



**Homeland
Security**



Public Safety Architecture Framework

The SAFECOM Program
Department of Homeland Security
Volume I: Definitions and Guidelines

Version 1.0
February 10, 2006



SAFECOM

Background on Public Safety and Wireless Communications

Inadequate and unreliable wireless communications have been issues plaguing public safety organizations for decades. In many cases, agencies cannot perform their mission-critical duties. These agencies are unable to share vital voice or data information via radio with other jurisdictions in day-to-day operations and in emergency response to incidents including acts of terrorism and natural disasters.

According to a report published by the National Task Force on Interoperability (February 2003), the public safety community has identified the following key issues that hamper public safety wireless communications:

- Incompatible and aging communications equipment
- Limited equipment standards
- Limited and fragmented radio spectrum
- Limited and fragmented planning and coordination
- Limited and fragmented budget cycles and funding

In short, the Nation is heavily invested in an existing infrastructure that is largely incompatible. The SAFECOM Program was established by the Office of Management & Budget and approved by the President's Management Council to address the public safety communications issues identified above.

The SAFECOM Program

SAFECOM, a communications program of the Department of Homeland Security's (DHS) Office for Interoperability and Compatibility (OIC), with its federal partners, provides research, development, testing and evaluation, guidance, tools, and templates on communications-related issues to local, tribal, state, and federal public safety agencies. The OIC is managed by the Science and Technology (S&T) Directorate's Office of Systems Engineering and Development (SED).

SAFECOM, a public safety practitioner-driven program, is working with existing federal communications initiatives and key public safety stakeholders to address the need for better technologies and processes for the cross-jurisdictional and multi-disciplinary coordination of existing systems and future networks. SAFECOM harnesses diverse federal resources in service of the public safety community. The scope of this community is broad, including more than 60,000 local and state public safety agencies and organizations. Federal customers include agencies engaged in public safety disciplines such as law enforcement, firefighting, public health, and disaster recovery, as well as federal agencies that provide funding and support to state and local public safety agencies. SAFECOM makes it possible for the public safety community to leverage resources by promoting coordination and cooperation across all levels of government.

SAFECOM's Near-Term Initiatives

- Develop a process to advance standards that improve public safety communications interoperability
- Develop and disseminate grant guidance for all agencies providing grants for public safety communications and interoperability
- Provide tools and models for communications and interoperability training and technical assistance
- Create a one-stop shop for public safety communications and interoperability
- Develop, test, and evaluate technologies for public safety communications and interoperability

SAFECOM'S Long-Term Goals

- Achieve a systems-of-systems environment supported by communications standards, tools, and best practices
- Facilitate coordination of funding assistance through tailored grant guidance to maximize limited resources available for public safety communications and interoperability
- Pilot tools and methods as national models for public safety at the rural, urban, state, and/or regional levels
- Provide policy recommendations to promote efficiency in public safety communications

Publication Notice

Abstract

This document provides definitions, guidelines, and uses of the Public Safety Architecture Framework (PSAF).

The PSAF supports the development of interoperable and interactive architectures for public safety organizations. It uses a structured approach and common methodologies for defining and resolving wireless communications interoperability challenges related to public safety.

Change Log

Version	Date	Changes
1.0 Draft	April 5, 2005	Initial Draft Document
1.0 Draft	June 2, 2005	Edited text and organization
1.0 Draft	December 15, 2005	Minor text additions and edits as proposed by the PSAF working group and the executive level of SAFECOM
1.0	February 10, 2006	Text and format edits.

ACKNOWLEDGEMENTS

The SAFECOM program extends its appreciation to the many public safety practitioners, individuals, and government organizations that directly contributed to the creation of the PSAF.

Executive Summary

The SAFECOM process for identifying and developing standards began with the Public Safety Statement of Requirements (PS SoR). Those requirements are driving the vision for a migration from current *as-is* architectures to the future *to-be* interoperable public safety communications enterprise architecture. The Public Safety Architecture Framework (PSAF) provides an industry-validated enterprise architecture methodology to plan and develop the migration from current public safety architectures to the interoperable systems outlined in the PS SoR.

Three key living documents describe and reflect the PSAF methodology:

- *PSAF Volume I* provides definitions, guidelines, and related background material.
- *PSAF Volume II* contains detailed descriptions of the three PSAF views and the products that create each of the views.
- *PSAF Volume III* will document procedures for using the methodology outlined in *PSAF Volume I* and *PSAF Volume II* upon development of a supporting PSAF tool vetted with the practitioner community. Note that *PSAF Volume III* will likely be a user guide, although for simplicity it is referred to here as *PSAF Volume III*.

PSAF Volume I and *PSAF Volume II* draw upon the organization and discussion of architecture principles and concepts published in Department of Defense Architecture Framework (DoDAF) documents.¹

The PSAF documents will evolve as public safety provides additional input and as lessons are learned through application in the field. Although the fundamental approach will remain the same, the PSAF documents will be modified as necessary to ensure the usefulness of the PSAF across multiple disparate agencies. Lessons learned during development and piloting of the PSAF methodology may result in updates to Volume I & II. As the PSAF evolves, best practices will be developed to support a variety of applications including interoperability analysis, gap analysis, systems planning, systems migration, business case development, and RFP development.

Audience

PSAF Volume I and *PSAF Volume II* describe process architecture goals to technology architects and engineers tasked with implementing public safety wireless communications networks. While volumes I and II are not meant for end-user public safety practitioners, future documentation will target end-user practitioner needs.

Structured Process Concepts

The term *architecture framework* (AF) may not be as commonly known as *enterprise architecture* (EA), yet both concepts are associated with the same structured process that industry and government around the globe use to accomplish mission goals and save resources. While the concept of an enterprise

¹ DoD Architecture Framework Working Group, *DoD Architecture Framework Version 1.0*, “Volume I: Definitions and Guidelines,” and “Volume II: Product Descriptions,” February 2004.

architecture has its roots in the information technology (IT) world, it also fits the voice, data, and video applications of the public safety wireless communications world.

Enterprise Architecture Successes

The Enterprise Architecture Interest Group (www.eaig.org) points out impressive EA implementation successes by such companies as Volkswagen of America, Disney, Best Buy, GM, and Swiss Mobile. At the same time, the General Accountability Office (GAO) has, for over a decade, promoted the creation of EAs through the use of AFs. The GAO recognizes that AFs can clarify and help optimize the interdependencies and relationships between business operations, the underlying infrastructure, and the supporting applications across a large federated organization.² The Office of Management and Budget (OMB), Federal Enterprise Architecture Program Management Office, and Federal Departments and Agencies have concurred with this assessment and are actively undertaking EA planning and implementation. It is logical that public safety apply the same structured approach that uses a common methodology provided by an AF, to produce the Public Safety Architecture Framework (PSAF) for defining and resolving large-scale interoperability challenges.

Structured Approach to Interoperability

The architecture framework outlines “what” the overall structured approach is for assisting interoperability and, through the details of this structure, indicates “how” the architecture and its components will operate through the development of interface standards. In short, the PSAF provides rules and guidance for developing and presenting architecture descriptions.

The PSAF provides the following three perspectives (or views) of public safety communications and information systems. The combination of these three views form a comprehensive architecture description.

- The Operational View (OV) — Shows how public safety performs its mission
- The Systems View (SV) — Shows the systems of equipment and the flows of information that support public safety
- The Technical Standards View (TV) — Shows the technical rules and guidelines that allow these systems to interoperate.

The PSAF supports the development of interoperating and interacting architectures. It defines the preceding three related views of architecture: OV, SV, and TV as depicted in [Figure 4](#) in [Section 2.2](#). Each view is composed of sets of architecture data elements that are depicted via graphic, tabular, or textual products. The PSAF also clearly defines the relationships between these architectural views and the data elements they contain.

Quick Model Analysis

By using the PSAF to develop architectural models, you can perform a swift, simple, and automated analysis to determine if the communication systems of two public safety agencies in the same city, or two

² GAO-04-798T, “The Federal Enterprise Architecture and Agencies’ Enterprise Architectures are Still Maturing,” May 19, 2004.

different counties, for example, can interoperate. You apply the PSAF in the same way to both organizations to create common architectural descriptions of each. This provides an accurate comparison of organizations. If you determine the two systems are non-interoperable, the PSAF will also identify the interfaces that need further standards development.

While the PSAF will greatly assist the standards process related to communications interoperability by focusing on interfaces, it will not dictate specific technical solutions. This limitation will allow public safety to later consider creative and competing alternative architectures, as the PSAF is applied to various technologies.

The PSAF is a necessary step in identifying gaps in public safety needs and is therefore necessary to identify where standards need to be developed. As such, the PSAF, and the standards, will be carefully vetted by practitioners within the public safety governance structure.

Version 1.0 of the PSAF defines a common public safety architecture development, presentation, and integration approach for mission-critical operations as well as business operations and processes. The intent of the PSAF is to ensure the comparison and relation of architecture descriptions across organizational boundaries, including jurisdictional and first responder discipline boundaries.

This document applies to architectures developed by and for fire response organizations, emergency medical, and law enforcement agencies and services. In addition, any agency that needs to integrate with public safety agencies will find it useful to apply the PSAF.

Organization of this Volume

Volume I includes the following sections:

- Section 1 **Introduction** describes the purpose of an architecture framework, identifies the components of the PSAF, and outlines related Government policies.

(See Section 1, “Introduction.”)

- Section 2 **Architecture Basics — Views, Products, and Data** contains a brief outline of architecture, including view definitions, products, and data models.

(See Section 2, “Architecture Basics — Views, Products, and Data.”)

- Section 3 **Architecture Uses** includes a product-by-use matrix (Figure 7 in Section 3.6) that provides guidelines for determining products relevant to each of the public safety processes. Provides representative uses of the three views and the value of architectures in the sense of varying uses for different users.

(See Section 3, “Architecture Uses.”)

- Section 4 **Techniques for Using Architecture Information** contains a brief overview of some techniques for using architectures in conducting analyses. Outlines interface profiles and human factors.
- (See Section 4, “Techniques for Using Architecture Information.”)
- Section 5 **Architecture Guidelines, Description Process, and Integration** contains a description of architecture development guidelines and includes a set of guiding principles, PSAF compliance guidelines. Also contains a generic process for developing an architecture description, as well as a discussion of architecture integration.
- (See Section 5, “Architecture Guidelines, Description Process, and Integration.”)
- Section 6 **Architecture Data Model, Repository, and Tools** discusses the benefits of repository-based architectures and the need for a common Architecture Repository System (ARS) for storing and retrieving architecture data and automated tools to enable substantive analysis.
- (See Section 6, “Architecture Data Model, Repository, and Tools.”)
- Section 7 **Architecture Framework Evolution** describes some of the candidate areas for further evolution of the PSAF.
- (See Section 7, “Architecture Framework Evolution.”)
- Appendix A **Glossary of Acronyms** lists the terminology and acronyms used in this document.
- (See Appendix A, “Glossary.”)
- Appendix B **Dictionary of Terms** developed at the SAFECOM-AGILE-NIST (National Institute of Standards and Technology) Summit on Interoperable Communications for Public Safety.
- (See Appendix B, “Dictionary of Terms.”)
- Appendix C **Dictionary of UML Terms** identifies Universal Modeling Language terms used in this document. UML is a graphical language for visualizing, specifying, constructing, and documenting the artifacts of a software-intensive system.
- (See Appendix C, “Dictionary of UML Terms.”)

Appendix D **References** identifies the prior publications referenced in this document.
(See Appendix D, “References.”)

Table of Contents

1	Introduction	1
1.1	Purpose and Scope.....	1
1.2	Architecture Overview	1
1.3	Related Government Policy and Legislation	2
1.3.1	OMB Circular A-130.....	2
1.3.2	Federal Enterprise Architecture Reference Models.....	3
1.3.3	National Response Plan.....	5
1.3.4	Public Safety Statement of Requirements	6
2	Architecture Basics - Views, Products, and Data	7
2.1	Architecture Descriptions.....	7
2.2	Architecture View Definitions.....	7
2.2.1	Operational View.....	8
2.2.2	Systems View	8
2.2.3	Technical Standards View	8
2.3	All Views.....	9
2.4	Architecture Products	9
2.5	Integrated Architecture	11
2.6	Architecture Data Model	12
2.7	Architecture Framework Data Model.....	12
3	Architecture Uses	13
3.1	Representative Uses of the Three Views	13
3.1.1	Use of the Operational View	14
3.1.2	Use of the Systems View.....	15
3.1.3	Use of the Technical Standards View.....	16
3.2	Linkages Among the Views	16
3.3	Relationships Among Products	17
3.4	Uses of Integrated Architectures	17
3.5	The Value of Architectures – Different Uses for Different Users.....	18
3.5.1	Interoperability Between Public Safety Agencies	18
3.5.2	Legacy/Project 25 System Extended with Interim Interoperability Device	20
3.5.3	Legacy System to Project 25 System	20
3.5.4	Migration to PS SoR-Based System.....	21
3.6	Products According to Use.....	21
3.1.1	Overview and Summary Information (AV-1)	22
3.1.2	Integrated Dictionary (AV-2).....	23
3.1.3	Operational Node Connectivity Description (OV-2).....	23
3.1.4	Operational Information Exchange Matrix (OV-3).....	23
3.1.5	Operational Activity Model (OV-5).....	24
3.1.6	Systems Interface Description (SV-1).....	24

3.1.7	Technical Standards Profile (TV-1)	24
4	Techniques for Using Architecture Information	26
4.1	Key Interface Profiles	26
4.1.1	The Situation for Assessing Interoperability	26
4.1.2	The Key Interface Profile Approach	26
4.2	Human Factors	27
4.2.1	Benefits and Cost	27
4.2.2	Including Human Factors	27
5	Architecture Guidelines, Description Process, and Integration	31
5.1	Architecture Guidelines	31
5.1.1	Guiding Principles	31
5.1.2	PSAF Compliance Guidance	32
5.2	The Generic Six-Step Architecture Description Process	33
5.2.1	Determine the Intended Use	34
5.2.2	Determine the Scope	34
5.2.3	Determine Information to Capture	35
5.2.4	Determine Products to Build	35
5.2.5	Gather Data and Build Products	35
5.2.6	Use Architecture for its Intended Purpose	36
5.3	Architecture Integration	36
5.3.1	Two Types of Architecture Integration	36
5.3.2	Scope of Cross-Architecture Integration	37
5.3.3	The Value of Integration	38
6	Architecture Data Model, Repository, and Tools	39
6.1	Overview	39
6.2	Architecture Data	39
6.3	Benefits of Standards/Repository-Based Architectures	39
6.4	Architecture Framework Data Model	40
6.5	Public Safety Architecture Repository System	40
6.6	Architecture Tools	41
7	Architecture Framework Evolution	43
7.1	PS SoR-Based Public Safety Operations	43
7.2	Executable Architectures	43
7.3	Other Evolution Plans	44
	Appendix A -- Glossary of Acronyms	45
	Appendix B -- Dictionary of UML Terms	55
	Appendix C -- References	61

List of Figures

Figure 1:	Products Keyed to OMB Circular A-130.....	3
Figure 2:	Federal Enterprise Architecture Reference Models	4
Figure 3:	Federal Enterprise Architecture Business Reference Model Version 2.0	5
Figure 4:	Linkages Among the Views	8
Figure 5:	Operational Architecture Granularity Required for Systems Analyses	15
Figure 6:	Relationships Among the Products and Architecture Data Elements	17
Figure 7:	Architecture Products by Use.....	22
Figure 8:	The Six-Step Process of Building an Architecture Description	34
Figure 9:	Four Levels of Architecture Integration.....	37

List of Tables

Table 1	List of Products	10
---------	------------------------	----

1 Introduction

1.1 Purpose and Scope

The Public Safety Architecture Framework (PSAF) defines a common approach for public safety architecture³ description, development, presentation, and integration. It applies for public safety operations as well as business operations and processes. The intent of the PSAF is to ensure the comparison of architecture descriptions across organizational boundaries (e.g., discipline, local, regional, state, tribal, national, and multinational).

1.2 Architecture Overview

This section offers a quick overview of a few basic PSAF concepts. See [Section 2](#) for greater detail. An *architecture description* is a representation of a defined domain in terms of its component parts. The PSAF defines three major perspectives, or views, that logically combine to describe an architecture:

- Operational View (OV)
- Systems View (SV)
- Technical Standards View (TV)

An *architecture description* may be defined several ways. It is a representation of a defined domain, or area of activity, in terms of its component parts. An architecture description is also defined as a representation of a current or future real-world configuration of resources, rules, and relationships.

An architecture description is composed of *architecture products* that are interrelated within each view and are interrelated across views. Architecture products are data elements you depict graphically, textually, and tabularly to identify architecture components and model their relationships. Architecture products describe characteristics pertinent to the architecture's intended use.

An architecture is considered an *integrated architecture* when the data elements of products are defined in one view the same as architecture data elements in another view. That is, they have the same names, definitions, and values. In an integrated architecture, an architecture description has integrated OVs, SVs, and TVs. Common points of reference link the OVs and the SVs, as well as the SVs and the TVs.

The term *architecture* is generally used both to refer to an architecture description and an 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 implementation phase of the system development life-cycle process, the architecture description is then transformed into a real implementation of capabilities and assets in the field. The PSAF itself does not address this representation-to-implementation transformation process, but references policies that are relevant to that process.

³ “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.” (IEEE STD 1471, 2000)

Note that this document uses the term *architecture* as a shorthand for *architecture description*, but occasionally for emphasis uses the term *architecture description*. References to architecture implementations use the term *architecture implementation*. Supplements to the PSAF will define specific processes, which will detail the creation of architecture descriptions that help architectural implementation for a defined purpose.

1.3 Related Government Policy and Legislation

Several Federal policies related to the development of architecture descriptions are worth noting. The next sections highlight aspects of the following policies:

- OMB Circular A-130
- Federal Enterprise Architecture Reference Models
- National Response Plan
- Public Safety Statement of Requirements

1.3.1 OMB Circular A-130

OMB provides guidance on putting into effect the Information Technology Management Reform Act (ITMRA) (now the Clinger-Cohen Act), in Management of Federal Information Resources, revision November 30, 2000. This publication is also known as Circular No. A-130⁴ (OMB, 2000). The document addresses both strategic and capital planning information resources management (IRM) by integrating the agency's IRM plans, strategic plans, performance plans, and financial management plans, as well as the budget process.

With regard to architectures, Circular No. A-130:

- Defines an EA as “the explicit description and documentation of the current and desired relationships among business and management processes and information technology.” The EA includes principles, an EA framework, a standards profile, current and target architectures, and a transition strategy to move from the current to the target architecture.
- Directs agencies to create an EA 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)

⁴ <http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html#1>

Figure 1 correlates the PSAF’s products with the architectural parts discussed in Circular No. A-130. Complete descriptions of each product are provided in *PSAF Volume II: Product Descriptions*. In any architecture effort, the intended use of the architecture determines the specific products built. Guidelines on products by use are provided in Section 3.

Figure 1: Products Keyed to OMB Circular A-130

OMB Circular A-130 Reporting Requirements	Corresponding Public Safety 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 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)	Overview and Summary Information (AV-1)

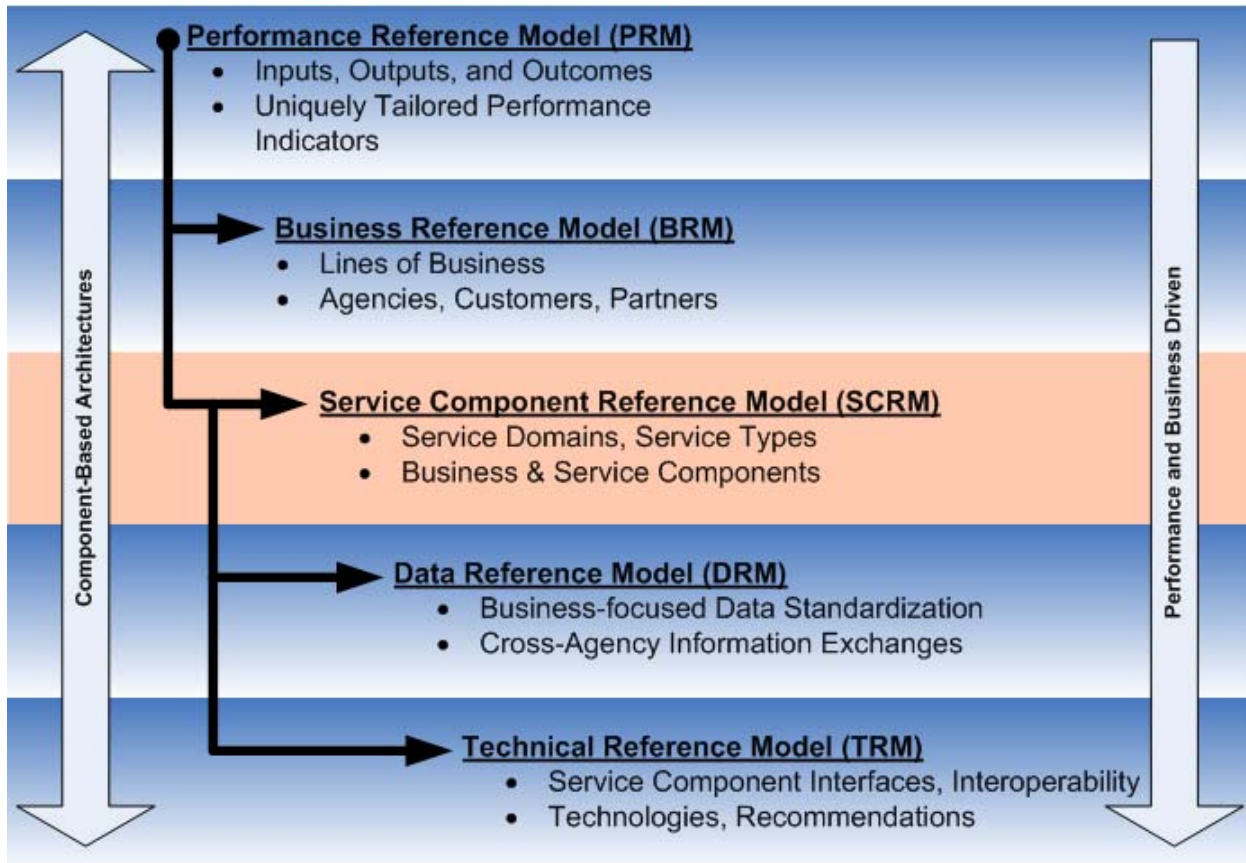
1.3.2 Federal Enterprise Architecture Reference Models

OMB is developing the Federal Enterprise Architecture (FEA),⁵ a business-based set of reference models for Government-wide improvement. The FEA is being constructed through a collection of interrelated

⁵ <http://www.whitehouse.gov/omb/egov/a-1-fea.html>

reference models that help OMB’s cross-agency analysis and identification of duplicate investments, gaps, and opportunities for collaboration. Figure 2 illustrates the set of five FEA reference models.

Figure 2: Federal Enterprise Architecture Reference Models

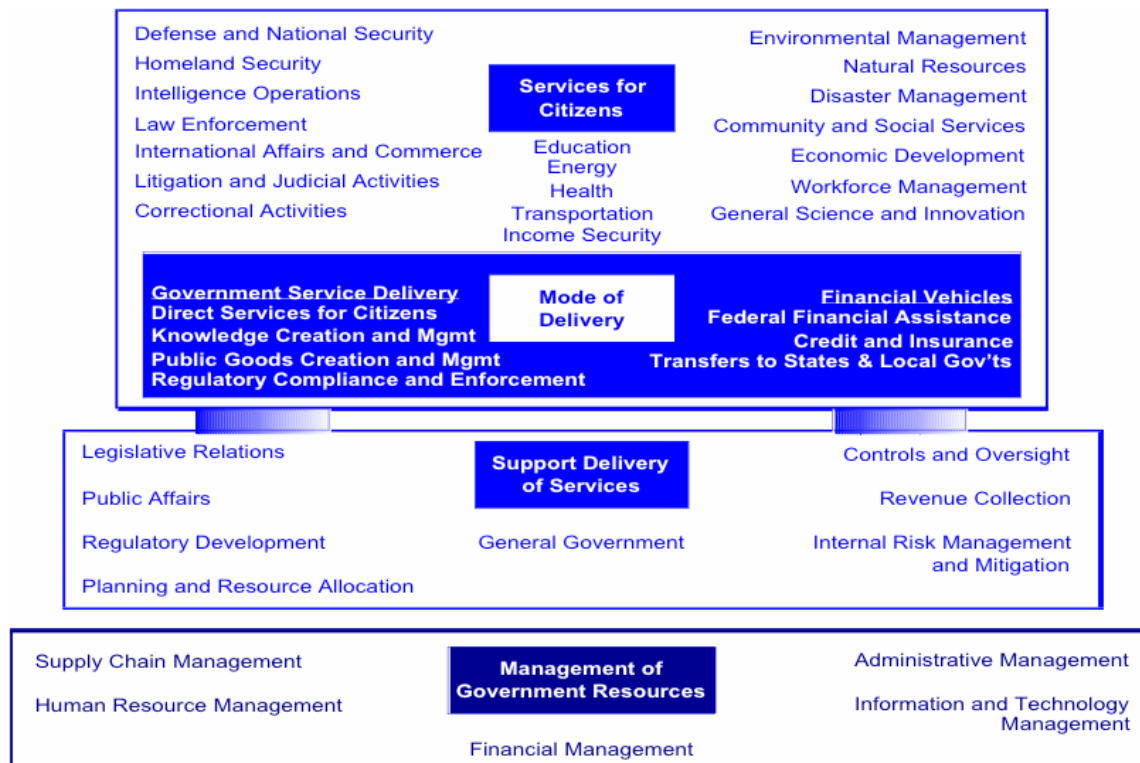


The Business Reference Model (BRM) serves as the foundation for the FEA. The BRM defines a structure of the Federal Government’s lines of business, including operations and services for the citizen, independent of the organizations that perform them. All Federal organizations must map their internal lines of business and activities into one or more of these lines of business. Version 2.0 of the BRM, published in June 2003, is structured in terms of four business areas:

- Services for Citizens — Purpose of the 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 Figure 3 shows, each business area contains multiple lines of business.

Figure 3: Federal Enterprise Architecture Business Reference Model Version 2.0



Version 1.0 of the Service Component Reference Model (SRM), Version 1.1 of the Technical Reference Model (TRM), Version 1.0 of the Data Reference Model (DRM), and Version 1.0 of the Performance Reference Model (PRM) have been released. The FEA Program Management Office website⁶ provides information on the FEA and associated reference models.

1.3.3 National Response Plan

In 2004, two integral documents were released that call the public safety community to action. In December 2004, DHS released the National Response Plan (NRP),⁷ which is built on the principles of the National Incident Management System (NIMS)⁸ that was released on March 1, 2004. The NIMS is a national framework for incident management at all jurisdictional levels.

“This framework forms the basis for interoperability and compatibility that will, in turn, enable a diverse set of public and private organizations to conduct well-integrated and effective incident management operations. It does this through a core set of concepts, principles, procedures, organizational processes, terminology, and standards requirements applicable to a broad community of NIMS users.”

Interoperable and compatible communications systems and technologies are fundamental to an effective NIMS. These allow for multiple jurisdictions to work seamlessly with one another in a domestic incident.

⁶<http://www.whitehouse.gov/omb/egov/a-1-fea.html>

⁷http://www.dhs.gov/interweb/assetlibrary/NRP_FullText.pdf

⁸http://www.fema.gov/pdf/nims/nims_doc_full.pdf

However, interoperable and compatible communications, according to the NIMS, can only be achieved through standards. These standards must be founded on validated requirements and developed by existing consensus-based standards development organizations. NIMS also advocates the use of laboratories to evaluate equipment against standards.

The NRP provides the impetus by which to execute NIMS' interoperable and compatible communications standards. The NRP, predicated on the NIMS, is a nationwide template enabling effective prevention, preparedness, and response to acts of terrorism, major disasters, and other emergencies. It provides a phased approach to execution of the template, which includes employing NIMS standards.

NIMS, in conjunction with the Public Safety Wireless Communications and Interoperability Statement of Requirements, are the logical inputs to the OV products of the future communication and information sharing systems developed by application of the PSAF.

1.3.4 Public Safety Statement of Requirements

The Public Safety Statement of Requirements (PS SoR) V1.0⁹ was released on April 26, 2004. The PS SoR, for the first time, provides the Nation's approximately 50,000 public-safety agencies with a "shared vision" in terms of how to use "in-the-field information resources" more efficiently when responding to a variety of emergency events. The PS SoR also offers guidance on how the communications industry can better align its research and development efforts with the needs of public safety.

The PS SoR was developed in coordination with the National Public Safety Telecommunications Council ([NPSTC](#)), the National Institute of Standards and Technology (NIST) Office of Law Enforcement Standards (OLES), and the Department of Justice's (DOJ) Advanced Generation of Interoperability for Law Enforcement or the NIJ CommTech Program. The requirements contain interoperability scenarios that range from law enforcement traffic stops to large-scale, cross-jurisdictional responses describing how technology can enhance public safety in various situations. The operational scenarios provide requirements that fill the following needs:

- Define how technology should function in the field
- Drive technology interface standards
- Define user's needs in the development of new technologies
- Provide a guide for research and development, testing and evaluation programs

⁹ http://www.safecomprogram.gov/SAFECOM/library/technology/1200_statementof.htm

2 Architecture Basics - Views, Products, and Data

2.1 Architecture Descriptions

An architecture description represents a defined domain, at the current or a future point in time, in terms of the following:

- Its component parts
- What those component parts do
- How the component parts relate to each other
- The rules and constraints governing the component parts

What constitutes each of the elements of this definition depends on the degree of detail of interest. For example, for the State of Colorado, domains, or areas of interest, can be at any level from the State of Colorado as a whole, down to individual function areas or groups of functional areas. Component parts can be anything from “Boulder Fire Department” as a component of the State of Colorado, down to a “wireless base station” as a component part of a communications network, or “workstation A” as a component of “system X”. What those parts do can be as general as their high-level operational concept, or as specific as their lowest-level action. 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 use.

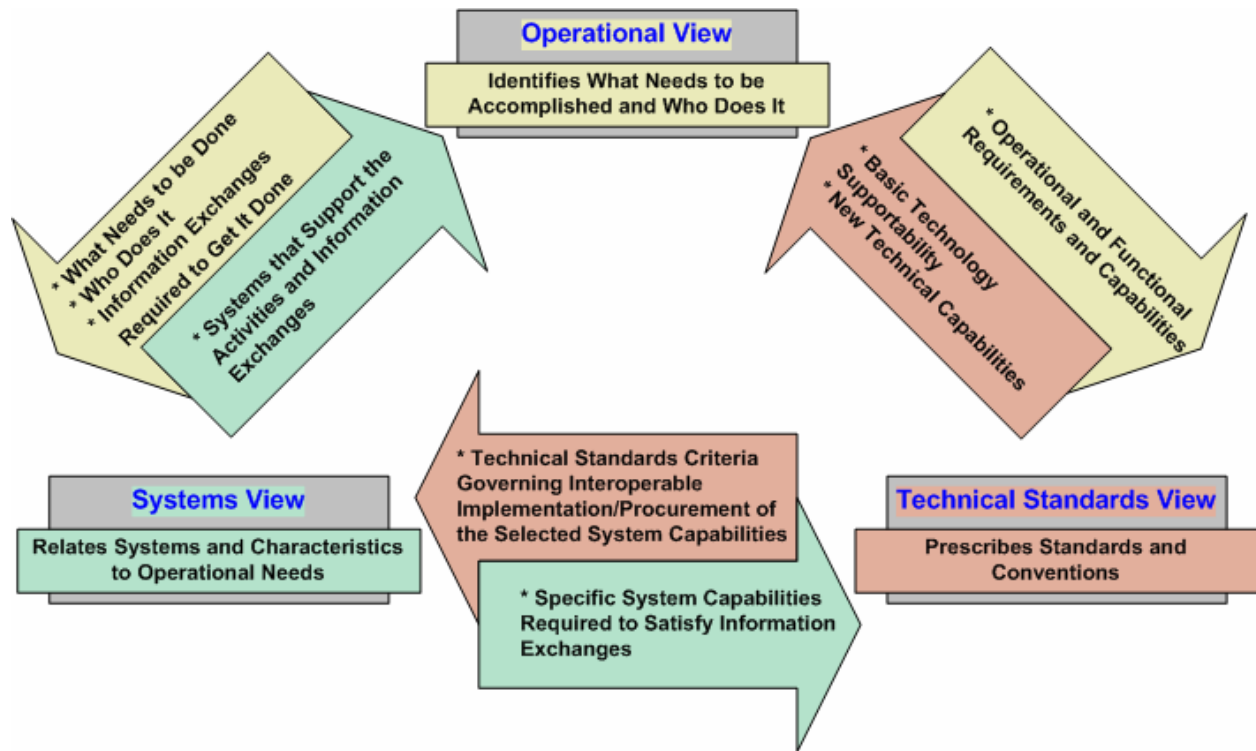
2.2 Architecture View Definitions

The PSAF defines three major perspectives (or views) that logically combine to describe an architecture description:

- Operational View (OV)
- Systems View (SV)
- 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. See [Figure 4](#).

Figure 4: Linkages Among the Views



2.2.1 Operational View

The OV is a description of the tasks and activities, operational elements, and information exchanges required to accomplish public safety missions. Public safety missions include protection of persons through proactive law enforcement, emergency medical services, and fire protection as well as the supporting or facilitating 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 the information exchanges. For example, the PSAF draws OV data from the PS SoR scenarios for “to be” architectures.

2.2.2 Systems View

The SV is a set of graphical and textual products that describes systems and interconnections, which provide public safety functions. Public safety functions include both public safety operations and business functions. The SV associates systems resources to the OV. These systems resources support the operational activities and assist the exchange of information among operational nodes.

2.2.3 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 and functional 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 profiles that govern systems and system elements for a given architecture. The TV products do not enforce the use of any one specific vendor or solution, but provide the technical standards and best practices that have been established. These technical standards and best practices fulfill the functional requirements of the ideal future operational state, as defined and documented in the PS SoR.

2.3 All Views

Some overarching aspects of the architecture relate to all three 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.

The scope includes the subject area and timeframe for the architecture. The setting in which the architecture exists comprises the interrelated conditions that form the context for the architecture. These conditions include: tactics; techniques; and procedures; relevant goals and vision statements; concepts of operations; scenarios; and environmental conditions. In short, the AV products document *what* the architecture aims to achieve.

2.4 Architecture Products

Each PSAF view is composed of architecture data elements you depict graphically, textually, and tabularly to identify architecture components and model their relationships. You develop architecture products in the course of building a given architecture description. Architecture products, such as an integrated dictionary or an operational activity model, for example, describe characteristics pertinent to the purpose of the architecture.

You develop architecture products in the course of building a given architecture description. All products you use as part of an architecture description, even those whose primary purpose is graphical, should contain explanatory text. For example, for graphical products, it is essential to spell out any acronyms appearing in the graphic, and to define in the accompanying product text what they illustrate.

It is important to distinguish between an architecture view and an architecture product. A view represents a perspective on a given architecture, while a product is an illustration, or example, of a particular aspect of that perspective. Thus, a view consists of one or more products. This is analogous to building a house — there is the designer perspective (or view), the owner perspective, and the builder perspective. All of these depict the same thing, a house, but each perspective is tailored for the respective viewpoint, i.e. the builder needs detailed blueprints while the owners need the less detailed overall floorplan and possible color schemes.

PSAF Volume II provides a description of each product. *PSAF Volume III*, which will detail several specific real-world uses, will describe the distinct, step-by-step method for employing the PSAF to achieve the specific aims documented in the AV-1, the Overview and Summary Information. Relationships among products are discussed briefly in [Section 3.3](#) and in more detail in *PSAF Volume II*.

[Table 1](#) lists PSAF products and organizes them by the applicable view. The first column provides an alphanumeric reference identifier and a formal name for each product. The second column generally describes the product content. The sequence of products in the table does not imply a recommended sequence for developing the products.

Table 1: List of Products

PSAF Product	General Description
Applicable View: All	
Product: AV-1 Name: Overview and Summary Information	Scope, purpose, intended users, environment depicted, analytical findings
Product: AV-2 Name: Integrated Dictionary	Architecture data repository with definitions of all terms used in all products
Applicable View: Operational	
Product: OV-1 Name: High-level Operational Concept Graphic	High-level graphical/textual description of operational concept
Product: OV-2 Name: Operational Node Connectivity Description	Operational nodes, connectivity, and information exchange needlines between nodes
Product: OV-3 Name: Operational Information Exchange Matrix	Information exchanged between nodes and the relevant attributes of that exchange
Product: OV-4 Name: Organizational Relationships Chart	Organizational, role, or other relationships among organizations
Product: OV-5 Name: Operational Activity Model	Operational activities, capabilities, relationships among activities, inputs and outputs; overlays can show cost, performing nodes, or other pertinent information
Product: OV-6a Name: Operational Rules Model	One of three products used to describe operational activity – identifies business rules that constrain operation
Product: OV-6b Name: Operational State Transition Description	One of the three products used to describe operational activity – identifies business process responses to events
Product: OV-6c Name: Operational Event-Trace Description	One of the three products used to describe operational activity – traces actions in a scenario or sequence of events
Product: OV-7 Name: Logical Data Model	Documentation of the system data requirements and the structural business process rules of the OV
Applicable View: Systems	
Product: SV-1 Name: Systems Interface Description	Identification of systems nodes, systems, and systems items and their interconnections, within and between nodes
Product: SV-2 Name: Systems Communications Description	Systems nodes, systems, and system items, and their related communications
Product: SV-3 Name: 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.
Product: SV-4 Name: Systems Functionality Description	Functions performed by systems, and the system data flows among system functions
Product: SV-5 Name: Operational Activity to Systems Function Traceability Matrix	Mapping of systems back to capabilities, or mapping of system functions back to operational activities
Product: SV-6 Name: Systems Data Exchange Matrix	Provides details of system data elements exchanged between systems, and the attributes of that exchange

PSAF Product	General Description
Product: SV-7 Name: Systems Performance Parameters Matrix	Performance characteristics of SV elements for the appropriate time frame
Product: SV-8 Name: Systems Evolution Description	Planned incremental steps towards migrating a suite of systems to a more efficient suite, or toward evolving a current system to a future implementation
Product: SV-9 Name: 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
Product: SV-10a Name: 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
Product: SV-10b Name: Systems State Transition Description	One of three products used to describe system functionality – identifies responses of a system to events
Product: SV-10c Name: 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 OV
Product: SV-11 Name: Physical Schema	Physical implementation of the Logical Data Model entities, e.g., message formats, file structures, physical schema
Applicable View: Technical Standards	
Product: TV-1 Name: Technical Standards Profile	Listing of standards that apply to SV elements in a given architecture
Product: TV-2 Name: Technical Standards Forecast	Description of emerging standards and potential impact on current Systems View elements, within a set of time frames

You can develop additional products for a given architecture description beyond those products required for a minimally integrated architecture. The use matrix (see [Figure 7](#)) provides guidelines on what architecture products are applicable to various uses of architecture. It emphasizes the development of architectures to support decision-making for a number of public safety processes. The matrix demonstrates the need for an integrated architecture across three views, for most uses, and the need for integration between the staffs of the operational and acquisition communities.

The architecture products appropriate for any individual use case are highly dependent on the specific situation, objectives, and scope of the effort. Therefore, architects should consider the guidelines provided in the use matrix, but make decisions based on the specifics of their particular architecture and its intended use. In the course of developing the architecture products, one or more references may be required to ensure that specific architectures are complete. These references will include relevant public safety material such as the NRP, the NIMS, and the PS SoR.

2.5 Integrated Architecture

The PSAF provides guidelines, rules, and product descriptions for developing and presenting architecture descriptions that ensure a common denominator for understanding, comparing, and integrating Families of Systems (FoS), Systems of Systems (SoS), and interoperating and interacting architectures.

An architecture description is considered an integrated architecture when products and their constituent architecture data elements defined in one view are the same (same names, definitions, and values) as the

architecture data elements referenced in another view. 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-6 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.¹⁰

Integrated architectures provide important tools to assist coordination between requirements document developers, planners, programmers, budgeters, system developers, and public safety agencies working towards interoperability. These architectures clarify roles, boundaries, and interfaces between components or large Systems-of-Systems and influence participants in requirements generation, acquisition, resource allocation, interoperability enforcement, and waiver processes. Integrated architectures are the primary tool for enterprise-level systems management.

An integrated architecture consists of AV-1, AV-2, OV-2, OV-3, OV-5, SV-1, and TV-1 at a minimum. Depending on the architecture's intended use, you might need to develop additional products for a given architecture description. PSAF Volume II contains a matrix that provides guidelines for which additional products you can develop depending on the use you intend. PSAF Volume III provides instruction as to which of the listed models will be created, the order of creation and the modeling guidelines that will enable the public safety community to achieve goals specified in the AV-1. There will be several real-world examples in PSAF Volume III, such as interim interoperability device selection, legacy system migration, and others.

2.6 Architecture Data Model

An architecture data model provides a structured data element representation that defines relationships among an architecture's pertinent 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 or 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 import and export, product extraction, and direct exchange.

2.7 Architecture Framework Data Model

The National Information Exchange Model (NIEM) and the Global Justice XML Data Model (GJXDM) are being proposed for the Architecture Framework Data Model (AFDM) regarding specification of the architecture data. The NIEM/GJXDM is an object-oriented data model, database, and XML schema specification, generated from the database. It represents the semantics and structure of common data elements and types required to exchange information consistently within the justice and public safety communities. This data model can be extended to allow product view information to be created and stored in a database in a way that assists analysis across products generated by different users for different architectures. While the NIEM/GJXDM does not currently support the PSAF namespaces, analysis is underway to extend it to support the PSAF. Subsequent versions of the PSAF will note the progress of this work effort.

¹⁰See *PSAF Volume II* for detailed descriptions and relationships of these products.

3 Architecture Uses

Public safety requirements are often developed, validated, and approved as stand-alone solutions to counter specific scenarios. This approach fosters an environment in which public safety components make acquisition decisions that, in an interdisciplinary or inter-jurisdictional context, are not fully informed by, or coordinated with, other public safety components. Proposed systems struggle through a budget process and acquisition pipeline that is inefficient, time consuming, and does not inherently support interoperability. Piecemeal, stovepipe procurements of new and legacy systems result in a less than optimal performance.

To address these challenges, the PSAF promotes a capability-based construct that assists planning in an uncertain environment by identifying a broad set of capabilities as participating elements in an overarching system of systems. To accomplish this transition, public safety must put into effect a decision process that performs the following tasks:

- Assesses legacy and proposed systems in the aggregate.
- Defines desired interdisciplinary and inter-jurisdictional capabilities.
- Derives and validates mission-area requirements.
- Considers the full range of solutions.

To achieve substantive improvements in future interdisciplinary and inter-jurisdictional public safety operations and interoperability in the, coordination among public safety components is essential. The decision process must be reformed to employ a synchronized, collaborative, and integrated systems engineering approach that better assists capability-based planning.

Further, as public safety enters an era of network-centered, multi-discipline, multi-jurisdictional operations, the ability to portray and understand complex many-to-many relationships becomes even more important. Capabilities must be able to “plug-and-play” in an interdisciplinary and inter-jurisdictional, nation-wide, multimedia 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.

PSAF Volume II defines the products that allow the description of a capability-based integrated architecture.

3.1 Representative Uses of the Three Views

This section describes the uses of the three views.

- Operational View (OV)
- Systems View (SV)
- Technical Standards View (TV)

3.1.1 Use of the Operational View

The 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 assisting numerous actions and assessments across public safety, including the following examples:

- Examining business processes for re-engineering or technology insertion
- Training personnel
- Examining policy implications
- Coordinating interdisciplinary and inter-jurisdictional relationships
- Defining the operational and functional 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)

The following sections detail the analysis of operations processes, and information exchange relationships.

3.1.1.1 Analyze Operations Processes

OVs are generally driven by local policy 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. This way you can analyze the organization's operations and find a way to either make those 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, current operations cannot be conducted strictly in conformance with current policy because of inefficiencies induced, for example, by lack of supporting infrastructure, or by node and information exchange degradation resulting from threats, denial of service, or acts of nature.






A pure OV is material-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, to examine ways in which new systems could ease streamlining of the processes. In such cases, an OV may have material constraints and requirements that must be addressed. For this reason, it may be necessary to include some high-level SV products or architecture data elements as overlays to augment information into the OV products.

3.1.1.2 Describe Information Exchange Relationships

OVs can describe activities and information exchanges at any level of detail and to any breadth of scope 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, it may be necessary to show how specific information supports a specific organizational unit during particular circumstances. Examples include how specific information supports fire suppression during a certain type of contingency in southern California, and how specific information assists a community service organization logistics re-supply during adverse weather conditions.

An important point is that the type of analysis or assessments that are of interest should often drive the OV degree of granularity. To derive real meaning, you must examine current and postulated solution characteristics in the context of operational missions and requirements, Thus the nature of the planned analysis dictates which operational and functional requirements attributes you need to articulate. Figure 5 illustrates this point.

Figure 5: Operational Architecture Granularity Required for Systems Analyses

<p style="text-align: center;">Degrees of Operational View Granularity</p> <p> = Minimum level of analysis required</p>	Node/system relationships and trade-offs	System-to-system interoperability assessments	Supporting infrastructure assessments and alternatives	Information and data provisioning, standardization, and integration
<p>Starting Point...</p> <ul style="list-style-type: none"> • General processes and relationships • Needs for information 				
<p>Plus...</p> <ul style="list-style-type: none"> • Processes decomposed to specific activities • Information flows and attributes such as timelines are specified • Required level of interoperability defined for each needline 				
<p>Plus...</p> <ul style="list-style-type: none"> • Supporting security requirements and support communications quality, quantity, and timeliness requirements 				
<p>Plus...</p> <ul style="list-style-type: none"> • Information decomposed into data structures and data elements 				

3.1.2 Use of the Systems View

In the PSAF, “system” refers to “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 PSAF, a “system” may be partially or fully automated.

The SV describes the systems of concern, and the connections among those systems in the context of the OV. You can use the SV for many purposes, including:

- Systems baselining
- Making investment decisions on cost-effective ways to satisfy operational requirements
- Evaluating interoperability improvements

An SV addresses specific technologies and “systems.” These technologies can be existing, emerging, and planned or conceptual, depending on the purpose of the architecture effort. Examples include reflection of the current state, transition to a target state, and analysis of the future investment strategies.

For many purposes, an SV will need to further detail the information exchanges described in the OV to translate node-to-node exchanges into system-to-system transactions, communications capability 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. In this case, a data model at a corresponding level of detail is useful, specifically one that includes the system data elements and their attributes and relationships.

3.1.3 Use of the Technical Standards View

The 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 system migration and evolution.

A number of technical references exist, such as the PS SoR 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 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 systems 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 or gap analysis. The SV requirements drive the TV to address a common set of applicable standards or interface specification. To be internally consistent and integrated, an architecture description must provide explicit linkages among its various views. [Figure 4](#) illustrates some primary linkages among the three views.

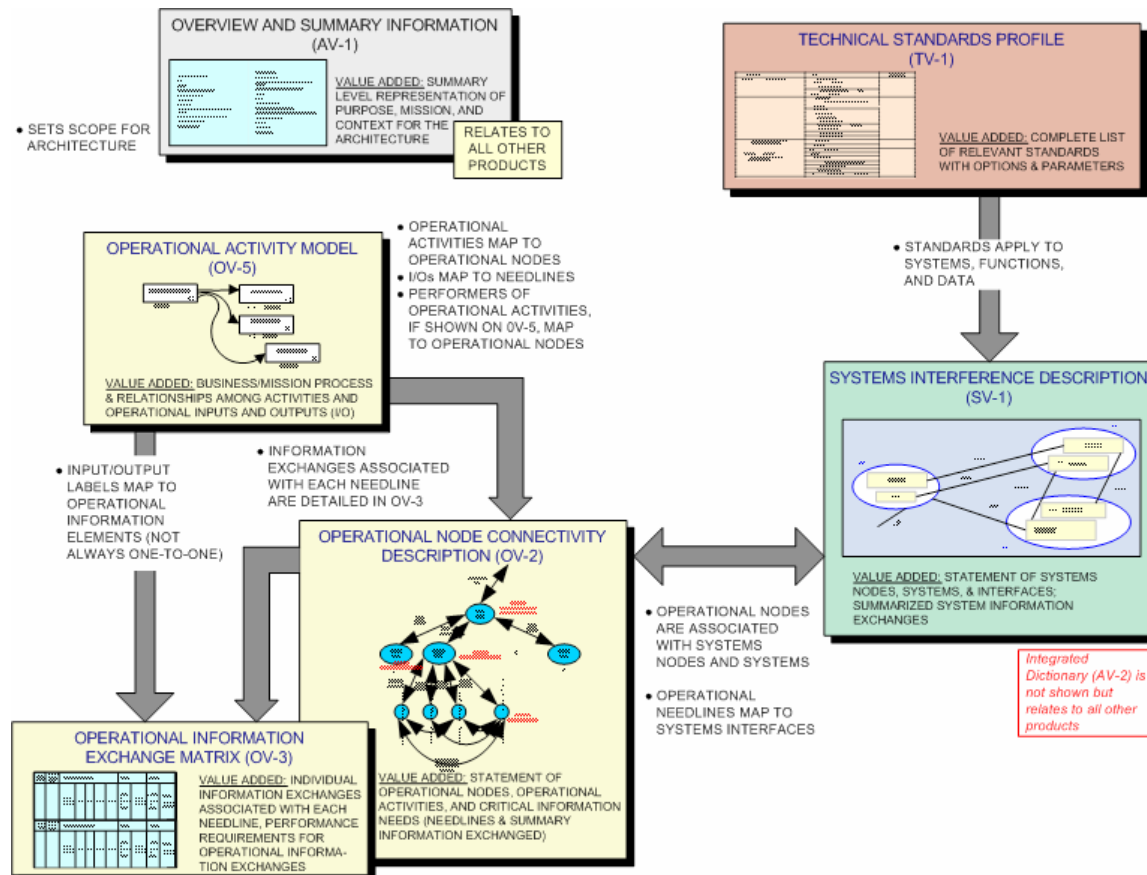
Interoperability is a typical architecture focus that demonstrates the criticality of developing these interview relationships. In [Figure 4](#), the OV describes the nature of each information exchange in detail sufficient to determine the degree of operational interoperability required. The SV identifies which systems support the operational and functional requirements, translates the required degree of interoperability into a set of system data exchanges executed by the system functions, and compares current or proposed implementations with required operational capabilities. The TV articulates the criteria that govern the implementation of each required system that will result in the fielding of a, compliant, 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 effect of these metrics on operational mission and task effectiveness.

Integration of the three views of any given architecture is critical to making the architecture description useful as an analytical tool. One way to encourage such 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 *PSAF Volume II*. The specifics of precisely how the PSAF will be modeled, what information will be captured, and the manner in which this data will be used are all explicitly captured in *PSAF Volume III*.

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. Relationships exist among the architecture data elements that compose the various products, creating relationships among the products. Figure 6 portrays some of the major relationships among selected products. See Section 2, in *PSAF Volume II*, for an in-depth discussion.

Figure 6: Relationships Among the Products and Architecture Data Elements



3.4 Uses of Integrated Architectures

Integrated architectures provide a logical, structured approach for defining: how public safety operates, the associated information flow, the relation between that information flow and system capabilities, and the relation between system capabilities and technical standards. Because architectures provide an ability to understand interdisciplinary and inter-jurisdictional relationships, they can provide significant insights into associated operational concepts, interoperability issues, and systems-related issues. Architecture insights also support strategic planning, evolving an organization toward a common goal, and analyzing the effects of change.

Architecture uses include identifying capability needs, relating needs to systems development and integration, attaining interoperability and supportability, and managing system investments. Integrated

architectures can also provide a context for making resource allocation and trade-off decisions in planning, budgeting, and acquisition.

Architecture content must be geared to the intent of the architecture. [Section 3.5](#) introduces the potential users of the architecture. *PSAF Volume III* will provide step-by-step guidance for using the PSAF to produce the architectures to achieve the goals of the public safety community.

3.5 The Value of Architectures – Different Uses for Different Users

This section provides specific examples for using the PSAF in different scenarios. These examples will be further defined in *PSAF Volume III*, where real-world uses of the PSAF in support of these specific goals will be laid out, step-by-step.

3.5.1 Interoperability Between Public Safety Agencies

The primary goal of the PSAF is to provide the process and tools for planning of interoperable communications and information sharing. The need for interoperability among public safety agencies can be found in many day-to-day examples, and in the larger task force incidents that (unfortunately) make national news. Consider the Beltway snipers case that made daily headlines:

On October 19, 2002, shots rang out at the Ponderosa Steakhouse in Ashland, Virginia, approximately 15 miles north of Richmond. A 37-year-old man was shot by the Beltway snipers that terrorized the citizens in Virginia, Maryland, and the District of Columbia from the beginning of October to their capture at a Maryland rest stop on October 24. Members of the Sniper Task Force, charged with investigating and pursuing the suspects, were credited for finally solving the case.

The Sniper Task Force was made up of law enforcement officials from the following State, regional, and local jurisdictions and Federal agencies:

- Montgomery County, MD
- Prince George’s County, MD
- Hanover County, VA
- Fairfax County, VA
- Prince William County, VA
- Spotsylvania County, VA
- Ashland, VA
- Washington, D.C.
- Virginia State Police
- Maryland State Police
- Federal Bureau of Investigation
- Bureau of Alcohol, Tobacco and Firearms

The job of a task force becomes more arduous without adequate and interoperable wireless communications.

To discuss public safety wireless communication and interoperability, over one hundred State and local public policy makers came together on October 2001 at the National Public Safety Wireless Interoperability Forum. In response to the Forum, the National Task Force on Interoperability (NTFI) was formed in 2002. It produced the useful, well-received guide, *WHY CAN'T WE TALK? Working Together To Bridge the Communications Gap To Save Lives*,¹¹ on achieving interoperability.

The guide's introduction states:

“In an era where technology can bring news, current events, and entertainment to the farthest reaches of the world, many law enforcement officers, firefighters, and emergency medical service personnel working in the same jurisdiction cannot communicate with one another. The inability of our public safety officials to readily communicate with one another threatens the public's safety and often results in unnecessary loss of lives and property. Recognizing that solutions to this national issue can only be achieved through cooperation between all levels of government, 18 national associations representing State and local elected and appointed officials and public safety officials formed a task force to address this issue. This guide is the result of the significant commitment by members of this task force who shared their knowledge, experience, and wisdom.”

Member associations of the NTFI included the following organizations:

- Association of Public Safety Communications Officials - International, Inc.
- International Association of Chiefs of Police
- International Association of Fire Chiefs
- International City/County Management Association
- Major Cities Chiefs
- Major County Sheriffs' Association
- National Association of Counties
- National Association of State Chief Information Officers
- National Association of State Telecommunications Directors
- National Conference of State Legislatures
- National Criminal Justice Association
- National Emergency Management Association
- National Governors Association
- National League of Cities
- National Public Safety Telecommunications Council
- National Sheriffs' Association
- The Council of State Governments

¹¹ <http://www.agileprogram.org/nt>

- The United States Conference of Mayors

Chapter 4 of the guide is titled, “How Can You Achieve Interoperability?” The following excerpt from that chapter notes the role of planning:

Developing a plan for improving interoperability

A well-developed, coordinated plan is the cornerstone to any successful initiative and accomplishes the following:

- *Defines the vision, goals, and objectives of what you are ultimately trying to accomplish.*
- *Describes the specific problems or needs that are to be addressed.*
- *Identifies any potential partners and their roles and staffing requirements.*
- *Proposes a detailed budget and timeline.*
- *Outlines a marketing strategy.*
- *Includes an operational plan that addresses how the project will be funded now and in the future.*

Without adequate planning you will not know what you have, where you want to go, or what you need to get there. Mistakes will be made, time and money will be wasted, and the end result may not be what you intended.

The primary goal of the PSAF is to provide the process and tools for planning of interoperable communications and information sharing.

3.5.2 Legacy/Project 25 System Extended with Interim Interoperability Device

Public safety vendors and public safety practitioners are expending a great deal of effort to produce and use devices that provide some measure of interim interoperability. These devices are intended to fulfill short-term interoperability gaps in an agency’s current system with a minimal impact on the operation and management of the communications system. With an ever-increasing variety of products to choose from, decisions as to what an agency is trying to accomplish, procure, and install are more difficult than ever. The PSAF can help to assist this decision-making process by providing a methodology for analysis of the current system, the desired feature set, and managing future compatibility with the next generation of public safety communications standards, for example, the new Project 25 (P25) standards.

3.5.3 Legacy System to Project 25 System

Many public safety agencies have communication systems that practitioners refer to as “legacy systems”. These systems may be antiquated when compared to new and emerging public safety communication standards. The Project 25 (P25) suite of communications standards is one such example of a new set of standards. As the P25 standards near completion, migration from a legacy system to a P25-based system will become more common. This migration will necessarily be complex. The PSAF is intended to guide this process through a repeatable methodology that practitioners can leverage from the smallest public safety agency to the largest. *PSAF Volume III* will provide a more detailed example of this concept.

3.5.4 Migration to PS SoR-Based System

As the technical solution space defined by the PS SoR becomes refined and products begin to become available to public safety agencies, it will be important to make technical selections that remain consistent with the overall public safety standardization effort. The PSAF will ultimately assist a migration from current architectures to one defined by the PS SoR. Through the same conceptual process discussed in [Section 3.5.1](#), the PSAF will guide the creation of the “as is” architecture description and the “to be” architecture description, where “as is” is the current architecture in use and “to be” is the new architecture desired. Once these two architectures are defined through application of the PSAF, you can develop a detailed migration strategy, allowing for the greatest user flexibility possible.

3.6 Products According to Use

This section specifies the products required for an integrated architecture, and provides guidelines for product development based on the intended use of the architecture. The architecture products appropriate for any individual use case are highly dependent on the specific situation, objectives, and scope of the effort. As an architect, you should consider the guidelines provided in this section, while making decisions based on the specifics of the particular architecture and its intended use.

An integrated architecture consists of, at a minimum, AV-1, AV-2, OV-2, OV-3, OV-5, SV-1, and TV-1. This is the set of products required to satisfy the definition of an OV, SV, and TV as provided in [Section 2.2](#). This is also the minimum set of products to describe those overarching aspects of the architecture that add context and meaning. To ensure the architecture is, in fact, integrated across the views, the products must at least contain those architecture data elements marked with an “*” in the architecture data element tables provided for each architecture product in *PSAF Volume II*. Depending on the intended use, you should develop additional products for a given architecture description.

[Figure 7](#): provides guidelines for product development based on intended use. [Figure 7](#): is not an exhaustive list, but it provides initial insight into the use of the various architecture products for supporting PSAF processes. Future versions of the PSAF are expected to expand the uses described.

Rows in [Figure 7](#): are organized based on major public safety processes. Columns delineate products relevant to use of an integrated architecture in conducting analysis critical to process success.

Figure 7: Architecture Products by Use

Recommended Uses of Architecture	Applicable Architecture Products																					
	AV		OV							SV											TV	
	1	2	1	2	3	4	5	6	7	1	2	3	4	5	6	7	8	9	10	11	1	2
Capability-based Analysis for IT Investment Decisions	●	●	●	●	●	●	●	●	○	●	○	●	●	●	●	●	●	●	●	●	●	○
Modernization Planning and Technology Insertion/Evolution	●	●	○	●	○	○	●	○	○	●	○	○	○	○	○	●	●	●	○	○	○	○
System Design and Development	●	●	○	●	●	○	●	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○
System Interoperability and Supportability	●	●	●	●	○	●	○	○	○	●	○	○	○	○	○	○	○	○	○	○	○	○
Integrated Test and Evaluation	●	●	○	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Operations Planning and Execution	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Communications Plans	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Exercise Planning and Execution	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Organization Design	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○

- Product is highly applicable
- Product is often or partially applicable
- Product is required for an integrated architecture
- Product is usually not applicable

The icons briefly described at the bottom of Figure 7: are further spelled out below:

- A solid black circle indicates the product is highly applicable to the indicated use. This means you should develop the product when the architecture is intended to support the indicated use.
- A white circle with a center black dot indicates the product is often or partially applicable. This means you should consider developing the designated product when the architecture is intended to support the indicated use.
- A light gray cell indicates the product is required to support an integrated architecture.
- A blank cell indicates that the product is usually not applicable. There is usually no need to develop the designated product when the architecture is intended to support the indicated use

An integrated architecture describes its domain from all three views: OV, SV, and TV. The next sections discuss certain products from each view that are essential for integrated architectures.

3.1.1 Overview and Summary Information (AV-1)

Regardless of the intended use of the architecture, the Overview and Summary Information (AV-1) is essential for the following:

- Documenting the assumptions, constraints and limitations that may affect high-level decision processes involving the architecture
- Identifying the approving authority and the completion date
- Recording the level of effort and costs, both projected and actual, that are required to develop the architecture
- Recording the time frame covered and the organizations within the scope of the architecture

AV-1 includes:

- Explanation of the need for and intended use of the architecture
- What it should demonstrate
- Types of analyses that will be applied to it
- Who is expected to perform the analyses
- What decisions are expected to be made based on the analysis
- Who is expected to make those decisions
- What actions are expected to result

AV-1 identifies the viewpoint from which the architecture is developed. It also includes the context, which includes such things as: mission, local policy, relevant goals and vision statements, concepts of operation, scenarios, and information assurance context.

In addition, AV-1 states findings and recommendations that have been developed based on the architecture effort. Examples of findings include identification of shortfalls (gap analysis), recommended systems implementations, and opportunities for technology insertion. AV-1 contains sufficient textual information to enable a reader to select a single architecture from among the many that may be read in more detail. AV-1 provides the contextual information that dictates everything that follows within the architecture. What models are built, how they are built, and the analysis that is assisted by them are all dependent on the specified requirements of the architecture within AV-1.

3.1.2 Integrated Dictionary (AV-2)

An Integrated Dictionary (AV-2) is included in every architecture description, regardless of the intended use. A byproduct of the architecture development process, it 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.

3.1.3 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 or human role, such as Incident Commander, an organization, for example, the Boulder Fire Department, or an organization type, that is, a logical or functional grouping such as emergency medical services. Regardless of the intended use and level of detail, it is important to identify key players. OV-2 is highly applicable for all architecture uses.

3.1.4 Operational Information Exchange Matrix (OV-3)

The Operational Information Exchange Matrix (OV-3) identifies information elements and relevant attributes of each information exchange, and associates the exchange to the producing or consuming

operational nodes and activities as well as to the needline 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 for some architecture uses an adequate specification of the requirement to exchange information.

3.1.5 Operational Activity Model (OV-5)

The Operational Activity Model (OV-5) describes the operations normally conducted while achieving a mission or 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 outside the scope of the architecture:

- 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 activities) that need to be scrutinized further
- Provide a necessary foundation for depicting activity sequencing and timing in OV-6a, OV-6b, and OV-6c

Regardless of the intended use and level of detail, OV-5 is highly applicable for most architectures.

3.1.6 Systems Interface Description (SV-1)

The Systems Interface Description (SV-1) links together OVs and SVs by depicting the assignment of systems functions, and systems nodes and their associated interfaces, to the operational nodes and their associated needlines, as described in OV-2. OV-2 depicts the operational nodes representing organizations, organization types, and human roles. SV-1 depicts the system nodes that house operational nodes, for example, platforms, units, facilities, and locations, as well as the corresponding systems functions, which are resident at these systems nodes and support the operational nodes. Most architecture uses involve analysis of alternative material solutions. Therefore, knowledge of the systems, their locations, and their functions is essential to this type of analysis.

While SV-1 is highly applicable for most uses, it is usually not applicable for conducting business process re-engineering or functional process improvement, where the intent is to address activities and processes of independent systems.

3.1.7 Technical Standards Profile (TV-1)

The Technical Standards Profile (TV-1) consists of the set of systems standards that govern systems implementation and operation of a given architecture. The standards generally involve what hardware and software you can put into practice and what system data formats you can use. That is, TV-1 delineates which standards you can use 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, especially where interoperability is critical.

While TV-1 is critical to understanding the technical aspects of an architecture, it is usually not applicable for uses that tightly focus on operational aspects. The TV-1 speaks to standards and best practices, but does mandate the use of a particular manufacturer's products or solutions.

4 Techniques for Using Architecture Information

Several analytical techniques for using architecture information have been developed. The key interface profiles and human factors topics described in the next, introductory sections will be discussed in more detail in *PSAF Volume III*.

4.1 Key Interface Profiles

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

4.1.1 The Situation for Assessing Interoperability

Enterprise architectures and interfaces go hand-in-hand. When a new system, application, or database is deployed, it is inevitable that stakeholders will need to define, design, and implement interfaces to other applications, systems, and databases that exist within the enterprise. For an architecture whose domain is interoperability, all-important considerations are: knowing what needs to interface, how it needs to interface, and when an interface is required.

An approach for achieving interoperability that relies on the use of globally scoped standards generally cannot scale to the enterprise level. (Globally scoped means standardizing everything, from communications protocols to button sizes on a device.) The inability to reach a consensus on a single standards profile will often lead to “multiple standards” -- an oxymoron -- for a given service area. An interface approach can be more manageable and legacy-friendly than globally scoped standards, because it does not dictate the internals of every system. The interface approach is the method being used in P25 standardization.

Interfaces are defined by functional and physical characteristics that exist at a common boundary with co-functioning items. Interfaces allow the compatibility of systems, equipment, software, and system data. An interface may be designated as key if it satisfies one or more of the following criteria:

- It spans organizational boundaries.
- It is mission-critical.
- Capability, interoperability, or efficiency issues exist at that interface.
- The interface is vulnerable or important from a security perspective.

It may be more difficult to achieve necessary attributes when different agents (e.g., discipline, agency, organization) have ownership and authority over the hardware and software capabilities at the interface.

4.1.2 The Key Interface Profile Approach

An integrated architecture relates mission-focused operations to the information flows through specific interfaces between communications systems and subsystems as well as their hardware and software. An integrated architecture also includes the technical standards applicable to 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 to achieve mission-based capabilities.

Key Interface Profiles (KIPs) provide a network-centered approach for managing interoperability across a system of systems based on configuration control of its key interfaces. The KIP interface specification is a set of documentation produced as a result of interface analysis that:

- Designates an interface as key.
- Evaluates the interface to understand its architectural, interoperability, test, and configuration management characteristics.
- Documents those characteristics with solution sets for issues identified during analysis.

4.2 Human Factors

This section discusses the importance of human factors in enterprise architectures and characterizes ways of addressing human factors within the architecture.

4.2.1 Benefits and Cost

Architectures provide opportunities to address the role of the human factor in accomplishing public safety operations and business processes. Human factors play a significant role in how information is accessed and displayed. They 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.

One simple example is the size of buttons on radios for firefighters. Firefighters often wear fire-retardant gloves that make pressing small buttons difficult if not impossible. Not taking this type of human factor into consideration could result in wasted dollars and an unusable technology. Modest investment in human systems integration during architecture development can reduce total ownership costs.

4.2.2 Including Human Factors

Architectures provide a construct for describing human activities and the flow of information needed by humans to accomplish or support public safety 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 presented. For example, before the detailed “how to” guidelines of human-computer interfaces can be put into effect, the human dimension of the OV must be considered. This will help designers determine the scope of information to be displayed or made available to humans as well as how that information is displayed.

Considering human factors in an architecture extends beyond interface design to such issues as manpower, personnel, training, and safety. Systems must be supported by sufficient manpower and training resources to operate the system effectively.

Modest investment in human systems integration during architecture development can reduce total ownership costs. Every engineering change proposal that can be eliminated and every training program that can be reduced saves resources. Taking human factors carefully into account in architecture

development and systems design will also enhance overall systems performance by helping design effective training programs, validate adequate staffing requirements, and improve human performance.

Providing supplementary information on human factors within an architecture can link various aspects of the architecture from the human use perspective. It also can 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.

5 Architecture Guidelines, Description Process, and Integration

5.1 Architecture Guidelines

The PSAF contains four main types of guidance for architecture description:

- A detailed description of the product types
- A discussion of standard architecture data elements and definitions
- Guidelines that include a set of principles for building architecture descriptions compliant with the PSAF
- A process for using the PSAF to build an integrated architecture description

Section 2.4 introduced the products, and Section 6 contains a discussion of standard architecture data elements and definitions. This section discusses the last two aspects of PSAF guidance, namely architecture guiding principles and a process for building an integrated architecture description.

5.1.1 Guiding Principles

The following sections outline a set of principles for describing architectures. Such principles are critical to building architecture descriptions.

5.1.1.1 Build with a Purpose in Mind

An architecture must have a specific and commonly understood purpose to increase the efficiency of the effort and the utility of the resulting description. The purpose determines the breadth and depth of the scope, which characteristics to capture, and what timeframes to consider. This principle applies equally to the description of a whole architecture, or to any portion of each of the views within an architecture. This principle can also apply to groups of architectures.

Note: If architecture descriptions that various organizations build are to be compared, it is important that they all be built from the start for the purpose of comparison. If any product does not support the purpose of the architecture, don't waste time and resources building.

5.1.1.2 Exercise Simplicity to Achieve the Stated Purpose

Developing overly complex architectures is costly in time and money. Focusing the architecting effort is essential to obtaining an acceptable return on investment. Determine the level of detail appropriate to achieving the objectives of the architecture. Consider the following areas:

- Scope of the activity model
- Levels of decomposition of the activity model
- Degree of aggregation or de-aggregation in the definition of the operational nodes and system nodes
- Level of specificity in defining information elements in information exchanges

For example, in some efforts the use intelligence as an information element might be sufficient. Other efforts may need to decompose intelligence into either specific types of intelligence reports

or may need to even further decompose intelligence into the subject areas of the information. Examples are geographic locations, equipment type and numbers, and groups involved.

- Level of decomposition in defining a system

5.1.1.3 Use a Format that Leads to Quick Understanding

Structure architecture descriptions in a way that assists quick understanding and guides the human thinking process to discovering, analyzing, and resolving issues. Exclude extraneous information and use common terms and definitions. Using standard modeling techniques to produce a graphical representation of the architecture products often provides an excellent medium for rapid human understanding.

5.1.1.4 Specify a Common Format Applicable Across Public Safety

Like the preceding principle, specifying a common format 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. It dictates that products of a given type developed for different architectures must display similar information about their respective domains, and in similar formats. Apply a common format and information content that is appropriate for each product type, such as in this PSAF.

To relate public safety architectures, it is critical to capture external interfaces. Architecture descriptions must clearly describe external interfaces with local, state, tribal, and Federal components in a manner consistent with the method for describing relationships.

5.1.1.5 Ensure Modularity, Reusability, Extensibility, and Decomposability

Develop architecture descriptions with related pieces that can be recombined with a minimal amount of tailoring. This principle will support reuse for multiple purposes. The set of products to build, the characteristics to capture in those products, and the high-level steps to use the PSAF are designed to ensure you can follow these guiding principles.

5.1.2 PSAF Compliance Guidance

The following paragraphs provide guidance on compliance with the PSAF. To comply with the PSAF:

- Ensure interoperability, which is fundamental to any application of the PSAF.
- Provide the appropriate set of products based on intended use.
- Adhere to the PS SoR, the National Response Plan (NRP), and the National Incident Management System (NIMS).
- Use the common terms and definitions specified in this document.

5.1.2.1 Interoperability

Interoperability is fundamental to any application of the PSAF. Architecture descriptions must capture specific interoperability requirements. Enterprise architects must 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 required attributes of each operational information exchange (see OV-3 in [Section 3.6.1.4](#)) is the level of interoperability required to meet mission needs.

5.1.2.2 Build the Appropriate Products Based on Intended Use

Determine the products to build based on the intended use of the architecture. Architectures must identify each product by the name the framework specified. They also must capture the architecture data elements specified in *PSAF Volume II*.

5.1.2.3 Adhere to the PS SoR, NRP, and NIMS

The PS SoR defines the functional and operational aspects of future public safety communications requirements. As such, any use of the PSAF must take the PS SoR into account from a variety of perspectives, such as migration and gap analyses.

NIMS integrates effective practices in emergency preparedness and response into a comprehensive national framework for incident management. The NRP provides the impetus by which the interoperable and compatible communications standards that NIMS identifies will be executed. The NRP, predicated on the NIMS, is a nation-wide template for the prevention of, preparedness for, and response to acts of terrorism, major disasters, and other emergencies. It provides a phased approach to putting the template into effect, which includes employing the standards identified by NIMS.

5.1.2.4 Use Common Terms and Definitions

Use common or standardized terms and definitions in architecture descriptions. The criticality of common language during architecture product creation, analysis, comparison, and integration cannot be overemphasized. 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 misunderstandings of shared information, and assists with architecture consistency and validation.

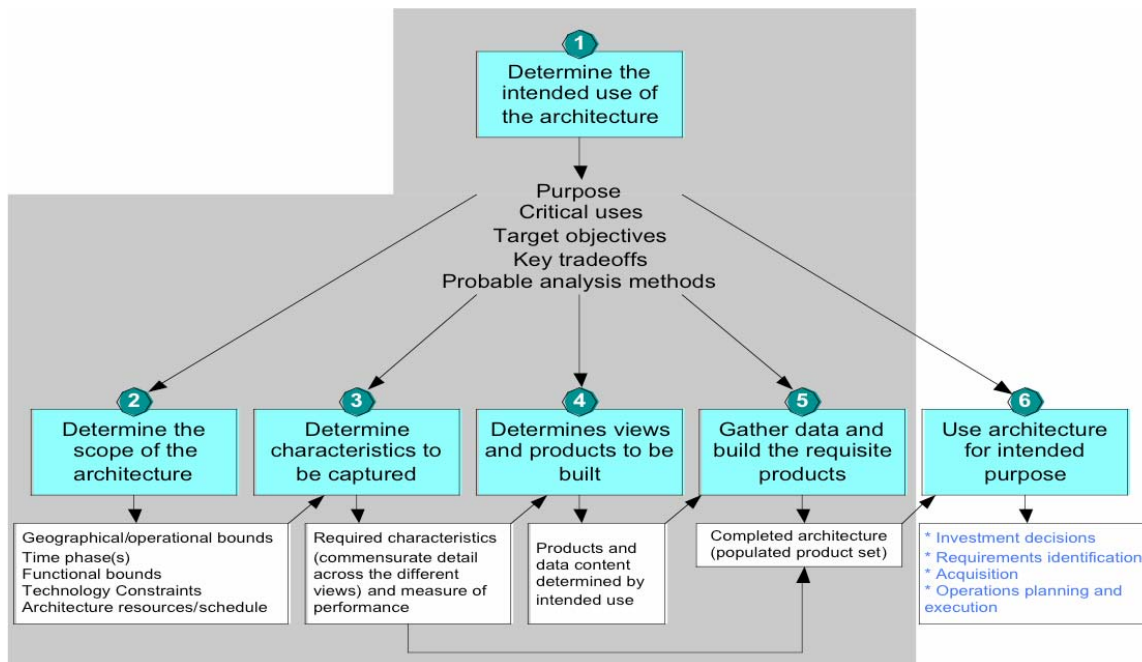
The PSAF defines a standard for architecture product names, standard architecture data elements, their attributes, and their relationships. The PS SoR defines the requirements for these architecture data elements as entities. It also defines their relationships. The PSAF requires that every architecture description contain an integrated dictionary that defines terms used in the architecture.

5.2 The Generic Six-Step Architecture Description Process

This section describes ways to apply the PSAF in building architecture descriptions. A high-level, six-step process that emphasizes guiding principles has been developed to provide some general guidance to the architect. This generic process should be tailored to specific organizations and purposes. A more specific process for public safety will be defined in *PSAF Volume III*.

The steps, outlined in the following sections, are fundamental to describing an architecture in accord with the PSAF. They appear in the general sequence in which they will often be performed. [Figure 8](#): depicts this six-step process. For simplification, feedback loops have been largely eliminated. Note, however, that you are likely to encounter many such iterations. The gray shaded area covering steps one through five is within the scope of this document and PSAF Volume II.

Figure 8: The Six-Step Process of Building an Architecture Description



5.2.1 Determine the Intended Use

Step 1: *Determine the intended use of the architecture description.*

Build descriptions 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 the following, as specifically as possible:

- The issues the description is intended to explore
- The questions it is expected to help answer
- The interests and perspectives of the audience and users

In addition, consider the types of analysis you expect to be performed. For example, knowing that the architecture may be used as input to specific models or simulations can affect what products you include and how you structure them. This kind of focus will make the architecture description effort more efficient and the resulting architecture more appropriately balanced and useful.

5.2.2 Determine the Scope

Step 2: *Determine the architecture description’s scope, context, environment, and any other assumptions to be considered.*

Once you determine the purpose or use, you can determine the prospective content of the architecture description. Consider, but do not limit your consideration to, the following items:

- 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
- The projected availability and capabilities of specific technologies during the time frame to be depicted

Project management factors that contribute to the preceding determinations include the resources available for describing the architecture, as well as the resources and level of expertise available for analyzing it, and the availability of the necessary architecture data.

5.2.3 Determine Information to Capture

Step 3: *Based on the intended use and the scope, determine what information the architecture description needs to capture.*

Take care in determining the architecture information you must include to satisfy the intended purpose. If pertinent information is omitted, the architecture description may not prove useful. If unnecessary information is included, the architecture effort may turn out to be infeasible, or the description may become confusing or cluttered with superfluous details. Take care to predict the future uses of the architecture description so that, within resource limitations, you can structure it to accommodate future tailoring, extension, or reuse.

Architecture measures are a critical aspect of an integrated architecture description. Therefore you should consider them even at this early step in the architecture development effort. The developer should strive to ensure each of the three views has measures identified to correctly determine what products need to be built, their level of detail, and the attributes to be captured in them. Measures may be both quantitative and qualitative. If the developer is unable to determine such measures, the end result will have less meaning and value to senior decision makers.

5.2.4 Determine Products to Build

Step 4: *Determine products to build.*

Based on the understanding gained in steps 1 through 3 and referring to [Section 5.2](#), determine what architecture data must be gathered to identify the products to build that describe the architecture.

5.2.5 Gather Data and Build Products

Step 5: *Gather the architecture data and build the requisite products.*

Collect, correlate, and compose the necessary architecture data that will form the basis for the products. *PSAF Volume II* defines the architecture data elements associated with each product definition.

To assist integration with other architectures, develop architectures for compliance with the Public Safety Wireless Interoperability Statement of Requirements, and include relationships with applicable local, tribal, State, and Federal components. If the architecture description needs some retailoring to serve its purpose, strive to perform the retailoring as efficiently as possible. It may be useful, resources permitting, to conduct some proof-of-principle analysis at various stages. This involves making trial runs of step six using carefully selected subsets of the areas to be analyzed. Take care to ensure the products built are internally consistent and properly integrated. Use of automated tools and an architecture data repository

can assist the architecture development process as well as the use of common terms and definitions, and compliance with the Public Safety Wireless Interoperability Statement of Requirements.

5.2.6 Use Architecture for its Intended Purpose

Step 6: *Use the architecture description for its intended purpose.*

By following step 1, your architecture description will have a particular purpose in mind. The ultimate purpose may be to support, for instance, investment decisions, requirements identification, system acquisition, interoperability evaluation, or operations assessment. The architecture description assists and enables these purposes but does not provide definitive answers. For that, you must apply human and, perhaps, automated analysis. The PSAF does not attempt to dictate how you perform this analysis. Instead, its intent is to promote architecture descriptions sufficiently complete, understandable, and integration-capable to serve as one basis for such analysis.

5.3 Architecture Integration

5.3.1 Two Types of Architecture Integration

The two types of architecture integration are:

- Integration across the three views of an architecture
- Integration across two or more architectures

The term *integrated architecture* refers to an architecture description that has integrated OVs, SVs, and TVs. Common points of reference link OVs and SVs and also link SVs and TVs. For example, SV-5 relates operational activities from OV-5 to system functions from SV-4. The system functions are related to systems in the SV-1, thus bridging the OV and SV. The standards in the TV-1 are cross-listed in certain systems products such as network protocol and systems data exchange, thus bridging the SV and TV.

In an integrated architecture, you develop products and their constituent architecture data elements such that architecture data defined in one view is the same (i.e., same names, definitions, and values) as the corresponding architecture data referenced in another view.

To integrate multiple architecture descriptions, you must ensure sufficient commonalities to support identification of critical relationships. 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 support 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?

Three critical aspects of being able to integrate architectures are:

- Adherence to the PSAF

- Adherence to the PS SoR, NRP, and NIMS
- Use of a common taxonomy for architecture data element values such as names of operational nodes

Adherence to the PSAF provides both a common approach for developing architectures and a basic foundation for relating architectures. Public safety 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 PSAF-compliant architecture repository such as the Public Safety Architecture Repository System (ARS, see [Section 6.5](#)) can assist integration, because it ensures products are PSAF-compliant.

5.3.2 Scope of Cross-Architecture Integration

The PSAF reflects the scope of cross-architecture integration in terms of mission areas and levels of interactions. The PS SoR defines four levels of operations: single discipline/single jurisdiction, single discipline/multiple jurisdictions, multiple disciplines/single jurisdiction, and multiple disciplines/multiple jurisdictions. [Figure 9](#): illustrates these four levels in the context of a hierarchical view of operational missions. Note that the need to integrate multiple architecture descriptions is certainly not limited to cross-organizational considerations.

Figure 9: Four Levels of Architecture Integration



The first type of cross-architecture integration involves a single first responder discipline within a single jurisdiction. An example objective may be to ensure that information can flow appropriately and efficiently across and between the different functional areas within a single jurisdiction and discipline.

The second type of cross-architecture integration illustrated in [Figure 9](#): still involves a single discipline, but the scope includes operations across multiple jurisdictions. 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 crosscut multiple disciplines, within a single jurisdiction. An example involves architectures whose objectives are to investigate opportunities to exploit or leverage common infrastructure capabilities.

The fourth type of cross-architecture integration involves multiple disciplines and multiple jurisdictions, where vertical and horizontal relationships need to be articulated and examined. An example is the

integration of multiple jurisdictions at the local, tribal, State, or Federal levels to assess the effectiveness of support to command and control and to operations. This could involve examining trade-offs between hierarchical support policies and practices.

5.3.3 The Value of Integration

An integrated architecture, as defined in [Section 2.5](#), 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. Integrated views help assess interoperability and help 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 public safety. 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 breadth of public safety and its diversity of missions in sufficient level of detail to support all types of analyses enabled by the architecture construct.

The depiction and assessment of large enterprise capabilities requires both broad, high-level architectures and detailed, low-level architectures. High-level architectures depict multiple missions and business areas, while low-level architectures assess single missions or subsets of missions. High-level architectures provide the framework and context for lower-level architectures by depicting primary relationships and dependencies. Assessing the capability of detailed, low-level architectures in the context of a large enterprise requires an integration of high- and low-level architectures.

6 Architecture Data Model, Repository, and Tools

6.1 Overview

Architecture data are the underlying basic elements that comprise a given architecture. The PSAF products are those graphical, textual, and tabular items you develop in the course of gathering architecture data, identifying their composition into related architecture products and modeling the relationships among those products to describe characteristics pertinent to the architecture purpose or intended use.

The key to maintaining architecture product interoperability is the preservation of meaning and relationships during architecture data reuse. An architecture data model defines the relationships among data to provide a structured organization of pertinent data elements. Agreement on an architecture data model is essential to the reuse of architecture data, as well as to the implementation of architecture databases. This is true regardless of the technology chosen — for example, relational or 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 import and export, product extraction, and direct exchange.

This discussion outlines architecture data and architecture benefits, the framework data model, the Public Safety Architecture Repository System (ARS), and architecture tools.

6.2 Architecture Data

Although the PSAF 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 product must build on a set of common architecture data elements. *PSAF Volume II* provides a data element table for each product with metadata definitions, 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. Further, the Integrated Dictionary stores the data elements that a product should capture for a given architecture.

An architecture data repository assists defining and depicting the requisite architecture data elements and their appropriate relationships. Using architecture data elements from a common data model, the Global Justice XML Data Model (GJXDM) builds architecture products based on common modeling techniques for example, PSAF products. This approach ensures consistency of architecture data types and relationships across the architecture description. Ensuring that the architecture data elements associated with the architecture description are GJXDM-compliant also assists integration across various architecture descriptions to support data model interchange. An example is the National Highway Traffic Safety Administration (NHTSA) Uniform Prehospital Emergency Medical Services (EMS) Dataset.

6.3 Benefits of Standards/Repository-Based Architectures

An architecture is 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 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, interoperability, or comparison
- Data reuse where data is developed once, and reused many times
- Flexible partitioning from different points of view, to include different disciplines or functional areas, and 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 Architecture Framework Data Model

The GJXDM is being proposed for the Architecture Framework Data Model (AFDM) for specification of the architecture data. The GJXDM is an object-oriented data model, database, and XML schema specification, generated from the database. The GJXDM represents the semantics and structure of common data elements and types required to exchange information consistently within the justice and public safety communities. This data model can be extended to allow product view information to be created and stored in a database in a way that assists analysis across products generated by different users for different architectures. While the GJXDM doesn't currently support the PSAF application, analysis is underway to extend it to support the PSAF. Subsequent versions of the PSAF will note the progress of this work effort.

6.5 Public Safety Architecture Repository System

The need for interoperability is one of the principal drivers behind the development of the PSAF. As the public safety community uses the PSAF, the resulting architectures will need to be stored in a central common repository to enable various analyses. An example would involve the differing voice radio systems within a multi-jurisdictional geographical area to determine current levels of interoperability and non-interoperability. It might entail the provision of recommendations of the standards-driven best practice methods by which the maximum legacy investment can be leveraged while enabling cross-organizational and -jurisdictional communications, when required.

The Public Safety Architecture Repository System (ARS) will enable the collection and analysis of architectures across multiple jurisdictions, geographical areas, and disciplines in a consistent yet flexible way. The ARS will permit the capture of architecturally pertinent data from any remote location that has Internet access. The captured data will be stored in a screening environment until it is vetted by an

architect, at which time it will be transferred seamlessly into the “live” environment. Once within the “live” repository, the data will be available for analysis on both a stand-alone basis and in combination with architectural data from other jurisdictions and disciplines. The ARS will have, furthermore, an analysis suite within the repository that allows an authorized user to run previously specified default and ad-hoc reports.

All of the value of an architectural effort is derived from the analysis that it affords the user. A centralized repository, in this case the ARS, is the key to deriving value from the PSAF and resulting enterprise architectures.

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 SAFECOM Program is currently evaluating several architecture tools and methods for storing the architecture data captured. Once practitioners in the field have tested tools and interfaces, *PSAF Volume III* will be compiled and published, in order to describe the best practices and use of the selected tool and interface.

Available commercial architecture tools are advancing rapidly in terms of technology, but no single tool yet provides all of the desired features. Generic architecture tools criteria and a tools adoption approach that incorporates best practices and current experience will be found in *PSAF Volume III*. Tools will be grouped into:

- Architecture modeling tools for producing architecture models
- Repository tools that store architecture elements and models
- Modeling tools with scalable repositories for architecture data

Criteria will be provided for evaluating:

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

7 Architecture Framework Evolution

The PSAF will continue to evolve to better fulfill the changing needs of its user community. The next sections discuss areas for future evolution of the PSAF.

7.1 PS SoR-Based Public Safety Operations

The requirements set forth in the PS SoR effectively establish a future domain for public safety communications. This domain consists of a loosely defined network hierarchy where the interfaces and the links between the interfaces have been defined. In addition, public safety operational and functional requirements have been defined in a qualitative manner, with quantitative definitions to follow in a subsequent version of the PS SoR.

The PSAF should always be used with the PS SoR firmly in mind. In other words, no architecture should be developed with the PSAF that doesn't comply with, or move toward the requirements stated in the PS SoR. Further versions of the PSAF will accommodate this goal in a more automated fashion.

7.2 Executable Architectures

There is an interest in evolving toward executable architectures to enable additional types of analyses 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 as they are often generated directly from the architecture models via an automated process.

These specialized tools can achieve several purposes:

- 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 processed.
- Trade-offs between systems can be assessed.
- Architecture measures can be evaluated (if metrics have been defined). This can support cost-benefit analyses and quantitative acquisition decisions.

Keep in mind some key factors while constructing and using executable architectures. 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 over time from the actual architecture models, leading to the architecture being ignored in favor of the implemented design within the simulation. Another possible negative outcome is that the simulation falls into disuse, as it is not able to keep up with the pace of architecture modifications.

No standards currently exist for the format of, or process for, constructing executable architectures. Some 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. The architecture data elements and the attributes required to construct executable models are specified in *PSAF 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 for validation and refinement on the results of the executable efforts. Efforts to construct executable architectures for their own sake have generally not been beneficial to the programs in question. Executable architectures have immediate implications for process improvement, but also directly support the investment decision process by providing realistic and repeatable cost-benefit analyses.

7.3 Other Evolution Plans

Other areas for future evolution of the PSAF include:

- Addressing baseline (current) and objective (target) architectures
- Alignment with the Federal Enterprise Architecture Reference Models
- Expansion of architecture uses
- More in-depth treatment of how architecture can be used to measure effectiveness, for example, through measures of effectiveness, capabilities, and measures of performance
- Architecture data management strategy for repository-based architectures
- Common taxonomy of architecture data. As progress is made in the evolution of common architecture-related data entries and the evolution of corresponding repositories of architectures and architecture data, the PSAF will evolve to address these subjects and provide guidance for their use
- Expansion of PSAF training

Appendix A -- Glossary of Acronyms

Note: The following acronyms are derived from various sources, including the National Incident Management System (NIMS), the National Response Plan (NRP), Unified Modeling Language (UML), and Public Safety Architecture Framework (PSAF) and Public Safety Statement of Requirements (PS SoR) documents. The next release of this document will identify and use these acronyms consistently.

A**A&I**

Architecture and Interoperability

ACL

Access Control List

AFDM

Architecture Framework Data Model

AFWG

Architecture Framework Working Group

API

Application Program Interface

ARS

Architecture Repository System

ATM

Asynchronous Transfer Mode

AV

All-Views

AV-1

Overview and Summary Information

AV-2

Integrated Dictionary

B**BRM**

Business Reference Model

C**COTS**

Commercial Off-The-Shelf

C4FM

Compatible Four-Level Frequency Modulation

D**DB**

Database

DBMS

Database Management System

DDL

Data Definition Language

DFD

Data flow diagram

DoDAF

DoD Architecture Framework

DOJ

Department of Justice

DRM

Data Reference Model

E**EAN**

Extended Area Network

EM

Emergency Management

EMS

Emergency Medical Services

EPA

Environmental Protection Agency

ERD

Entity Relationship Diagram

F

FBI

Federal Bureau of Investigation

FEA

Federal Enterprise Architecture

FEMA

Federal Emergency Management Agency

FIPS

Federal Information Processing Standard

FoS

Family of Systems

FRP

Federal Response Plan

G

GUI

Graphical User Interface

GJXDM

Global Justice XML Data Model

H

HCI

Human-Computer Interface

HR

Human Resources

HTML

Hypertext Markup Language

I

IAN

Incident Area Network

IC

Incident Commander or Incident Command

ICD

Interface Control Document

ICP

Incident Command Post

ICS

Incident Command System

IDEF

Integration Definition Methods

IDEF0

IDEF Function Modeling Method

IDEF1X

IDEF Data Modeling Method

IDEF3

IDEF Process Description Capture Method

IFC

Incident Fire Commander

ILEC

Incident Law Enforcement Commander

IMBE

Improved multiband excitation

I/O

Input and Output

IP

Internet Protocol

IT

Information Technology

J

JAN

Jurisdiction Area Network

K

KI

Key Interface

KIP

Key Interface Profile

L

LAN

Local Area Network

LEC

Law Enforcement Commander

LMR

Land Mobile Radio

LPC

Linear predictive coding

M**M&S**

Modeling and Simulation

N**NHTSA**National Highway Traffic Safety
Administration**NIMS**

National Incident Management System

NISTNational Institute of Standards and
Technology**NPSTC**National Public Safety Telecommunications
Council**NRP**

National Response Plan

O**OCL**

Object Constraint Language

OLES

Office of Law Enforcement Standards

OMB

Office of Management and Budget

OMG

Object Management Group

OO

Object-Oriented

OTAR

Over-The-Air Rekeying

OV

Operational View

OV-1

High-Level Operational Concept Graphic

OV-2

Operational Node Connectivity Description

OV-3

Operational Information Exchange Matrix

OV-4

Organizational Relationships Chart

OV-5

Operational Activity Model

OV-6Operational Activity Sequence and Timing
Descriptions**OV-6a**

Operational Rules Model

OV-6b

Operational State Transition Description

OV-6c

Operational Event-Trace Description

OV-7

Logical Data Model

P**PAN**

Personal Area Network

PDA

Personal Digital Assistant

PRM

Performance Reference Model

PS

Public Safety

PSAF

Public Safety Architecture Framework

P25

Project 25

R**R&D**

Research and Development

ROI

Return On Investment

S**SA**

Structured Analysis

SF

System Function

SoS

System of Systems

SRM

Service Component Reference Model

SV

Systems View

SV-1

Systems Interface Description

SV-2

Systems Communications Description

SV-3

Systems-Systems Matrix

SV-4

Systems Functionality Description

SV-5

Operational Activity to Systems
Functionality Traceability Matrix

SV-6

Systems Data Exchange Matrix

SV-7

Systems Performance Parameters Matrix

SV-8

Systems Evolution Description

SV-9

Systems Technology Forecasts

SV-10

Systems Functionality and Timing
Descriptions

SV-10a

Systems Rules Model

SV-10b

Systems State Transition Description

SV-10c

Systems Event-Trace Description

SV-11

Physical Schema

T

TCP

Transmission Control Protocol

TDMA

Time division multiple access

TRM

Technical Reference Model

TV

Technical Standards View

TV-1

Technical Standards Profile

TV-2

Technical Standards Forecast

U

UC

Unified Command

UML

Unified Modeling Language

UOB

Unit of Behavior

URR

Universal Reference Resources

V

VPN

Virtual Private Network

W

WAN

Wide Area Network

X

XML

Extensible Markup Language

Appendix A -- Dictionary of Terms

A

Architecture Data Element

One of the data elements that make up the PSAF products. Also referred to as architecture data type. (PSAF)

C

Command

The act of directing, ordering, or controlling by virtue of explicit statutory, regulatory, or delegated authority. (NIMS)

Communications Medium

A means of data transmission

D

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 relationships among the elements and their attributes or characteristics. (PSAF)

Data-Entity

The representation of a set of people, objects, places, events, or ideas that share the same characteristic relationships.

F

Family of Systems

A set or arrangement of independent systems that can be arranged or interconnected in various ways to provide different capabilities.

Format

The arrangement, order, or layout of data. (Derived from IEEE 610.5)

Functional Area

A major area of related activity.

I

Incident

An occurrence or event, natural or human-caused, that requires an emergency response to protect life or property. Incident can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response. (NIMS)

Incident Command Post

The field location at which the primary tactical-level, on-scene incident command functions are performed. The ICP may be collocated with the incident base or other incident facilities and is normally identified by a green rotating or flashing light. (NIMS)

Incident Command System

A standardized on-scene emergency management construct specifically designed to provide for the adoption of an integrated organizational structure that reflects the complexity and demands of single or multiple incidents, without being hindered by jurisdictional boundaries. ICS is the combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in the management of resources during incidents. It is used for all kinds of emergencies and is applicable to small as well as large and complex incidents. ICS is used by various jurisdictions and functional agencies, both public and private,

to organize field-level incident management operations. (NIMS)

Incident Commander

The individual responsible for all incident activities, including the development of strategies and tactics and the ordering and the release of resources. The IC has overall authority and responsibility for conducting incident operations and is responsible for the management of all incident operations at the incident site. (NIMS)

Independent Systems

A communications system that serves some communications service requirements for a public safety agency but does not or cannot provide standardized interfaces to other agencies' communication systems.

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. (PSAF)

Information Exchange

The collection of information elements and their performance attributes such as timeliness, quality, and quantity values. (PSAF)

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 public safety agency.

Integrated Architecture

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 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.

Interoperability (Communications)

Communications interoperability is the ability of public safety agencies to talk across disciplines and jurisdictions via radio communications systems, exchanging voice and data with one another on demand, in real time, when needed. (PS SoR)

J

Jurisdiction

A range or sphere of authority. Public agencies have jurisdiction at an incident related to their legal responsibilities and authority. Jurisdictional authority at an incident can be political or geographical (e.g., city, county, tribal, State, or Federal boundary lines) or functional (e.g., law enforcement, public health). (NIMS)

L

Liaison

A form of communication for establishing and maintaining mutual understanding and cooperation. (NIMS)

Liaison Officer

A member of the Command Staff responsible for coordinating with representatives from cooperating and assisting agencies. (NIMS)

Link

A representation of the physical realization of connectivity between systems nodes.

Local Government

A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the

council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government; an Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; a rural community, unincorporated town or village, or other public entity. See Section 2 (10), Homeland Security Act of 2002, Pub. L. 107-296, 116 Stat. 2135 (2002). (NIMS)

M

Mission Area

The general class to which an operational mission belongs.

Note: Within a class, the missions have common objectives.

Mission

An objective together with the purpose of the intended action. (Multiple tasks accomplish a mission.)

Multi-Jurisdictional Incident

An incident requiring action from multiple agencies that each have jurisdiction to manage certain aspects of an incident. In the Incident Command System (ICS), these incidents will be managed under Unified Command. (NIMS)

N

National Incident Management System (NIMS)

A system mandated by HSPD-5 that provides a consistent nationwide approach for Federal, State, local, and tribal governments, the private sector, and nongovernmental organizations to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. To provide for interoperability and compatibility among local, tribal, State, and Federal capabilities, the NIMS includes a core set of concepts, principles, and terminology. HSPD-5 identifies these as the ICS; multi-agency coordination systems; training;

identification and management of resources (including systems for classifying types of resources); qualification and certification; and the collection, tracking, and reporting of incident information and incident resources. (NIMS)

National Response Plan (NRP)

A plan mandated by HSPD-5 that integrates Federal domestic prevention, preparedness, response, and recovery plans into one all-discipline, all-hazards plan.

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.

O

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. (PSAF)

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. (PSAF)

Operational Node

A node that performs a role or mission. (PSAF)

Organization

An administrative structure with a mission.

P

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. Note: Multiple activities make up a process.

Product

Data elements you depict graphically, textually, and tabularly to identify architecture components and model their relationships. Architecture products describe characteristics pertinent to the architecture’s intended use. (PSAF)

R

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. (PSAF)

Requirement

A need or demand.

Role

A function or position (Webster’s Dictionary)

Rule

Statement that defines or constrains some aspect of the enterprise.

S

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. (PSAF)

System Data Element

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. (PSAF)

System Data Exchange

The collection of System Data Elements and their performance attributes such as timeliness, quality, and quantity values. (PSAF)

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. (PSAF)

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.

T

Task

A unit of discrete work, not specific to a single organization, system, or individual, that enables the accomplishment of missions or functions. Note: Multiple processes accomplish a single task; a single process may support multiple tasks.

Task Force

Any combination of resources assembled to support a specific mission or operational need. All resource elements within a Task Force must have common communications and a designated leader. (NIMS)

Tribal

Any Indian tribe, band, nation, or other organized group or community, including any Alaskan Native Village as defined in or established pursuant to the Alaskan Native Claims Settlement Act (85 stat. 688) (43 U.S.C.A. and 1601 et seq.), that is recognized

as eligible for the special programs and services provided by the United States to Indians because of their status as Indians. (NIMS)

U

Unified Command

An application of ICS used when there is more than one agency with incident jurisdiction or when incidents cross political jurisdictions. Agencies work together through

the designated members of the UC, often the senior person from agencies and/or disciplines participating in the UC, to establish a common set of objectives and strategies and a single IAP. (NIMS)

Universal Reference Resources

Reference models and information standards that serve as sources for guidelines and attributes that must be consulted while building architecture products. (PSAF)

Appendix B -- Dictionary of UML Terms

A

Abstract Class

A class that cannot be directly instantiated.
Contrast: concrete class.

Abstraction

1. The act of identifying the essential characteristics of a thing that distinguishes it from all other kinds of things. Abstraction involves looking for similarities across sets of things by focusing on their essential common characteristics. An abstraction always involves the perspective and purpose of the viewer; different purposes result in different abstractions for the same things. All modeling involves abstraction, often at many levels for various purposes.
2. A kind of dependency that relates two elements that represent the same concept at different abstraction levels.

Action

The specification of an executable statement that forms an abstraction of a computational procedure. An action typically results in a change in the state of the system and can be realized by sending a message to an object or modifying a link or a value of an attribute.

Action Sequence

An expression that resolves to a sequence of actions.

Action State

A state that represents the execution of an atomic action, typically the invocation of an operation.

Activation

The execution of an action.

Active Class

A class whose instances are active objects.

Active Object

An object that owns a thread and can initiate control activity. An instance of active class.

Activity Graph

A special case of a state machine that is used to model processes involving one or more classifiers.

Actor (Class)

A coherent set of roles that users of use cases play when interacting with these use cases. An actor has one role for each use case with which it communicates.

Actual Parameter

Synonym: argument.

Adornments

Textual or graphical items that are added to an element's basic notation and are used to visualize details from the element's specification. (One of two annotation mechanisms in UML)

Aggregate (Class)

A class that represents the whole in an aggregation (whole-part) relationship.

Aggregation

A special form of association that specifies a whole-part relationship between the aggregate or whole, and a component part.

Annotation Mechanisms

Annotations of existing items in a UML diagram. The two annotation mechanisms are specifications and adornments.

Architecture

The organizational structure and associated behavior of a system. An architecture can be recursively decomposed into parts that interact through interfaces, relationships that connect parts and constraints for assembling parts. Parts that interact through interfaces include classes, components and subsystems.

Artifact

A piece of information that is used or produced by a software development process, such as an external document or a work

product. An artifact can be a model, description, or software.

Association

The semantic relationship between two or more classifiers that involves connections among their instances.

Attribute

A named property of a class that describes a range of values that instances of the property may hold.

B

Building Blocks

Things, relationships, and diagrams that compose something.

C

Class

A description of a set of objects that share the same attributes, operations, methods, relationships and semantics. A class may use a set of interfaces to specify collections of operations it provides to its environment.

Class Diagram

A diagram that shows a collection of declarative, or static, model elements, such as classes, types, and their contents and relationships.

Collaboration

The specification of how an operation or classifier, such as a use case, is realized by a set of classifiers and associations playing specific roles used in a specific way. The collaboration defines an interaction.

Collaboration Diagram

A diagram that shows interactions organized around the structure of a model, using either classifiers and associations or instances and links. Unlike a sequence diagram, a collaboration diagram shows the relationships among the instances. Sequence diagrams and collaboration diagrams express similar information, but show it in different ways.

Component

A modular, deployable and replaceable part of a system that encapsulates implementation and exposes a set of interfaces. A component is typically specified by one or more classifiers (e.g., implementation classes) that reside on it and may be implemented by one or more artifacts (e.g., binary, executable or script files).

Component Diagram

A diagram that shows the organizations and dependencies among components.

Concrete Class

A class that can be directly instantiated.
Contrast: abstract class.

Constraint

A semantic condition or restriction. Certain constraints are predefined in the UML; others may be user-defined. Constraints are one of three extensibility mechanisms in the UML.

Container

1. An instance that exists to contain other instances and that provides operations to access or iterate over its contents (e.g., arrays, lists, sets).
2. A component that exists to contain other components.

Containment Hierarchy

A namespace hierarchy consisting of model elements and the containment relationships that exist between them. A containment hierarchy forms a graph.

Context

A view of a set of related modeling elements for a particular purpose, such as specifying an operation.

D

Dependency

A relationship between two modeling elements, in which a change to one modeling element (the independent element) will affect the other modeling element (the dependent element).

Deployment Diagram

A diagram that shows the configuration of run-time processing nodes and the components, processes, and objects that live on them. Components represent run-time manifestations of code units.

Derivation

A relationship between an element and another element that can be computed from it. Derivation is modeled as a stereotype of an abstraction dependency with the keyword *Derive*.

Derived Element

An element that can be computed from other elements and is included for clarity or for design purposes, even though it adds no semantic information.

Diagram

A graphical presentation of a collection of model elements, most often rendered as a connected graph of arcs (relationships) and vertices (other model elements). The UML supports the following diagrams: class diagram, object diagram, use case diagram, sequence diagram, collaboration diagram, statechart diagram, activity diagram, component diagram and deployment diagram.

E**Effect**

Specifies an optional procedure to be performed when the transition fires.

Element

An atomic constituent of a model.

Entry Action

An action executed upon entering a state in a state machine, regardless of the transition taken to reach that state.

Event

The specification of a significant occurrence that has a location in time and space. In the context of statechart diagrams, an event is an occurrence that can trigger a transition.

Exit Action

An action executed upon exiting a state in a state machine, regardless of the transition taken to exit that state.

Extend

A relationship from an extension use case to a base use case, specifying how the behavior defined for the extension use case augments (subject to conditions specified in the extension) the behavior for the base use case. The behavior is inserted at the location defined by the extension point in the base use case. The base use case does not depend on performing the behavior of the extension use case.

F**Fire**

See “Transition.”

G**Guard**

A Boolean predicate that provides fine-grained control over the firing of the transition. It must be true for the transition to fire. It is evaluated at the time the event is dispatched. There can be at most one guard per transition.

Generalizable Element

A model element that may participate in a generalization relationship.

Generalization

A taxonomic relationship between a more general element and a more specific element. The more specific element is fully consistent with the more general element and contains additional information. An instance of the more specific element may be used where the more general element is allowed. See: “Inheritance.”

I**Inheritance**

The mechanism by which more specific elements incorporate structure and behavior of more general elements related by behavior.

Instance

An individual entity with its own identity and value.

Interaction

A specification of how stimuli are sent between instances to perform a specific task. The interaction is defined in the context of a collaboration.

Interaction Diagram

A generic term that applies to several types of diagrams that emphasize object interactions. These include collaboration and sequence diagrams.

Interface

A named set of operations that characterize the behavior of an element.

L**Link**

A semantic connection among a tuple of objects. An instance of an association.

Link End

An instance of an association end.

M**Metadata**

The architecture data types, possibly expressed in the form of a physical schema.

Message

A specification of the conveyance of information from one instance to another, with the expectation that activity will ensue. A message may specify the raising of a signal or the call of an operation.

Model

A semantically complete abstraction of a system.

N**Node**

A node is a classifier that represents a run-time computational resource, which generally has at least a memory and often processing

capability. Run-time objects and components may reside on nodes.

Notes

Notes may contain any combination of text or graphics. A note that renders a comment has no semantic impact; it does not alter the meaning of the model to which it is attached. Notes are used to specify requirements, observations, reviews and explanations, in addition to rendering constraints.

O**Object**

An entity with a well-defined boundary and identity that encapsulates state and behavior. State is represented by attributes and relationships; behavior is represented by operations, methods and state machines. An object is an instance of a class.

Object Diagram

A diagram that encompasses objects and their relationships at a point in time. An object diagram may be considered a special case of a class diagram or a collaboration diagram.

Operation

An operation is the implementation of a service that can be requested from any object of the class to affect behavior.

P**Package**

A package is a general-purpose mechanism for organizing elements into groups.

Postcondition

A constraint that must be true at the completion of an operation.

Precondition

A constraint that must be true when the operation is invoked.

R**Realization**

The relationship between a specification and its implementation; an indication of the

inheritance of behavior without the inheritance of structure.

Refinement

A relationship that represents a more complete specification of something that has already been specified at a certain level of detail. For example, a design class is a refinement of an analysis class.

Relationship

A semantic connection among model elements. Examples include: dependency, association, generalization, and realization.

S

Sequence Diagram

A diagram that shows object interactions arranged in a time sequence. In particular, it shows the objects participating in the interaction and the sequence of messages exchanged. Unlike a collaboration diagram, a sequence diagram includes time sequences but does not include object relationships. A sequence diagram can exist in a generic form (describes all possible scenarios) and in an instance form (describes one actual scenario). Sequence diagrams and collaboration diagrams express similar information, but show it in different ways.

Signal

The specification of an asynchronous stimulus communicated between instances. Signals may have parameters.

Specification

A declarative description of what something is or does.

Source

A source designates the originating state vertex of the transition.

State

A condition or situation during the life of an object during which it satisfies some condition, performs some activity, or waits for some event.

State Machine

A behavior that specifies the sequences of states that an object or interaction goes

through during its life in response to events, together with its responses and actions.

Statechart Diagram

A diagram that shows a state machine.

Stereotype

A new type of modeling element that extends the semantics of the metamodel. Stereotypes must be based on certain existing types or classes in the metamodel. Stereotypes may extend the semantics, but not the structure of pre-existing types and classes. Certain stereotypes are predefined in the UML; others may be user defined. Stereotypes are one of three extensibility mechanisms in the UML.

Stimulus

The passing of information from one instance to another, such as raising a signal or invoking an operation. The receipt of a signal is normally considered an event.

Swim Lane

A partition on an activity diagram for organizing the responsibilities for actions. Swim lanes typically correspond to organizational units in a business model.

T

Tagged Value

An extensibility mechanism that adds a new property to things.

Target

Designates the target state vertex that is reached when the transition is taken.

Things

The abstractions that are first-class citizens in a model: relationships tie these things together; diagrams group collections of things. There are four kinds of things in the UML: structural things, behavioral things, grouping things, and annotational things.

Thread (of Control)

A single path of execution through a program, a dynamic model, or some other representation of control flow. Also, a stereotype for the implementation of an active object as a lightweight process.

Time Event

An event that denotes the time elapsed since the current state was entered.

Time Expression

An expression that resolves to an absolute or relative value of time.

Trace

A dependency that indicates an historical or process relationship between two elements that represent the same concept without specific rules for deriving one from the other.

Transient Object

An object that exists only during the execution of the process or thread that created it.

Transition

A relationship between two states indicating that an object in the first state will perform certain specified actions and enter the second state when a specified event occurs and specified conditions are satisfied. On such a change of state, the transition is said to fire.

Trigger

Specifies the event that fires the transition. There can be at most one trigger per transition.

Type

A stereotyped class that specifies a domain of objects together with the operations applicable to the objects, without defining the physical implementation of those objects. A type may not contain any methods, maintain its own thread of control, or be nested. However, it may have attributes and associations. Although an object may have at most one implementation class, it may conform to multiple different types.

Use Case Diagram

A diagram that shows the relationships among actors and use cases within a system.

Use Case Instance

The performance of a sequence of actions being specified in a use case. An instance of a use case.

Use Case Model

A model that describes a system’s functional requirements in terms of use cases.

U

Use Case (Class)

The specification of a sequence of actions, including variants, that a system or other entity can perform, interacting with actors of the system.

Appendix C -- References

- 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.
- DHS, 2004 *National Incident Management System*, Available: http://www.fema.gov/pdf/nims/nims_doc_full.pdf, March 2004.
- DHS, 2004 *Public Safety Statement of Requirements*, Available: http://www.safecomprogram.gov/SAFECOM/library/technology/1200_statementof.htm, March 2004.
- DoDAF Working Group, 2004 DoD Architecture Framework Working Group, *DoD Architecture Framework Version 1.0*, “Volume I: Definitions and Guidelines,” February 2004.
- DoDAF Working Group, 2004 DoD Architecture Framework Working Group, *DoD Architecture Framework Version 1.0*, “Volume II: Product Descriptions,” February 2004.
- FIPS, 1993 *Integration Definition for Function Modeling (IDEF0) method*, 1993, pp. 183
- FIPS, 1993 *Integration Definition for Function Modeling (IDEF1X) method*, 1993, pp. 184
- 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.
- Levis, 2000 Levis, A., and Wagenhals, L., “C4ISR Architectures I: Developing a Process for C4ISR Architecture Design,” *Systems Engineering*, Vol. 3, No. 4, Fall 2000.
- Neill, 2002 Neill, C.J., and Holt, J.D., “Adding Temporal Modeling to the UML to Support Systems Design,” *Systems Engineering*, Vol. 5, No. 3, Fall 2002.
- 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*, November 30, 2000.
- OMG, 2003 Object Management Group, *Unified Modeling Language Specification*, Version 1.5, Framingham, Massachusetts, Available: <http://www.omg.org>, March 2003.
- OMG, 2001 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.