C	Standard	yes

5.9 Frameworks

There are no specific OA standards identified at this time for Frameworks.

5.10 Information Management

OA compliance in the area of information management consists of:

- Implementers shall use the SQL family of standards and/or the JDO or JDBC standards for the management of persistent data/objects as listed below.
- The SQL family of standards cited below covers a wide range of capabilities. Implementers should select a subset of those standards suitable for their applications and having wide industry acceptance and consistent implementations.
- The use of the Java related portions of the SQL family of standards and the JDO and JDBC standards, is limited to those OA applications utilizing Java.

Information Management Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
Structured Query Language (SQL)	Part 1: Framework (SQL/Framework)	ISO/IEC 9075-1:1999	Mandatory	ISO	Standard	Yes (emerging) 2.3.1
Structured Query Language (SQL)	On-Line Analytical Processing (SQL/OLAP)	ISO/IEC 9075-1:1999/Amd 1:2001	Mandatory	ISO	Standard	No
Structured Query Language (SQL)	Part 2: Foundation (SQL/Foundation)	ISO/IEC 9075-2:1999	Mandatory	ISO	Standard	Yes (emerging) 2.3.1
Structured Query Language (SQL)	On-Line Analytical Processing (SQL/OLAP)	ISO/IEC 9075-2:1999/Amd 1:2001	Mandatory	ISO	Standard	No
Structured Query Language (SQL)	Part 3: Call-Level Interface (SQL/CLI)	ISO/IEC 9075-3:1999	Mandatory	ISO	Standard	Yes (emerging) 2.3.1
Structured Query Language (SQL)	Part 4: Persistent Stored Modules (SQL/PSM)	ISO/IEC 9075-4:1999	Mandatory	ISO	Standard	Yes (emerging) 2.3.1
Structured Query Language (SQL)	Part 5: Host Language Bindings (SQL/Bindings)	ISO/IEC 9075-5:1999	Mandatory	ISO	Standard	Yes (emerging) 2.3.1
Structured Query Language (SQL)	On-Line Analytical Processing (SQL/OLAP)	ISO/IEC 9075-5:1999/Amd 1:2001	Mandatory	ISO	Standard	No
Structured Query Language (SQL)	Part 9: Management of External Data (SQL/MED)	ISO/IEC 9075-9:2001	Mandatory	ISO	Standard	Yes (emerging) 2.3.1
Structured Query Language (SQL)	Part 10: Object Language Bindings (SQL/OLB)	ISO/IEC 9075-10:2000	Mandatory	ISO	Standard	Yes (emerging) 2.3.1
Structured Query Language (SQL)	Part 13: SQL Routines and Types Using the Java TM Programming Language (SQL/JRT)	ISO/IEC 9075-13:2002	Mandatory (Applicable if Java is used)	ISO	Standard	No
Structured Query Language (SQL)	Remote database access for SQL with security enhancement	ISO/IEC 9579:2000	Mandatory	ISO	Standard	Yes (emerging) 2.3.1
Structured Query Language (SQL)	SQL multimedia and application packages -- Part 1: Framework	ISO/IEC 13249-1:2002	Mandatory	ISO	Standard	No
Structured Query Language (SQL)	SQL multimedia and application packages -- Part 2: Full-Text	ISO/IEC 13249-2:2000	Mandatory	ISO	Standard	No
Structured Query Language (SQL)	SQL Multimedia and Application Packages -- Part 3: Spatial	ISO/IEC 13249-3:1999	Mandatory	ISO	Standard	Yes (emerging) 2.3.1

Information Management Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
Structured Query Language (SQL)	SQL multimedia and application packages -- Part 5: Still Image	ISO/IEC 13249-5:2001	Mandatory	ISO	Standard	No
Structured Query Language (SQL)	SQL multimedia and application packages -- Part 6: Data mining	ISO/IEC 13249-6:2002	Mandatory	ISO	Standard	No
Java Data Objects (JDO)	Java object persistence to Object Oriented or Object/Relational Data Stores	Version 1.0:3/25/2002	Mandatory (Applicable if Java is used)	Sun, Inc. Java Community Process	Standard	No
JDBC 3.0 Specification	Java object persistence to Object/Relational Data Stores	Version: 3.0, December1, 2001	Mandatory (Applicable if Java is used)	Sun, Inc. Java Community Process	Standard	No

5.11 Resource Management

There are no OA standards identified at this time for Resource Management.

5.12 Security Services

All OA systems will need to address security services and determine the security services to be implemented (e.g. authentication, encryption). If a specific security service (e.g. authentication) is required and there is a standard for that service in the following list, that security service shall be implemented in accordance with the applicable standards listed below. Additionally,

- All DoD-owned or controlled information systems, other than weapon systems, that receive, process, store, display or transmit DoD information, regardless of mission assurance category, classification or sensitivity shall adhere to DoD Directive 8500.1 [9].
- Any conflict in OACE security standards with DoD Directive 8500.1 will be resolved by following the policy of Directive 8500.1.
- If security service technology requires an evaluation, all evaluations shall follow the Common Criteria process.

Security Services Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
The Common Criteria, version 2.1	Common Criteria to evaluate the security of IT systems	ISO/IEC 15408	Mandatory	ISO	Standard	Yes, 6.2
Security Requirements for Cryptographic Modules	Cryptographic modules that protect sensitive but unclassified data	FIPS 140-2	Mandatory	NIST	Standard	Yes, 6.2.3.1.1
Secure Hash Standard	Message authentication	FIPS 180-1	Mandatory	NIST	Standard	Yes, 6.2.3.1.1.1
Digital Signature Standard		FIPS 186-2	Mandatory	NIST	Standard	Yes, 6.2.3.1.1.1
Advanced Encryption Algorithm	Encryption of sensitive but unclassified data	FIPS 197	Mandatory	NIST	Standard	No
The Keyed Message Authentication Code	Message authentication	FIPS 198	Mandatory	NIST	Standard	Yes, Emerging, 6.3.3.2.1
The Directory: Authentication Framework	Format for certificates containing Public Key information	ITU-T Rec. X.509 Version 3	Mandatory	ITU	Standard	Yes, 6.2.3.1.1.2
Kerberos Network Authentication	Provides access control and authentication mechanisms for network devices	RFC 1510	Mandatory	IETF	Proposed Standard	Yes, 6.2.2.2.1

Security Services Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
Transport Layer Security	Security mechanisms (e.g., confidentiality) for TCP-based applications	RFC 2246	Mandatory	IETF	Proposed Standard	Yes, Emerging, 6.3.2.1.1
Transport Layer Security Extensions	Extensions to TLS (backwards compatible to RFC 2246)	RFC 3546	Mandatory	IETF	Proposed Standard	No (just published June 2003)
GSS-API	Provides a programming interface for various security services	RFC 2743	Mandatory	IETF	Proposed Standard	Yes, Emerging, 6.3.2.2.1
RADIUS	Access control for remote users (e.g., port authentication)	RFC 2865	Mandatory	IETF	Draft Standard	Yes, Emerging, 6.3.2.2.2.2
RADIUS Attributes for Tunnel Protocol Support IANA Considerations for RADIUS	To support compulsory tunneling	RFC 2868	Guidance	IETF	Informational	No
IANA Considerations for RADIUS	IANA for RADIUS Specifies the use of X.509	RFC 3575	Mandatory	IETF	Proposed Standard	No
Internet X.509 PKI Certificate and CRL	certificates for use in an Internet environment	RFC 3280	Mandatory	IETF	Proposed Standard	Yes, Emerging, 6.3.3.1.1.2.2

Security Services Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
Lightweight Directory Access Protocol Version 3	Specifies the use of LDAP services for X.509 certificates	RFC 3377	Mandatory	IETF	Proposed Standard	No (call out v2, but v2 is obsolete)
Security Architecture for the Internet	Specifies security services (confidentiality, authentication, integrity) for IP packets	RFC 2401	Mandatory	IETF	Proposed Standard	Yes, Emerging, 6.3.3.2.1
IP Authentication Header	Authentication services for IP packets	RFC 2402	Mandatory	IETF	Proposed Standard	Yes, Emerging, 6.3.3.2.1
IP Encapsulating Security Payload	Confidentiality services for IP packets	RFC 2406	Mandatory	IETF	Proposed Standard	Yes, Emerging, 6.3.3.2.1
Internet Security Association and Key Management	Key Management services for IP packets	RFC 2408	Mandatory	IETF	Proposed Standard	Yes, Emerging, 6.3.3.2.1
Port Authentication	Authentication services for ports on network devices	IEEE 802.1x	Mandatory	IEEE	Standard	No
Enhanced Security (for wireless)	Replacement for WEP	IEEE 802.11i	Emerging	IEEE	Draft (not yet released to public)	No

5.13 Time Synchronization

All OACE components will require time synchronization capability. All OACE components shall provide time synchronization capability using NTP implemented in accordance with the standard listed below. In the event that NTP does not meet mission requirements, an IRIG time synchronization service may be provided and shall be implemented in accordance with the standard listed below.

Time Synchronization Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
Network Time Protocol (NTP) Version 3	Time Synchronization across a network	RFC 1305	Mandatory	IETF	Draft Standard	Yes 3.2.1.2.1.4
IRIG Serial Time Code Formats, Format B (IRIG-B)	Time Synchronization via an I/F cable	IRIG STANDARD 200-98, IRIG-B	Mandatory	Range Commander's Council	Standard	Yes, mentioned in C4ISR.3.2.2.3

5.14 Programming Languages

For development of new software in OA:

- Either Java or C++ shall be used for new software development.
- Virtual machines used for execution of OA Java applications shall implement the Sun JVM specification listed below, corresponding to that JVM provided in Version 1.4 of the Java Development Kit (JDK), with any deviations from the specification clearly documented and rationales for said deviations provided. JVM vendors shall be required to make all reasonable efforts to maintain compatibility with Sun's JVM for Version 1.4 of the JDK.
- Java compilers used in OA application development shall be compatible with the Java Language Specification, as listed below.
- If C++ is used, compilers and libraries shall be used which are compatible with the specification listed below.
- Ada 95 shall not be used for new software development; its use shall be limited to supporting recent legacy applications. When Ada 95 is used, compilers, libraries and associated utilities shall be used which are compatible with the specification listed below.

The Programming Language standards are provided below.

Programming Languages Standards

<u>Standard Title</u>	<u>Purpose</u>	<u>Standard ID</u>	<u>OACE Status</u>	<u>Standards Organization</u>	<u>Standards Status</u>	<u>In JTA?</u>
<i>The Java Virtual Machine Specification, Second Edition</i>	Specification of the Java Virtual Machine (JVM)	Authors: Tim Lindholm, Frank Yellin; Copyright 1997-1999 by Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, CA 94303	Mandatory	Sun Microsystems (owns Java Trademark)	Standard	No
<i>The Java Language Specification, Second Edition</i>	Specification of the syntax and semantics of the Java programming language	Authors: James Gosling et al.; Copyright 2000 by Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, CA 94303	Mandatory	Sun Microsystems (owns Java Trademark)	Standard	No
<i>Programming Languages - C++</i>	Specification of the C++ Programming Language	14882:1998	Mandatory	ANSI/ISO/IEC	Standard	No
<i>Information Technology-Programming Languages-Ada</i>	Specification of the Ada 95 Programming Language	8652:1995	Mandatory	ISO/IEC	Standard	No

6 OACE Compliance Assessment

There are three types of OACE Compliance Assessments defined. These three types of assessments are covered in the following three subsections. All OACE compliance claims shall clearly identify which type of assessment (of the three) is being made.

A government program manager may make a claim of OACE compliance once that manager believes that all of the requirements for one (or more) of the three compliance assessment types described within this section have been met. A “Validated Claim” is one that has the concurrence of the PEO IWS Open Architecture Program Office. Validating a claim involves having a neutral party, under the direction of PEO IWS Open Architecture Program Office, verifying the specific claim. Validation of OACE assessment claims will be covered by a separate OA document.

6.1 OACE System Compliance Assessment

The over-all goal of the OACE development is to produce OACE Compliant systems for use aboard Navy platforms. An OACE compliant system is one with all application programs are compliant (as defined within Section 6.2) and whose infrastructures are also totally compliant (as described within Section 6.3). An OACE System may be composed of a number of OACE Infrastructures (computer pools) each of which may have different selections for the Technology Areas described within Section 5 of this document (e.g. RTI NDDS versus Splice publish-subscribe middleware).

6.2 OACE Application Program Compliance Assessment

An OACE compliant application program is a unit of software that can be run on an OACE Infrastructure (i.e. a pool of processors) that only requires the capabilities specified within Section 5 of this document for the Technology Areas that have OACE compliance statements. OACE compliant application programs are required to identify a specific Fully OACE Compliant compliance category they will run within. Note that the resource requirements of the Application Program must be identified in order to determine and configure the pool of computing that it will run over.

6.3 OACE Infrastructure Compliance Assessment

An OACE Infrastructure is an instantiation of a pool of computing which has been built to run OACE compliant application programs. An OACE compliant infrastructure is an instantiation of a pool of computing which meets all of the requirements described within Section 5 of this document AND which does NOT use any additional capabilities (whether from standards, products or services) from the Technology Areas that have OACE compliance statements.

To make a compliance claim, the OACE defined capabilities must not only exist, they must be configured to operate and perform the functions that they are intended as described in Section 5 of this document. For example the information transfer routing products usually have a number of routing protocols implemented; however, for the infrastructure to be OACE Infrastructure compliant, the OACE defined functions must be the only ones actively running (e.g. OSPFv2).

6.4 Documenting OACE Compliance Assessment Claims

A claim should be written based on the compliance statements in Section 5 of this document. All OACE compliance claims shall clearly identify which type of claim (i.e. system, application program or infrastructure) is being made. All OACE compliance claims referenced against this document shall identify a particular Fully OACE Compliant compliance category (or categories) supported (i.e. Level 3, 4 or 5). Any OACE compliance assessment claims referenced against this document for a system shall specifically identify any exceptions to OACE compliance requirements provided within Section 5 of this document.

An example of a system compliance assessment claim (i.e. for a system with one OACE Infrastructure) is: the XYZ fire control system is OA Common Functions (Level 4) category, OACE Version 1 compliant using the Linux Operating System **real time** functionality and the RTI NDDS publish-subscribe middleware.

6.5 OACE Infrastructure Components

For an OACE infrastructure to be fully compliant it must be built from components (e.g. network routers, computers, operating systems, ...) that implement all of the OACE standards applicable to each component and all components must be configured to use the standards. Such components that are capable of supporting OACE compliant capabilities are usually also capable of supporting proprietary capabilities. For this reason, components used to build an OACE infrastructure should neither be described nor claimed to be "OACE compliant" but rather "**fully OACE supportive**". The key issue is how such components are applied (e.g. configured or coded) to implement a specific infrastructure that determines whether that infrastructure is compliant or not. It is recommended that when a component is successfully used to build a compliant infrastructure that this be used to show by example that this component is fully OACE supportive.