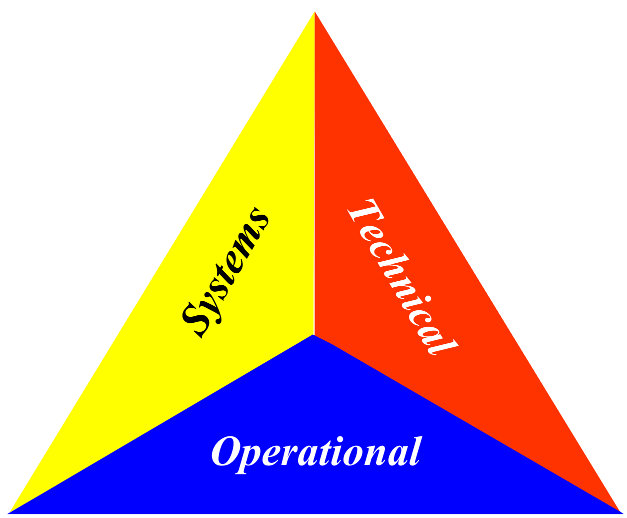
DoD Architecture Framework Working Group

DoD Architecture Framework Version 1.0



Volume I: Definitions and Guidelines

9 February 2004

TABLE OF CONTENTS

SECTION **PAGE**

TABLE OF CONTENTS (Cont)

TABLE OF CONTENTS (Cont)

LIST OF FIGURES

FIGURE **PAGE**

TABLE

EXECUTIVE SUMMARY

> **Architecture**: the structure of components, their relationships, and the principles and guidelines governing their design and evolution over time.
>
> DoD Integrated Architecture Panel, 1995, based on IEEE STD 610.12

The Department of Defense (DoD) Architecture Framework (DoDAF), Version 1.0, defines a common approach for DoD architecture description development, presentation, and integration for both warfighting operations and business operations and processes. The Framework is intended to ensure that architecture descriptions can be compared and related across organizational boundaries, including Joint and multinational boundaries.

This document applies to architectures developed by and for the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff (CJCS), the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as “the DoD Components”).

The Framework supports the development of interoperating and interacting architectures as referenced in DoD issuances. It defines three related views of architecture: Operational View (OV), Systems View (SV), and Technical Standards View (TV) as depicted in **Figure ES-1**. Each view is composed of sets of architecture data elements that are depicted via graphic, tabular, or textual products. The All-DoD Core Architecture Data Model (CADM) defines the entities and relationships for architecture data elements.

The Framework is partitioned into two volumes and a deskbook:

- Volume I provides definitions, guidelines, and related background material.
- Volume II contains descriptions for each product.
- The DoDAF Deskbook provides supplementary information to Framework users.

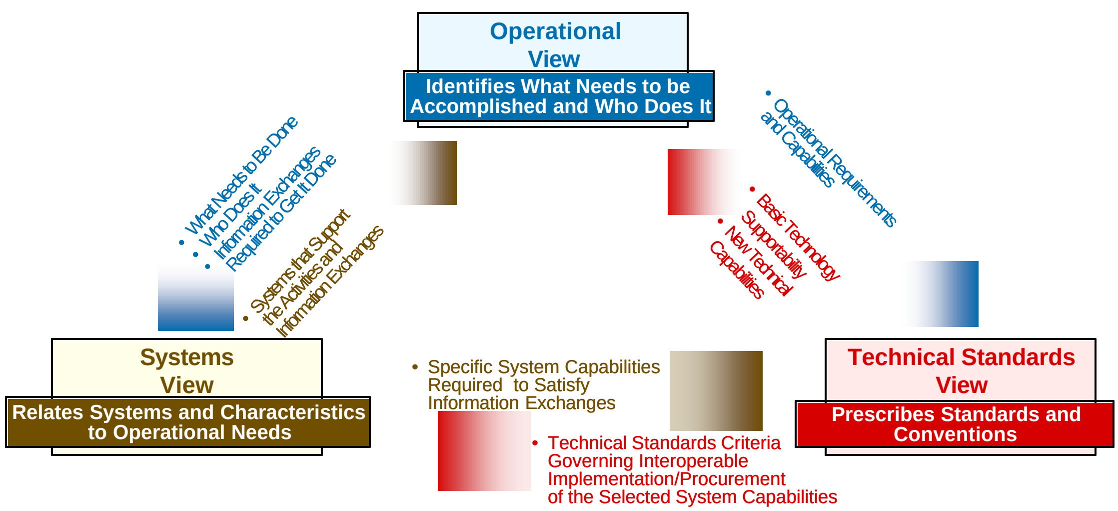


Figure ES-1. Linkages Among Views

Version 1.0 of the DoDAF is an evolution of the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Architecture Framework, Version 2.0, dated 18 December 1997, and supercedes it. This evolution reflects and leverages the experience that the DoD Components have gained in developing and using architecture descriptions. The most significant changes in this version of the Framework include guidelines on determining architecture content based on intended use; focus on using architectures in support of DoD's Programming, Budgeting, and Execution (PPBE) process; Joint Capabilities Integration and Development System (JCIDS); and the Defense Acquisition System; and increasing emphasis on the architecture data elements. Changes from the preceding C4ISR Architecture Framework, Version 2.0, are outlined on page ES-3.

As DoD moves toward Net-Centric Operations and Warfare (NCOW), architectures continue to provide a critical mechanism for understanding operational concepts and their relation to capabilities, anticipating changes in operational concepts or changes in automated capabilities, and acquiring both materiel and non-materiel assets. The DoD Components have made significant progress in using architectures. Examples of using architectures to support budgeting, identification of capability gaps, acquisition, and operations include the Air Force Task Force capability-based analysis, Navy's Mission Capability Package analysis approach, and OSD/Joint Staff concept of improving interoperability through focusing on key interfaces. Descriptions of the analytical techniques developed by each of these efforts are included in the Deskbook portion of the Framework.

The DoDAF, Version 1.0, was developed under the auspices of the DoDAF Working Group (AFWG), with review and comments from a broad spectrum of DoD Components. The Architecture and Interoperability Directorate of the Deputy Assistant Secretary of Defense (Chief Information Officer), under the Assistant Secretary of Defense for Networks and Information Integration[1] facilitated the coordinated development and evolution of the C4ISR Architecture Framework, Version 2.0, to the DoDAF, Version 1.0.

---

[1] The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence has been re-designated as the Assistant Secretary of Defense for Networks and Information Integration.

What's New in the DoD Architecture Framework, Version 1.0

Changes in the DoD Architecture Framework from its predecessor C4ISR Architecture Framework, Version 2.0

Changes are based on recommendations from the AFWG and community feedback on the C4ISR Architecture Framework, Version 2.0.

1. Document is restructured, with key guidance in Volume I, product descriptions in Volume II, and supplementary information in the Deskbook.

2. Guidelines are provided for product selection based on the intended use of the architecture. A minimum set of products necessary to comply with DoD instructions on integrated architectures is specified.

3. Document moves toward a repository-based approach by placing greater emphasis on architecture data elements comprising the products, not just architecture products. The following are provided:

    - An overview of the CADM
    - For each product, a table of architecture data elements associated with the product including attributes and definitions
    - For each product, an entity-relationship diagram of corresponding CADM entities
    - An introduction to the DoD Architecture Repository System
    - General information on automated tools

4. The Technical View has been retitled the Technical Standards View to provide a better description of the intent and content of the view. The acronym remains TV.

5. Product descriptions and graphics in Volume II have been refined for clarity and are provided in the following structured format:

    - Definition
    - Purpose
    - Detailed Description
        - Narrative, including definitions of architecture data elements
        - One or more generic templates, and/or examples
        - Equivalent representation using the Unified Modeling Language (UML)
        - Guidance on using the UML representation
    - Architecture Data Element table
    - Relevant CADM entities and relationships

6. An overview of DoD and Federal policies concerning architectures is provided.

7. Information has been added on the value of architectures, architecture measures, and use of architectures to support DoD processes.

8. Several techniques for developing architectures are provided in the Deskbook. These include:

   - Two architecture development processes
   - Example architectures developed using structured analysis, Unified Modeling Language, and Object-Oriented Methodology
   - Notional examples of selected products portraying NCOW
   - Representing the role of humans in architectures
   - Description of a Capability Maturity Profile
   - Representing Security/Information Assurance in architecture
   - Developing architecture descriptions at increasing levels of detail

9. Analytical techniques for using architecture products and architecture data elements to support DoD processes are described in the Deskbook. These include:

   - Air Force's Task Force capability-based analysis
   - Navy's Mission Capability Package analysis approach
   - Office of the Assistant Secretary of Defense for Networks and Information Integration/J6 Key Interface process for addressing interoperability at interfaces
   - Architecture input to C4I Support Plans
   - The role of architectures in Capital Planning and Investment Control

10. Additional information included in the Deskbook addresses:

   - CADM support of architectural concepts
   - Criteria and approach for assessing architecture tools
   - The Federal Enterprise Architecture reference models
   - Updated Universal Reference Resources

1 INTRODUCTION

"The Defense Science Board and other major studies have concluded that one of the key means for ensuring interoperable and cost-effective military systems is to establish comprehensive architectural guidance for all of DoD." [USD(A&T), ASD(C3I), J6, 1997]

1.1 PURPOSE AND SCOPE

The purpose of the Department of Defense (DoD) Architecture Framework (DoDAF), Version 1.0, is to provide guidance for describing architectures for both warfighting operations and business operations and processes. The Framework provides the guidance, rules, and product descriptions for developing and presenting architecture descriptions that ensure a common denominator for understanding, comparing, and integrating Families of Systems (FOSs), Systems of Systems (SoSs), and interoperating and interacting architectures. This DoDAF is an evolution of concepts introduced in the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Architecture Framework.[2] The DoDAF supercedes the C4ISR Architecture Framework.

> **Architecture**: the structure of components, their relationships, and the principles and guidelines governing their design and evolution over time
>
> DoD Integrated Architecture Panel,
> 1995, based on IEEE STD 610.12, 1990[3]

The Framework defines three views of an architecture description: Operational, Systems, and Technical Standards. Each view is composed of sets of architecture data elements that are depicted via graphic, tabular, or textual products. The All-DoD Core Architecture Data Model (CADM) defines the entities and relationships for architecture data. This document provides guidance on how to develop an architecture description that is comparable with other architectures developed according to this guidance. Guidance on how to use these architectures to facilitate coordination between requirements document developers, system acquirers and developers, and interoperability enforcers is beyond the scope of this document. However, supplemental information concerning the use of architectures is provided in the Deskbook.

This document applies to architectures developed by and for the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff (CJCS), the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components").

Section 2 provides highlights of some of the more important policy documents that have influenced architecture development within DoD.

---

[2] C4ISR Architecture Framework, Version 1.0, 7 June 1996, and Version 2.0, 18 December 1997.

[3] IEEE STD 610.22 in 1990 defined "architecture" as "the organizational structure of a system or component." In 2000, IEEE STD 1472 provided the following definition: "An architecture is the fundamental organization of a system embodied in its components, their relationships to each other, and to the environment and the principles guiding its design and evolution."

1.2 ARCHITECTURE DESCRIPTIONS

An architecture description is a representation of a defined domain, as of a current or future point in time, in terms of its component parts, what those parts do, how the parts relate to each other, and the rules and constraints under which the parts function. What constitutes each of the elements of this definition depends on the degree of detail of interest. For example, domains can be at any level, from DoD as a whole down to individual functional areas or groups of functional areas. Component parts can be anything from "U.S. Air Force" as a component of DoD, down to a "satellite ground station" as a component part of a communications network, or "workstation A" as a component part of system "x." What those parts do can be as general as their high-level operational concept or as specific as the lowest-level action they perform. How the parts relate to each other can be as general as how organizations fit into a very high-level command structure or as specific as what frequency one unit uses in communicating with another. The rules and constraints under which they work can be as general as high-level doctrine or as specific as the e-mail standard they must use.

The term *architecture* is generally used both to refer to an architecture description and an architecture implementation. Hereafter in this document, the term *architecture* will be used as a shortened reference to *architecture description*. Occasionally the term *architecture description* is used for emphasis. References to architecture implementations will use the term *architecture implementation*. An architecture description is a representation of a current or postulated "real-world" configuration of resources, rules, and relationships. Once the representation enters the design, development, and acquisition portion of the system development life-cycle process, the architecture description is transformed into a real implementation of capabilities and assets in the field. The Framework itself does not address this representation-to-implementation transformation process but references policies that are relevant to that process.

1.3 DEFINITIONS OF VIEWS

In the Framework, there are three major perspectives (i.e., views) that logically combine to describe an architecture description. These are the Operational View (OV), Systems View (SV), and Technical Standards View (TV). Each of the three views depicts certain architecture attributes. Some attributes bridge two views and provide integrity, coherence, and consistency to architecture descriptions.

1.3.1 Definition of the Operational View

The OV is a description of the tasks and activities, operational elements, and information exchanges required to accomplish DoD missions. DoD missions include both warfighting missions and business processes. The OV contains graphical and textual products that comprise an identification of the operational nodes and elements, assigned tasks and activities, and information flows required between nodes. It defines the types of information exchanged, the frequency of exchange, which tasks and activities are supported by the information exchanges, and the nature of information exchanges.

1.3.2 Definition of the Systems View

The SV is a set of graphical and textual products that describes systems and interconnections providing for, or supporting, DoD functions. DoD functions include both warfighting and business functions. The SV associates systems resources to the OV. These systems resources support the operational activities and facilitate the exchange of information among operational nodes.

1.3.3 Definition of the Technical Standards View

The TV is the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements. Its purpose is to ensure that a system satisfies a specified set of operational requirements. The TV provides the technical systems implementation guidelines upon which engineering specifications are based, common building blocks are established, and product lines are developed. The TV includes a collection of the technical standards, implementation conventions, standards options, rules, and criteria organized into profile(s) that govern systems and system elements for a given architecture.

1.3.4 Architectural Aspects that Concern All Views

There are some overarching aspects of architecture that relate to all three of the views. These overarching aspects are captured in the All-Views (AV) products. The AV products provide information pertinent to the entire architecture but do not represent a distinct view of the architecture. AV products set the scope and context of the architecture. The scope includes the subject area and timeframe for the architecture. The setting in which the architecture exists comprises the interrelated conditions that compose the context for the architecture. These conditions include doctrine; tactics, techniques, and procedures; relevant goals and vision statements; concepts of operations; scenarios; and environmental conditions.

1.4 DEFINITIONS OF PRODUCTS

Architecture products are those graphical, textual, and tabular items that are developed in the course of building a given architecture description and that describe characteristics pertinent to the purpose of the architecture. When used as part of an architecture description, all products, even those whose primary presentation is graphical, should contain explanatory text. For example, for graphical products, it is essential that any acronyms appearing in the graphic be spelled out and a definition of what they illustrate be included in the accompanying product text. The architecture products are listed in **Table 1-1**. A description of each product is provided in Volume II. Relationships among products are discussed briefly in section 3.3 and in more detail in Volume II.

Table 1-1. Architecture Products

Applicable View	Framework Product	Framework Product Name	General Description
All Views	AV-1	Overview and Summary Information	Scope, purpose, intended users, environment depicted, analytical findings
All Views	AV-2	Integrated Dictionary	Architecture data repository with definitions of all terms used in all products
Operational	OV-1	High-Level Operational Concept Graphic	High-level graphical/textual description of operational concept
Operational	OV-2	Operational Node Connectivity Description	Operational nodes, connectivity, and information exchange needlines between nodes
Operational	OV-3	Operational Information Exchange Matrix	Information exchanged between nodes and the relevant attributes of that exchange
Operational	OV-4	Organizational Relationships Chart	Organizational, role, or other relationships among organizations
Operational	OV-5	Operational Activity Model	Capabilities, operational activities, relationships among activities, inputs, and outputs; overlays can show cost, performing nodes, or other pertinent information
Operational	OV-6a	Operational Rules Model	One of three products used to describe operational activity—identifies business rules that constrain operation
Operational	OV-6b	Operational State Transition Description	One of three products used to describe operational activity—identifies business process responses to events
Operational	OV-6c	Operational Event-Trace Description	One of three products used to describe operational activity—traces actions in a scenario or sequence of events
Operational	OV-7	Logical Data Model	Documentation of the system data requirements and structural business process rules of the Operational View
Systems	SV-1	Systems Interface Description	Identification of systems nodes, systems, and system items and their interconnections, within and between nodes
Systems	SV-2	Systems Communications Description	Systems nodes, systems, and system items, and their related communications lay-downs
Systems	SV-3	Systems-Systems Matrix	Relationships among systems in a given architecture; can be designed to show relationships of interest, e.g., system-type interfaces, planned vs. existing interfaces, etc.
Systems	SV-4	Systems Functionality Description	Functions performed by systems and the system data flows among system functions
Systems	SV-5	Operational Activity to Systems Function Traceability Matrix	Mapping of systems back to capabilities or of system functions back to operational activities
Systems	SV-6	Systems Data Exchange Matrix	Provides details of system data elements being exchanged between systems and the attributes of that exchange
Systems	SV-7	Systems Performance Parameters Matrix	Performance characteristics of Systems View elements for the appropriate time frame(s)
Systems	SV-8	Systems Evolution Description	Planned incremental steps toward migrating a suite of systems to a more efficient suite, or toward evolving a current system to a future implementation
Systems	SV-9	Systems Technology Forecast	Emerging technologies and software/hardware products that are expected to be available in a given set of time frames and that will affect future development of the architecture
Systems	SV-10a	Systems Rules Model	One of three products used to describe system functionality—identifies constraints that are imposed on systems functionality due to some aspect of systems design or implementation
Systems	SV-10b	Systems State Transition Description	One of three products used to describe system functionality—identifies responses of a system to events
Systems	SV-10c	Systems Event-Trace Description	One of three products used to describe system functionality—identifies system-specific refinements of critical sequences of events described in the Operational View
Systems	SV-11	Physical Schema	Physical implementation of the Logical Data Model entities, e.g., message formats, file structures, physical schema
Technical	TV-1	Technical Standards Profile	Listing of standards that apply to Systems View elements in a given architecture
Technical	TV-2	Technical Standards Forecast	Description of emerging standards and potential impact on current Systems View elements, within a set of time frames

It is important to distinguish between an architecture view and an architecture product. As stated earlier, a view represents a perspective on a given architecture, while a product is a specific representation of a particular aspect of that perspective. Thus, a view consists of one or more products.

In the course of developing the products, one or more references, such as the Joint Technical Architecture and others, may be required to ensure that specific architectures are complete and in conformance with current policy and formal direction. These references are described in the DoDAF Deskbook under Universal Reference Resources.

1.5 DEFINITION OF AN INTEGRATED ARCHITECTURE

An architecture description is defined to be an *integrated architecture* when products and their constituent architecture data elements are developed such that architecture data elements defined in one view are the same (i.e., same names, definitions, and values) as architecture data elements referenced in another view. The term *integrated architecture* refers to an architecture description that has integrated Operational, Systems, and Technical Standards Views. That is, there are common points of reference linking the OV and the SV and also linking the SV and the TV. For example, SV-5 relates operational activities from OV-5 to system functions from SV-4; the SV-4 system functions are related to systems in SV-1, thus bridging the Operational and Systems Views.

Integrated architectures with Doctrine, Organization, Training, Materiel, Leadership & education, Personnel, and Facilities (DOTMLPF) information provide important tools to facilitate coordination between requirements document developers, planners, programmers, budgeters, system acquirers and developers, and interoperability enforcers. These architectures clarify roles, boundaries, and interfaces between components of large SoSs and influence participants in requirements generation, acquisition, resource allocation, interoperability enforcement, and waiver processes. Integrated architectures are the primary tool for enterprise-level systems integration.

An integrated architecture as referenced in DoDI 5000.2, DoDI 4630.8, CJCSI 3170.01, and CJCSI 6212.01 consists of AV-1, AV-2, OV-2, OV-3, OV-5, SV-1, and TV-1, at a minimum. Additional products should be developed for a given architecture description depending on the architecture's intended use. Section 3.6 contains a use matrix that provides guidelines for which additional products should be developed based on intended use.

1.6 HISTORY OF THE FRAMEWORK

In the mid 1990s with the increasing focus on joint and multinational operations, DoD realized the need for a common approach for describing architectures. Until that time, the individual Commands, Services, and Agencies in DoD traditionally described their architectures using techniques, vocabularies, and presentation schemes that suited their unique needs and purposes.

In October 1995, the Deputy Secretary of Defense directed that a DoD-wide effort be undertaken to define and develop better means and processes for ensuring that Command, Control, Communications, Computers, and Intelligence capabilities meet the needs of warfighters. In response to that direction, a C4ISR Integration Task Force (ITF) was established under the direction of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD[C3I]). The C4ISR Architecture Framework, Version 1.0, dated 7 June 1996, was developed as a product of the Integrated Architectures Panel (IAP), one of several panels established by the ITF.

In October 1996, the ASD(C3I) and Joint Staff/J6 established the C4ISR Architecture Working Group to continue the effort begun by the IAP. The effort resulted in the publication of the C4ISR Architecture Framework, Version 2.0, dated 18 December 1997. In February 1998, the Architecture Coordination Council, co-chaired by the Under Secretary of Defense for Acquisition and Technology (USD[A&T]), ASD(C3I), and Joint Staff/J6, published a memorandum mandating the use of Version 2.0 for all C4ISR architecture descriptions [USD(A&T), ASD(C3I), J6, 1997].

The utility of the C4ISR Architecture Framework, combined with both Federal and DoD policy encouraging the use of architectures, led DoD to evolve the document into the DoDAF in 2003. The DoD Chief Information Officer (CIO) established the Architecture Framework Working Group (AFWG) to accomplish this evolution under the direction of the Director, Architectures and Interoperability. The working group was composed of representatives of the Joint Staff, Military Services, and various DoD Components. This document is the result of the AFWG collaboration effort.

1.7 ORGANIZATION OF THIS VOLUME

The remainder of this document is organized in the following manner. Section 2 contains a brief discussion of the Federal and DoD policies that address architecture. Section 3 includes a product-by-use matrix that provides guidelines for determining products relevant to each of the DoD processes and provides a description of how the products relate to the process. Section 4 contains a brief overview of some techniques for using architectures in conducting analyses. Section 5 contains a description of architecture development guidelines and includes a set of guiding principles, DoDAF compliance guidelines, and a generic process for developing an architecture description. Section 6 consists of a discussion of the benefits of repository-based architectures, CADM as a specification of the architecture data model, the DoD Architecture Repository System (DARS) as a common repository for storing and retrieving architecture data, and automated tools. Section 7 describes some of the candidate areas for further evolution of the Framework.

Volume II contains a detailed discussion of each of the Framework products. Each product discussion includes a textual description and one or more generic templates or examples that illustrate the general format of the product. Each product discussion also defines the architecture data elements that need to be captured in that product and includes a CADM extract of relevant entities and relationships. The Unified Modeling Language representations are also provided.

A DoDAF Deskbook is provided as a companion to the Framework itself. The Deskbook provides example approaches for developing architectures and using architecture products and data elements, and provides information on architecture-related topics such as the selection of automated tool sets and Universal Reference Resources.

2 RELATED GOVERNMENT POLICY AND LEGISLATION

Several Federal, DoD, and Joint Staff policies influence the development of architecture descriptions throughout the DoD and the Intelligence Community. Aspects of these policies relating to architectures are highlighted below. This listing is not intended to be all inclusive, but rather representative.

2.1 FEDERAL POLICY

Federal policy, based on Congressional Acts and Office of Management and Budget (OMB) guidance, are a significant influence for DoD policy.

2.1.1 Clinger-Cohen Act of 1996

In 1996, recognizing the importance of information technology for effective government, the Congress and the President enacted the Information Technology Management Reform Act (ITMRA) and the Federal Acquisition Reform Act. These two Acts are known as the Clinger-Cohen Act (CCA), which focuses on the need for Federal Agencies to improve the way they select and manage information technology (IT) resources. The CCA states "information technology architecture, with respect to an executive agency, means an integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the agency's strategic goals and information resources management goals." Chief Information Officers are assigned responsibility for "developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the executive agency." The DoDAF grew out of this and related policies that identified the need for a unified architecture framework to be applied during the development of those architecture descriptions dictated by policy. See http://wwwoirm.nih.gov/policy/itmra.html for additional information on the CCA.

2.1.2 OMB Circular A-130

OMB provides guidance on the implementation of ITMRA in Management of Federal Information Resources, revision November 30, 2000, also known as Circular No. A-130 [OMB, 2000]. Guidance addresses both strategic and capital planning information resources management (IRM) by integrating the agency's IRM plans, strategic plans, performance plans, financial management plans, and budget process.

With regard to architectures, the Circular:

- Defines an Enterprise Architecture as 'the explicit description and documentation of the current and desired relationships among business and management processes and information technology'. The Enterprise Architecture includes principles, an Enterprise Architecture framework, a standards profile, current and target architectures, and a transition strategy to move from the current to target architecture.
- Directs agencies to create an Enterprise Architecture that should include the following parts:

– Business Processes

– Information Flows and Relationships

– Applications

– Data Descriptions and Relationships

– Technology Infrastructure

– Technical Reference Model

– Standards Profile

– Information Assurance

– Transition Strategy (for moving from the current state to the target architecture)

Figure 2-1 correlates the DoDAF's products with the architectural parts discussed in Circular No. A-130. Complete descriptions of each product are provided in Volume II. In any architecture effort, the specific products built are determined by the intended use of the architecture. Guidelines on products by use is provided in section 3.
See http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html#1 for the complete text of Circular No. A-130.

OMB Circular A-130 Reporting Requirements	Corresponding DoD Framework Products For Current Architecture and Target Architecture		
BUSINESS PROCESSES	Operational Node Connectivity Description (OV-2)	Operational Activity Model (OV-5) Organizational Relationships Chart (OV-4)	Operational Rules Model (OV-6a) Operational State Transition Description (OV-6b) Operational Event-Trace Description (OV-6c)
INFORMATION FLOWS & RELATIONSHIPS	High-Level Operational Concept Graphic (OV-1)	Operational Node Connectivity Description (OV-2)	Operational Information Exchange Matrix (OV-3)
APPLICATIONS	Systems Interface Description (SV-1)	Systems Functionality Description (SV-4) Operational Activity to Systems Function Matrix (SV-5)	Systems Rules Model (SV-10a) Systems State Transition Description (SV-10b) Systems Event-Trace Description (SV-10c)
DATA DESCRIPTIONS & RELATIONSHIPS	Systems Interface Description (SV-1)	Logical Data Model (OV-7) Physical Schema (SV-11)	Systems Data Exchange Matrix (SV-6)
TECHNOLOGY INFRASTRUCTURE	Systems Communications Description (SV-2)	Systems Performance Parameters Matrix (SV-7)	Systems-Systems Matrix (SV-3)
TECHNICAL REFERENCE MODEL	(Not a Framework Product, but a Universal Reference Resource Within the Framework)		
STANDARDS PROFILE (Including Security Standards)	Technical Standards Profile (TV-1)		
INFORMATION ASSURANCE	All		
TRANSITION STRATEGY	Systems Technology Forecast (SV-9) Technical Standards Forecast (TV-2)	Systems Evolution Description (SV-8)	Overview and Summary Information (AV-1)

Figure 2-1. Products Keyed to OMB Circular A-130

2.1.3 Federal Enterprise Architecture Reference Models

OMB is developing the Federal Enterprise Architecture (FEA), a business-based set of reference models for Government-wide improvement. The FEA is being constructed through a collection of interrelated reference models that facilitate OMB's cross-agency analysis and identification of duplicative investments, gaps, and opportunities for collaboration. **Figure 2-2** illustrates this set of reference models.

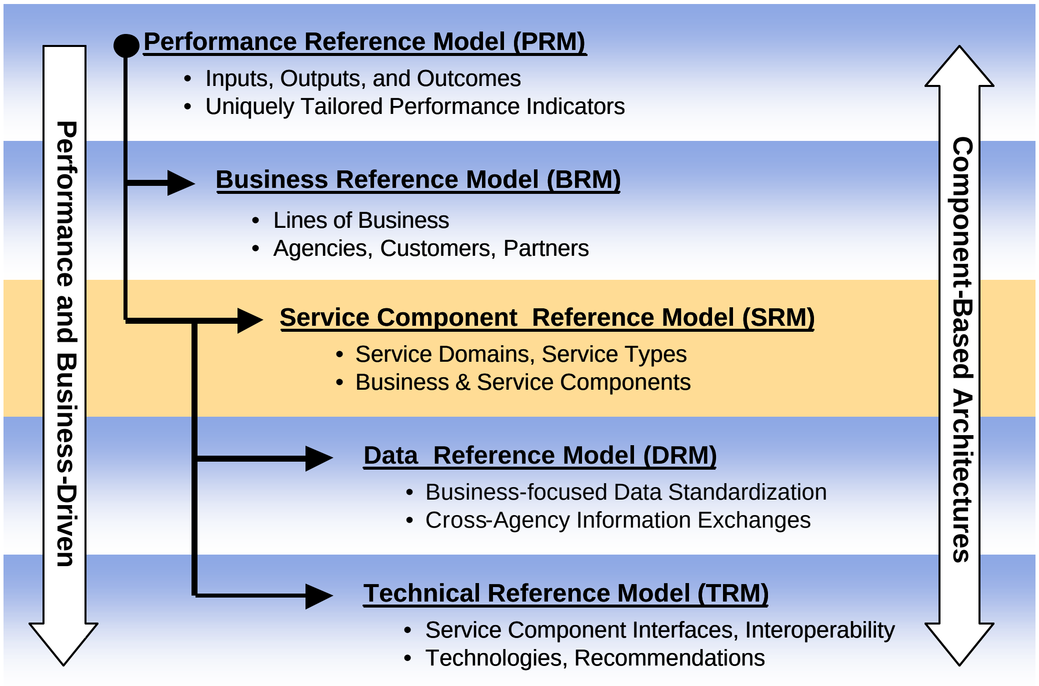


Figure 2-2. Federal Enterprise Architecture Reference Models

The Business Reference Model (BRM) serves as the foundation for the FEA. The BRM defines a structure of the Federal Government's lines of business, including operations and services for the citizen, independent of the organizations that perform them. All Federal organizations must map their internal lines of business and activities into one or more of these lines of business. Version 2 of the BRM, published in June 2003, is structured in terms of four business areas:

- Services for Citizens: Purpose of government
- Mode of Delivery: Mechanisms the government uses to achieve its purpose
- Support Delivery of Services: Support functions necessary to conduct government operations
- Management of Government Resources: Resource management functions that support all areas of the Government's business

As shown in **Figure 2-3**, each business area contains multiple lines of business. The Defense and National Security Operations line of business from Version 1.0 of the BRM has been replaced by three lines of business in Version 2.0: Defense and National Security, Homeland Security, and Intelligence Operations.

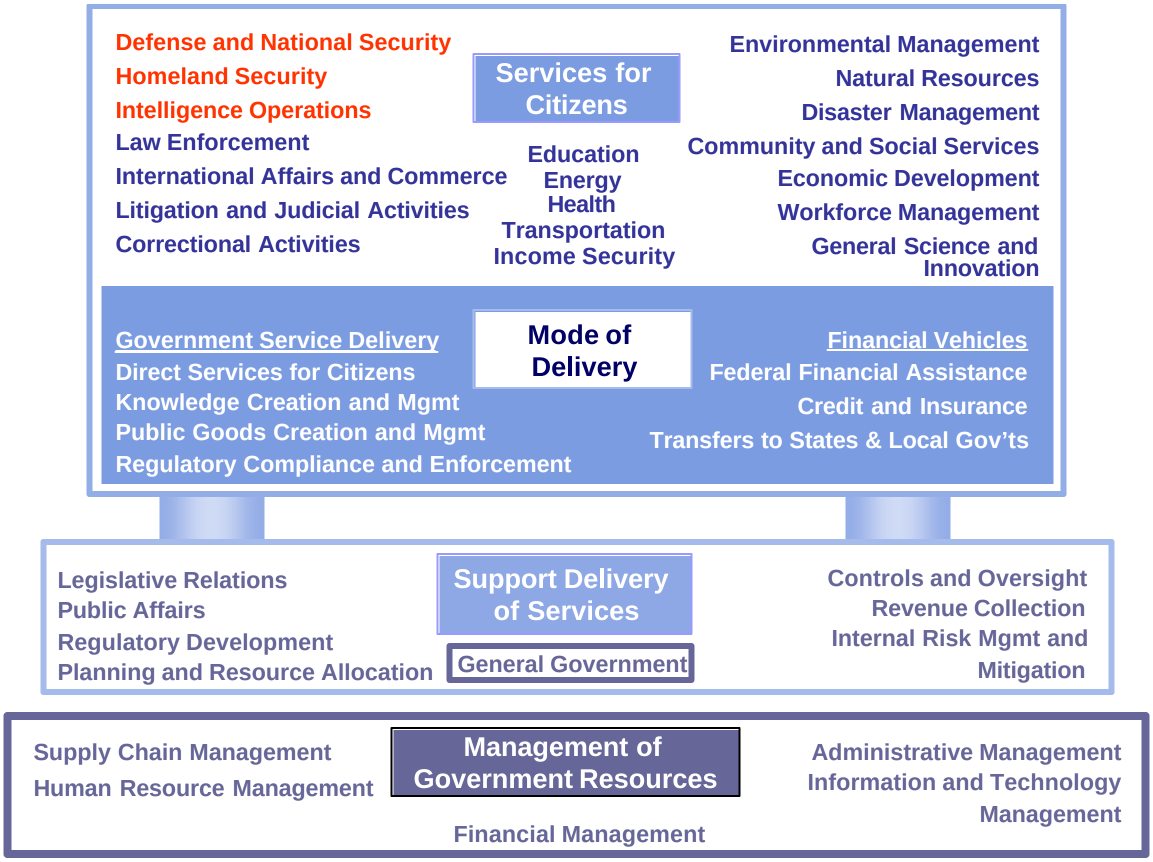


Figure 2-3. Federal Enterprise Architecture Business Reference Model Version 2.0

Version 1.0 of the Service Component Reference Model (SRM) and Technical Reference Model (TRM) were released in June 2003. The draft Performance Reference Model (PRM) was released in July 2003. A description of these reference models and additional information on FEA is provided in the Deskbook. The FEA Program Management Office Web site (http://www.feapmo.gov/) provides information on the FEA and associated reference models.

2.2 DOD POLICY

DoD has published several issuances since early 2002 that specifically address the use of architectures. DoD issuances are available at http://www.dtic.mil/whs/directives.

2.2.1 DoDD 4630.5

DoD Directive "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," January 11, 2002, directs the use of a mission-related, outcome-based approach that considers both materiel and non-materiel aspects to ensure interoperability and supportability of IT and NSS.

The directive establishes DoD policy that "IT and NSS interoperability and supportability requirements shall be characterized through operational mission area integrated architectures; operational concepts; and Capstone Requirements Documents derived from Joint Mission Areas (JMAs) and business/administrative mission areas. The Joint Operational Architecture (JOA), the Joint Systems Architecture (JSA), and the Joint Technical Architecture (JTA) shall serve as the foundation for development of mission area integrated architectures."

2.2.2 DoDI 4630.8

DoD Instruction "Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," May 2, 2002, implements updated policy and responsibilities as defined in DoDD 4630.5, implements an approach that considers both materiel and non-materiel aspects, and defines an outcome-based, mission-area focused process addressing interoperability. "Based on the JMAs, DoD Components shall develop mission area integrated architectures with Operational, Systems, and Technical Standards Views. Where appropriate, these architectures shall be further codified into Capstone Requirements Documents (CRDs) that consider both materiel and non-materiel aspects for fulfilling JMA requirements. The mission area integrated architectures are the common foundation for the IT and NSS interoperability and supportability process for acquisition, procurements, and fielded capabilities."

2.2.3 DoDD 5000.1

DoD Directive "The Defense Acquisition System," May 12, 2003, establishes management policies with a simple and flexible approach for managing all DoD acquisition programs. It establishes a process that focuses on improved integration of requirements and acquisition processes, evolutionary acquisition strategies, disciplined technology development, interoperability, supportability, and affordability. The directive specifies, "System concepts shall be founded in an operational context, consistent with the National Military Security Strategy, Defense Planning Guidance, Joint Concepts, and joint integrated architectures."

2.2.4 DoDI 5000.2

DoD Instruction "Operation of the Defense Acquisition System," May 12, 2003, implements DoDD 5000.1 and establishes a simplified and flexible management framework for translating mission needs and technology opportunities, based on approved mission needs and requirements, into stable, affordable, and well-managed acquisition programs that include weapon systems and automated information systems. The instruction defines how integrated architectures are to be used in the requirements and acquisition processes. Key statements referencing architectures are:

- "The Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD[AT&L]), the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)), the Joint Staff, the Military Departments, the Defense Agencies, Combatant Commanders, and other appropriate DoD Components shall work collaboratively to develop joint integrated architectures for capability areas as agreed to by the Joint Staff."
- "The DoD Chief Information Officer (CIO) shall lead the development and facilitate the implementation of the Global Information Grid Integrated Architecture, which shall underpin all mission area and capability architectures."
- "The integrated architectures will be used by the USD(AT&L) to lead the development of integrated plans or roadmaps. The Department of Defense shall

> use these roadmaps to conduct capability assessments, guide systems development, and define the associated investment plans as the basis for aligning resources and as an input to the Defense Planning Guidance, Program Objective Memorandum development, and Program and Budget Reviews."

2.2.5 DoDD 8000.1

DoD Directive "Management of DoD Information Resources and Information Technology," February 27, 2002 (Administrative Re-issuance, March 20, 2002), establishes policy for DoD IRM, including IT, and provides direction on establishing CIOs. The directive states that an integrated DoD architecture with Operational, System, and Technical Standards Views shall be developed, maintained, and applied to determine interoperability and capability requirements, promote standards, accommodate accessibility and usability, and implement security requirements across the DoD enterprise to provide the basis for efficient and effective acquisition and operation of IT capabilities.

2.2.6 DoDD 8100.01

DoD Directive "Global Information Grid (GIG) Overarching Policy," September 19, 2002, establishes policy and assigns responsibilities for GIG configuration management, architecture, and relationships with the Intelligence Community and Defense Intelligence Components.

GIG is defined as the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policymakers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), system data, security services, and other associated services necessary to achieve information superiority.

The GIG Architecture is established as the information technology architecture required by the CCA. Heads of DoD Components are assigned responsibility for ensuring that their architectures are developed and maintained compliant with the GIG Architecture.

The Assistant Secretary of Defense for Networks and Information Integration (ASD[NII]) as the DoD CIO, in consultation with the DoD CIO Executive Board, the USD (AT&L), and JS/J6, is responsible for developing, maintaining, and enforcing compliance with the GIG Architecture. The DoD CIO will direct the development of associated implementation and transition plans. The OSD Principal Staff Assistants (PSAs) must coordinate with the DoD CIO to ensure that architectures developed to meet the combat support and business needs of the PSAs accurately reflect and utilize current and planned common GIG assets. The Heads of the DoD Components must ensure that the DoD Component architectures are developed and maintained compliant with the GIG Architecture.

2.3 JOINT STAFF POLICY

Joint Staff directives, instructions, and manuals are available at http://www.dtic.mil/doctrine/doctrine.htm.

2.3.1 CJCSI 3170.01C

Chairman of the Joint Chiefs of Staff Instruction "Joint Capabilities Integration and Development System," June 24, 2003, establishes the policies and procedures of the Joint Capabilities Integration and Development System (JCIDS). JCIDS replaces the "Requirements Generation System" as defined in CJCSI 3170.01B, dated April 15, 2001. JCIDS is based on the need for a joint concepts-centric capabilities identification process. Initial Capabilities Documents (ICDs) replace Mission Need Statements as the initial documentation of mission capability needs in support of Milestone A. ICDs will eventually be based on integrated architectures. Capability Development Documents (CDDs) and Capability Production Documents (CPDs) replace Operational Requirements Documents. CDDs capture the information necessary to develop a proposed program and must be validated and approved before Milestone B. CPDs address production elements specific to a single increment of an acquisition program and must be validated and approved before Milestone C. This instruction sets the stage for transition to a process founded on joint concepts and integrated architectures. As integrated architectures are developed, they will provide the construct for analysis to identify capability shortfalls, compare alternatives for improving joint warfighting capabilities, and associated resource implications. Throughout the JCIDS process, proposals are evaluated to ensure they are consistent with National Security Strategy, Joint Operations Concepts, and integrated architectures.

2.3.2 CJCSM 3170.01M

Chairman of the Joint Chiefs of Staff Manual "Operation of the Joint Capabilities Integration and Development System," June 24, 2003, sets forth guidelines and procedures for the development and staffing of JCIDS documents and the operation of the JCIDS process. As part of the guidance on the conduct of JCIDS analyses, the manual addresses the use of integrated architectures to frame desired capabilities. Integrated architecture products must be included in mandatory appendixes for the ICD, CDD, and CPD.

2.3.3 CJCSI 6212.01C

Chairman of the Joint Chiefs of Staff Instruction "Interoperability and Supportability of National Security Systems, and Information Technology Systems," Draft June 2003, establishes policies and procedures for the J6 interoperability requirements certification and supportability of JCIDS. The instruction details a methodology to develop interoperability Key Performance Parameters derived from a set of top-level information exchange requirements and based on the format and content of the integrated architecture products described in the most current version of the DoDAF.

2.4 ORGANIZATION-SPECIFIC GUIDANCE

In addition to the broader scope instructions and regulations described above, there are organization-specific guidance documents that apply. Some examples are the Army Enterprise Architecture Guidance Document [DISC4, 1998], the Navy's Architecture Development Process Model [Department of the Navy, undated], and the Air Force Instruction 33-124 [Department of the Air Force, 2000], all consisting of adaptations of the C4ISR Architecture Framework, Version 2.0, or requirements to use the Framework. The National Reconnaissance Office (NRO) has developed its NRO Architecture Framework based on the C4ISR Architecture Framework, Version 2.0 [NRO, 2001]. The North Atlantic Treaty Organization (NATO) Command, Control, and Consultation (C3) Board has approved the Architecture Framework for C3 Systems, which is contained within the NATO Interoperability Management Plan, Volume II [NATO, 2000]. This NATO Framework includes many of the products from the C4ISR Framework and is mandatory for NATO C3 architecture development and use.

3 ARCHITECTURE USES

The DoD acquisition system has traditionally used a threat-based, force-planning construct to develop forces, systems, and platforms based on a specific threat and scenario. Requirements were often developed, validated, and approved as stand-alone solutions to counter those specific threats or scenarios, not as participating elements in an overarching system of systems. This approach fosters an environment in which DoD Components make acquisition decisions that, in a joint context, are not fully informed by, or coordinated with, other components. Proposed systems struggle through a budget process and acquisition pipeline that is inefficient, time consuming, and does not support interoperability. Additionally, acquisition management focuses solely on materiel solutions and does not adequately or fully consider the profound implications that changes in joint Doctrine, Organization, Training, Leadership & education, Personnel, and Facilities (DOTLPF) may hold for the advancement of joint warfighting. Piecemeal procurements of new and legacy systems result in less than optimal performance.

Defense Planning Guidance directs DoD to transition to a capability-based, force-planning construct. In contrast to the threat-based construct, a capability-based construct facilitates force planning in an uncertain environment by identifying the broad set of capabilities required to address the challenges of the twenty-first century. To accomplish this transition, DoD must implement a decision process that assesses legacy and proposed systems in the aggregate; defines desired joint capabilities; derives mission area requirements; validates these requirements; and considers the full range of Doctrine, Organization, Training, Materiel, Leadership and education, Personnel, and Facilities (DOTMLPF) solutions. To achieve substantive improvements in joint warfighting and interoperability in the battlespace of the future, coordination among DoD Components is essential from the start of the Joint Capabilities Integration and Development Systems (JCIDS) process. The decision process must be reformed to employ a synchronized, collaborative, and integrated systems engineering approach that better facilitates capability-based force planning.

Furthermore, as DoD enters into an era of Net-Centric Operations and Warfare, the ability to portray and understand complex many-to-many relationships becomes even more important. Capabilities must be able to "plug and play" in a Joint, global, multimedia, and multilingual environment. To achieve this ability, there must be a mechanism for incorporating information technology (IT) consistently, controlling the configuration of technical parts, ensuring compliance with technical "building codes," and ensuring efficient processes. Architectures provide this mechanism by serving as a means for understanding and managing complexity.

DoD and the Chairman of the Joint Chiefs of Staff instructions such as the Operation of the Defense Acquisition System [DoDI 5000.2, 2003], Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS) [DoDI 4630.8, 2002], JCIDS [CJCSI 3170.01, 2003]; and Interoperability and Supportability of National Security Systems, and Information Technology Systems [CJCSI 6212.01C, 2003], specify the use of integrated architectures to optimize warfighting and business capabilities. Volume II defines the products that allow the description of a capability-based integrated architecture. This section contains a description of the uses of the three views, defines some key product relationships, and provides guidelines on products by use. In the product-by-use matrix, rows are organized based on major DoD processes. The matrix columns delineate the products suggested as relevant to the use of an integrated architecture in conducting analysis critical to the process success.

3.1 REPRESENTATIVE USES OF THE THREE VIEWS

3.1.1 Use of the Operational View

The Operational View (OV) describes the tasks and activities necessary to successfully perform a mission, the participating nodes, and the associated information exchanges. OV descriptions are useful for facilitating numerous actions and assessments across DoD. These include examining business processes for reengineering or technology insertion, training personnel, examining doctrinal and policy implications, coordinating Joint and multinational relationships, and defining the operational requirements to be supported by resources and systems (e.g., communications throughput, specific node-to-node interoperability levels, information transaction time windows, and security protection needed).

OVs are generally driven by doctrine or emerging concepts. However, in some cases, external forces compel an organization to operate in a way that is not reflective of doctrine or defined concepts. In those cases, it may be useful to build an architecture description that shows how the organization actually operates, so its operations can be analyzed and a way can be found either to make the operations reflective of doctrine or defined operations concepts or to present a case to change doctrine or the defined operations concepts. In some cases, actual (i.e., current) operations cannot be conducted strictly in conformance with current policy because of inefficiencies induced, for example, by lack of supporting infrastructure or node and information exchange degradation resulting from threat forces, denial of service, or acts of nature.

A pure OV is materiel independent. However, operations and their relationships may be influenced, or pushed by new capabilities such as collaboration technology, where process improvements are in practice before policy can reflect the new procedures. There may be some cases, as well, in which it is necessary to document the way processes are performed given the restrictions of current systems, in order to examine ways in which new systems could facilitate streamlining the processes. In such cases, an OV may have materiel constraints and requirements that must be addressed. For this reason, it may be necessary to include some high-level Systems View (SV) products or architecture data elements as overlays to augment information onto the OV products.

OVs can describe activities and information exchanges at any level of detail and to any breadth of scope that is appropriate for the use or purpose at hand. It may be necessary to show only broad operational activities, in which case the information exchanges would be depicted at a commensurately high level. At a lower level of detail, if articulating interoperability distinctions and requirements is the focus, it may be necessary to show specific node-to-node information exchanges and the details of the exchanges. At an even lower level of detail, for other purposes, it may be necessary to show how specific information supports a specific organizational unit during particular circumstances (such as how specific information supports the Theater Joint Intelligence Center during a certain type of contingency in the Southwest Asian Theater or how specific information assists a logistics re-supply organization during adverse weather conditions).

An important point to make here is that often the OV degree of granularity should be driven by the type of analysis or assessments that are of interest. Because examination of current and postulated solution characteristics must be performed in context with operational missions and requirements in order to have real meaning, the nature of the planned analysis dictates which operational requirements attributes need to be articulated. **Figure 3-1** illustrates this point.

■ = Minimum level of analysis required

Degrees of Operational View Granularity	Types of Systems Analysis Planned (Examples): Node/system relationships and trade-offs	System-to-system interoperability assessments	Supporting infrastructure assessments and alternatives	Information and data provisioning standardization, integration
Starting Point ... • General processes and relationships • Needs for information	■			
Plus ... • Processes decomposed to specific activities • Information flows and attributes such as timeliness are specified, • Required level of interoperability defined for each needline		■		
Plus ... • Supporting security requirements and supporting communications quality, quantity, and timeliness requirements			■	
Plus ... • Information decomposed into data structures and data elements				■

Figure 3-1. Operational Architecture Granularity Required for Systems Analyses

3.1.2 Use of the Systems View

As used in the Framework, "system" is defined as "any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions." In the context of the Framework, a "system" may be partially or fully automated.

The Systems View (SV) describes the systems of concern and the connections among those systems in context with the OV. The SV may be used for many purposes, including systems baselining, making investment decisions concerning cost-effective ways to satisfy operational requirements, and evaluating interoperability improvements. An SV addresses specific technologies and "systems." These technologies can be existing, emerging, planned, or conceptual, depending on the purpose of the architecture effort (e.g., reflection of the current state, transition to a target state, or analysis of future investment strategies).

For many purposes, an SV will need to further detail the information exchanges described in the OV in order to translate node-to-node exchanges into system-to-system transactions, communications capacity requirements, security protection needs, and so forth. For other purposes, it may be necessary to break these system-to-system exchanges down into the system functions that support the production and transmission of specific system data elements of those exchanges. For the latter case, a data model at a corresponding level of detail would be useful, specifically one that includes the system data elements and their attributes and relationships.

3.1.3 Use of the Technical Standards View

The Technical Standards View (TV) describes a profile of the minimal set of time-phased standards and rules governing the implementation, arrangement, interaction, and interdependence of systems. The appropriate use of the TV is to promote efficiency and interoperability and to ensure that developers can adequately plan for evolution.

There are a number of existing technical references such as the Joint Technical Architecture [DISA, 2002]; the Levels of Information Systems Interoperability [C4ISR AWG, 1998]; and numerous policies, directives, and conventions in addition to Service-level and Agency-level technical architectures. In many cases, an effort to develop a TV consists of extracting the portions of these sources that are applicable to the scope of the architecture description being developed and tailoring their guidance to the purpose at hand.

With respect to system-to-system interoperability, the TV delineates the technical implementation criteria or "rules" with which the system(s) should comply as reflected in the SV.

3.2 LINKAGES AMONG THE VIEWS

The high-level operational concept should drive the OV. The OV in turn drives the SV to identify shortfalls and systems requirements. The SV requirements drive the TV to address a common set of applicable standards. To be internally consistent and integrated, an architecture description must provide explicit linkages among its various views. **Figure 3-2** illustrates some of the primary linkages that describe the interrelationships among the three views.

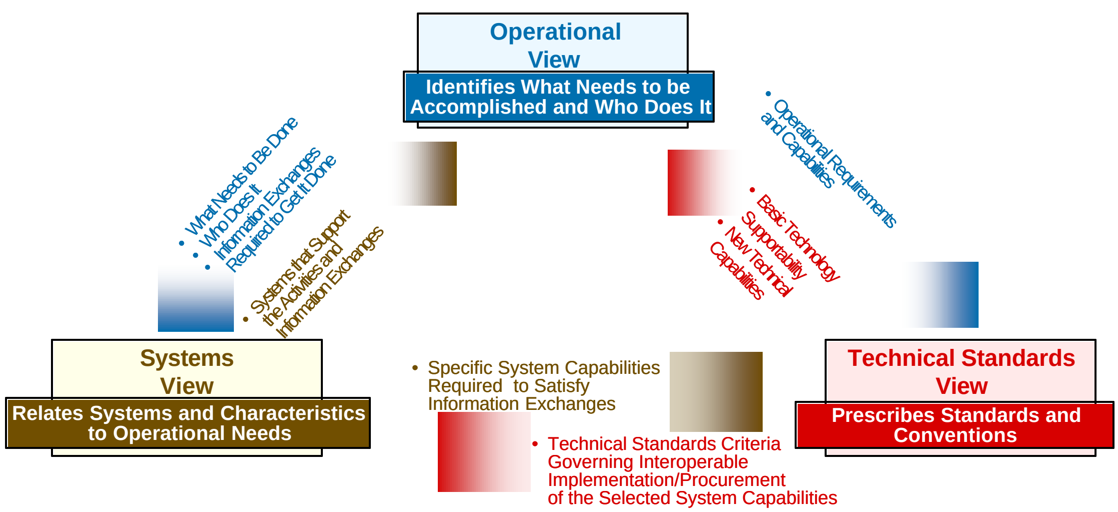


Figure 3-2. Fundamental Linkages Among the Views

Interoperability is a typical architecture focus that demonstrates the criticality of developing these inter-view relationships. In Figure 3-2, the OV describes the nature of each information exchange in detail sufficient to determine the degree of operational interoperability required. The SV identifies which systems support the operational requirements, translates the required degree of interoperability into a set of system data exchanges executed by system functions, and compares current/postulated implementations with the required operational capabilities. The TV articulates the criteria that govern the compliant implementation of each required system that will result in the fielding of an interoperable system. Thus, the three views and their interrelationships provide the basis for deriving measures such as interoperability or performance and also provide the basis for measuring the impact of the values of these metrics on operational mission and task effectiveness.

As stated above, integration of the three views of any given architecture is critical if the architecture description is to be useful as an analytical tool. One way to encourage this kind of integration is to ensure that individual products across the three views are closely related. Some critical connections have been built into the product set; the individual products and product interrelationships are discussed briefly in section 3.3 of this document and in detail in Volume II.

3.3 RELATIONSHIPS AMONG PRODUCTS

Individual architecture products are not stand-alone entities but represent depictions of subsets of architecture data describing various aspects of an architecture. As such, relationships exist among the architecture data elements that compose the various products, creating relationships among the products. **Figure 3-3** portrays some of the major relationships among selected products. See section 7, Volume II for an in depth discussion.

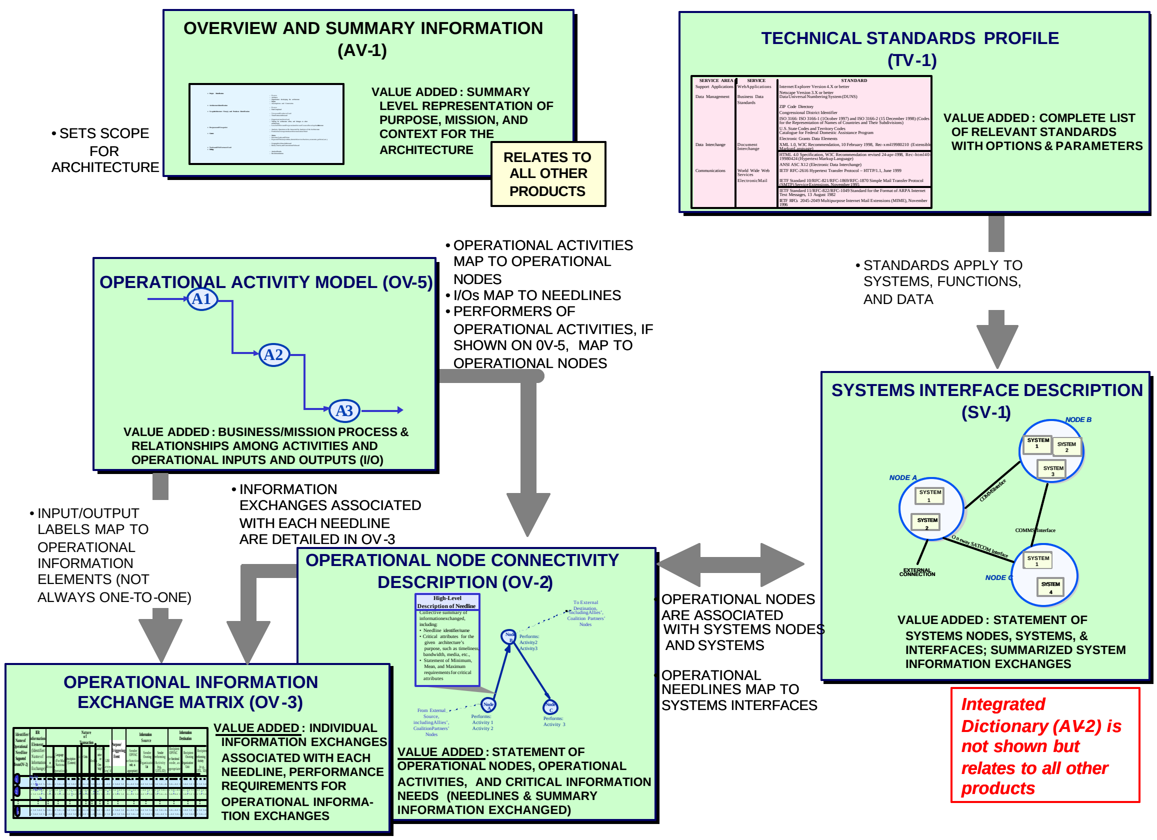


Figure 3-3. Relationships Among Products

3.4 USES OF INTEGRATED ARCHITECTURES

Integrated architectures provide a logical, structured approach for defining how forces operate, the associated information flow, the relation between that information flow and system capabilities, and the relation between system capabilities and technical standards. Much architectural work has focused on Joint operations and processes, systems, and technologies that crosscut organizational domains. Because architectures provide an ability to understand these complex relationships, they can provide significant insights into associated operational concepts, interoperability issues, and systems-related issues. Insights provided by architectures also support strategic planning, evolving an organization toward a common goal, and analyzing impacts of change.

Architecture uses include identifying capability needs, relating needs to systems development and integration, attaining IT interoperability and supportability, and managing IT investments. The use of integrated architectures has been specifically addressed in the DoD policy on JCIDS and the Defense Acquisition System. Integrated architectures can also provide a context for making resource allocation and tradeoff decisions in the Planning, Programming, Budgeting, and Execution (PPBE) process. **Figure 3-4** illustrates, at a high level, these major processes and their relationships to architectures.

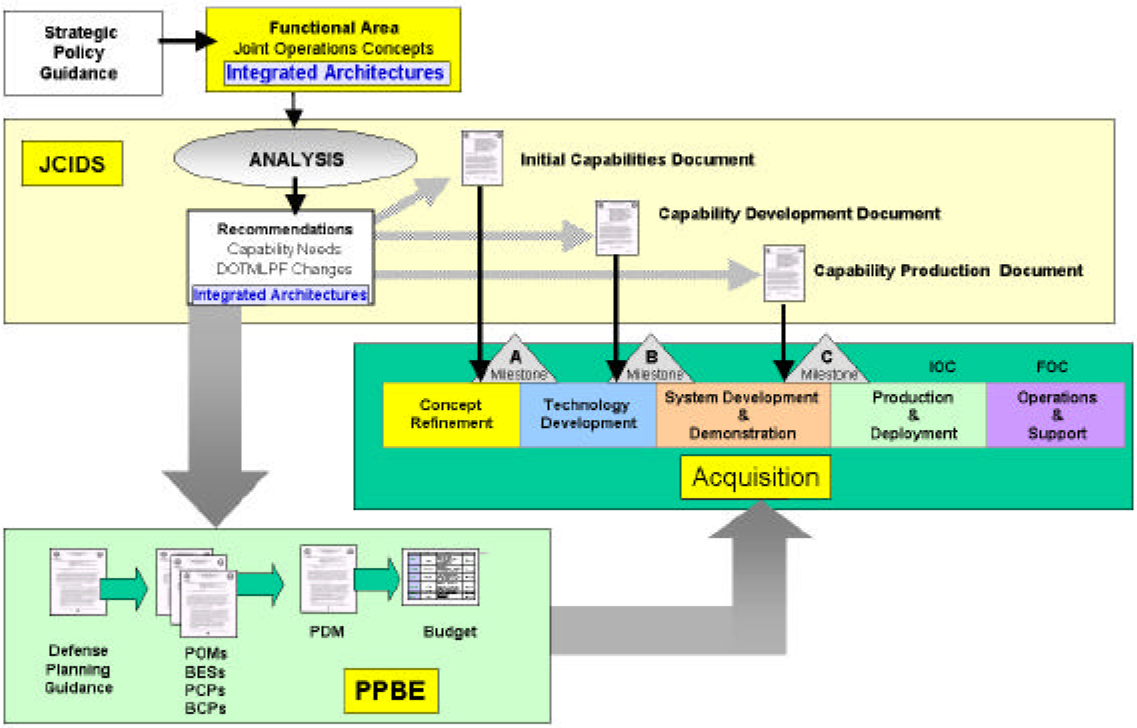


Figure 3-4. Architectures Related to the Requirements, Acquisition, and Budgeting Processes

Architecture content must be geared to the intended use of the architecture. Section 3.5 introduces potential architecture users, and section 3.6 provides guidelines for suggested content by architecture use for the major DoD processes: JCIDS, Acquisition, PPBE, and Operations.

3.5 THE VALUE OF ARCHITECTURES – DIFFERENT USES FOR DIFFERENT USERS

Different communities can have different interests in architectures. Well-defined architectures provide significant contributions to these various communities of interest and their various uses of architectures. Some types of uses are:

- **Investment decision making** – e.g., Principal Staff Assistants, the Joint Staff, Services, and Agencies can examine programmatic considerations such as consolidations, proposed systems, and new IT in context with Joint interoperability needs, integration or leveraging opportunities, and expected impact on mission effectiveness.
- **Capability and interoperability analysis** – e.g., the Joint Staff, Combatant Commands, Services, and Agencies can analyze architectures in terms of their support to joint concepts, identify capability needs, and determine the operational and support-related performance attributes of a system(s) that provide the capabilities required by the warfighter.
- **Acquisition program management and system development** – e.g., Services and Agencies developing systems can use architectures to determine system concepts related to operational concepts and ensure interoperability within a family of systems/system of systems (FoS/SoS).
- **Operational planning** – e.g., Combatant Commanders and Joint Task Force planners can examine how various mission participants, systems, and information need to play together; what problems may be encountered; and what quick fixes may be available.

For example, a system developer is probably concerned with building or procuring a capability to satisfy a specific operational requirement in a formal requirements document and with developing a Command, Control, Communications, Computers and Intelligence, Support Plan. On the other hand, the Office of the Secretary of Defense (OSD) may be searching for opportunities to satisfy several similar operational requirements with a single, leveraged capability. Either the system developer or OSD could have been the original architect of a given architecture. No matter what organization developed the architecture, for whatever original purpose and scope, other users can leverage that architecture to help answer their particular questions of concern. This ability to reuse architectures for multiple uses is critical for obtaining the full value from every architecture effort and moving the DoD toward a coherent, consistent enterprise.

In addition to DoD users, Federal Government agencies also have an interest in DoD architectures. For example, the General Accounting Office conducts audits to ensure that DoD and other Departments are in compliance with Office of Management and Budget requirements for an enterprise architecture with specified information content.

Figure 3-5 illustrates different interests that various DoD communities might have with respect to using architectures. The illustration focuses on decisions regarding systems. The figure depicts five communities of interest, their likely perspectives or business concerns, and the value that they may be seeking from a given architecture. These different values are reflected in the figure by the nature of the questions they would hope to answer through architecture analysis.

Figure 3-5 is not all encompassing. The same architecture may provide value to various other communities of interest, such as the Joint Requirements Oversight Council (JROC), Joint Warfighting Capability Assessment (JWCA) Teams, Military Communications-Electronics Board and Joint Battle Center. The intent of Figure 3-5 is to convey that architectures have value to multiple user communities with different interests and different perspectives.

As indicated at the left of Figure 3-5, the scope of interest with respect to interoperability, integration, and cost-effectiveness generally broadens from the bottom to the top of the figure. Though these factors are certainly important to all five example communities of interest, the breadth of concern increases from organization-internal focus to cross-organizational or joint concern.

Increasing Breadth of Inter-operability, Integration, and Investment Concerns (↑)

Community of Interest	Typical Perspective	Representative Architectural Insights Desired
⑤ OSD Principal Staff Assistants	DoD-wide Interoperability & POM Investment Decisions	Why do the DoD enterprises (Services, Agencies) need to build or procure the systems they are proposing? Can other DoD capabilities be leveraged to perform the same functions? Can any of the proposed systems be adapted/modified to meet broader DoD interests? Are the proposed systems compliant with GIG and other directives? "How are processes simplified and work unified across DoD organizations?"
④ Joint Staff	Cross-Command Interoperability & JROC/JWCA Investment Decisions	Do the systems proposed by the various enterprises interoperate under any JTF scenario and integrate into any theater? Do these systems add to overall Joint Warfighting effectiveness without unnecessary duplication of functionality?
③ Combatant Commander	Joint Warfighting Capability & CC Investment Strategies	Do the systems proposed by the various enterprises interoperate under JTF operations postulated for this theater, and integrate into this theater's infrastructure? Do they enhance C4ISR support to Joint force operations?
② Service or Agency Enterprise	Enterprise Operations, Fit, and Conformance & Enterprise Investment Decisions	Do the systems proposed by system developers conform with this enterprise's strategic direction? with the enterprise technical architecture? with the enterprise's rightsizing policy? How are processes simplified and work unified across the Service or Agency Enterprise?
① System Developer	ICD/CDD/CPD Satisfaction & Acquisition Strategy	Does the capability or system under consideration satisfy the target MNS/ORD? Is the proposed design cost-effective in context with alternative acquisition strategies?

Figure 3-5. Illustrative Architecture Value to Different Communities of Interest

3.6 PRODUCTS ACCORDING TO USE

The intent of this section is to specify the products required for an integrated architecture and to provide guidelines for product development based on the intended use of the architecture. The architecture products appropriate for any individual use case is highly dependent on the specific situation, objectives, and scope of the effect. Therefore, architects should consider the guidelines provided in this section but make decisions based on the specifics of their particular architecture and its intended use.

An integrated architecture as referenced in DoDI 5000.2, DoDI 4630.8, CJCSI 3170.01, and CJCSI 6212.01 consists of AV-1, AV-2, OV-2, OV-3, OV-5, SV-1, and TV-1, at a minimum. This is the minimum set of products required to satisfy the definition of an OV, SV, and TV as provided in section 1.3 and to describe the overarching aspects of the architecture that add context and meaning. In order that the architecture is, in fact, integrated across the views, the products must, at a minimum, contain those architecture data elements marked with an "*" in the architecture data element tables provided for each architecture product in Volume II. Additional products should be developed for a given architecture description, depending on the intended use.

There are many common areas of analysis related to the uses discussed in this section. These include analysis of system functionality, duplication, and gaps; assessments of connectivity and interoperability; and dynamic architecture behavior and performance. These analysis techniques are applicable to many of the uses described here.

This section addresses the use of integrated architectures in support of the PPBE process, JCIDS, Defense Acquisition System, and Operations, and provides guidelines on specific architecture products to achieve that support. As depicted in **Figure 3-6**, PPBE, JCIDS, and the Defense Acquisition System are closely related processes with significant overlaps. Similarly, analysis associated with Operations can identify operational needs or resource requirements into PPBE, JCIDS, and Defense Acquisition System. Therefore, uses described under one of these areas may be applicable across several areas.

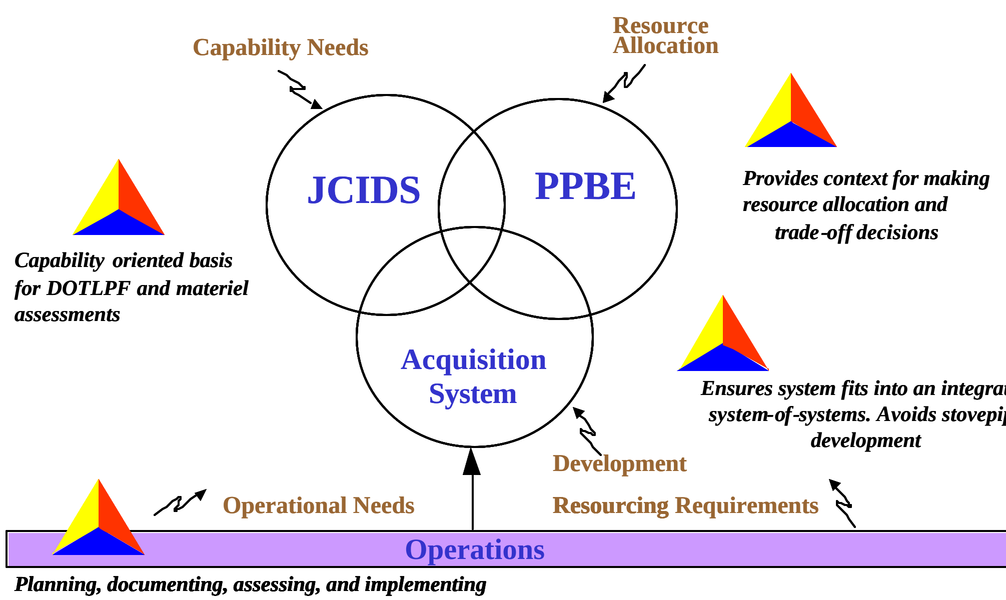


Figure 3-6. Using Architectures to View DoD In an Integrated Manner and to Support DoD Processes

Figure 3-7 provides guidelines for product development based on intended use. Figure 3-7 is not an exhaustive list. Instead it is intended to provide initial insight into the use of the various architecture products in supporting DoD processes. Future versions of the Framework are expected to expand the uses described. Each of the recommended architecture uses is described in the subsections below.

The following legend is used in the figure:

- A light gray cell (■) indicates the product is required in order to have an integrated architecture.
- A dark gray cell (■) indicates the identified product is specified in policy.
- A solid black circle (●) indicates the product is highly applicable to the indicated use (i.e., the product should be developed when the architecture is intended to support the indicated use).
- A white circle with a center black dot (⊙) indicates that the product is often or partially applicable (i.e., consideration should be given to developing the designated product when the architecture is intended to support the indicated use).
- A blank cell indicates that the product is usually not applicable (i.e., there is usually no need to develop the designated product when the architecture is intended to support the indicated use.

3.6.1 Products Required for an Integrated Architecture

As previously discussed, an integrated architecture is one that describes the domain from all three views: OV, SV, and TV. Certain products from each view are designated as essential for integrated architectures. They are discussed in this subsection.

3.6.1.1 Overview and Summary Information (AV-1)

Regardless of the intended use of the architecture, the Overview and Summary Information (AV-1) is essential for documenting the assumptions, constraints, and limitations that may affect high-level decision processes involving this architecture. AV-1 also identifies the approving authority, the completion date, and records the level of effort and costs (projected and actual) required to develop the architecture, as well as the time frame covered and the organizations that fall within the scope of the architecture. AV-1 includes an explanation of the need for the architecture, what it should demonstrate, the types of analyses (e.g., Activity-Based Costing) that will be applied to it, who is expected to perform the analyses, what decisions are expected to be made on the basis of an analysis, who is expected to make those decisions, and what actions are expected to result. AV-1 identifies the viewpoint from which the architecture is developed and the context, which includes such things as mission, doctrine, relevant goals and vision statements, concepts of operation, scenarios, and information assurance context. AV-1 also states the findings and recommendations that have been developed based on the architecture effort. Examples of findings include identification of shortfalls, recommended systems implementations, and opportunities for technology insertion. AV-1 contains sufficient textual information to enable a reader to select one architecture from among many to read in more detail.

3.6.1.2 Integrated Dictionary (AV-2)

An Integrated Dictionary (AV-2) is included in every architecture description regardless of the intended use. It is a by-product of the architecture development process and is not developed individually. It consists of textual definitions in the form of a glossary, a repository of architecture data, their taxonomies, and their metadata (i.e., data about the architecture data). AV-2 provides a central repository for a given architecture's data and metadata. AV-2 enables the set of architecture products to stand alone, allowing them to be read and understood with minimal reference to outside resources.

APPLICABLE ARCHITECTURE PRODUCTS

RECOMMENDED USES OF ARCHITECTURE:

	All View		Operational View (OV)							Systems View (SV)											Tech Stds View	
	1	2	1	2	3	4	5	6	7	1	2	3	4	5	6	7	8	9	10	11	1	2
Planning, Programming, Budgeting Execution Process																						
Capability-Based Analysis for IT Investment Decisions	●	●	●	●	●	●	●	●	⊙	●	⊙	●	●	●	●	●	●	●	●		●	⊙
Modernization Planning and Technology Insertion/Evolution	●	●	⊙	●	⊙	⊙	●	⊙		●	⊙	⊙	⊙	●	⊙	●	●	●			●	●
Portfolio Management	●	●		●			●	⊙		●			⊙	●		⊙	●				⊙	
Joint Capabilities Integration and Development System																						
JCIDS Analysis (FAA, FNA, FSA)	●	●	●	●	⊙	⊙	●	●		●	⊙		⊙	●							⊙	
ICD/CDD/CPD/CRD	●	●	●	●	●		●	●		●	⊙	⊙	●	●	●	⊙	⊙	⊙	●		●	⊙
Analysis of Alternatives (AoA)	●	●	●	●	⊙		●	●		●	⊙	⊙	●	●	⊙	⊙	⊙	⊙			⊙	⊙
Acquisition Process																						
Acquisition Strategy	●	●	●	●	⊙		●	⊙		●	⊙			●							●	
C4ISP	●	●	●	●	●		●	●		●			⊙		●	⊙					●	⊙
System Design and Development	●	●		●	●		●	●	⊙	●	●	●	●	●	●	●	●	⊙	⊙	⊙	●	⊙
Interoperability and Supportability of NSS and IT Systems	●	●	●	●	●	⊙	●	⊙	⊙	●	⊙	●	●		●	●	⊙	⊙	⊙	⊙	●	⊙
Integrated Test & Evaluation	●	●		●	●	⊙	●	●	⊙	●	●	●	●	●	●	●			●	⊙	●	
Operations (Assessment, Planning, Execution, …)																						
Operations Planning & Execution	●	●	●	●	●	●	●	●	⊙	●	●	⊙	⊙	●	⊙	⊙					⊙	
CONOPS & TTP	●	●	●	●	●	●	●	●		●	⊙	⊙	⊙	⊙							⊙	
Communications Plans	●	●	●	●		⊙	⊙			●	●						⊙	⊙			●	⊙
Exercise Planning & Execution	●	●	●	●	●	●	●	●		●	●	⊙	⊙	⊙	⊙						⊙	
Organizational Design	●	●	●	●	●	●	●	⊙	⊙	⊙	⊙			⊙								
BPR/FPI	●	●	⊙	●	●	●	●	●	⊙													

● = Product is highly applicable

⊙ = Product is often or partially applicable

(dark shading) = Product is specifically addressed in policy

(light shading) = Product is required for an integrated architecture

blank = Product is usually not applicable

Figure 3-7. Architecture Products by Use

3.6.1.3 Operational Node Connectivity Description (OV-2)

The main features of the Operational Node Connectivity Description (OV-2) are the operational nodes and the needlines between them that indicate a need to exchange information. The product delineates the key players and their need to exchange information necessary to conduct the corresponding operational activities of Operational Activity Model (OV-5). Operational nodes may represent an operational/human role (e.g., Air Operations Commander), an organization (e.g., OSD) or organization type, that is, a logical or functional grouping (e.g., Logistics Node, Intelligence Node). Regardless of the intended use and level of detail, it is important to identify the key players. OV-2 is highly applicable for all architecture uses noted in Figure 3-7.

3.6.1.4 Operational Information Exchange Matrix (OV-3)

The Operational Information Exchange Matrix (OV-3) identifies information elements and relevant attributes of the information exchange and associates the exchange to the producing or consuming operational nodes and activities and to the needline that the exchange satisfies. OV-3 documents the need or operational requirement to exchange certain kinds of information that meet certain performance and security attributes. While OV-3 has wide utility and is highly applicable for most uses, the OV-2 needlines provide an adequate specification of the requirement to exchange information for some architecture uses. For example, knowledge of the information elements and their exchange attributes is not essential to architecture uses, such as portfolio management, or when the domain of the architecture is limited to the communications infrastructure.

3.6.1.5 Operational Activity Model (OV-5)

The Operational Activity Model (OV-5) describes the operations that are normally conducted in the course of achieving a mission or a business goal. It describes capabilities, operational activities (or tasks), input and output (I/O) flows between activities, and I/O flows to and from activities that are outside the scope of the architecture. An OV-5 can be used to:

- Clearly delineate lines of responsibility for activities when coupled with OV-2
- Uncover unnecessary operational activity redundancy
- Make decisions about streamlining, combining, or omitting activities
- Define or flag issues, opportunities, or operational activities and their interactions (information flows among the activities) that need to be scrutinized further
- Provide a necessary foundation for depicting activity sequencing and timing in the Operational Rules Model (OV-6a), Operational State Transition Description (OV-6b) and Operational Event-Trace Description (OV-6c)

Regardless of the intended use and level of detail, OV-5 is highly applicable for most architecture uses noted in Figure 3-7. However, if the architecture domain is the communications and network infrastructure, then the need for OV-5, OV-3, and their corresponding system data exchanges (SV-6) falls outside the scope of the architecture use.

3.6.1.6 Systems Interface Description (SV-1)

The Systems Interface Description (SV-1) links together the Operational and Systems Views by depicting the assignments of systems/system functions, and systems nodes (and their associated interfaces) to the operational nodes (and their associated needlines) described in OV-2. OV-2 depicts the operational nodes representing organizations, organization types, and/or human roles, while SV-1 depicts the systems nodes that house operational nodes (e.g., platforms, units, facilities, and locations) and the corresponding systems/system functions, which are resident at these systems nodes and which support the operational nodes. Most architecture uses involve the analysis of alternative materiel solutions; therefore, knowledge of the systems, their locations, and their functions is essential to analysis.

While SV-1 is highly applicable for most uses, it is usually not applicable for conducting Business Process Re-Engineering/Functional Process Improvement where the intent is to address activities and processes independent of systems.

3.6.1.7 Technical Standards Profile (TV-1)

The Technical Standards Profile (TV-1) consists of the set of systems standards rules that govern systems implementation and operation of a given architecture. The standards generally govern what hardware and software may be implemented and what system data formats may be used. That is, TV-1 delineates which standards may be used to implement the systems, system hardware/software items, communications protocols, and system data formats. Knowledge of the technical standards for the systems in use is relevant for most architecture uses, including, for example, C4I Support Plans (C4ISPs), where the absence of such knowledge may lead to failed plans and inability to receive or transmit information due to incompatibility of systems.

While TV-1 is critical to understanding technical aspects of an architecture, it is usually not applicable for uses that tightly focus on operational aspects. For example, it is usually not applicable for conducting Business Process Re-Engineering/Functional Process Improvement (BPR/FPI) where the intent is to address activities and processes independent of systems and technical standards considerations.

The following subsections describe each of the major DoD processes and relate the suggested products to their intended use.

3.6.2 Planning, Programming, Budgeting, and Execution Process

The PPBE process has replaced the Planning, Programming, and Budgeting System (PPBS) as the primary resource allocation process of the DoD. PPBE is a biennial (2-year) cycle during which the department will formulate 2-year budgets during even-numbered years and then focus on budget execution and program performance in odd-numbered years. DoD policy has not formalized the use of architectures in the PPBE but DoD Components, such as the Navy and Air Force, have noted that architectures provide a context for developing program priorities, formulating programmatic modifications, and making IT investment decisions.

3.6.2.1 Capability-Based Analysis for IT Investment Decisions

Integrated architectures model warfighting operations, DoD business processes and IT support for those operations and processes. Capability-based analysis requires information from most architecture products. In the OV, the operational mission requirements (OV-1, OV-2, OV-4, and OV-5), operational threads (OV-6), and operational information exchange requirements (OV-3) are defined. They have relationships to their counterparts in the Systems View: the systems, system functions, and system interfaces (SV-1, SV-3, SV-4, and SV-5); system data and exchange attributes (SV-6); behavior and dynamic execution threads (SV-10); and system performance requirements (SV-7) describe the implementation of these operational requirements. In addition, systems evolution plans (SV-8) and technology forecasts (SV-9) are needed to make informed decisions about system evolution and future system investments. Technical standards (TV-1) that constrain the systems design and system investment decisions are also needed, while forecasts of technical standards (TV-2) may be needed depending on the architecture time frame.

When the domain concerns the network infrastructure and communications, a communications description (SV-2) may be needed for the analysis as well. In cases where the architecture domain deals with the storage and manipulation of persistent system data, a data model may also be applicable (OV-7). Architecture analysis techniques can identify gaps and overlaps and estimate the impact to mission of systems delays, eliminations, performance shortfalls, interoperability issues, and so forth. A variation of the Systems Evolution Description (SV-8) known as the Capability Evolution Description[4] (CED) depicts required program plans aligned to capability objectives and increments over time.

3.6.2.2 Modernization Planning and Technology Insertion/Evolution

While strategy and doctrine are drivers for changes in both warfighting operations and DoD business processes, technology insertion/evolution is also a significant factor for modernization. The need to maintain currency in technology is a constant driver in modernization planning and generates resource requirements from all DoD Components. Integrated architectures can relate capabilities, operational activities, system functions, systems, system parameters, technology, and technical standards. Because architectures provide a basis for understanding and assessing these relationships, they can support PPBE decisions related to technology insertion/evolution.

The Operational Activity to Systems Function Traceability Matrix (SV-5) which is derived from the relationships between operational activities (OV-5) and their attributes (e.g., operational nodes from OV-2, and operational threads from OV-6c) on the one hand, and systems and system functions (SV-1) on the other hand, provides the ability to correlate systems to capabilities. The systems performance attributes (SV-7) provide a basis for comparing performance parameters of existing systems with desired performance parameters of modernized systems. TV-1 documents the existing constraints that might influence modernization decisions. The systems evolution descriptions (from SV-8) document evolution plans for existing and new systems, hardware/software items, system functions, etc., and their associated standards (from TV-1). Technology forecasts (SV-9) and forecasts of technical standards (TV-2) provide a construct for documenting the impact of inserting emerging technologies and standards on

---

[4] CED is described in the Deskbook sections on Air Force Capability-Based Analysis and Navy's Mission Capability Package Approach.

existing systems elements as well as system evolution plans. They provide the basis for making decisions on retiring or evolving existing systems and replacing them with new systems or with updated system capabilities. This ability to relate technology to operational and performance improvement enables the creation of a technology investment roadmap that is defensible in terms of the systems and capabilities provided.

3.6.2.3 Portfolio Management

SV-1 depicts the systems and system functions in the portfolio, how they interact among themselves and with their environment, their configurations and installation, and how they support warfighting operations and business processes modeled in OV-2 and OV-5. The Operational Activity to Systems Function Traceability Matrix (SV-5) derived from operational activities (OV-5) and their attributes (e.g., operational nodes from OV-2) on the one hand, and systems and system functions (SV-1) on the other hand, provides the basis for understanding the relative contribution of various systems to achieving mission capabilities. This understanding then provides a basis for determining optimal resource allocations across the portfolio of systems.

The Systems Evolution Description (SV-8) and the CED, a variant of SV-8, provide a basis for portfolio investment decisions by depicting the evolution of systems, system integration, and system improvements over time. The CED provides a description of the evolution and acquisition of system improvements that is traceable to mission capabilities. Using CEDs, portfolios of programs can be bundled by the capability increments that establish the evolution of the FoS.

3.6.3 Joint Capabilities Integration and Development System

CJCSI 3170.01C, dated June 24, 2003, replaces the "Requirements Generations System" defined in CJCSI 3170.01B, dated April 15, 2001, with JCIDS. JCIDS is established to satisfy the need for a joint concepts-centric capabilities identification process.

3.6.3.1 JCIDS Analysis

As defined in CJCSI 3170.01C and CJCSM 3170.01, JCIDS analysis consists of:

- Functional Area Analysis (FAA) – identify the tasks to be reviewed
- Functional Needs Analysis (FNA) – based on the tasks identified in the FNA, identify capability gaps or redundancies
- Functional Solution Analysis (FSA) – for the capability gaps or redundancies identified in the FSA, assess the potential DOTMLPF approaches

Per CJCSM 3170.01, national strategy, Universal Joint Task Lists (UJTLs), and integrated architectures should be used in conducting the FAA. Based on cross-capability analysis and cross-system analysis, the FAA identifies the tasks to be reviewed in the FNA. OV-5 used in association with the UJTLs can provide insight into the tasks to be accomplished, the relationships and information flows between those tasks, and the materiel solutions (systems or system functions from SV-1) supporting the tasks. OV-6 provides critical timing and sequence attributes and documents the operational threads. SV-5 provides a basis for identifying activities (and associated capabilities) not supported by existing materiel solutions (i.e., systems and system functions).

In conducting the FNA for the tasks identified in the FAA, the Operational Node Connectivity Description (OV-2) identifies the key players (operational nodes) and the operational information exchange requirements for tasks/activities of interest. If communication or networking is a focus of interest, the Systems Communication Description (SV-2) provides the basis for identifying existing connectivity. SV-5, used in conjunction with the system functions to systems mapping (described in SV-1), can identify areas where needed system functions are not provided by any system or where the same system function is provided by multiple systems. This contributes toward identifying capability gaps and redundancies.

The first step of the FSA is determining whether an integrated DOTMLPF approach can fill the capability needs identified in the FNA. Operational activities (OV-5) and their DOTMLPF attributes such as:

- Doctrine influencing the activities (controls from OV-5)
- Organizations responsible for the activities (OV-2 operational nodes)
- Training or skill set needed to conduct the activities (human roles represented by operational nodes in OV-2)
- Leadership and education (through OV-2 nodes and their association with the organizational hierarchy of OV-4)
- Personnel (humans conducting operations)
- Facilities specified as systems nodes in SV-1, as well as operational threads (OV-6c) that describe capabilities

If the analysis determines that the capability can only be met with a materiel solution, the FSA should always consider existing and future materiel programs that can be modified to meet the capability need. These OV and SV elements and relationships provide a basis for comparison between alternative DOTMLPF approaches. Potential changes in DOTMLPF attributes can be overlayed on OV-5 and OV-6c to aid in assessing their impact. The integrated DOTMLPF implications of any proposed materiel solution will always be considered throughout the process.

The FSA results in determining the best materiel approach but does not define a specific system solution. Rather, the FSA sets the boundary conditions within which the Analysis of Alternatives (AoA) should be performed. SV-5, relating capabilities to activities and then mapping the activities to system functions, can be used with SV-1 and/or SV-2 (if communications or networking is the focus of interest), and possibly SV-4 (to adequately define system functions) to provide a basis for assessing various approaches for achieving a capability via a materiel approach. OV-3 may be used to describe information exchange requirements. The technical standards (TV-1) may be applicable to factor technical constraints to the JCIDS analysis process.

3.6.3.2 Initial Capabilities Document/Capability Development Document/Capability Production Document/Capstone Requirements Document

The Initial Capabilities Document (ICD) replaces Mission Need Statements as the initial documentation of need for the Concept Refinement phase of acquisition. The ICD describes gaps in capability for a particular functional or mission area. The Capability Development Document (CDD) defines an increment of operational capability to support the System Design and Development phase of acquisition. The CDD provides the measurable and testable operational performance parameters, including Key Performance Parameters (KPPs). KPPs are those system attributes considered most essential for the capability. The Capability Production Document (CPD) provides the information necessary to support production, testing, and deployment of a capability increment and supports the Production and Deployment phase of acquisition. The CPD refines the performance attributes and KPPs initially developed in the CDD.

The Capstone Requirements Document (CRD) describes overarching thresholds, goals, and standards in functional areas and is useful for FoS and SoS approaches [JS/J8, 2003].[5] Under JCIDS, CRDs are developed only at the direction of the JROC. Eventually CRDs are to be replaced with integrated architectures.

Integrated architectures along with joint operating and functional concepts provide a common construct for analysis to identify capability shortfalls or redundancies and compare alternatives for improving joint warfighting capabilities. The specifications for each of the documents mandate that integrated architecture products be included as an appendix. The products mandated by these documents are OV-1, OV-2, OV-3, OV-5, OV-6, SV-1, SV-6, and TV-1. If the focus is a communications or networking system policy specifies that SV-2 should be developed in lieu of the SV-1. However, the framework recommends that both SV-1 and SV-2 be developed. SV-10 is cited as optional for a CPD; however the Framework recommends the SV-10 as highly applicable.

In the OV, the operational mission requirements (OV-1, OV-2, and OV-5), operational information exchange requirements (OV-3), and operational threads (OV-6) are defined. OV-6c depicts the dynamic behavior of the mission process with timing and sequencing attributes and can contribute to establishing operational performance requirements. OV-6b depicts how activities change in response to external and internal events and can also contribute toward establishing operational performance requirements. Documentation of the operational nodes (OV-2), the systems (SV-1), their interfaces, and the systems connectivity (SV-2) (if communications is the focus) supports the identification of key players, the systems that support them, and the communications infrastructure supporting their interfaces. SV-6 used in conjunction with OV-3 provides a basis for determining interoperability requirements by translating required information exchanges to data exchanges between systems; thus, identifying systems where interoperability is required. The Systems Event-Trace Description (SV-10c) can contribute to establishing system-related performance parameters, since it reflects system-specific aspects or refinements of critical sequences of events described in the OV. SV-10b can also contribute to establishing system-related performance parameters, since it depicts how systems change in response to external and internal events. Technical standards constraining the system elements are documented in TV-1.

---

[5] JS/J8 briefing, "Introduction to JCIDS," 2003, http://dod5000.dau.mil/.

In addition to the architecture products specified in CJCSM 3170.01, the Framework lists two additional products as highly applicable. These products are the Systems Functionality Description (SV-4) and the Operational Activity to Systems Function Traceability Matrix (SV-5). The Operational Activity Model (OV-5) used in conjunction with OV-6c describe capabilities required. SV-4 supports identification of a hierarchy of required system functions and identifies the system data elements whose exchange attributes are described in SV-6. SV-5 relates capabilities to systems (by mapping capabilities to operational activities from OV-5, operational activities to system functions from SV-4, and system functions to systems).

CJCSM 3170.01 states that an interoperability KPP is based on the top-level information flows (OV-3) that are to be supported by the proposed system(s). Top-level information flows and their associated operational performance requirements and attributes are depicted as information exchanges in OV-3. These operational information exchanges are then related to systems, system functions, systems performance parameters, and interoperability requirements via SV-6 exchange attributes and, if needed, system performance attributes (SV-7).

Systems evolution plans (SV-8) and technology forecasts (SV-9) are sometimes needed to make informed decisions about system evolution and future system investments. Technical standards (TV-1) constrain the systems design and system investment decisions, while forecasts of technical standards (TV-2), which denote when a future version of a specific standard may be adopted, may also be needed depending on the time frame for the architecture.

3.6.3.3 Analysis of Alternatives

Following JCIDS analysis and after the ICD is approved, an Analysis of Alternatives (AoA) is developed to assess specific alternatives for the materiel approach defined in the FSA. The CDD and CPD use the AoA.

Alternative architectures, each depicting a different configuration of DOTMLPF attributes (from FSA) to meet a certain capability, can support the analysis of alternatives. A comparison of the alternative architectures can provide a measure of the degree to which they satisfy enterprise objectives (e.g., in terms of mission effectiveness, capability satisfaction, capability cost, and so forth). The architecture products applicable to the FAA, FNA, and FSA are also useful in analyzing alternative materiel solutions. Since the analysis within the AoA is at a more detailed system level than that performed in the FSA, a more detailed level of SV information would be expected.

OV-2 identifies the key players (operational nodes) and the need to exchange information. OV-3 may be used to describe information exchange requirements. OV-5 used in conjunction with OV-6c describe capabilities required. SV-5, relating capabilities to activities and then mapping the activities to system functions, can be used with SV-1 and/or SV-2 (if communication or networking is the focus of interest). AoA involves documenting system functions (SV-4) to provide a basis for assessing various approaches for achieving a capability using a materiel approach. AoA might involve documenting system interfaces (SV-3) in terms of their Status (e.g., existing, planned, potential, deactivated), Purpose (e.g., C2, intelligence, logistics), Classification level (e.g, Secret, TS/SCI), Means (e.g., Joint Worldwide Intelligence Communications System, SIPRNET), Standard, and Key Interface Designation. In addition, systems exchange attributes (SV-6) and systems performance parameters (SV-7) may be applicable when assessing alternative materiel solutions. The Systems Evolution Description (SV-8) is useful in evaluating alternatives by examining planned evolution or retirement of existing systems. The technical standards (TV-1) may be applicable to factor technical constraints to the JCIDS analysis process. The Systems Technology Forecast (SV-9) in conjunction with the Technical Standards Forecast (TV-2) can identify emerging technologies and enabling future standards that can be considered in evaluating the potential materiel solutions.

3.6.4 Acquisition Process

DoDD 5000.1 "The Defense Acquisition System" and DoDI 5000.2 "Operation of the Defense Acquisition System," both dated May 12, 2003, establish management policies that provide a simpler and more flexible approach for managing DoD acquisition programs. Integrated architectures are cited as supporting the development of capability assessments, guiding systems development and defining associated investment plans. **Figure 3-8** relates the acquisition process to architecture-based analysis.

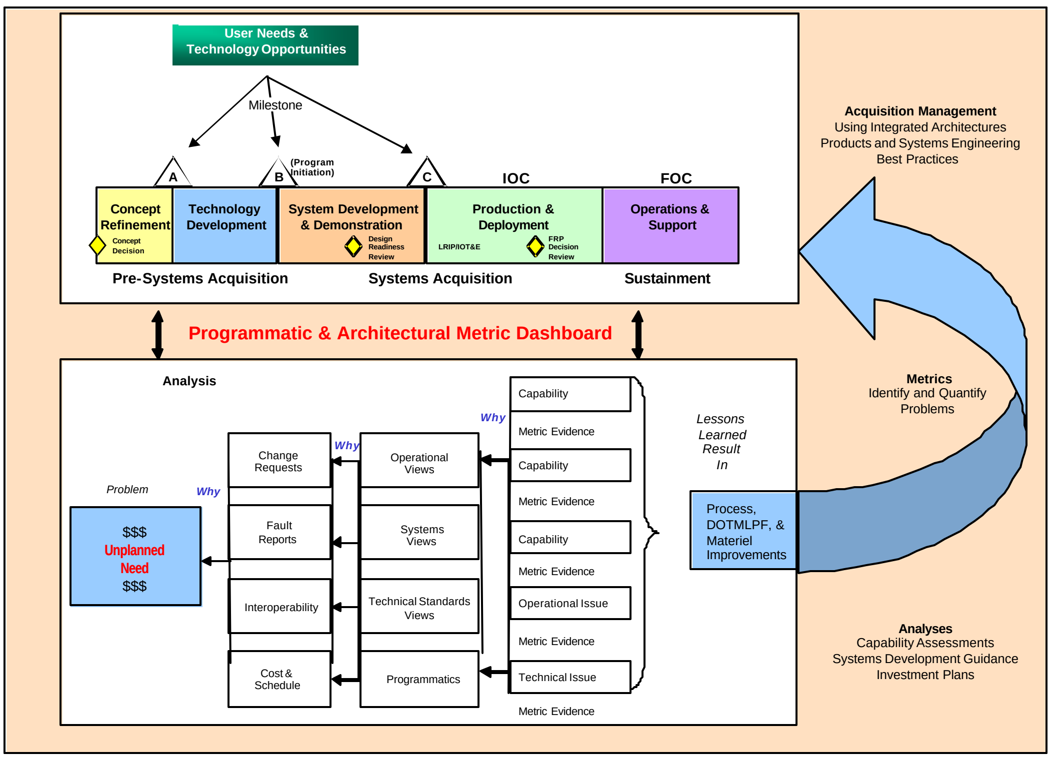


Figure 3-8. Acquisition Process and Architecture-Based Analysis

3.6.4.1 Acquisition Strategy

An acquisition strategy guides program execution from initiation through procurement of systems, subsystems, hardware and software items, spares, and services beyond the initial production contract award and during post-production support. The acquisition strategy is an iterative process that describes the relationship between essential elements of a program. An architecture description supports a strategy oriented toward efficiently satisfying needs recorded and maintained in the architecture. OV-2 and OV-5 products provide the basis for understanding operational needs, in terms of what needs to be done (operational activities from OV-5), who is responsible for executing them (operational nodes from OV-2). OV-3 may be applicable and would be used in cases where it is important to understand the information elements needed to conduct those activities and the exchange attributes of those information elements across operational nodes.

SV-1 depicts the relationships between systems/system functions and their interfaces. OV-6 provides critical timing and sequence attributes and documents the operational threads. SV-5 provides a basis for identifying activities (and associated capabilities) not supported by existing systems. SV-5 also provides an understanding of the relation between capability needs to multiple systems and the contribution of an individual system toward achieving a capability objective. TV-1 provides the set of existing systems standards that may influence and constrain the acquisition decisions.

Risk management is included within the acquisition strategy. Risk management includes the creation of program goals, thresholds, and objectives that describe the cost, schedule, and performance parameters to include the risk involved over the acquisition life cycle. Using an integrated architecture ensures that the system to be acquired is addressed in the context of a whole environment rather than a separate entity. The architecture can support identification of operational dependencies outside the sphere of the specific system under development. This facilitates determining the effect of a schedule change or performance change in the achievement of the required capability objective.

Architecture-based metrics can aid the Program Manager (PM) to address risk. **Figure 3-9** suggests potential architecture-based metrics that can be used to identify and monitor risk. The PM can use information from the architecture products to identify risk areas. The PM can then explain how to reduce system-level risk to acceptable levels through an effective progress review program.

3.6.4.2 Command, Control, Communications, Computers, and Intelligence (C4I) Support Plan

The C4I Support Plan (C4ISP) describes and evaluates the information, infrastructure, and other IT and NSS interfaces required by an acquisition program. The C4ISP analysis focuses on identifying derived information support requirements and ensuring each requirement is satisfied to meet a given capability need within the system's operational environment. Analysis addresses, but is not limited to, information and system data exchanges, information timeliness, impact, quality, quantity, assuredness, robustness, flexibility, scalability, spectrum needs, and net-centric attributes. Policy specifies the following architecture products be included in the C4ISP: OV-1, OV-2, OV-3, OV-6c, SV-1, SV-6, and TV-1.

In the OV, the operational mission requirements (OV-1, OV-2), operational information exchange requirements (OV-3), and operational threads (OV-6c) are defined. The Operational Event-Trace Description (OV-6c) depicts the dynamic behavior of the mission process with timing and sequencing attributes and can contribute to establishing operational performance requirements. Documentation of the operational nodes (OV-2), the systems (SV-1), and their interfaces supports the identification of key players and the systems that support them. SV-6 used in conjunction with OV-3 provides a basis for determining interoperability requirements by translating required information exchanges to data exchanges between systems, thus, identifying systems where interoperability is required. Technical standards constraining the system elements are documented in TV-1.

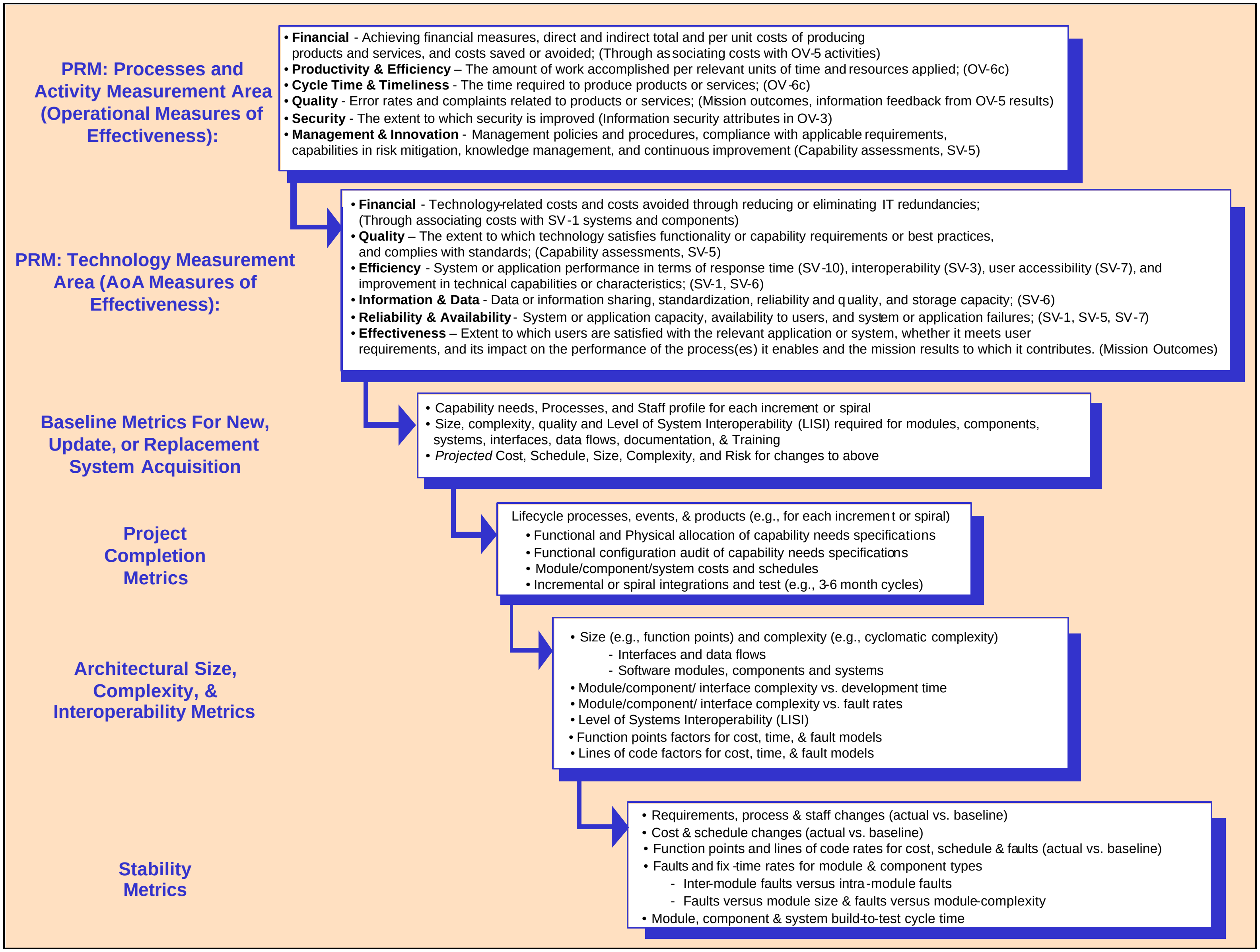


Figure 3-9. Architecture-Based Metrics

The Framework recommends OV-5 as highly applicable because it provides a basis for understanding the relationships among activities. The Framework suggests consideration of SV-7 and TV-2 as often applicable. The policy document requires “relevant specific system and component performance parameters such as reliability, maintainability, and availability”; this information is contained in SV-7. For multi-year C4ISPs, information from TV-2 can show the expected evolution of standards coincident with the development of the system. The Deskbook provides more detailed discussion on the development of the C4ISP.

3.6.4.3 System Design and Development

An architecture describes the system under development in the context of the larger environment supporting a given mission or business area. The architecture products supporting system design and development would generally be developed at a more detailed level than the comparable products used to support JCIDS analysis or AoA.

Before system design and development can begin, the operational requirements would have been defined during JCIDS analysis. These operational requirements drive the system design and are indicated in the matrix as key to developing systems that meet the requirements. An architecture can provide specification of system functions (SV-4) and the trace between the required operational capabilities and system functions (SV-5). The architecture describes required system data exchanges, systems interfaces and interoperability, communication networks (SV-1, SV-2, SV-3, SV-6), and required system performance parameters (SV-7). The systems evolution descriptions (from SV-8) document evolution plans for existing and new systems, hardware/software items, system functions, etc., and their associated standards (from TV-1).

The following products are listed as often applicable by the Framework. SV-10 (a, b, and c) depicts the dynamic behavior of a system performing the system functions described in SV-4. The Logical Data Model (OV-7) and Physical Schema (SV-11) are applicable when the domain deals with persistent system data. Technology forecasts (SV-9) and technical standards forecasts (TV-2) provide a construct for documenting the impact of inserting emerging technologies and standards on existing systems elements as well as system evolution plans.

While the system designers and developers would primarily use the SV and TV products mentioned above (plus OV-7, depending on the scope of the effort), the OV products noted in Figure 3-7 are considered highly applicable because they are a necessary foundation for the creation of the SV products.

3.6.4.4 Interoperability and Supportability of IT and NSS Systems

Architectures can provide the basis for determining interoperability and supportability requirements based on operational needs and then assessing the ability of the associated systems to support those requirements. OV-1, OV-2, OV-3, and OV-5 define requirements for exchanging information. SV-6, used in conjunction with OV-3, provides a basis for determining interoperability requirements by translating required information exchanges to system data exchanges between systems; thus, identifying systems where interoperability is required. The architecture provides for identification and specifications of interfaces (SV-1 and SV-2 where applicable), characteristics of interfaces between systems (SV-3), system functions and system data elements (SV-4), system performance parameters (SV-7), and IT standards (TV-1). When the domain deals with persistent system data, OV-7 and SV-11 can support assessments of system data interoperability and database design specifications.

The following products are listed as often applicable by the Framework. OV-4 documents authority sources, while OV-6 describes operational threads and defines capabilities when used with OV-5. SV-10 depicts the dynamic behavior of a system performing the system functions described in SV-4. The systems evolution descriptions (from SV-8) document evolution plans for existing and new systems, hardware/software items, system functions, etc., and their associated standards (from TV-1). Technology forecasts (SV-9) and technical standards forecasts (TV-2) provide a construct for documenting the impact of inserting emerging technologies and standards on existing systems elements as well as system evolution plans.

3.6.4.5 Integrated Test and Evaluation

Per DoDI 5000.1, testing and evaluation should assess interoperability, facilitate integration into fielded forces, and confirm performance against documented capability needs. The integrated architecture for a FoS, SoS, network of systems, or individual system provides many of the factors that form the basis for testing and evaluation. OV-2 describes required operational connectivity, OV-3 describes information exchange requirements associated with the activities to be supported, OV-5 defines operational activities, and OV-6c provides the timing and sequencing of the operational activities based on a scenario or sequence of events. All of which can contribute to the development of realistic testing scenarios.

The SV supports testing by describing required systems interfaces (SV-1) and communications interfaces (SV-2), characteristics of interfaces between systems (SV-3), system functions (SV-4), system data exchanges between systems and associated system interoperability requirements (SV-6), performance characteristics (SV-7), and systems conditions, events, timing, and sequence attributes (SV-10). TV-1 specifies the required IT standards. The traceability between systems/system functions and operational requirements is documented in SV-5. Testing and evaluation results and the ability of the systems/system functions to meet operational capabilities and needs may also be tracked in this product. OV-7 and SV-11 are applicable when the domain deals with persistent system data.

3.6.5 Operations

3.6.5.1 Operations Planning and Execution

An integrated architecture facilitates the creation and execution of Operations Plans (OPLANS) through the OV and its bridge to the SV. Architecturally based or traceable OPLANS can be assessed for interoperability and to predict communications gaps or capability shortfalls. The OV products (OV-1 through OV-5) describe how forces organize and interact. They identify activities, the relationships between the activities, associated information flows, and relate the activities and information flows to operational nodes and organizations. OV-6 provides the additional perspective of time sequencing of activities. SV-1 depicts what systems are available to support operations, where they are located, and how they interface. SV-2 defines the physical connections (including placement on a network or grid) of the systems required to conduct operations. The traceability between systems (execution) and operational plans is documented in SV-5.

OV-7 is applicable when the domain deals with persistent system data. SV-6 is noted as often or partially applicable. When used in conjunction with OV-3, the SV-6 provides a basis for operations execution by translating required information exchanges to system data exchanges between systems. Characteristics of interfaces between systems (SV-3), system functions and system data elements (SV-4), and systems performance parameters (SV-7) are sometimes applicable depending on the operations' scope. TV-1 specifies the IT standards that constrain systems.

3.6.5.2 Concept of Operations and Tactics, Techniques, and Procedures

Current and future concept of operations (CONOPS) and tactics, techniques, and procedures (TTP) can be modeled in the OV. Conversely, an architecture can be used to generate and update core portions of CONOPS, specifically Concepts of Employment, and TTP documents. The OV provides a basis for assessing operational concepts and procedures for effectiveness and DOTMLPF impacts. The OV lends itself particularly to assessing impacts of doctrine, training, personnel, and materiel.

OV-2 depicts needlines between operational nodes thereby specifying required operational connections. OV-3 identifies information exchange requirements. OV-4 identifies the command structure and relationships among organizations. OV-5 denotes activities required to conduct the CONOPS. SV-1 identifies the systems supporting the activities defined in the OV, the physical locations of those systems, and the interfaces between them. The Framework lists the Operational Activity Model (OV-5) as highly applicable. OV-5, used in conjunction with OV-6c describes capabilities required. SV-5 can be used to trace the CONOPS to the systems that enable them.

In addition, the Framework lists SV-4 as partially applicable as it supports identification of a hierarchy of required system functions and identifies the system data elements whose exchange attributes are described in SV-6. Characteristics of communications infrastructure (SV-2), and the interfaces between systems (SV-3), may also be applicable depending on the domain of the CONOPS. TV-1 specifies the IT standards that constrain systems.

3.6.5.3 Communications Plan

OV-2 identifies needlines and thus documents the need to exchange information between operational nodes. Knowledge of the key players (operational nodes) and their need to communicate is essential for building a communications infrastructure that will satisfy its potential users. However, detailed knowledge of the information elements and their exchange attributes (OV-3), as well as knowledge of the operational activities (OV-5) is not needed for this architecture use. For example, once the telephone company has knowledge of its potential customers (how many, and the kind of communications processing they typically require), knowledge of how they will use the telephone (i.e., for what communication purpose) is not needed to build the telephone network. SV-1 systems nodes specify the locations where the operational nodes, or users of the communications network, are physically located. SV-1 also specifies the systems that need access to the communications network. SV-2 specifies the communication infrastructure that will be available for their use, including security aspects such as firewalls. SV-2 is a key product for use in a communications plan as it defines the physical connections (including placement on a network or grid) of the systems to satisfy operational nodes communication needs. TV-1 identifies the standards for the communications systems, communications links, and communications networks.

The following products are partially applicable. OV-4 provides an understanding of organizational relationships, while OV-5 identifies the activities and relationship between the activities to be supported by the communication plan. Systems evolution descriptions (from SV-8) document evolution plans for existing and new systems, hardware/software items, system functions, etc., and their associated standards (from TV-1). Technology forecasts (SV-9) and technical standards forecasts (TV-2) provide a construct for documenting the impact of emerging technologies and standards on existing systems elements as well as on system evolution plans.

3.6.5.4 Exercise Planning and Execution

Architectures describe activity-based processes and their relation to systems. The designated OV product set (OV-1 though OV-6) identifies activities, the relationship between the activities, associated information flow, and relates the activities and information flow to operational nodes and organizations. An understanding of the relationships among these architecture elements can facilitate the design and development of exercise plans while SV-1 and SV-2 define the IT environment where the exercises can be executed or operational activities simulated.

SV-3, SV-4, SV-5, and SV-6 are partially applicable, because they provide additional information on the IT environment in which the exercise will occur. Similarly, TV-1 is partially applicable, since it identifies the standards for the systems, hardware/software items, system functions, etc.

3.6.5.5 Organizational Design

The designated OV product set (OV-1 through OV-5) identifies activities, the relationship between the activities, associated information flow, and relates the activities and information flow to operational nodes and organizations. An understanding of the relationships among these architecture elements provides the basis for determining duplications of effort and assessing the efficiency and utility of various organizational structures.

SV-1, SV-2, and SV-5 are partially applicable, because they relate the IT environment to the organization. Similarities or differences in IT requirements and usage could influence organizational design decisions.

3.6.5.6 Business Process Re-engineering/Functional Process Improvement

The warfighting or business operational process can be modeled in the OV to determine overlaps, bottlenecks, and other activity and organizational sub-optimizations. Also, new required missions, activities, and organizational functions or imperatives can be modeled to determine the most satisfactory implementation. The designated OV product set (OV-2 through OV-6) identifies activities, the relationship between the activities, associated information flow, and relates the activities and information flow to operational nodes and organizations. Specifically, OV-5 and OV-6c can be used together to model the operational process flow or workflow. Various models may be generated and used as a tool to conduct what-if analysis of the various workflows.

4 TECHNIQUES FOR USING ARCHITECTURE INFORMATION

Several analytical techniques for using architecture information have been developed by DoD user communities. Capability-Based Analysis, Mission Capability Packages, Key Interface Profiles, and Human Factors are described in more detail in the Deskbook. In addition, capability analysis and human factors are addressed in the Volume II product descriptions. Attributes that depict capabilities and relate them to systems, and attributes that represent the human role and set of skills needed to perform tasks and activities, have been added to products where applicable. Subsections below provide an introduction and overview of some of these topics.

4.1 CAPABILITY-BASED ANALYSIS

This section introduces the Air Force approach for capability-based analysis and associated Capability Reports.

4.1.1 The Situation

There is a strong interest within many DoD organizations to define and explore capability-based approaches for needs determination, analysis, planning, and acquisition. The Air Force, in their work on Air Force Task Forces, has developed concepts relating capabilities to integrated architectures and Doctrine, Organization, Training, Materiel, Leadership & education, Personnel, and Facilities (DOTMLPF).

4.1.2 Capability Reports

The Air Force has defined a set of Capability Reports that use architecture information to analyze capabilities and provide the resulting analysis in a manner that supports decision makers. The reports have the potential for providing a significant bridge between integrated architecture information and capability information that can provide the basis for decision making.

4.2 MISSION CAPABILITY PACKAGES

This section describes impediments to systems interoperability and integration within the DoD processes and introduces Mission Capability Packages (MCPs). The Navy developed MCPs as an approach for using architectures to achieve a rationalized and interoperable family of systems (FoS) providing required levels of mission capabilities.

4.2.1 The Situation

The traditional approach of allocating resources on a program-by-program basis is a major impediment to building a capability-focused FoS or system of systems (SoS). This approach has proved inadequate when addressing interoperability issues, mission capabilities, and the integration of related programs. The primary reason is because success in planning, programming, and budgeting is often measured by the durability and survivability of programs, not by the capability they provide to the operating forces. During the Defense Acquisition System's process (DoD 5000 series documentation), interoperability and integration generally receive insufficient attention. The execution of complex development efforts is carried out and problems other than interoperability become more immediately pressing. Modernization decisions on legacy systems are not necessarily apparent to the requirements, and to acquisition administrators and decision makers. The results of those decisions frequently impact interoperability.

4.2.2 The MCP Approach

The approach to remedy this situation is to integrate capability needs identification and analysis with the Planning, Programming, Budgeting, and Execution (PPBE) process to make milestones and other important program decisions dependent upon compliance with validated and approved architectures. At the heart of this solution is the concept of using relevant operational, systems, and technical architecture data derived from the architecture products listed in Table 1-1 of this volume and providing mission/capability-oriented collections of:

- Concepts of operations, processes, and organizational structures
- Sensors, networks, systems, and weapons
- Personnel, skills, and support services

These collections are treated as an integrated system and are termed MCPs (derived from the NCOW approach). **Figure 4-1** shows how the architecture views are used to support the analysis of FoS and SoS.

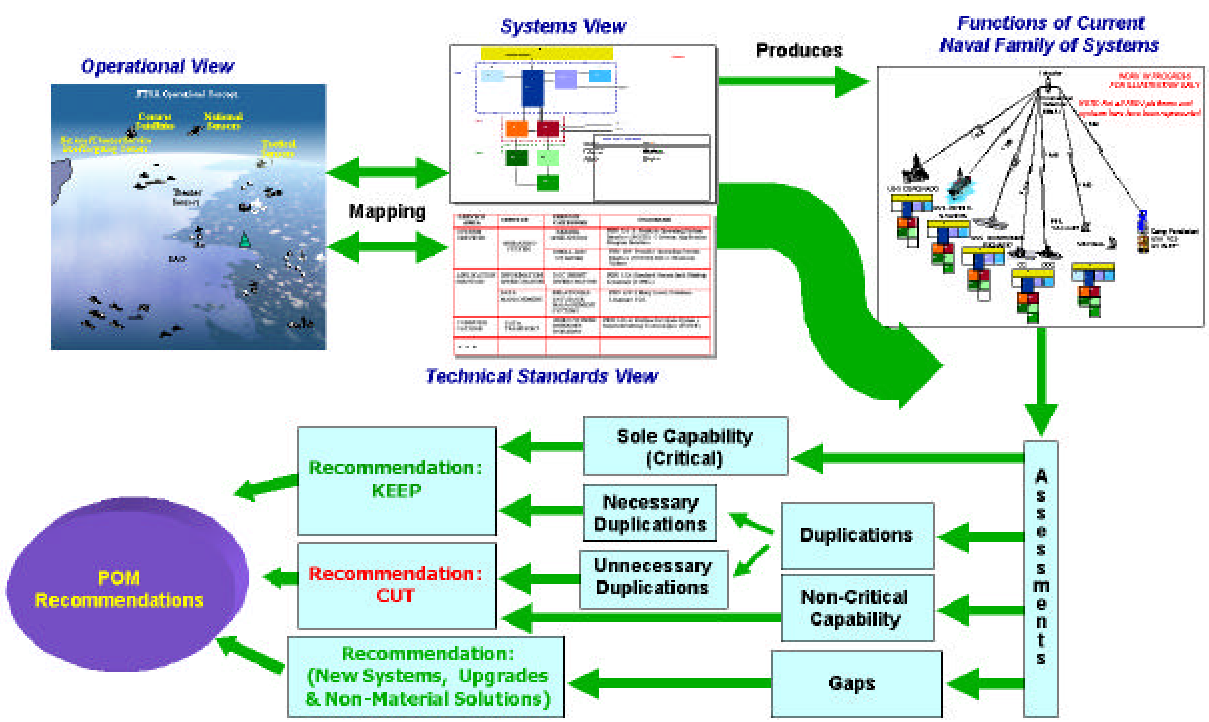


Figure 4-1. Using Architectures and Analysis to Influence POM Decisions

Because the use of architectures and architecture products are being mandated in DoD policy, this proposed MCP approach uses a capability-based architecture as the foundation for integrating the requirements, resource planning, and acquisition processes that currently exist. Analytical techniques included in the MCP approach address:

- Identifying duplications and gaps in systems and system functionality
- Examining system connectivity and interoperability
- Assessing architecture performance and behavior
- Aligning the evolution of system technologies and standards into an acquisition strategy

4.3 KEY INTERFACE PROFILES

This section characterizes key interfaces and summarizes the approach to their use in interoperability and other architecture-related issues.

4.3.1 The Situation

Enterprise architectures and interfaces go hand in hand. When a new system, application, or database is deployed into a new environment, it is inevitable that the stakeholders will need to define, design, and implement interfaces to other applications, systems, and databases that exist in the enterprise architecture. Knowing what needs to interface, how it needs to interface, and when an interface is required are all imperative for an architecture.

An approach for achieving interoperability that relies on the use of globally scoped standards generally cannot scale to the enterprise level. The inability to reach a consensus on a single standards profile will often lead to “multiple standards” (an oxymoron) for a given service area. Joint Staff/J6 and the Office of the Secretary of Defense for Networks and Information Integration developed the concept of managing interoperability through key interfaces as an outgrowth of the Global Information Grid architecture effort. An interface approach can be more manageable and legacy friendly than globally scoped standards because it does not dictate the internals of every system.

Per Military Handbook 61A, interfaces are defined by functional and physical characteristics that exist at a common boundary with co-functioning items and allow systems, equipment, software, and system data to be compatible. An interface may be designated as key when it spans organizational boundaries; is mission critical; there are capability, interoperability, or efficiency issues at that interface; or the interface is vulnerable or important from a security perspective. It may be more difficult to achieve necessary attributes when different agents (service, agency, organization) have ownership and authority over the hardware and software capabilities at the interface, or the interface impacts multiple acquisition programs.

4.3.2 The Key Interface Profile Approach

An integrated architecture relates mission-focused operations to information flow through specific interfaces between communications, hardware, and software. An integrated architecture also includes the technical standards applicable at those interfaces. Thus, an integrated architecture provides the basis for identifying key interfaces; defining capability, interoperability, or efficiency issues at both the functional and technical levels; and resolving those issues such that mission-based capabilities are achieved. Key Interface Profiles (KIPs) provide a net-centric approach for managing interoperability across the GIG based on configuration control of key interfaces. The KIP is the set of documentation produced as a result of interface analysis that designates an interface as key; analyzes it to understand it's architectural, interoperability, test and configuration management characteristics; and documents those characteristics in conjunction with solution sets for issues identified during analysis.

4.4 HUMAN FACTORS

This section discusses the importance of human factors in information technology (IT) and characterizes ways of addressing human factors within the architecture.

4.4.1 The Situation

While architectures provide a strong focus on the use of IT, they also provide opportunities to address the role of the human in accomplishing military operations or DoD business processes. Human factors play a significant role in how information is accessed and displayed and are also a strong influence in the design and operation of systems. If human factors are not represented in the architecture, then factors affecting design, manpower, training, and other human factor issues may be overlooked to the detriment of overall systems performance and mission accomplishment. Modest investment in human systems integration during architecture development has the potential to reduce total ownership costs.

4.4.2 Including Human Factors

Architectures provide a construct for describing human activities and the flow of information needed by humans to accomplish or support military operations. For most systems, humans play a significant role in how systems perform and are operated. Human factors should play a significant role in how systems are designed and how information is displayed. Before the detailed "how to" guidelines of human-computer interfaces can be implemented, the human dimension of the Operational View should be included and must factor in the analysis to help designers determine the scope of what information should be displayed or made available to humans.

Considering human factors in an architecture extends beyond computer interface design to issues such as manpower, personnel, training, and safety. Systems must be supported by sufficient manpower, and humans must be adequately trained, to operate the system in the context of an operational mission.

Modest investment in human systems integration during architecture development has the potential to reduce total ownership costs. Every engineering change proposal eliminated and every training program that can be reduced saves costs. Taking into account human factors in architecture development will also enhance overall systems performance by helping in the design of effective training programs, in validating adequate manning requirements, and by improving human performance through systems design.

Providing supplementary information on human factors within an architecture can link various aspects of the architecture from the human-use perspective and help collectively define and describe the role of the human in the overall system. The inclusion of human factors can characterize the logical relationship between the human and the "machine" operating as a total unit. Supplementing the architecture with human factors information supports human performance analyses as well as other systems engineering analyses such as requirements analysis, technical analysis, (system) performance analysis, and cost-benefit analysis.

4.5 ARCHITECTURE MEASURES

The Information Technology Reform Act requires organizations to define measures of performance (MOPs) for evaluating the impact and progress of their information systems. An integrated architecture description (one that consists of all three views) is essential to meet this requirement. For example, systems and/or system attributes (identified in the Systems View) and their MOPs must be assessed with respect to the utility they provide to the missions (identified in the Operational View in terms of measures of effectiveness [MOEs]). Similarly, systems must be assessed with respect to the standards and conventions that apply (identified in the Technical Standards View).

A major thrust of Federal legislation enacted in the mid 1990s is the requirement to justify proposed and existing systems investments by reporting improvements in mission effectiveness. Today, there continue to be extensive investigations on what MOPs and metrics should be used for systems. Linkages among the views are needed to provide a cohesive audit trail from MOEs, capability needs, and MOPs to the supporting systems and their characteristics, and to the specific technical criteria governing the acquisition/development of the supporting systems. The Federal Enterprise Architecture Performance Reference Model draft [OMB, 2003] specifies some MOEs. The following are three hierarchical types of performance measures; they are also depicted at the bottom of **Figure 4-2**.

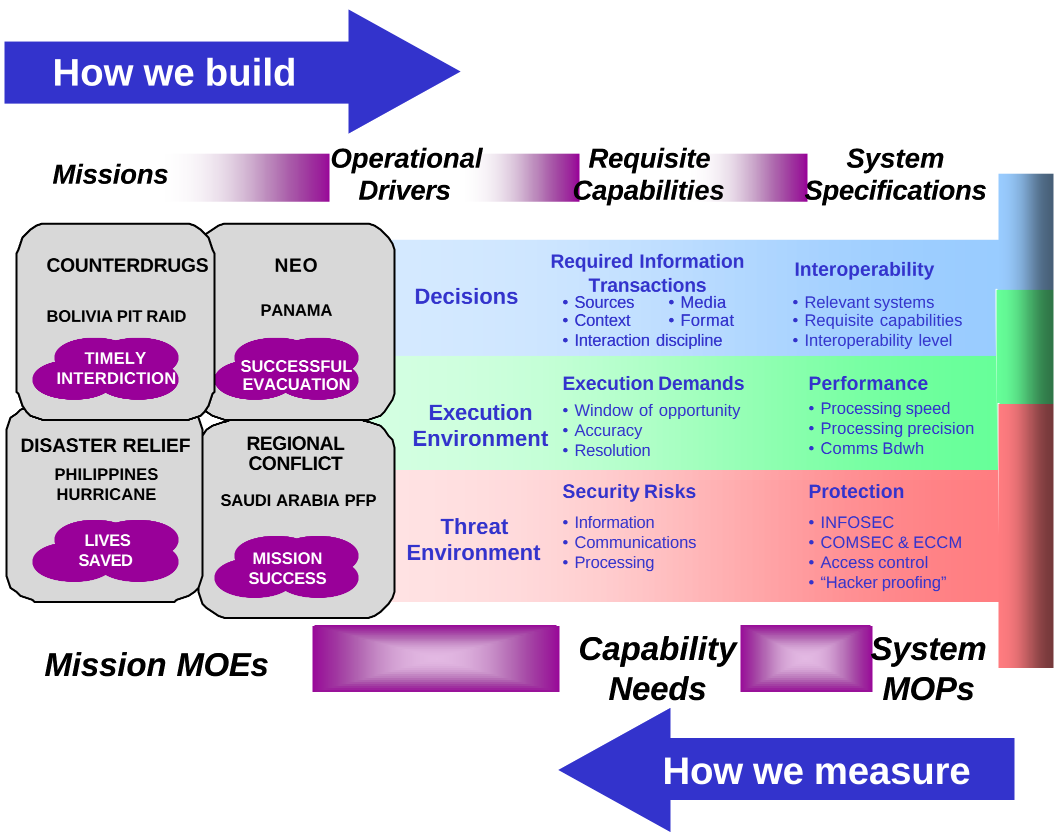


Figure 4-2. Cross-View Linkages and Measurements

- **Mission Measures of Effectiveness**. The first MOEs are generally subjective in nature, as they are derived from the overall high-level operational concept that is driving the creation of the architecture being developed. These operational MOEs reflect the necessary conditions or outcomes to ensure a reasonable or known degree of mission success. This starts the audit trail by which senior decision makers ensure their vision is being carried out in the architecture design.
- **Capability Needs**. The needs that must be met to ensure a reasonable degree of mission success are generally determined based on the critical decisions that need to be made, the nature of the execution environment, and the potential natural and adversary-induced threats that decision makers must consider. As indicated in the bottom of Figure 4-2, these measurable needs are expressed as "Capability Needs" that must be met by any viable systems solution.
- **System Measures of Performance**. Capability needs ultimately are translated into system specifications. For example, a need to satisfy a particular information exchange by disseminating a document of a certain size within a specified time window translates into a system-level exchange specification on the supporting communications system. The corresponding or demonstrated ability of the system to meet the specification is the system measure of performance.

Establishing strong linkages between the views of an architecture enables a better understanding of the implications of investment options on the ability to support the mission(s) of interest. Linkage between architecture views supports answering questions such as the following.

- How are typical system MOPs, such as speed, resolution, and interoperability, translated into the answer to the "so what?" question; i.e., how many more targets will be covered, or lives saved, as a result of bandwidth increasing from 56 kbps to T1 at a cost of $230M, or from increasing systems interoperability at a cost of $20M?
- What different types of crises can a given system effectively support if greater interoperability is achieved?
- Can a given force operate effectively under a variety of threat conditions?
- Can a virtual network be created by interfacing and scaling several smaller networks?

The ultimate linkages from systems and technology performance measures to mission MOEs generally require a sophisticated modeling and simulation (M&S) capability. A useful M&S capability may come close to wargaming a particular operation based on numerous assumptions, some validated, regarding decisionmaking basis, execution conditions and constraints, and postulated threats. The M&S capability will employ rule-of-thumb algorithms to generate a MOE's value based on various conditions with respect to their ability to be met or to be mitigated. Capabilities and other related attributes that enable M&S are detailed in Volume II.

5 ARCHITECTURE GUIDELINES, DESCRIPTION PROCESS, AND INTEGRATION

5.1 ARCHITECTURE GUIDELINES

The DoD Architecture Framework (DoDAF) contains four main types of guidance for architecture description: (1) a detailed description of the product types, (2) a discussion of standard architecture data elements and definitions, (3) guidelines that include a set of guiding principles and guidance for building architecture descriptions that are compliant with the Framework, and (4) a process for using the Framework to build an integrated architecture description. Section 1.4 introduced the products, and section 6 contains a discussion of the Core Architecture Data Model (CADM) and DoD Architecture Repository System (DARS). This section discusses the last two aspects of Framework guidance, namely architecture guiding principles and a process for building an integrated architecture description.

5.1.1 Guiding Principles

The following set of guiding principles for describing architectures is critical to the objectives of the guidance.

5.1.1.1 Architecture Descriptions Should be Built with a Purpose in Mind

An architecture should have a specific and commonly understood purpose to increase the efficiency of the effort and the utility of the resulting description. The purpose determines how wide and deep the scope should be, which characteristics to capture, and what time frames to consider. This principle applies equally to the description of an architecture as a whole or to any portion or view of an architecture. This principle can also apply to groups of architectures. If architecture descriptions built by various organizations are to be compared, it is important that they all be built from the start with the purpose of comparison in mind.

5.1.1.2 Architecture Descriptions Should be as Simple and Straightforward as Possible and Still Achieve the Stated Purpose

Developing overly complex architectures is costly in both time and money. Focusing the architecting effort is essential to obtain an acceptable return on investment. Care should be given to determining the level of detail appropriate to achieving the desired objectives of the architecture effort. The following are some of the areas that should be considered:

- Scope of the activity model
- Levels of decomposition of the activity model
- Degree of aggregation/disaggregation in the definition of the operational nodes and systems nodes. For example, in one architecture, the Joint Task Force (JTF) might be considered an operational node, but in another architecture, it may be necessary to decompose the JTF into its various operational elements such as the Joint Operations Center (JOC) and Joint Intelligence Center (JIC).

- Level of specificity in defining information elements in information exchanges. For example, in some efforts using *intelligence* as an information element might be sufficient. Other efforts may need to decompose *intelligence* into either specific types of intelligence reports or even further decomposition into the subject areas of the information (e.g., order of battle, military units, geographic locations, equipment type and numbers).
- Level of decomposition in defining a *system*. For example, the Global Command and Control System (GCCS) may be an appropriate level of specification for some efforts. In other architectures, it may be necessary to decompose GCCS into the primary applications relevant to the architecture.

5.1.1.3 Architecture Descriptions Should Facilitate, Not Impede, Communication Among Humans

Architecture descriptions must be structured to allow humans to understand them quickly and to guide the human thinking process in discovering, analyzing, and resolving issues. Extraneous information must be excluded and common terms and definitions must be used. Often, graphical representation of the architecture products using standard modeling techniques offers an excellent medium for rapid human understanding.

5.1.1.4 Architecture Descriptions Should be Relatable and Comparable Across DoD

Like the previous principle, this one requires the use of common terms and definitions. This principle also requires the use of a common set of architectural building blocks or reference documents as the basis for architecture descriptions. This principle dictates that products of a given type developed for different architectures must display similar information about their respective domains, in similar formats. The appropriate, common format and information content for each product type must be specified in architecture guidance, such as in this Framework.

In order to relate architectures, it is critical to capture external interfaces. Architecture descriptions must clearly describe external interfaces with Joint, multinational, and commercial components in a manner consistent with the method used to describe internal relationships.

5.1.1.5 Architecture Descriptions Should be Modular, Reusable, and Decomposable

Architecture descriptions should consist of related pieces that can be recombined with a minimal amount of tailoring, so that they can be used for multiple purposes. The set of products to be built, the characteristics to capture in those products, and high-level steps for using the Framework have been designed to ensure that the above principles are followed.

5.1.2 Framework Compliance Guidance

The following paragraphs provide guidance concerning compliance with the DoDAF. In order to comply with the Framework, architectures must:

- Provide the appropriate set of products based on intended use
- Use the common terms and definitions as specified in this document

- Be compliant with the Global Information Grid (GIG) Architecture
- Describe interoperability requirements in a standard way

5.1.2.1 Build the Appropriate Products Based on Intended Use

Determine the products to be built based on the intended use of the architecture. Figure 3-7 provides guidelines on products appropriate for various uses. Architectures must identify each product by the name specified in the Framework and capture the architecture data elements specified in Volume II.

5.1.2.2 Use Common Terms and Definitions

Architecture descriptions should use common and/or standardized terms and definitions. The criticality of common language during architecture product creation, analysis, comparison, and integration cannot be over emphasized. The control of vocabulary, to include the use of a common language for product names, architecture data elements, and common system data values helps to minimize potential misrepresentations and misunderstanding of shared information, and assists with architecture consistency and validation. The Framework defines a standard for architecture product names, standard architecture data elements, their attributes, and their relationships. The CADM defines the standard for these architecture data elements as entities and defines their relationships. The Framework requires that every architecture description contain an Integrated Dictionary that defines terms used in the architecture. Use of automated tools and a CADM-compliant data repository, such as DARS, facilitates commonality in architecture data names, attributes, and relationships.

5.1.2.3 Be Compliant with the GIG Architecture

Some issues that continually confront cross-organizational architecture analyses include aligning and interrelating architecture segments, ensuring correct and commonly understood interfaces across the boundaries, and identifying opportunities for integration. DoDD 8100.01, “GIG Overarching Policy,” requires that architectures developed by DoD Components must be compliant with the GIG Architecture.

As this Framework is finalized, the Directorate of Architectures and Integration in the Office of the Assistant Secretary of Defense for Networks and Information Integration is working with the DoD Community to develop a formal criteria for GIG compliance. At the time of this writing, the following are being considered:

- The architecture is integrated and architecture products conform to the DoDAF.
- The architecture is provided in database form in conformance with the CADM.
- The Technical Standards View derives from the current version of the Joint Technical Architecture or presents the case for new or unique standards, as necessary.
- The architecture is consistent with Net-Centric Operations and Warfare (NCOW) Reference Model.

5.1.2.4 Describe Interoperability Requirements

DoDI 4630.8, "Procedures for Interoperability and Supportability of IT and NSS," and CJCSI 6212.01C, "Interoperability and Supportability of NSS and IT Systems," define a mission-related, outcome-based process for achieving information technology (IT) and National Security Systems (NSS) interoperability. This process uses mission area integrated architectures as the basis for defining and relating IT and NSS interoperability requirements. Architecture descriptions should capture specific interoperability requirements. Architects should ensure that these requirements and the system and technical responses are clearly related to each other across the three views and their related products. One of the attributes of information exchange can be the level of interoperability required to meet mission needs.

5.2 THE GENERIC SIX-STEP ARCHITECTURE DESCRIPTION PROCESS

The following paragraphs discuss ways to apply the Framework in building architecture descriptions. A high-level, six-step process has been developed to provide some general guidance to the architect and to emphasize the guiding principles. This generic process should be tailored to specific organizations and purposes. The DoDAF Deskbook contains descriptions of some organizations' tailoring of the generic process. The Framework does not endorse any of these specific processes; they are simply provided as sources of inspiration for architects who are developing their own processes.

The following steps are fundamental to describing an architecture in accordance with the Framework and appear in the general sequence in which they often will be performed. **Figure 5-1** depicts this six-step process. For simplification, feedback loops have been largely eliminated. It should be understood, however, that many such iterations are likely to be encountered. The gray shaded area covering steps one through five is within the scope of Volumes I and II.

Step 1: **Determine the intended use of the architecture description**. Descriptions should be built with a specific purpose, whether the intent is support to investment decisions, requirements identification, system acquisition, interoperability evaluation, operations assessment, or any other intent. Before beginning to describe an architecture, an organization must determine, as specifically as possible, the issue(s) the description is intended to explore, the questions it is expected to help answer, and the interests and perspectives of the audience and users. In addition, the types of analysis that are expected to be performed must be considered; for example, knowing that the architecture may be used as input to specific models or simulations can affect what should be included and how the products should be structured. This focusing will make the architecture description effort more efficient and the resulting architecture more appropriately balanced and useful.

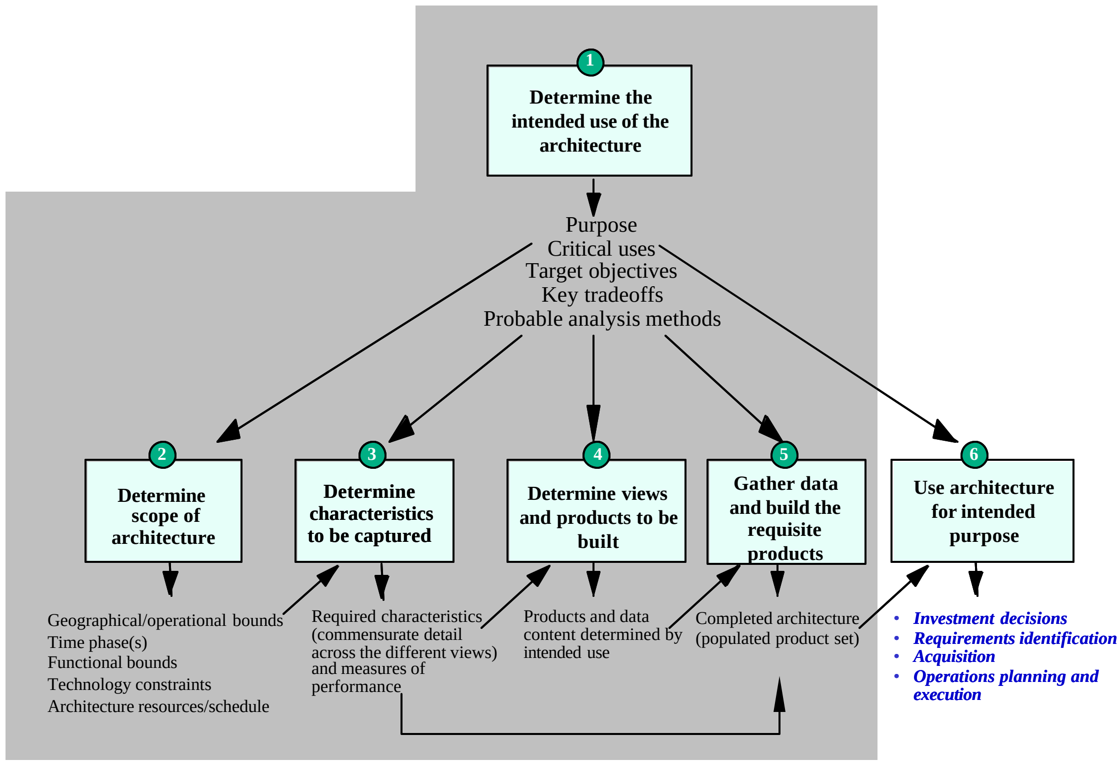


Figure 5-1. The Six-Step Process of Building an Architecture Description

Step 2: **Determine the architecture description's scope, context, environment, and any other assumptions to be considered**. Once the purpose or use has been decided, the prospective content of the architecture description can be determined. Items to be considered include, but are not limited to, the scope (missions, activities, organizations, time frames, etc.); the appropriate level of detail to be captured; the architecture's context within the "bigger picture"; operational scenarios, situations, and geographical areas to be considered; and the projected availability and capabilities of specific technologies during the time frame to be depicted. Project management factors that contribute to the above determinations include the resources available for describing the architecture, the resources and level of expertise available for analyzing the architecture, and availability of the necessary architecture data.

Step 3: **Based on the intended use and the scope, determine what information the architecture description needs to capture**. Care should be taken to determine the architecture information that needs to be included to satisfy the purpose. If pertinent information is omitted, the architecture description may not be useful; if unnecessary information is included, the architecture effort may prove infeasible given the time and resources available, or the description may be confusing and/or cluttered with details that are superfluous to the issues at hand. Care should be taken as well to predict the future uses of the architecture description so that, within resource limitations, it can be structured to accommodate future tailoring, extension, or reuse.

Architecture measures are a critical aspect of an integrated architecture description and should be considered at this early step in the architecture development effort. The developer wants to ensure each view (Operational, Systems, and Technical Standards) has measures identified in order to correctly determine what products need to be built, the level of detail in the products, and the attributes to be captured in the products. Measures may be both quantitative and qualitative. If the developer is unable to determine measures, then the end result will have less meaning to senior decision makers.

Step 4: **Determine products to be built**. Based on the understanding gained in Steps 1 through 3 and referring to the "Architecture Products by Use" Matrix (see Figure 3-7), determine which products to build and what architecture data must be gathered to build the products.

Step 5: **Gather the architecture data and build the requisite products**. The next step is to collect, correlate, and compose the necessary architecture data that will form the basis for the products. Volume II defines the architecture data elements associated with each product definition.

To facilitate integration with other architectures, architectures should be developed to be compliant with the GIG Architecture, and include relationships with applicable Joint and multinational components. If the architecture description needs some re-tailoring to serve its purpose, that tailoring should be done as efficiently as possible. It may be useful, resources permitting, to conduct some proof-of-principle analysis at various stages, i.e., make trial runs of step six using carefully selected subsets of the areas to be analyzed. Care should be taken to ensure that the products built are internally consistent and properly integrated. Use of automated tools and a CADM-compliant architecture data repository such as DARS can facilitate the architecture development process, assist in the use of common terms/definitions, and facilitate compliance with the GIG Architecture.

Step 6: **Use the architecture description for its intended purpose**. The architecture description will have been built with a particular purpose in mind. As stated in the discussion of Step 1, the ultimate purpose may be to support investment decisions, requirements identification, system acquisition, interoperability evaluation, operations assessment, or some other purpose. The architecture description facilitates and enables these purposes but does not provide conclusions or answers. For that, human and possibly automated analysis must be applied. The Framework does not attempt to dictate how this analysis should be performed; rather, the Framework intends to promote architecture descriptions that are sufficiently complete, understandable, and integratable to serve as one basis for such analysis.

5.3 ARCHITECTURE INTEGRATION

5.3.1 Two Types of Architecture Integrations

There are two types of architecture integration. The first type is integration across the three views of an architecture. The second type is integration across two or more architectures.

The term *integrated architecture* refers to an architecture description that has integrated Operational, Systems, and Technical Standards Views, i.e., there are common points of reference linking the Operational View (OV) and the Systems View (SV) and also linking the SV and the Technical Standards View (TV). For example, SV-5 relates operational activities from the Operational Activity Model (OV-5) to system functions from SV-4; the system functions are related to systems in the Systems Interface Description (SV-1), thus bridging the OV and SV. The standards in the Technical Standards Profile (TV-1) are cross-listed in certain systems products (such as network protocol and system data exchange), thus bridging the SV and TV. In an *integrated architecture*, products and their constituent architecture data elements are developed such that architecture data defined in one view are the same (i.e., same names, definitions, and values) as the corresponding architecture data referenced in another view.

In order to integrate multiple architecture descriptions, there must be sufficient commonalities so that critical relationships can be identified. Examples of these relations include:

- Activity sets (Do they overlap? Is one set a subset of the other? Does one activity set feed into the other? Are there dependencies between the sets?)
- Nodes (Are there organizations or systems nodes that are in multiple architectures and therefore supporting multiple activity sets?)
- Systems (What systems are represented in more than one architecture and therefore support multiple activity sets?)
- Standards (Are there conflicts between the technical standards in the multiple architectures?)

Four critical aspects of being able to integrate architectures are:

- Adherence to the Framework
- Compliancy with the GIG Architecture
- Compliance with the CADM
- Use of a common taxonomy for architecture data element values (such as names of operational nodes)

Adherence with the Framework provides both a common approach for developing architectures and a basic foundation for relating architectures. As noted in section 2.2.6, DoD has identified the GIG Architecture as the DoD IT architecture required by the Information Technology Reform Act (ITMRA) and has directed DoD Components to ensure that architectures they develop are compliant with the GIG Architecture. Compliancy with the GIG Architecture increases points of commonality across various architectures and aids in the ability to integrate those architectures. Adherence to the CADM ensures the use of common architecture data elements (or types). The CADM is discussed in section 6.4, the relevant CADM entities and relationships are provided as part of the product descriptions in Volume II, and an overview of the CADM is provided in the Deskbook. DoD currently does not have a common taxonomy for the architecture data element values, but such a taxonomy may develop as architecture development and use continues to mature. Use of a common Framework-compliant, CADM-compliant repository such as DARS can facilitate integration, because it ensures products are Framework-compliant, and ensures architecture data elements are CADM-compliant.

5.3.2 Scope of Cross-Architecture Integration

The scope of cross-architecture integration is illustrated here in terms of mission areas and levels of war. CJCSM 3500.04B, “Universal Joint Task Lists,” defines four levels of war: strategic national, strategic theater, operational, and tactical. **Figure 5-2** illustrates these four levels in context with a global, hierarchical view of operational missions. Note that the need to integrate multiple architecture descriptions is certainly not limited to Joint or cross-organizational considerations.

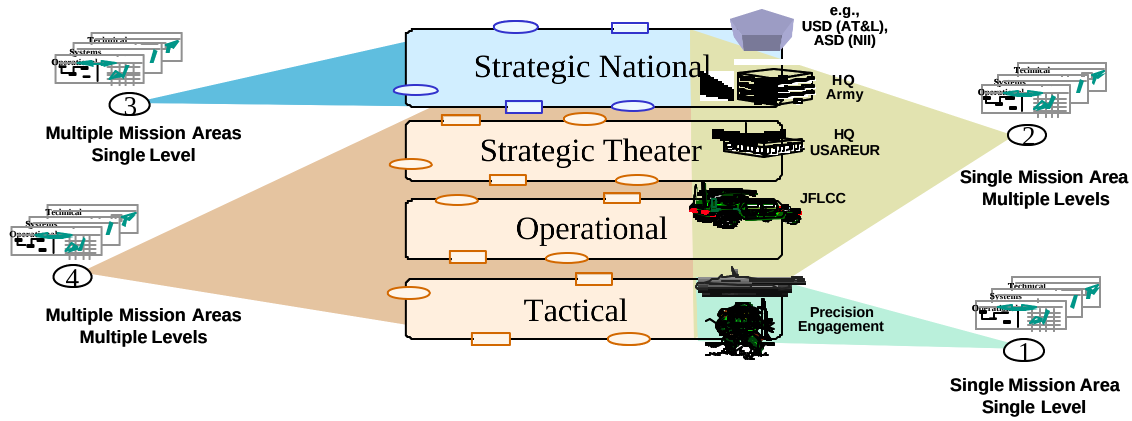


Figure 5-2. Four Levels of Architecture Integration

The first type of cross-architecture integration involves a single mission area within a single level of war. In the example shown in Figure 5-2, the focus is on Army operations at the tactical level. In addition to the obvious need to integrate the three views (and associated products) of an Army tactical architecture, there may be multiple architectures, in this case, at the same level covering different functional areas that need to be integrated, depending on the purpose and scope of the initiative. For example, development of a tactical-level Precision Engagement mission area architecture may require integrating tactical-level architectures depicting functional areas such as precision strike, intelligence preparation of the battlefield, and tactical command and control. The objective may be to ensure that information can flow appropriately and efficiently across and between the functional areas.

The second type of cross-architecture integration illustrated in Figure 5-2 still involves a single mission area, but the scope expands vertically to include operations across multiple levels of war. In this particular case, the objective may be examining opportunities to streamline operations or investments from top to bottom.

The third type of cross-architecture integration involves architecture initiatives that cross-cut multiple mission areas horizontally, within a single level of war. An example of this type involves architectures whose objectives are to investigate opportunities to exploit or leverage infrastructure capabilities.

The fourth illustrative type of cross-architecture integration involves multiple mission areas and multiple levels of war, where vertical and horizontal Joint relationships need to be articulated and examined. An example of this type is the integration of multiple mission area architectures at the strategic national, strategic theater, operational, and tactical levels in order to assess the effectiveness of intelligence support to command and control and to operations. This could involve examining tradeoffs between hierarchical support policies and practices, e.g., Theater-based JIC dissemination to lower-echelon users and direct dissemination from collectors to forces.

5.3.3 The Value of Integration

An integrated architecture, as defined in section 1.5, is essential for many types of analyses. Integrated views are necessary because they relate systems capabilities to how forces operate or how business is conducted, to assess interoperability, and to identify system duplications and gaps.

In addition, the ability to integrate multiple architectures is essential for addressing enterprise issues across a broad domain such as the DoD. It enables multiple groups to develop architectures with the focus that best meets their immediate needs. Those architectures can then be integrated to address issues that cross more than one area. No one architecture could hope to address the whole of DoD and its diversity of missions in sufficient detail where all of the various types of analyses, enabled by the architecture construct, could be supported. To depict and assess a large enterprise architecturally requires high-level, broad-scope architectures and detailed, more narrowly focused architectures. The high-level architectures may address multiple missions and business areas and depict primary relationships and dependencies. These architectures can provide a framing context for more detailed architectures that provide much finer granularity. The detailed architectures may address single missions or subsets of missions. To apply these more detailed architectures to the understanding of the enterprise, one must be able to integrate the architectures.

6 ARCHITECTURE DATA MODEL, REPOSITORY, AND TOOLS

6.1 OVERVIEW

This section discusses the benefits of repository-based architectures, introduces the Core Architecture Data Model (CADM), discusses the DoD Architecture Repository System (DARS), and provides an overview of automated tools.

Architectures have typically been developed as sets of graphical, tabular, or textual products. The products are mechanisms for visualizing, understanding, and assimilating the broad scope and complexities of the architecture data and architecture data relationships that comprise an architecture. The CADM provides the logical basis for moving architectures from compendiums of documents, spreadsheets, and graphics to architecture data that can be stored in architecture data repositories and manipulated with automated tools. The DARS is the common repository for architecture descriptions for the DoD. Multiple commercial tools may be used to manipulate the architecture data and generate products. However, interaction by architecture tools with DARS is still evolving.

6.2 ARCHITECTURE DATA

Although the Framework provides guidance on producing architecture descriptions via a set of products, these products are visual or textual representations of architecture data sets defining various attributes of the architecture. Because a given architecture data element frequently occurs in more than one product, the products must build on a set of common architecture data elements. In Volume II, a data element table for each product provides definitions of the metadata, i.e., the architecture data types that comprise the products. Attribute definitions are also defined for each architecture data type, which provide added detail about the data type characteristics. The architecture data elements provide structure for storing data about a given architecture that should be captured in the product and stored in the Integrated Dictionary.

An architecture data repository, consistent with the CADM, facilitates defining and depicting the requisite architecture data elements and their appropriate relationships. Using architecture data elements from a common data model (e.g., CADM) to build architecture products based on common modeling techniques (e.g., Framework products) ensures consistency of architecture data types and relationships across the architecture description. Ensuring that the architecture data elements associated with the architecture description are CADM-compliant also facilitates integration across various architecture descriptions.

6.3 BENEFITS OF STANDARDS-BASED REPOSITORY-BASED ARCHITECTURES

An architecture is considered to be repository-based if the architecture data portrayed in its architecture products are contained in a database, and if the architecture products are developed using modeling tools and techniques that are stored in a repository. Repository-based architectures—whose architecture data are structured in accordance with the CADM, are stored in a repository, and are manipulated with automated tools—provide efficiency and flexibility; enable architecture integration; and avoid complex, costly, and sometimes infeasible reconciliation. Benefits of repository-based architectures over graphic and text-based architectures include:

- Consistency across products and architecture views
- Consistency across multiple architectures facilitating integration or comparison
- Data reuse – developed once, used many times
- Flexible partitioning from different points of view (to include different mission areas or functional areas) – tailored to meet the need
- Basis for developing a taxonomy of data values
- Exchange among architecture data repositories, eliminating the need to manually re-enter architecture data
- Ability to use multiple architecture tools and modeling, simulation, and analysis tools
- Support for architecture data maintainability by standard import mechanisms from authoritative data sources
- Support for enterprise-level decision support systems, in which architecture data can be queried and analyzed, and reports generated for decision support

6.4 CADM AS A SPECIFICATION OF ARCHITECTURE DATA

The heart of interoperability is the preservation of meaning and relationships during architecture data reuse. An architecture data model is a structured representation of the architecture data elements pertinent to an architecture that also defines the relationships among architecture data. Agreement on an architecture data model is essential to the reuse of architecture data, as well as the implementation of architecture databases, regardless of the technology chosen (e.g., relational, object-oriented) for building and managing architecture databases. In addition, a common architecture data model can serve as the basis for defining common Extensible Markup Language (XML) tags for architecture data subject to import, export, product extraction, and direct exchange.

The CADM was developed cooperatively by representatives from the Office of the Secretary of Defense, Combatant Commands, Military Services, and Defense Agencies as the DoD standard architecture data model for Framework-based architecture data elements. [All-CADM, 200 3a, b, c] The CADM is built using the Integrated Definition for Data Modeling, IDEF1X [FIPS 184, 1993] methodology, notation, and forms. More than 95 percent of the entities and attributes from the CADM are approved as DoD architecture data standards. Using relational technology labels, for example, the entities from the CADM provide specifications for tables in a database, and the CADM attributes provide specifications for the fields (architecture data element attributes) in the rows of such tables.

The CADM abstraction shown in **Figure 6-1** depicts the following relationships (among many others):

- Operational Nodes perform many Operational Activities
- Operational Nodes require Information

- Information is related to (systems) Data
- Systems perform System Functions
- Systems have Performance characteristics, which are also related to a System Function being performed
- Standards apply to Systems and to System Functions

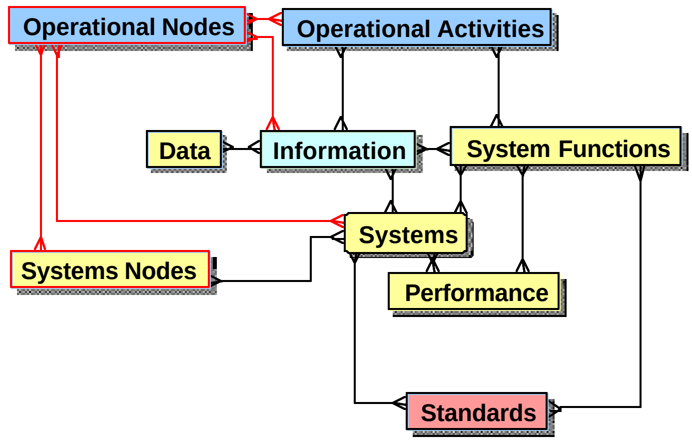


Figure 6-1. CADM Abstraction

CADM specifications define the entities and relationships for a DoD Architecture Framework (DoDAF) architecture data repository. CADM conformance comprises the minimum rules to enable conformant databases to exchange architecture data electronically. XML tags, structured according to the CADM, have been submitted to the DISA XML repository. The CADM is addressed in more depth in Volume II, and its specifications can be found on the Internet at http://www.dod.mil/nii/ (a data model diagram together with a three-volume report describing its entities and relation to Framework architecture data requirements).

6.5 DARS AS A REPOSITORY FOR ARCHITECTURE DATA

The Office of the Assistant Secretary of Defense for Networks and Information Integration is developing DARS as a DoDAF-compliant, CADM-compliant architecture data repository for hosting accredited DoD architecture data. Achieving initial operational capability in the summer of 2003, the repository is intended to be a central location for storing approved/ accredited architectures developed by the Commands, Services, and Agencies (C/S/As), and includes both legacy and newly accredited architectures. DARS provides a tightly controlled yet flexible repository integrating portal technologies, data/user auditing, security, query and retrieval, architecture data partitioning, and product visualization.

Intended users include those personnel (staff officers, civil servants, contractors) involved in designing and developing DoD architectures within individual Service and Agency components. Such users will include system architects, system technicians, database administrators, and system security officers.

DARS is an Oracle portal application operating in a Web-based environment (see **Figure 6-2**). It is initially targeted for use on the Secret Internet Protocol Router Network (SIPRNET). Future requirements may drive an expansion of the system to the Non-Secure Internet Protocol Router Network (NIPRNET). DARS permits personalized, Web-based access to user-specific interface screens and provides the ability to visualize architecture products and electronically modify, review, and exchange common and shared architecture information.

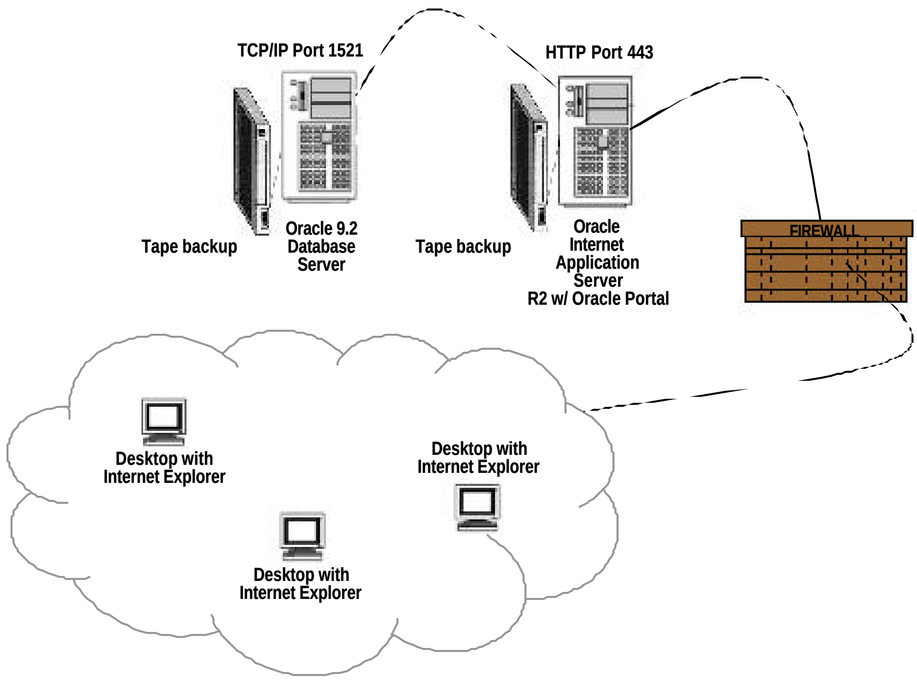


Figure 6-2. DARS Configuration

The DARS visualization capability provides for visual browsing of architecture products and is not intended to be an architecture design tool. It allows for the creation of on-the-fly visual representations for system users researching and analyzing current and target high-level architecture designs that have been captured by DARS.

DARS includes:

- CADM-compliant, structured architecture data
- A document repository for archiving legacy architecture segments that have been captured using non-database technologies (e.g., MS Word, MS PowerPoint, Adobe Acrobat)
- Reference architecture data

DARS can be used:

- As a reference for architecture data, lookup values, and codes
- To support documentation, guidance, training material, and other architecture-related information developed in non-structured form (e.g., MS Word, MS PowerPoint, Adobe Acrobat)

Users can query either structured or unstructured elements stored in the CADM-compliant area or the legacy document product archive.

DARS will provide a collaborative environment allowing users to share, review, and approve architecture segments based on C/S/A specific requirements. In the context of DARS, collaboration includes the:

- Ability to share complete architectures or architectural segments
- Ability to submit complete architectures or architectural segments—for review/approval/public consumption—to an approving authority based on C/S/A business processes
- Approval authority capability to grant/revoke interim approval authority
- Ability to track the architecture throughout the development and approval process
- Ability to pass notations between author and approving authority
- Approving authority notification of architectures requiring review
- Author notification of architecture review/approval

DARS architecture data will be physically partitioned by Service: Army, Air Force, Navy, and Marines, and, ultimately, possibly by the Joint Staff. In the full operating capability, architecture data will be partitioned at the C/S/A level, with each C/S/A responsible for content in their respective partitions.

C/S/As continue to maintain autonomous control over their architecture data stored within DARS. The Services, command, or unit that validates architecture data as accurate and complete also maintains the architecture data. Access privileges may be granted to other organizations, units, commands, or Services. Security and architecture data partitioning features allow users to maintain and share information on a record-by-record basis, ordered by organization to provide the highest level of security, from Service level to individual user. Each C/S/A is responsible for covering user account authorization, architecture product validation, architecture data access controls, roles, privileges, and rights. C/S/As may deem it necessary to further partition their architecture data by command, unit, organization, or area of responsibility. Each type of reference architecture data also will have organizational/Service-specific administrators.

The document management capability within DARS provides access to legacy architecture products in a variety of formats. Products may be (1) uploaded into private areas specifically established by organization, (2) shared with other Service-specific organizations, or (3) shared across C/S/As. Multiple versions of documents may also be stored for historical purposes. Documents (all formats except MS PowerPoint) will be indexed and available for key term searches.

The repository intent is to move selected architectural segments to and from commercial off-the-shelf (COTS) modeling toolsets for a formal rendition of current and target architecture designs. The Application Program Interface for DARS requires the COTS product to produce an export in XML format. Once the architecture segment data is exported, the XML file is uploaded to the parser to be formatted in CADM-compliant entities for loading into the DARS repository. The reverse process is implemented for extraction of architecture information from the repository for processing by a COTS toolset.

6.6 ARCHITECTURE TOOLS

Many types of architecture tools are now commercially available. Their primary role is to support architecture development, management of architecture data, analysis of architecture data, and transformation of architecture data into architecture products and other decision support reports. The Framework has had significant impact on the evolution of some of these software tools, specifically in achieving common forms of presentation.

The architecture tools available commercially are advancing rapidly, but today no single tool provides all the desired features. Generic architecture tools criteria and a tools adoption approach that incorporates best practices and current experience are provided in the Deskbook. Tools are grouped into (a) architecture modeling tools for producing architecture models and (b) repository tools that store architecture elements and models. c) modeling tools with scalable repositories for architecture data. Criteria are provided for evaluating:

- Architecture modeling tools (i.e., tools whose purpose is to create architecture models or products)
- Architecture repository tools (i.e., tools whose purpose is to create, store and provide access to architecture data)
- Customization (i.e., the ability of the tool suite to allow customization in support of varying user needs and user environments)
- Interoperability (i.e., the ability of the tool suite to interoperate with other tools)
- General characteristics (i.e., characteristics that apply to any of the tools in the tool suite such as usability and maintainability)
- Vendor characteristics (i.e., the ability of the vendor to support the tools set and to provide training for users)

7 ARCHITECTURE FRAMEWORK EVOLUTION

7.1 EVOLUTION OF THE FRAMEWORK

The Framework continues to evolve to better fulfill the changing needs of its user community. The following areas for future evolution of the Framework are discussed below:

- Portraying Net-Centric Operations and Warfare (NCOW)
- Executable architectures

Additional potential topics are listed in section 7.4

7.2 NET-CENTRIC OPERATIONS AND WARFARE

The DoD is moving toward a net-centric approach to operations, generally referred to as NCOW. NCOW includes the presence of a ubiquitous, secure, and robust network grid populated with all information including intelligence, non-intelligence, and raw and processed data. Central to this approach is the concept of task, post, process, and use (TPPU). Tasking includes user requests for information and is network-centric. Data-providers and users alike post information to the grid. Information and computing power is continuously shared with users over high bandwidth network communications. Processing in the NCOW context includes exploitation and analysis. Information is posted to the Global Information Grid (GIG) and becomes available to all appropriate users from that grid. Users can access information on the grid by either pulling information or subscribing to information, i.e., receiving information based on pre-defined criteria. The concept of post and use subsumes the traditional concept of pushing information from point to point. The basic principles of the Framework remain valid in the NCOW context. However, architecture products are expected to evolve as more experience is gained in developing architectures that portray NCOW. Notional examples of selected products portraying NCOW are provided in the Deskbook.

7.3 EXECUTABLE ARCHITECTURES

There is interest in evolving toward executable architectures to enable additional types of analysis and to support decision making. “Executable architecture” refers to the use of dynamic simulation software to evaluate architecture models. These executable architectures differ from the typical simulations because they are often generated directly from the architecture models via a semi-automated or automated process. Several purposes can be achieved with these specialized tools.

- The architecture model itself can be verified for internal self-consistency.
- Operational concepts can be simulated, observed dynamically, verified and refined.
- Operational plans can be examined and assessed.
- Tradeoffs between systems can be assessed.
- Architecture measures can be evaluated (given that metrics have been defined), which can support cost-benefit analyses and quantitative acquisition decisions.

However, there are some key factors in the process of constructing and using executable architectures that must be kept in mind. First, the aspect of automated or semi-automated generation directly from the architecture models is not simply for convenience. Rather, the driving factor is the accuracy of the executable model, in terms of consistency with the existing architecture models. Many typical simulation efforts diverge from the actual architecture models over time, leading to either the architecture being ignored in favor of the implemented design within the simulation, or, the simulation falls into disuse, as it is not able to keep up with the pace of the architecture modifications.

There are currently no standards for the format or process for constructing executable architectures. Research has been done on the minimum architecture elements needed to construct an executable architecture [Levis, 2000; Bienvenu, 2000; Axelsson, 2002; Neill, 2002], but additional research is still ongoing for specific architectural issues. Most executable models assume a distributed, message-passing paradigm for the architecture operations, which is very applicable in most of the situations encountered in current practice. However, the architecture data elements and the attributes required to construct executable models are specified in the DoD Architecture Framework (DoDAF) products (see Volume II).

It is also important to make the most of the executable architecture concept. The process by which this tool is applied must be integral to the overall systems engineering process. In other words, the development process must be configured to rely upon the results of the executable efforts for validation and refinement. Efforts to construct executable architectures for their own sake have generally not been beneficial to their programs. Executable architectures have immediate implications for process improvement, but also directly support the investment decision process by providing realistic and repeatable cost-benefit analyses.

7.4 OTHER EVOLUTION PLANS

Other areas for future evolution of the Framework include:

- Addressing baseline (current) and objective (target) architectures
- Alignment with the Federal Enterprise Architecture Reference Models
- Expansion of architecture uses beyond the Planning, Programming, Budgeting, and Execution process, Joint Capabilities Integration and Development System, Defense Acquisition System, and Operations
- More in-depth treatment of how architectures can be used to measure mission effectiveness (measures of effectiveness, capabilities, measures of performance)
- Architecture data management strategy for repository-based architectures that also addresses the use of DARS
- Common taxonomy of architecture data: As progress is made in the evolution of common architecture-related data entities and the evolution of corresponding repositories of architectures and architecture data, the Framework will evolve to address these subjects and provide guidance for their use
- Expansion of Framework training

ANNEX A
GLOSSARY

A

A&I	Architecture and Interoperability
A&T	Acquisition and Technology
ACC	Architecture Coordination Council
ACL	Access Control List
AFWG	Architecture Framework Working Group
AMS	Acquisition Management System
AoA	Analysis of Alternatives
API	Application Program Interface
ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
ASD(NII)	Assistant Secretary of Defense for Networks and Information Integration
AV	All-Views
AWG	Architecture Working Group

B

BPR	Business Process Reengineering
BRM	Business Reference Model

C

C2	Command and Control
C3	Command, Control, and Communications
C3	Command, Control, and Consultation (NATO usage)
C3I	Command, Control, Communications, and Intelligence
C4I	Command, Control, Communications, Computers, and Intelligence
C4ISP	Command, Control, Communications, Computers, and Intelligence Support Plan
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CADM	Core Architecture Data Model
CC	Combatant Commander
CCA	Clinger-Cohen Act of 1996 (also referred to as ITMRA)
CDD	Capability Development Document
CED	Capability Evolution Description

CIO	Chief Information Officer
CJCS	Chairman Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CONOPS	Concept of Operations
COTS	Commercial Off-the-Shelf
CPD	Capability Production Document
CPN	Colored PetriNet
CRD	Capstone Requirements Document
C/S/As	Commands, Services, and Agencies

D

DARS	DoD Architecture Repository System
DBMS	Database Management System
DDDS	DoD Data Dictionary System
DDL	Data Definition Language
DFD	Data Flow Diagram
DIAD	Department of the Navy Integrated Architecture Database
DoD	Department of Defense
DoDAF	DoD Architecture Framework
DoDD	DoD Directive
DoDI	DoD Instruction
DON CIO	Department of the Navy Chief Information Officer
DOTLPF	Doctrine, Organization, Training, Leadership & education, Personnel, and Facilities
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership & education, Personnel, and Facilities
DSS	Decision Support System
DTLOMS	Doctrine, Training, Leader Development, Organizations, Materiel, Soldiers

E

EEI	External Environment Interface
ER	Entity-Relationship
ERD	Entity Relationship Diagram

F

FAA	Functional Area Analysis
FEA	Federal Enterprise Architecture

FIPS	Federal Information Processing Standard
FNA	Functional Needs Analysis
FOC	Full Operational Capability
FoS	Family of Systems
FPI	Functional Process Improvement
FRP	Full Rate Production
FSA	Functional Solution Analysis

G

GCCS	Global Command and Control System
GIG	Global Information Grid
GUI	Graphical User Interface

H

HCI	Human Computer Interface
HR	Human Resources

I

IAP	Integrated Architectures Panel
IC	Intelligence Community
ICD	Initial Capabilities Document
ICD	Interface Control Document
ICOM	Input, Control, Output, and Mechanism
IDEF0	Integrated Definition for Activity Modeling
IDEF1X	Integrated Definition for Data Modeling
IER	Information Exchange Requirement
I/O	Input and Output
IOC	Initial Operational Capability
IOT&E	Initial Operational Test & Evaluation
IRM	Information Resources Management
ISP	Information Support Plan
IT	Information Technology
ITF	Integration Task Force
ITMRA	Information Technology Management Reform Act

J

JCIDS	Joint Capabilities Integration and Development System
JCS	Joint Chiefs of Staff

JF	Joint Forces
JIC	Joint Intelligence Center
JMA	Joint Mission Area
JOA	Joint Operational Architecture
JOC	Joint Operations Center
JROC	Joint Requirements Oversight Council
JSA	Joint Systems Architecture
JTA	Joint Technical Architecture
JTF	Joint Task Force
JWCA	Joint Warfighting Capability Assessment

K

KI	Key Interface
KIP	Key Interface Profile
KPP	Key Performance Parameters

L

LAN	Local Area Network
LISI	Levels of Information Systems Interoperability
LRIP	Low Rate Initial Production

M

MAIS	Major Automated Information System
MCEB	Military Communications Electronics Board
MCP	Mission Capability Package
MDAPS	Major Defense Acquisition Programs
MOE	Measure of Effectiveness
MOP	Measure of Performance
M&S	Modeling and Simulation
MTOE	Modified Table of Organization and Establishment

N

NATO	North Atlantic Treaty Organization
NCO	Net-Centric Operations
NCOW	Net-Centric Operations and Warfare
NIPRNET	Non-Secure Internet Protocol Router Network
NRO	National Reconnaissance Office
NSS	National Security Systems

O

OA	Operational Activity
OASD	Office of the Assistant Secretary of Defense
OIEM	Operational Information Exchange Matrix
OMB	Office of Management and Budget
OMG	Object Management Group
ONCD	Operational Node Connectivity Description
OO	Object-Oriented
OPLAN	Operational Plan
OSD	Office of the Secretary of Defense
OV	Operational View

P

PM	Program Manager
PPBE	Planning, Programming, Budgeting, and Execution
PPBS	Planning, Programming, and Budgeting System
PRM	Performance Reference Model
PSA	Principal Staff Assistants (OSD officials holding Presidential appointments, Assistants to the Secretary of Defense, and OSD Directors or equivalents who report directly to the Secretary or Deputy Secretary of Defense [DoDI 5025.1])

R

RGS	Requirements Generation System
ROI	Return On Investment

S

SA	Structured Analysis
SDEM	Systems Data Exchange Matrix
SECDEF	Secretary of Defense
SF	System Function
SIPRNET	Secret Internet Protocol Router Network
SoS	System of Systems
SRM	Service Component Reference Model
SSL	Secure Sockets Layer
SSM	Systems-Systems Matrix
SV	Systems View

T

TOE	Tables of Organization and Equipment
TPPU	Task, Post, Process, and Use
TRM	Technical Reference Model
TTP	Tactics, Techniques, and Procedures
TV	Technical Standards View

U

UJTL	Universal Joint Task List
UML	Unified Modeling Language
UOB	Unit of Behavior
URR	Universal Reference Resource
U.S.	United States
USD(A&T)	Under Secretary of Defense for Acquisition and Technology
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics

V

VJTA	Virtual Joint Technical Architecture
VPN	Virtual Private Network

W

WAN	Wide Area Network

X

XML	Extensible Markup Language

ANNEX B
DICTIONARY OF TERMS

The terms included in this Annex are used in some restrictive or special sense. Certain terms are not defined (e.g., event, function) because they have been left as primitives, and the ordinary dictionary usage should be assumed. Where the source for a definition is known, the reference has been provided in parentheses following the definition. Terms that are being used by both the DoD Architecture Framework (DoDAF) and the C4ISR Core Architecture Data Model (CADM) are marked with an asterisk.

*** Definitions shared between the Framework and CADM documents**

Analysis of Alternatives	The evaluation of operational effectiveness, operational suitability, and estimated costs of alternative systems to meet a mission capability. The analysis assesses the advantages and disadvantages of alternatives being considered to satisfy capabilities, including the sensitivity of each alternative to possible changes in key assumptions or variables. (CJCSI 3170.01C)
Analysis of Materiel Approaches	The JCIDS analysis to determine the best materiel approach or combination of approaches to provide the desired capability or capabilities. Though the AMA is similar to an AoA, it occurs earlier in the analytical process. Subsequent to approval of an ICD, which may lead to a potential ACAT I/IA program, Director Program Analysis & Evaluation provides specific guidance to refine this initial AMA into an AoA. (CJCSI 3170.01C)
Architecture Data Element	One of the data elements that make up the Framework products. Also referred to as architecture data type. (DoDAF)
Attribute	A property or characteristic. (Derived from DATA-ATTRIBUTE, DDDS 4363 (A)) A testable or measurable characteristic that describes an aspect of a system or capability. (CJCSI 3170.01C)
Capability	The ability to execute a specified course of action. (JP 1-02) It is defined by an operational user and expressed in broad operational terms in the format of an initial capabilities document or a DOTMLPF change recommendation. In the case of materiel proposals, the definition will progressively evolve to DOTMLPF performance attributes identified in the CDD and CPD. (CJCSI 3170.01C)
Capability Gaps	Those synergistic resources (DOTMLPF) that are unavailable but potentially attainable to the operational user for effective task execution. (CJCSI 3170.01C)
Capability Development Document	A document that captures the information necessary to develop a proposed program(s), normally using an evolutionary acquisition strategy. The CDD outlines an affordable increment of military useful, logistically supportable, and technically mature capability. (CJCSI 3170.01C)
Capability Production Document	A document that addresses the production elements specific to a single increment of an acquisition program. (CJCSI 3170.01C)
Capstone Requirements Document	A document that contains capability-based requirements that facilitates the development of CDDs and CPDs by providing a common framework and operational concept to guide their development. (CJCSI 3170.01C)

Communications Medium*	A means of data transmission.
Data	A representation of individual facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means. (IEEE 610.12)
Data Model	A representation of the data elements pertinent to an architecture, often including the relationships among the elements and their attributes or characteristics. (DoDAF)
Data-Entity*	The representation of a set of people, objects, places, events or ideas that share the same characteristic relationships. (DDDS 4362 (A))
Defense Acquisition System	The management process by which the Department of Defense provides effective, affordable, and timely systems to the users. (DoDD 5000.1)
DoD Component	The DoD Components consist of the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the Defense agencies, the DoD field activities, and all other organizational entities within the Department of Defense. (DoDD 8100.01)
Family of Systems	A set or arrangement of independent systems that can be arranged or interconnected in various ways to provide different capabilities. (DoDD 4630.5)
Format	The arrangement, order, or layout of data/information. (Derived from IEEE 610.5)
Functional Area*	A major area of related activity (e.g., Ballistic Missile Defense, Logistics, or C2 support). (DDDS 4198 (A))
Information	The refinement of data through known conventions and context for purposes of imparting knowledge.
Information Element	Information that is passed from one operational node to another. Associated with an information element are such performance attributes as timeliness, quality, and quantity values. (DoDAF)
Information Exchange	The collection of information elements and their performance attributes such as timeliness, quality, and quantity values. (DoDAF)
Information Exchange Requirement*	A requirement for information that is exchanged between nodes.
Information Technology	Any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes equipment used by a DoD Component directly, or used by a contractor under a contract with the Component, which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "IT" also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term "IT" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term "IT" includes National Security Systems (NSS). (DoDD 4630.5)

Initial Capabilities Document	Documents the need for a materiel approach to a specific capability gap derived from an initial analysis of materiel approaches executed by the operational user and, as required, an independent analysis of materiel alternatives. It defines the capability gap in terms of the functional area, the relevant range of military operations, desired effects and time. The ICD summarizes the results of the DOTMLPF analysis and describes why non-materiel changes alone have been judged inadequate in fully providing the capability. (CJCSI 3170.01C)
Integrated Architecture	An architecture consisting of multiple views or perspectives (Operational View, Systems View, and Technical Standards View) that facilitates integration and promotes interoperability across family of systems and system of systems and compatibility among related architectures (DoDD 4630.5) An architecture description that has integrated Operational, Systems, and Technical Standards Views with common points of reference linking the Operational View and the Systems View and also linking the Systems View and the Technical Standards View. An architecture description is defined to be an *integrated architecture* when products and their constituent architecture data elements are developed such that architecture data elements defined in one view are the same (i.e., same names, definitions, and values) as architecture data elements referenced in another view. (DoDAF)
Interoperability	The ability of systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. IT and NSS interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information, as required, for mission accomplishment. (DoDD 4630.5)
Joint Capabilities Integrated Development System	Policy and procedures that support the Chairman of the Joint Chiefs of Staff and the Joint Requirements Oversight Council in identifying, assessing, and prioritizing joint military capability needs. (CJCSI 3170.01C)
Key Performance Parameters	Those minimum attributes or characteristics considered most essential for an effective military capability. KPPs are validated by the JROC for JROC interest documents, by the Functional Capabilities Board for Joint Impact documents, and by the DoD Component for Joint Integration or Independent documents. CDD and CPD KPPs are included verbatim in the Acquisition Program Baseline. (CJCSI 3170.01C)
Link	A representation of the physical realization of connectivity between systems nodes.
Mission Area*	The general class to which an operational mission belongs. (DDDS 2305(A)) Note: Within a class, the missions have common objectives.
Mission*	An objective together with the purpose of the intended action. (Extension of DDDS 1(A)) Note: Multiple tasks accomplish a mission. (Space and Naval Warfare Systems Command)
Needline*	A requirement that is the logical expression of the need to transfer information among nodes.

Network*	The joining of two or more nodes for a specific purpose.
Node*	A representation of an element of architecture that produces, consumes, or processes data.
National Security Systems	Telecommunications and information systems operated by the Department of Defense – the functions, operation, or use of which (1) involves intelligence activities, (2) involves cryptologic activities related to national security, (3) involves the command and control of military forces, (4) involves equipment that is an integral part of a weapon or weapons systems, or (5) is critical to the direct fulfillment of military or intelligence missions. Subsection (5) in the preceding sentence does not include procurement of automatic data processing equipment or services to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (DoDD 4630.5)
Operational Activity Model	A representation of the actions performed in conducting the business of an enterprise. The model is usually hierarchically decomposed into its actions, and usually portrays the flow of information (and sometimes physical objects) between the actions. The activity model portrays operational actions not hardware/software system functions. (DoDAF)
Operational Activity	An activity is an action performed in conducting the business of an enterprise. It is a general term that does not imply a placement in a hierarchy (e.g., it could be a process or a task as defined in other documents and it could be at any level of the hierarchy of the Operational Activity Model). It is used to portray operational actions not hardware/software system functions. (DoDAF)
Operational Node	A node that performs a role or mission. (DoDAF)
Organization*	An administrative structure with a mission. (DDDS 345 (A))
Planning, Programming, Budgeting, and Execution Process	The primary resource allocation process of the DoD. One of three major decision support systems for defense acquisition, PPBE is a systematic process that guides DoD's strategy development, identification of needs for military capabilities, program planning, resource estimation and allocation, acquisition, and other decision processes.
Platform*	A physical structure that hosts systems or system hardware or software items.
Process	A group of logically related activities required to execute a specific task or group of tasks. (Army Systems Architecture Framework) Note: Multiple activities make up a process. (Space and Naval Warfare Systems Command)
Report	A combination of architecture data elements from one or more products combined with additional information. Reports provide a different way of looking at architecture data. (DoDAF)
Requirement*	A need or demand. (DDDS 12451/1 (D))
Role	A function or position. (Webster's)
Rule	Statement that defines or constrains some aspect of the enterprise.
Service	A distinct part of the functionality that is provided by a system on one side of an interface to a system on the other side of an interface. (Derived from IEEE 1003.0)

System	Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. (DoDAF)
System Data Element	A basic unit of data having a meaning and distinct units and values. (Derived from 8320.1) The architecture data element or type that stores data from the architecture domain (i.e., it has a value) that is produced or consumed by a system function and that has system data exchange attributes as specified in the Systems Data Exchange Matrix. (DoDAF)
System Data Exchange	The collection of System Data Elements and their performance attributes such as timeliness, quality, and quantity values. (DoDAF)
System Function*	A data transform that supports the automation of activities or information elements exchange. (DoDAF)
Systems Node	A node with the identification and allocation of resources (e.g., platforms, units, facilities, and locations) required to implement specific roles and missions. (DoDAF)
System of Systems	A set or arrangement of independent systems that are related or connected to provide a given capability. The loss of any part of the system will degrade the performance or capabilities of the whole. (DoDD 4630.5)
Task	A discrete unit of work, not specific to a single organization, weapon system, or individual, that enables missions or functions to be accomplished. (Extension from UJTL, JCSM 3500.04A, 1996). Note: Multiple processes accomplish a task; a single process may support multiple tasks. (Space and Naval Warfare Systems Command)
Universal Reference Resources	Reference models and information standards that serve as sources for guidelines and attributes that must be consulted while building architecture products. (DoDAF)

ANNEX C
REFERENCES

[All-CADM, 2003a]	All-DoD Core Architecture Data Model (All-CADM) for DoD Architecture Framework Version 1.0, Volume 1, *Overview Description*, Office of the DoD Chief Information Officer, Draft (In Preparation), February 2003, UNCLASSIFIED.
[All-CADM, 2003b]	All-DoD Core Architecture Data Model (All-CADM) for DoD Architecture Framework Version 1.0, Volume 2, *Technical Specification*, Office of the DoD Chief Information Officer, Draft (In Preparation), February 2003, UNCLASSIFIED.
[All-CADM, 2003c]	All-DoD Core Architecture Data Model (All-CADM) for DoD Architecture Framework Version 1.0, Volume 3, *Annexes*, Office of the DoD Chief Information Officer, Draft (In Preparation), February 2003, UNCLASSIFIED.
[ASN(RDA)CHENG, 2002]	Assistant Secretary of the Navy for Research, Development, and Acquisition, Chief Engineer, *Integration and Interoperability Strategy for Capabilities Based Acquisition*, Briefing, March 6, 2002.
[Axelsson, 2002]	Axelsson, J., "Model Based Systems Engineering Using a Continuous-Time Extension of the Unified Modeling Language (UML)," *Systems Engineering*, Vol. 5, No. 3, Fall 2002.
[Bienvenu, 2000]	Bienvenu, M., I. Shin, and A. Levis, "C4ISR Architectures III: An Object-Oriented Approach for Architecture Design," *Systems Engineering*, Vol. 3, No. 4, Fall 2000.
[Booch, 1999]	Booch, G., J. Rumbaugh, and I. Jacobson, *The Unified Modeling Language User Guide*, Addison-Wesley Publishing Company, Reading, Massachusetts, April 1999.
[C4ISR AWG, 1997]	C4ISR Architecture Working Group, *C4ISR Architecture Framework*, Version 2.0, 18 December 1997.
[C4ISR AWG, 1998]	C4ISR Architecture Working Group, *Levels of Information System Interoperability (LISI)*, 30 March 1998.
[C4ISR ITF, 1996]	C4ISR Integration Task Force, *C4ISR Architecture Framework*, Version 1.0, 7 June 1996.
[CJCSI 3170.01C, 2003]	Chairman, Joint Chiefs of Staff, Instruction, CJCSI 3170.01C, *Joint Capabilities Integration and Development System (JCIDS)*, June 24, 2003.
[CJCSM 3170.01, 2003]	Chairman, Joint Chiefs of Staff, Manual, CJCSM 3170.01, *Joint Capabilities Integration and Development System (JCIDS)*, June 24, 2003.
[CJCSM 3500.04C, 2002]	Chairman, Joint Chiefs of Staff, CJCSM 3500.04C, *Universal Joint Task List (UJTL)*, July 1, 2002.
[CJCSI 6212.01B, 2000]	Chairman, Joint Chiefs of Staff, J6, CJCSI 6212.01B, *Interoperability and Supportability of National Security Systems and Information Technology Systems*, 8 May 2000.
[CJCSI 6212.01C, 2003]	Chairman, Joint Chiefs of Staff, J6, CJCSI 6212.01C, *Interoperability and Supportability of National Security Systems and Information Technology Systems*, Draft 2003.

[DEB, 2000]	Defense Electronic Business, *Joint Electronic Commerce Architecture*, 2000.
[DeMarco, 1979]	DeMarco, Tom, *Structured Analysis and Systems Specification*, Prentice-Hall, Englewood Cliffs, New Jersey, 1979.
[Department of the Air Force, 2000]	Department of the Air Force, Air Force Instruction 33-124, Enterprise Information Technology Architectures, 1 May 2000.
[Department of the Navy, undated]	Department of the Navy Chief Information Officer, *Architecture Development Process Model*, Online, Available: www.doncio.navy.mil, undated.
[DISA, 2002]	Defense Information Systems Agency, *Joint Technical Architecture*, Version 4.0, 17 July 2002.
[DISC4, 1998]	Director for Information Systems, Command, Control, Communications and Computers (DSC4), *Army Enterprise Architecture Guidance Document*, Version 01.1, 23 December 1998.
[DoD JP 1-02, 2001]	Department of Defense Joint Publication, JP 1-02, "Dictionary of Military and Associated Terms," *Joint Publication 1-02*, August 2002.
[DoD TRM, 2001]	Department of Defense, *Technical Reference Model*, Version 2.0, 9 April 2001.
[DODD 4630.5, 2002]	Department of Defense Directive, DoDD 4630.5, *Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, January 11, 2002.
[DoDD 5000.1, 2003]	Department of Defense Directive, DODD 5000.1, *The Defense Acquisition System*, May 12, 2003.
[DoDD 8000.1, 2003]	Department of Defense Directive, DODD 8000.1, *Management of DoD Information Resources and Information Technology*, February 27, 2002; Administrative Reissuance March 20, 2002.
[DoDD 8100.01, 2003]	Department of Defense Directive, DODD 8100.01, *Global Information Grid Overarching Policy*, September 19, 2002.
[DoDI 4630.8, 2002]	Department of Defense Instruction, DODI 4630.8, *Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, May 2, 2002.
[DoDI 5000.2, 2003]	DoD Instruction 5000.2, *Operation of the Defense Acquisition System*, May 12, 2003.
[FIPS 183, 1993]	Integration Definition for Function Modeling (IDEF0), *Federal Information Processing Standards (FIPS) Publication 183*, 21 December 1993.
[FIPS 184, 1993]	Integration Definition for Data Modeling (IDEF1X), *Federal Information Processing Standards (FIPS) Publication 184*, 21 December 1993.
[HAREL, 1987a]	Harel, D., "Statecharts: A Visual Formalism for Complex Systems," *The Science of Computer Programming*, 1987, 8, pp. 231-274.
[HAREL, 1987b]	Harel, D., A. Pnueli, J.P. Schmidt, and R. Sherman, *On The Formal Semantics of Statecharts*, Proceedings, Second IEEE Symposium, Logic Computer Science, Dorset House, New York, 1987, pp. 54-64.

[IDEF3, 1995]	Information Integration For Concurrent Engineering (IICE) IDEF3, *Process Description Capture Method Report*, KBSI-IICE-90-STR-01-0592-02, Knowledge Based Systems, Incorporated, 1995.
[IEEE STD 1471, 2000]	Institute of Electrical and Electronics Engineers, IEEE STD 1471, *Recommended Practice for Architectural Description of Software-Intensive Systems*, The Institute of Electrical and Electronics Engineers, Inc., New York, New York, 2000.
[IEEE 610.12, 1990]	Institute of Electrical and Electronics Engineers, IEEE STD 610.12, *Standard Glossary of Software Engineering Terminology,* The Institute of Electrical and Electronics Engineers, Inc., Piscataway, New Jersey, 1990.
[ITMRA, 1996]	Information Technology Management Report Act (Clinger-Cohen Act of 1996).
[JS/J8, 2003]	Joint Staff, J8, *Introduction to the Joint Capabilities and Integration Development System*, Briefing, 2003, Online, Available: http://dod5000.dau.mil/.
[Levis, 2000]	Levis, A., and L. Wagenhals, "C4ISR Architectures I: Developing a Process for C4ISR Architecture Design," *Systems Engineering, Vol. 3*, No. 4, Fall 2000.
[Kristensen, 1998]	Kristensen, Lars M., S. Christensen, and Kurt Jensen, *The Practitioner's Guide To Coloured Petri Nets*, Springer-Verlag, 1998.
[Naqvi, 1989]	Naqvi, Shamim, and Shalom Tsur, *LDL: A Logical Language for Data and Knowledge Bases*, Computer Science Press, Rockville, Maryland, 1989.
[Neill, 2002]	Neill, C.J., and J. D. Holt, "Adding Temporal Modeling To The UML To Support Systems Design," *Systems Engineering, Vol. 5*, No. 3, Fall 2002.
[NATO, 2000]	Allied Data Publication 34, *NATO C3 Technical Architecture, Volume 2: Architectural Descriptions and Models*, Version 4.0, 7 March 2003, pp. 35-38.
[NRO, 2001]	National Reconnaissance Office, *National Reconnaissance Office Architecture Framework (DRAFT)*, Version 0.9, May 2001.
[OASD (C3I), 2000]	Office of the Assistant Secretary of Defense for (C3I), *Global Information Grid (GIG) Architecture (v1.0) DRAFT*, 31 December 2000.
[OMB, 2003]	Office of Management and Budget, *Business Reference Model (BRM) v2.0, Service Component Reference Model (SRM) v1.0, Technical Reference Model (TRM) v1.0, Released June 12, 2003, Performance Reference Model (PRM)*, Released July 2003.
[OMB, 2000]	Office of Management and Budget, *Circular A-130: Management of Federal Information Resources*, 30 November 2000.
[OMG, 2003]	Object Management Group, *Unified Modeling Language Specification*, Version 1.5, Framingham, Massachusetts, March 2003, Available: Internet: http://www.omg.org.
[OMG, 2001]	Object Management Group, *Unified Modeling Language Specification*, Version 1.4, Framingham, Massachusetts, Available: http://www.omg.org, September 2001.

[OMG, 2000]	Object Management Group, UML Primer 2000, *What Is OMG-UML and Why Is It Important?*, Framingham, Massachusetts, Available: http://www.omg.org/news/pr97/umlprimer.html, 2000.
[OMG, 2001]	Object Management Group, *UML 2001, Unified Modeling Language Specification*, Version 1.4, Framingham, Massachusetts, Available: http://www.omg.org, September 2001.
[Rumbaugh, 1991]	Rumbaugh, J., M. Blaha, W. Premerlani, F. Eddy, and W. Lorensen, *Object-Oriented Modeling and Design*, Prentice Hall, Englewood Cliffs, New Jersey, 1991.
[Rumbaugh, 1999]	Rumbaugh, J., I. Jacobson, and G. Gooch, *The Unified Modeling Language Reference Manual*, Addison-Wesley Publishing Company, Reading, Massachusetts, 1999.
[USD(A&T), ASD(C3I), J6, 1997]	Under Secretary of Defense (Acquisition & Technology), Assistant Secretary of Defense (Command, Control, Communications, and Intelligence [C3I], Joint Staff/J6 Memorandum, Subject: DoD Architecture Coordination Council, 14 January 1997.
[Warmer, 1999]	Warmer, Jos B., and Anneke G. Kleppe, *The Object Constraint Language*, Addison-Wesley, 1999.
[Zachman, 1987]	Zachman, J.A., A Framework for Information Systems Architecture, *IBM Systems Journal*, 26(3): 276-291, 1987, http://www.zifa.com/.