SAFECOM

PROGRAM OVERVIEW

ISART Conference

March 1-3, 2005

Thomas Coty
Director for Technology and Standards
thomas.coty@dhs.gov

SAFECOM was created to coordinate interoperability efforts across the Federal Government

SAFECOM serves as the umbrella program within the Federal Government to coordinate the efforts of local, state, federal, and tribal public safety agencies working to improve public safety response through more effective, efficient, interoperable wireless communications

- SAFECOM is one of the President's top three E-Government initiatives
- SAFECOM is a program driven by public safety practitioners
- Dedicated to develop better technologies and processes for the cross-jurisdictional and cross-disciplinary coordination of existing systems and future networks
- Responsible for outreach to local, state, and federal public safety agencies and to assist in interoperability planning and implementation

Intelligence Reform and Terrorism Prevention Act of 2004

SAFECOM ‘s Authority comes from the Intelligence Reform and Terrorism Prevention Act of 2004

- Enacted on December 17, 2004, this Act directs the Secretary of the Department of Homeland Security (DHS) to establish a program to enhance public safety interoperable communications at all levels of government. The program is authorized to:
  - Coordinate with other Federal agencies to establish a comprehensive national approach to achieving public safety interoperable communications;
  - Develop, with Federal agencies and State and local authorities, minimum capabilities for communications interoperability for Federal, State, and local public safety agencies;
  - Accelerate voluntary consensus standards for public safety interoperable communications;
  - Develop and implement flexible open architectures for short- and long-term solutions to public safety interoperable communications;

Intelligence Reform and Terrorism Prevention Act of 2004

SAFECOM 's Authority comes from the Intelligence Reform and Terrorism Prevention Act of 2004

Continued:

- Identify priorities for research, development, and testing and evaluation within DHS and assist other Federal agencies in doing the same with regard to public safety interoperable communications;
- Provide technical assistance to State and locals regarding planning, acquisition strategies, interoperability architectures training, and other functions necessary to achieve public safety communications interoperability;
- Develop and disseminate best practices to improve public safety communications interoperability; and
- Develop appropriate performance measures and milestones to measure the Nation's progress to achieving public safety communications interoperability.

Relevant Public Safety Key Strategic Initiatives

- Complete the comprehensive Public Safety Statement of Requirements (SoR)
- Provide technical assistance for public safety communications and interoperability
- Create a baseline of public safety interoperable communications across the country
- Research, develop, test, and evaluate (RDT&E) existing and emerging technologies for improved public safety communications and interoperability
- Develop a process to address standards necessary to improve public safety communications and interoperability

Relevant Public Safety Key Strategic Initiatives

- **Complete the comprehensive Public Safety Statement of Requirements (SoR)**

- **Provide technical assistance for public safety communications and interoperability**

- **Create a baseline of public safety interoperable communications across the country**

- **Research, develop, test, and evaluate (RDT&E) existing and emerging technologies for improved public safety communications and interoperability**

- **Develop a process to address standards necessary to improve public safety communications and interoperability**

Public Safety Statement of Requirements (SoR)

- Version 1.0 released April 2004.
- Version 1.1 draft is complete, ready for public safety vetting through SoR Working Group.
- Version 2.0 work is underway. Quantifying functional requirements. Work will be completed and vetted through SoR Working Group.

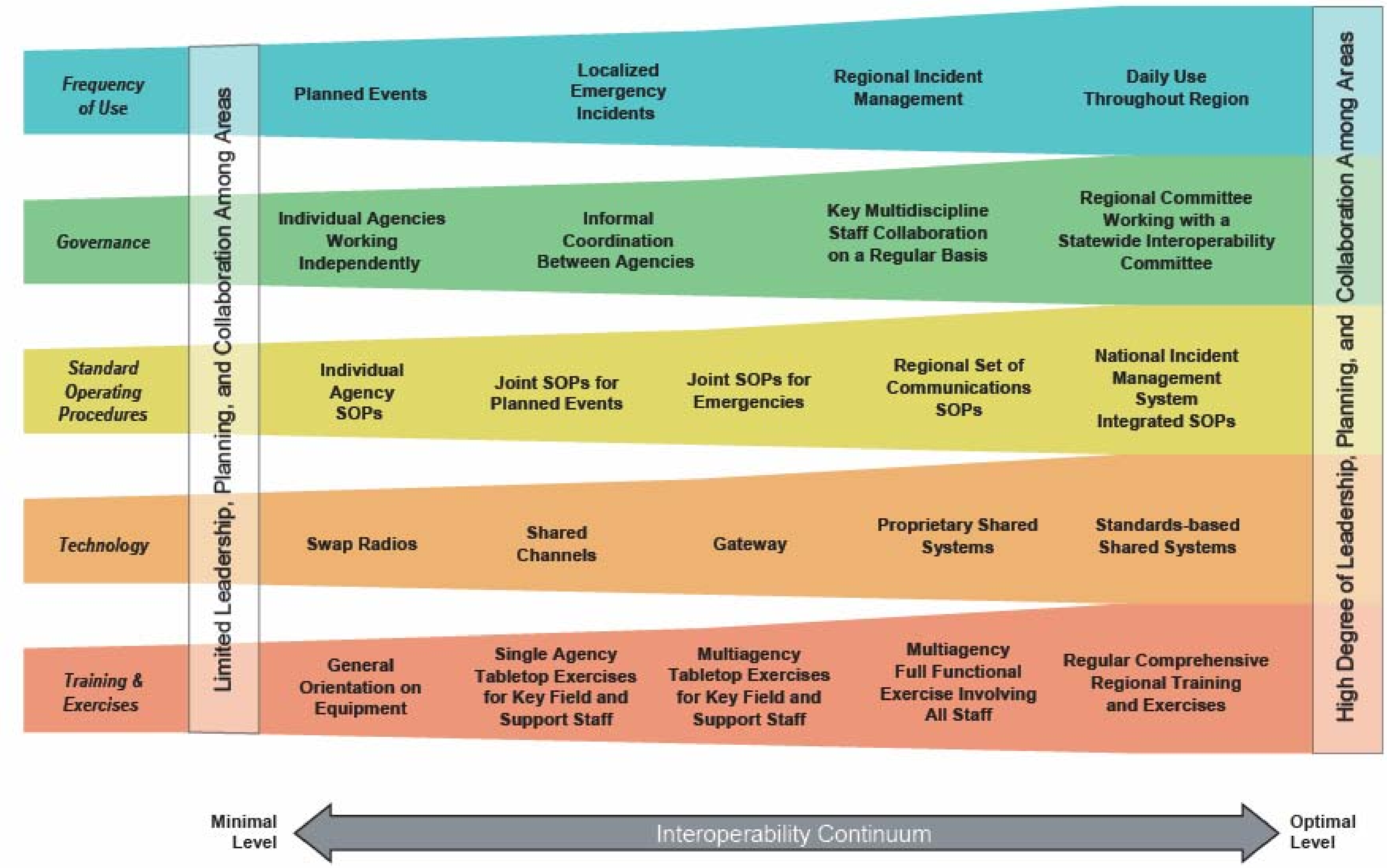
Relevant Public Safety Key Strategic Initiatives

- Complete the comprehensive Public Safety Statement of Requirements (SoR)
- **Provide technical assistance for public safety communications and interoperability**
- Create a baseline of public safety interoperable communications across the country
- Research, develop, test, and evaluate (RDT&E) existing and emerging technologies for improved public safety communications and interoperability
- Develop a process to address standards necessary to improve public safety communications and interoperability

Technical Assistance and Outreach

- SAFECOM’s technical assistance and outreach is program is evolving
- The initial effort was in the derived from the RapidCom project
- NPSTC Support Office

Communications Interoperability Continuum



Frequency of Use: Planned Events · Localized Emergency Incidents · Regional Incident Management · Daily Use Throughout Region

Governance: Individual Agencies Working Independently · Informal Coordination Between Agencies · Key Multidiscipline Staff Collaboration on a Regular Basis · Regional Committee Working with a Statewide Interoperability Committee

Standard Operating Procedures: Individual Agency SOPs · Joint SOPs for Planned Events · Joint SOPs for Emergencies · Regional Set of Communications SOPs · National Incident Management System Integrated SOPs

Technology: Swap Radios · Shared Channels · Gateway · Proprietary Shared Systems · Standards-based Shared Systems

Training & Exercises: General Orientation on Equipment · Single Agency Tabletop Exercises for Key Field and Support Staff · Multiagency Tabletop Exercises for Key Field and Support Staff · Multiagency Full Functional Exercise Involving All Staff · Regular Comprehensive Regional Training and Exercises

Limited Leadership, Planning, and Collaboration Among Areas

High Degree of Leadership, Planning, and Collaboration Among Areas

Minimal Level ◄ Interoperability Continuum ► Optimal Level

March 8, 2005

www.safecomprogram.gov

Statewide Communications Interoperability Planning

- SAFECOM worked in conjunction with NIJ, CommTech and the Virginia Commonwealth Interoperability Coordinator to develop a locally-driven, statewide strategic plan for communications interoperability
- Using SAFECOM's bottom-up approach, the Virginia planning process was driven by local and state public safety officials
  - Regional Focus Groups
  - Strategic Planning Session

Result: A collaborative, actionable plan that addresses the needs and challenges of Virginia's public safety community *as identified by Virginia's public safety community.*

Statewide Communications Interoperability Planning (SCIP) Methodology

Statewide Communication Interoperability Planning (SCIP) Methodology

An Approach Based on the Commonwealth of Virginia's Planning Process

Homeland Security

SAFECOM

Partnering to Save Lives

- A step-by-step process for developing a locally driven statewide strategic plan, based on the Virginia planning process

- Available at *www.safecomprogram.gov*

Relevant Public Safety Key Strategic Initiatives

- Complete the comprehensive Public Safety Statement of Requirements (SoR)
- Provide technical assistance for public safety communications and interoperability
- **Create a baseline of public safety interoperable communications across the country**
- Research, develop, test, and evaluate (RDT&E) existing and emerging technologies for improved public safety communications and interoperability
- Develop a process to address standards necessary to improve public safety communications and interoperability

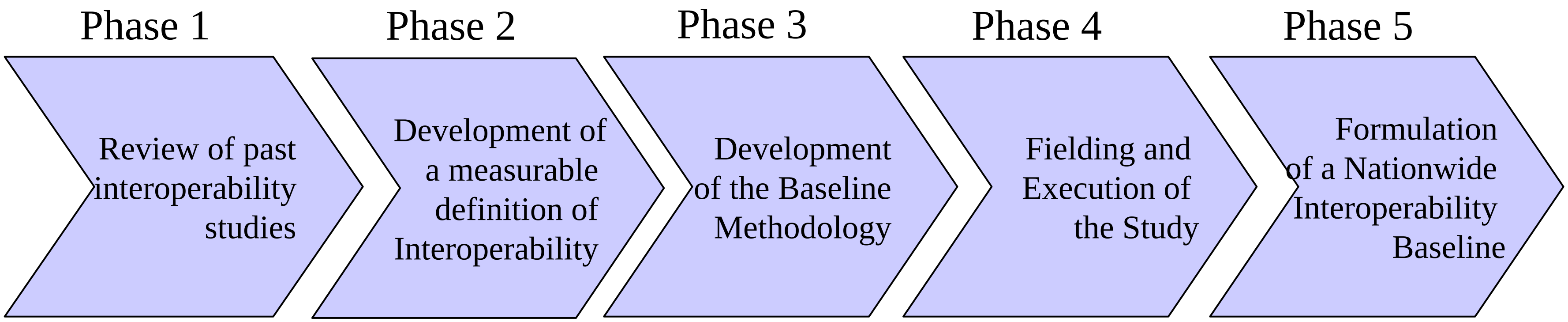
Interoperability Baseline

SAFECOM has begun the effort to quantify the current state of public safety communications. The purpose of the Interoperability Baseline effort is:

- To quantify the extent to which public safety communications are interoperable
- To make the case for the allocation of additional resources for interoperability
- To track the impact of federal programs and measure the success of these programs
- To establish an on-going process and mechanism to measure the state of interoperability on a recurring basis
- **To develop an interoperability baseline self-assessment tool for local and state public safety agencies**

Interoperability Baseline

How Will this be done?



Phase 1

Review of past interoperability studies

Phase 2

Development of a measurable definition of Interoperability

Phase 3

Development of the Baseline Methodology

Phase 4

Fielding and Execution of the Study

Phase 5

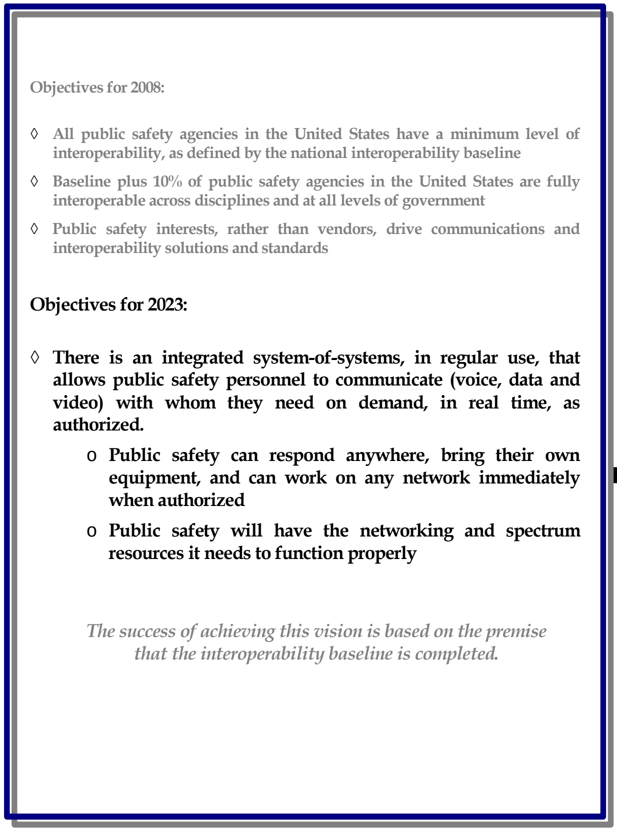
Formulation of a Nationwide Interoperability Baseline

- The Baseline contract was awarded to Booz Allen Hamilton in January 2005
- Phased approach over a 12 – 15 month Period of Performance
- Interoperability Baseline database results will be searchable by demographic, geographic, etc. categorizations
- The Baseline effort will deliver a self-assessment tool, providing public safety with a internet-based tool to assess their own level of interoperability

Relevant Public Safety Key Strategic Initiatives

- Complete the comprehensive Public Safety Statement of Requirements (SoR)
- Provide technical assistance for public safety communications and interoperability
- Create a baseline of public safety interoperable communications across the country
- **Research, develop, test, and evaluate (RDT&E) existing and emerging technologies for improved public safety communications and interoperability**
- **Develop a process to address standards necessary to improve public safety communications and interoperability**

Year 2023 Objectives



Objectives for 2008:

- ◊ All public safety agencies in the United States have a minimum level of interoperability, as defined by the national interoperability baseline
- ◊ Baseline plus 10% of public safety agencies in the United States are fully interoperable across disciplines and at all levels of government
- ◊ Public safety interests, rather than vendors, drive communications and interoperability solutions and standards

Objectives for 2023:

- ◊ There is an integrated system-of-systems, in regular use, that allows public safety personnel to communicate (voice, data and video) with whom they need on demand, in real time, as authorized.
  - o Public safety can respond anywhere, bring their own equipment, and can work on any network immediately when authorized
  - o Public safety will have the networking and spectrum resources it needs to function properly

The success of achieving this vision is based on the premise that the interoperability baseline is completed.

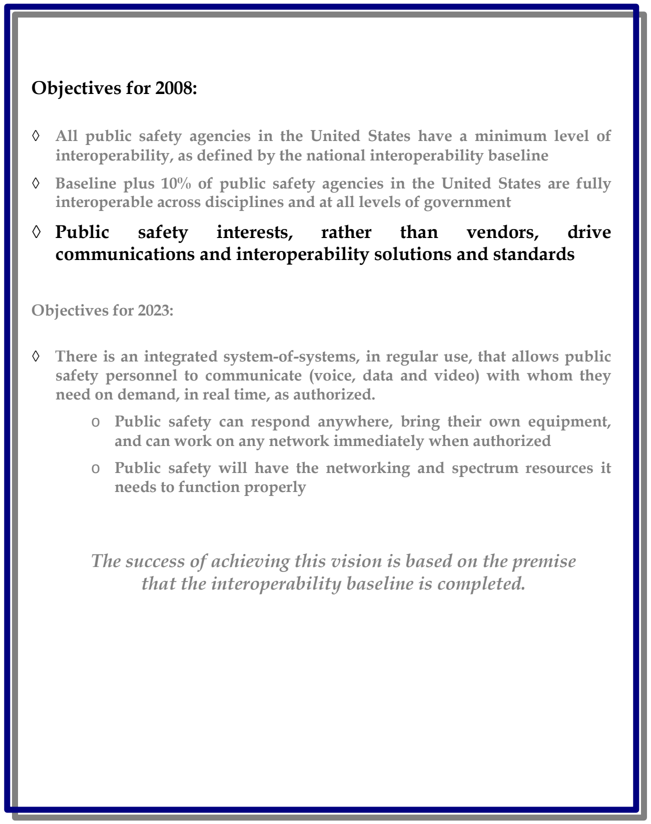
Objectives for 2023:

- ◊ There is an integrated system-of-systems, in regular use, that allows public safety personnel to communicate (voice, data and video) with whom they need on demand, in real time, as authorized.
  - o Public safety can respond anywhere, bring their own equipment, and can work on any network immediately when authorized
  - o Public safety will have the networking and spectrum resources it needs to function properly

Implications and Assumptions (2023)

An integrated “system-of-systems” in the year 2023 implies the widespread acceptance and use of interface standards by industry, and the widespread procurement and deployment of these systems by public safety

Year 2008 Objectives



Objectives for 2008:

- ◊ All public safety agencies in the United States have a minimum level of interoperability, as defined by the national interoperability baseline
- ◊ Baseline plus 10% of public safety agencies in the United States are fully interoperable across disciplines and at all levels of government
- ◊ **Public safety interests, rather than vendors, drive communications and interoperability solutions and standards**

Objectives for 2023:

- ◊ There is an integrated system-of-systems, in regular use, that allows public safety personnel to communicate (voice, data and video) with whom they need on demand, in real time, as authorized.
  - o Public safety can respond anywhere, bring their own equipment, and can work on any network immediately when authorized
  - o Public safety will have the networking and spectrum resources it needs to function properly

The success of achieving this vision is based on the premise that the interoperability baseline is completed.

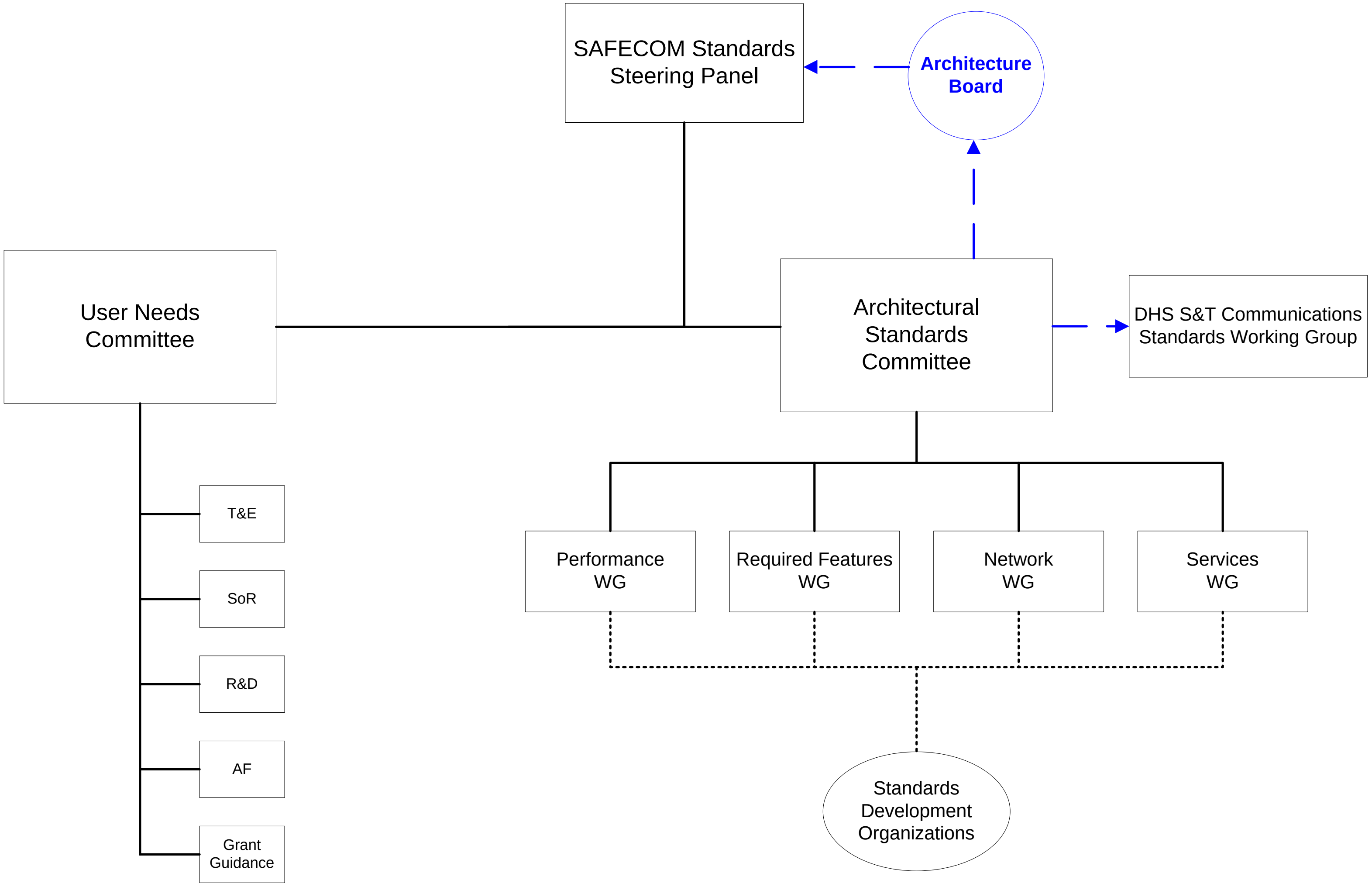
Objectives for 2008:

- ◊ **Public safety interests, rather than vendors, drive communications and interoperability solutions and standards**

Implications and Assumptions (2008)

- A disciplined, structured process will be required to ensure that public safety’s interests drive the development of solutions and interface standards (specifications)
- This disciplined process will be driven by public safety
- The foundation of this process will be based upon public safety requirements

Standards Process Organization


SAFECOM Standards Steering Panel
Architecture Board
User Needs Committee
Architectural Standards Committee
DHS S&T Communications Standards Working Group
T&E
SoR
R&D
AF
Grant Guidance
Performance WG
Required Features WG
Network WG
Services WG
Standards Development Organizations

Public Safety Statement of Requirements (SoR)

What is the SoR?

- The SoR is a practitioner created set of communications requirements
  - It is a living document
- Version 1.x
  - Currently focused on qualitative requirements
- Version 2.0
  - Will begin to focus on quantitative requirements

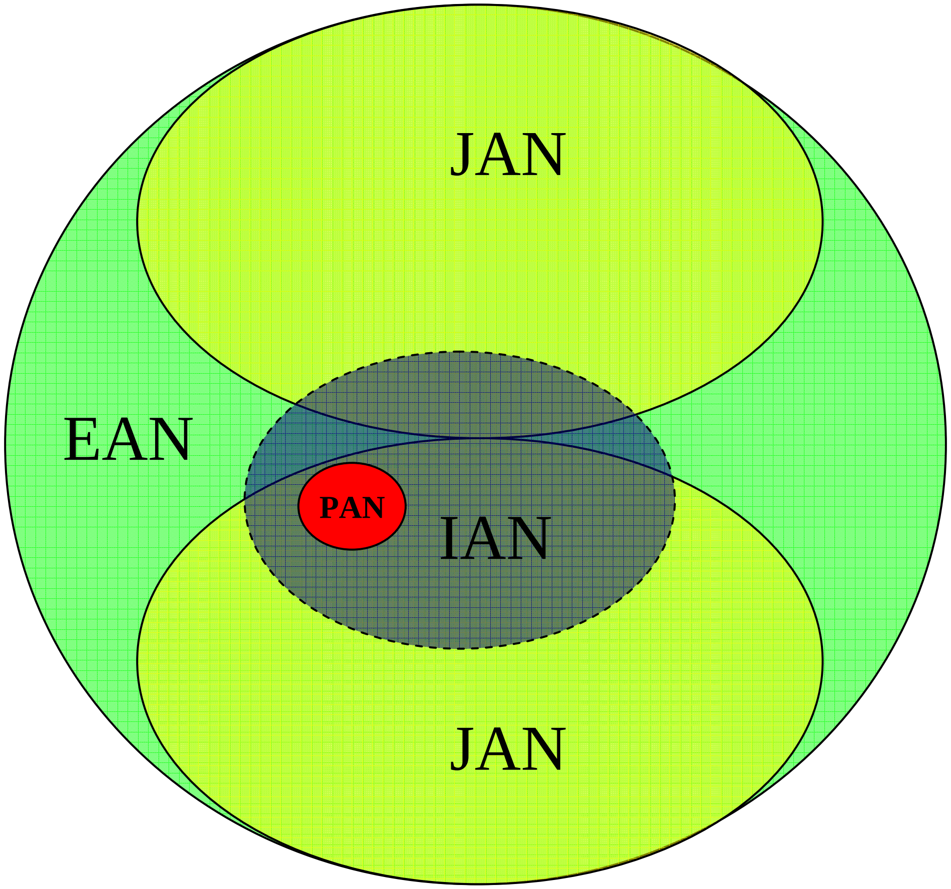
SAFECOM advocates the creation of a System of Systems architecture solution for interoperability.

The System of Systems involves interaction between the:

- Personal Area Network (PAN)
- Incident Area Network (IAN)
- Jurisdiction Area Network (JAN)
- Extended Area Network (EAN)

System Capabilities

- Practitioners seamlessly move between Jurisdictional Area Networks
- Practitioners join and leave networks as needed
- Allows for the creation and Growth of Temporary Networks
- System can recognize, register, authorize, and grant interoperable communications with the new resources

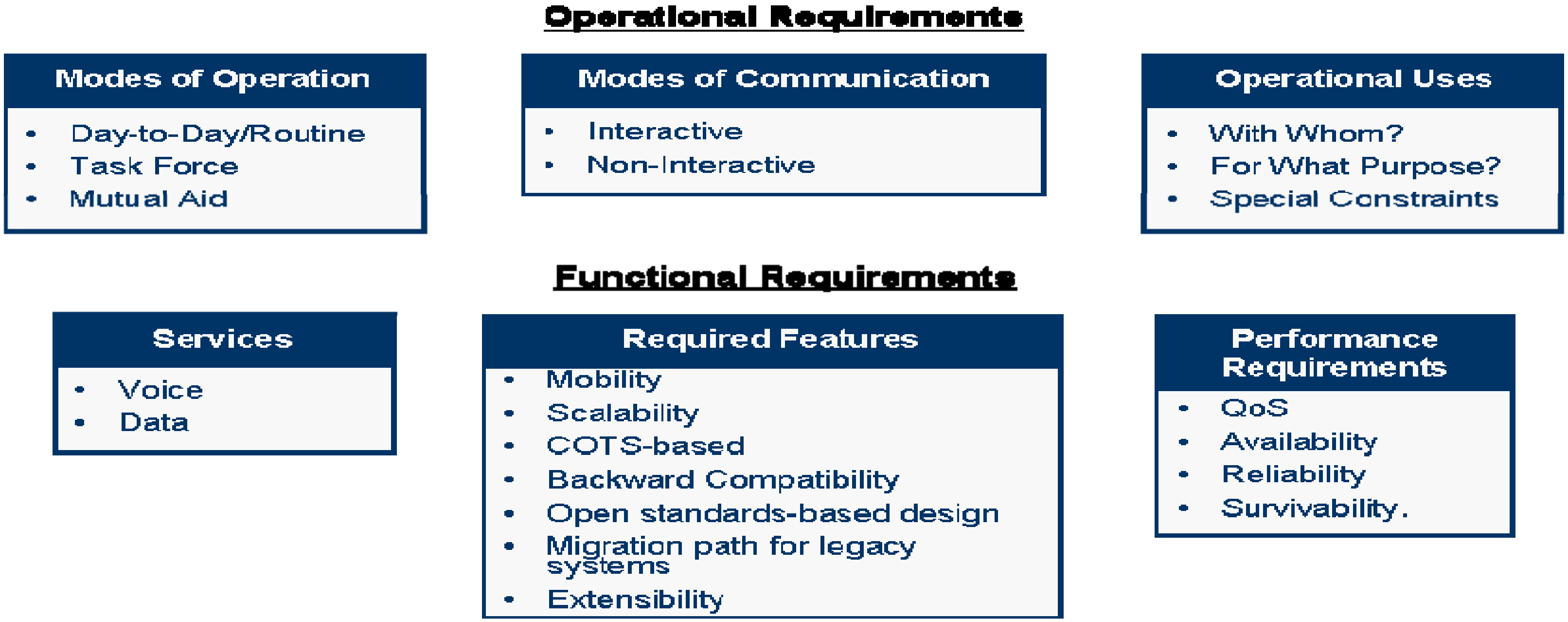


The System of Systems architecture builds from Personal Networks to Extended Networks, and puts an emphasis on the individual public safety practitioner

Different communications systems seamlessly integrate to form the various networks

Content of the SoR

- Defines public safety roles and functions, including First Responders and Supplemental Responders
- Defines the required communications services for the first responders, i.e. voice, data, video
- Provides real-world implementation scenarios with a focus on future-looking communications
  - Includes operationally focused scenarios.
- Contains Operational Requirements for each discipline and Functional Requirements of the technology



Operational Requirements

Modes of Operation
- Day-to-Day/Routine
- Task Force
- Mutual Aid

Modes of Communication
- Interactive
- Non-Interactive

Operational Uses
- With Whom?
- For What Purpose?
- Special Constraints

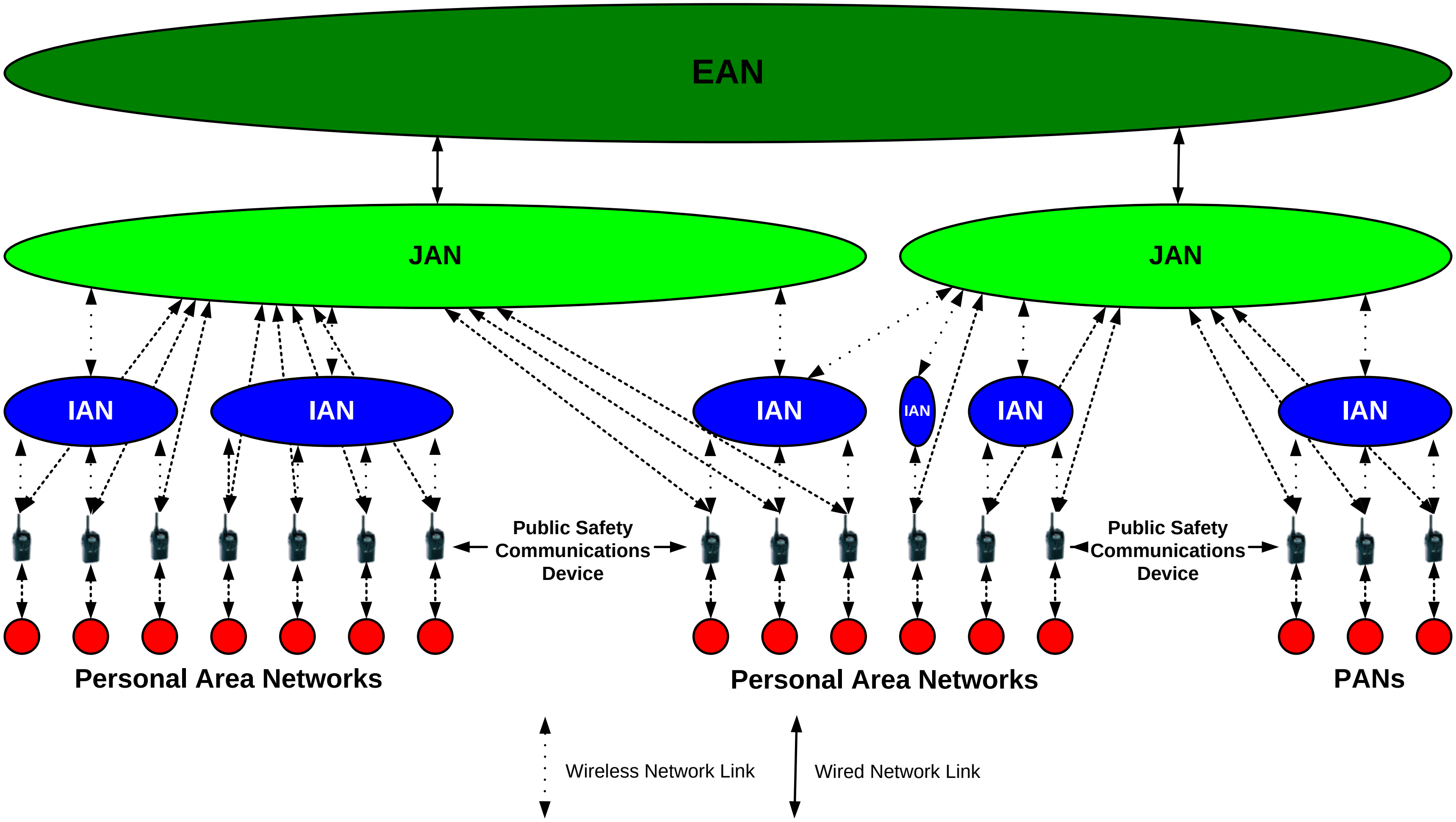
Functional Requirements

Services
- Voice
- Data

Required Features
- Mobility
- Scalability
- COTS-based
- Backward Compatibility
- Open standards-based design
- Migration path for legacy systems
- Extensibility

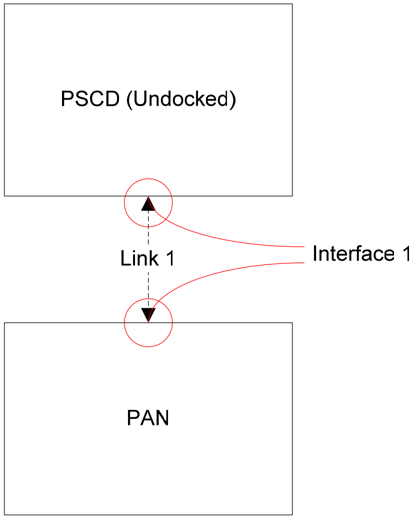
Performance Requirements
- QoS
- Availability
- Reliability
- Survivability.

Conceptual Network Diagram



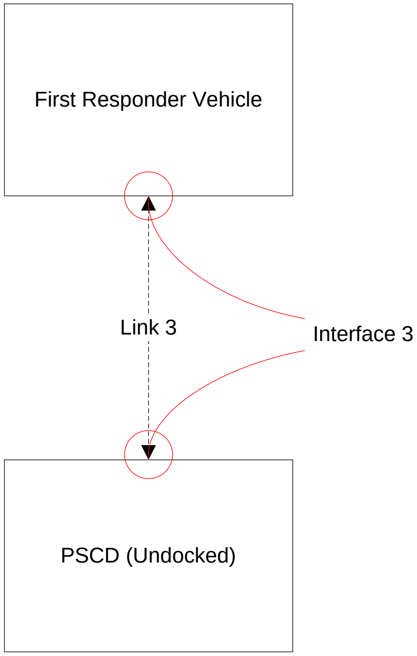
The Personal Area Network

- Current relevant protocols
  - 802.15.x
- Uses for the PAN
  - Biometric monitoring
  - Sensors (chemical, temp, etc.)
  - 3-D Geo-Location
  - Orientation
- Challenges
  - Interference if the PAN is wireless
  - Single point of failure of 1 transceiver is used to communicate to Public Safety Communications Device



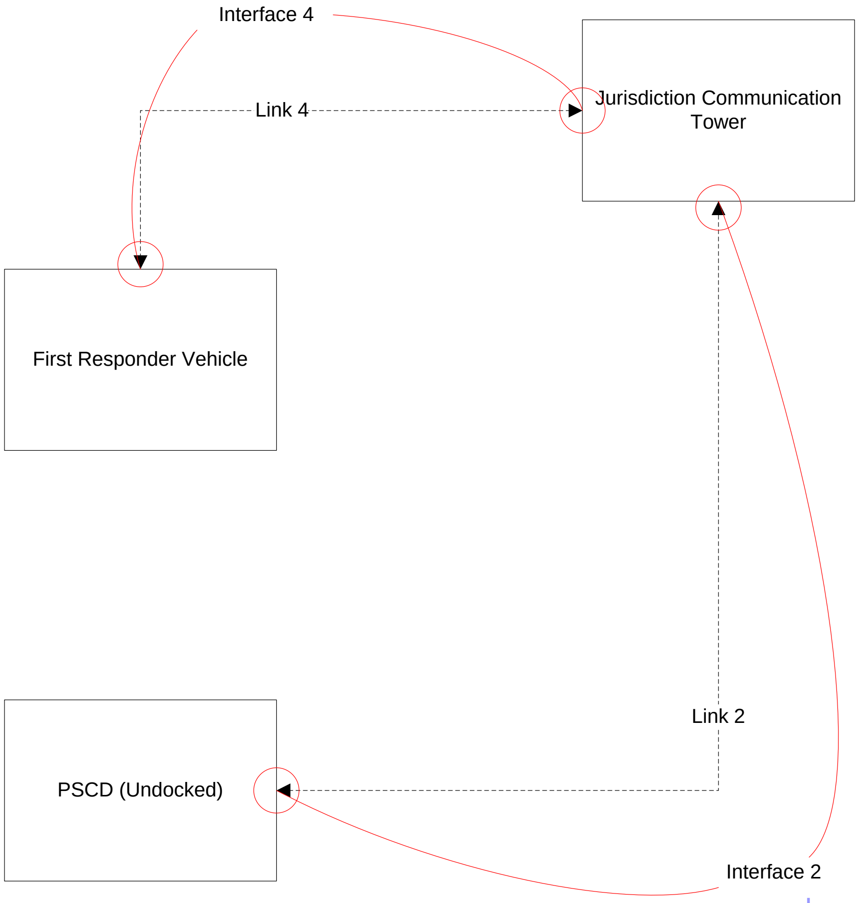
The Incident Area Network

- Current relevant protocols
  - 802.11x
- Uses for the IAN
  - Establishing an ad hoc network at a scene
  - Radio bridges can extend that network into a building
  - Allows for communication at an incident when there has been fixed infrastructure damage
- Challenges
  - Security with existing COTS protocols
  - Range with spectrum set aside (4.9GHz)



The Jurisdiction Area Network

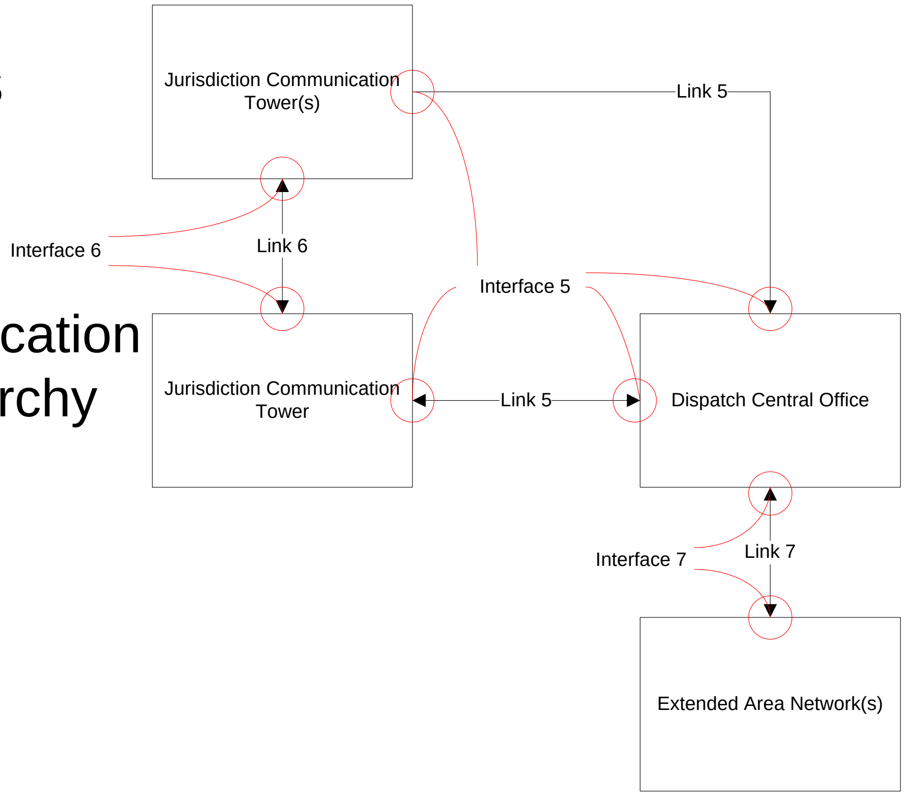
- Current relevant protocols
  - 802.16e/802.20
- Uses for the JAN
  - Primary means of communications for public safety (likened to today's LMR)
- Challenges
  - COTS protocol reuse
  - Potential spectrum questions



The Extended Area Network

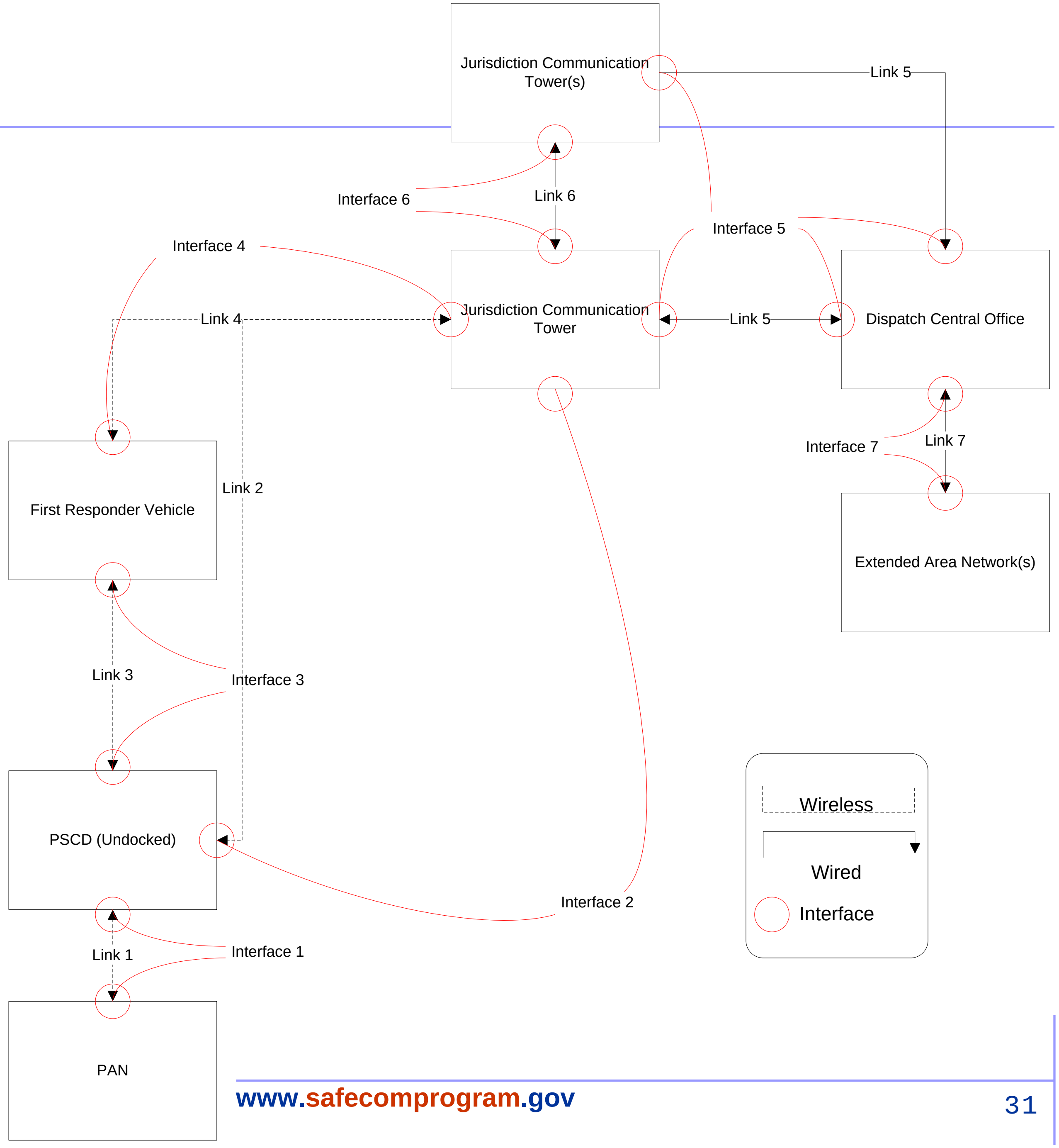
- Current relevant protocols
  - 802.3
- Uses for the EAN
  - Primary means of communication between public safety hierarchy

  (inter-jurisdictional, regional, state, Federal, tribal, etc.)
- Challenges
  - Unknown



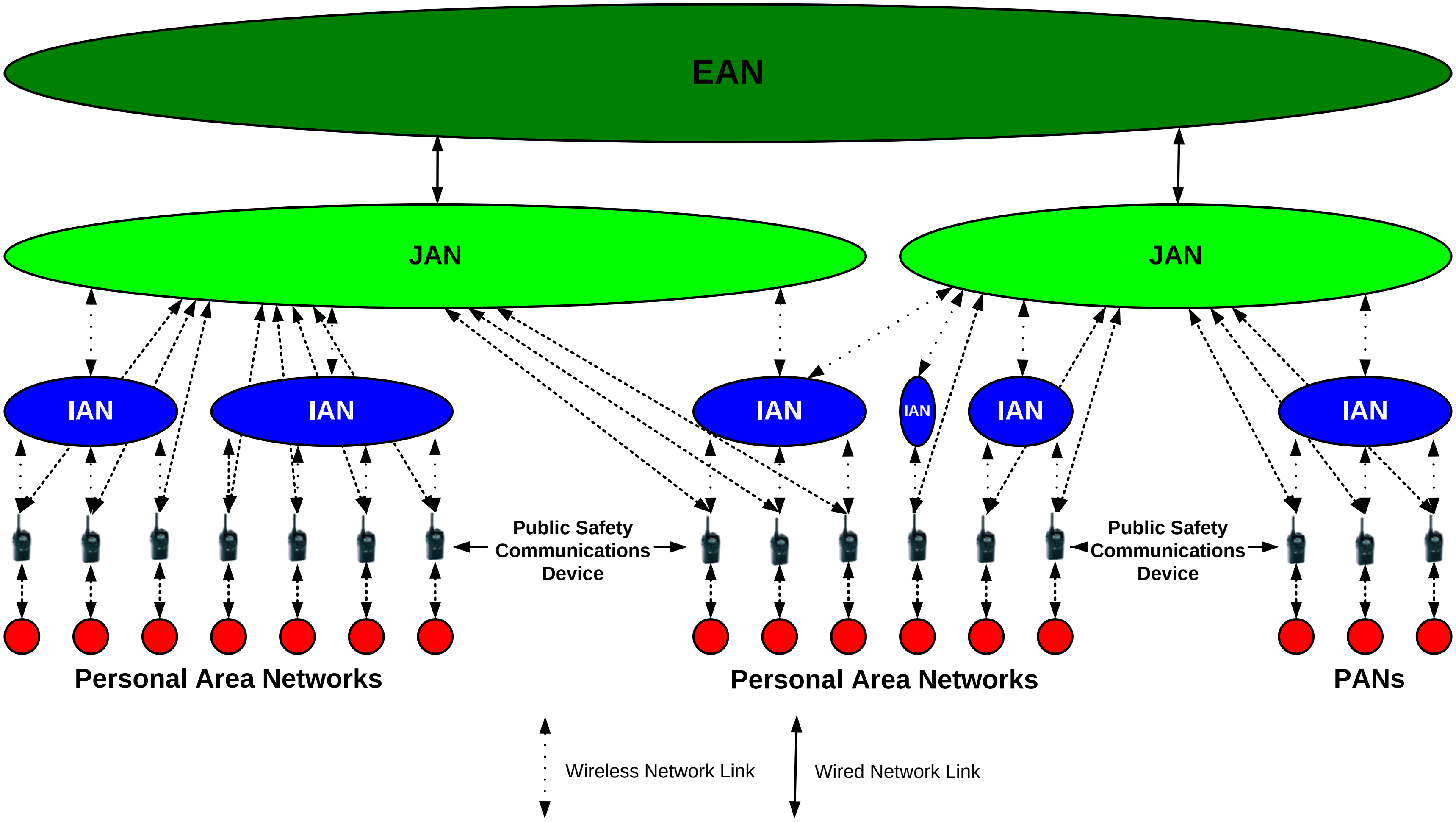
March 8, 2005

The Big Picture



March 8, 2005

Conceptual Network Diagram



Public Safety Architecture Framework (PSAF)

What is an Architecture?

Definition of Architecture:

An architecture is "the structure of components, their relationships, and the principles and guidelines governing their design and evolution over time."

- Derived from IEEE Std 610.12, 1990

What is an Architecture Framework?

Definition of Architecture Framework:

***Architecture Framework** defines what capabilities the architect/designer must deliver and how those capabilities must be constructed.*

i.e. – analogous to blueprint standards or building codes

What is an Architecture Framework?

The Framework is ...

- A discipline for examining processes and system alternatives in context with operations and the information required
- Common, pragmatic guidelines for describing architectures to enable comparisons and dovetailing
- Tailor-able and modifiable to suit requirements

The Framework is not...

- A single architecture
- A tool prescription
- A defined process

The WHAT and HOW

- The Architecture Framework will comprehensively describe **WHAT** the overall structured approach is to achieve a system-of-systems for nationwide interoperability

- Interface Standards define **HOW** the elements of the Architecture Framework will work together. That is, **HOW** interoperability through a system-of-systems approach will be achieved.

How Can a Framework Help An Architecture Effort?

Describe information needs and sources in context with the missions supported

- What?
- Where?
- Who responsible?
- How used?

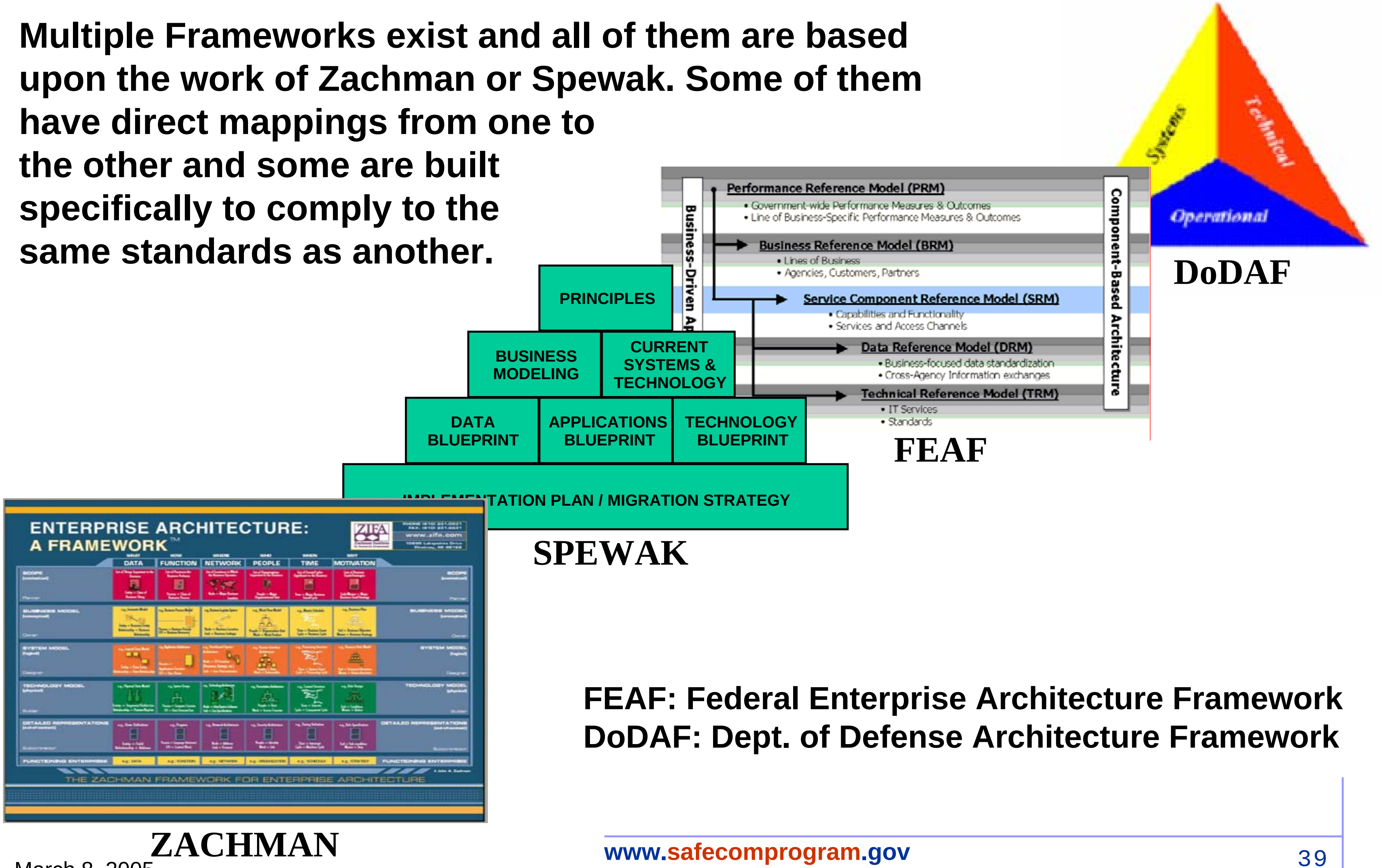
Identify and examine current and postulated business processes, systems, and technology with respect to satisfaction of stated requirements (SoR)

Refine investment strategies

- GAP analysis
- Direct Research & Development
- Direct Standards efforts
- Leverage across multiple agencies

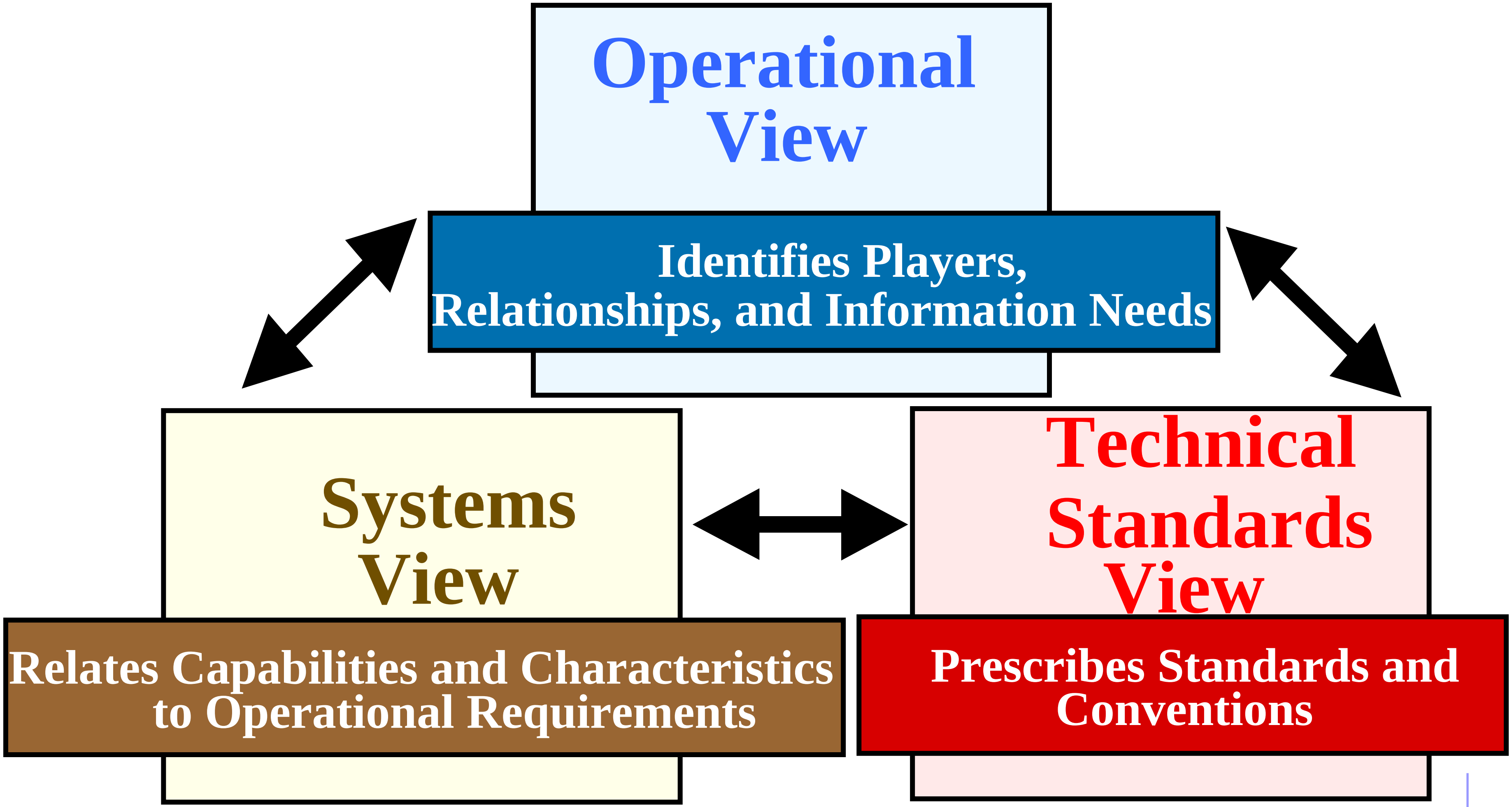
What Frameworks are there and how do they inter-relate?

Multiple Frameworks exist and all of them are based upon the work of Zachman or Spewak. Some of them have direct mappings from one to the other and some are built specifically to comply to the same standards as another.


Systems
Technical
Operational
DoDAF
Business-Driven Ap
Performance Reference Model (PRM)
• Government-wide Performance Measures & Outcomes
• Line of Business-Specific Performance Measures & Outcomes
Business Reference Model (BRM)
• Lines of Business
• Agencies, Customers, Partners
Service Component Reference Model (SRM)
• Capabilities and Functionality
• Services and Access Channels
Data Reference Model (DRM)
• Business-focused data standardization
• Cross-Agency Information exchanges
Technical Reference Model (TRM)
• IT Services
• Standards
Component-Based Architecture
FEAF
PRINCIPLES
BUSINESS MODELING
CURRENT SYSTEMS & TECHNOLOGY
DATA BLUEPRINT
APPLICATIONS BLUEPRINT
TECHNOLOGY BLUEPRINT
IMPLEMENTATION PLAN / MIGRATION STRATEGY
SPEWAK
ENTERPRISE ARCHITECTURE: A FRAMEWORK™
ZIFA
www.zifa.com
DATA
FUNCTION
NETWORK
PEOPLE
TIME
MOTIVATION
SCOPE
BUSINESS MODEL
SYSTEM MODEL
TECHNOLOGY MODEL
DETAILED REPRESENTATIONS
FUNCTIONING ENTERPRISE
THE ZACHMAN FRAMEWORK FOR ENTERPRISE ARCHITECTURE
ZACHMAN

FEAF: Federal Enterprise Architecture Framework
DoDAF: Dept. of Defense Architecture Framework

PSAF's Three Primary Views



Operational View

Identifies Players, Relationships, and Information Needs

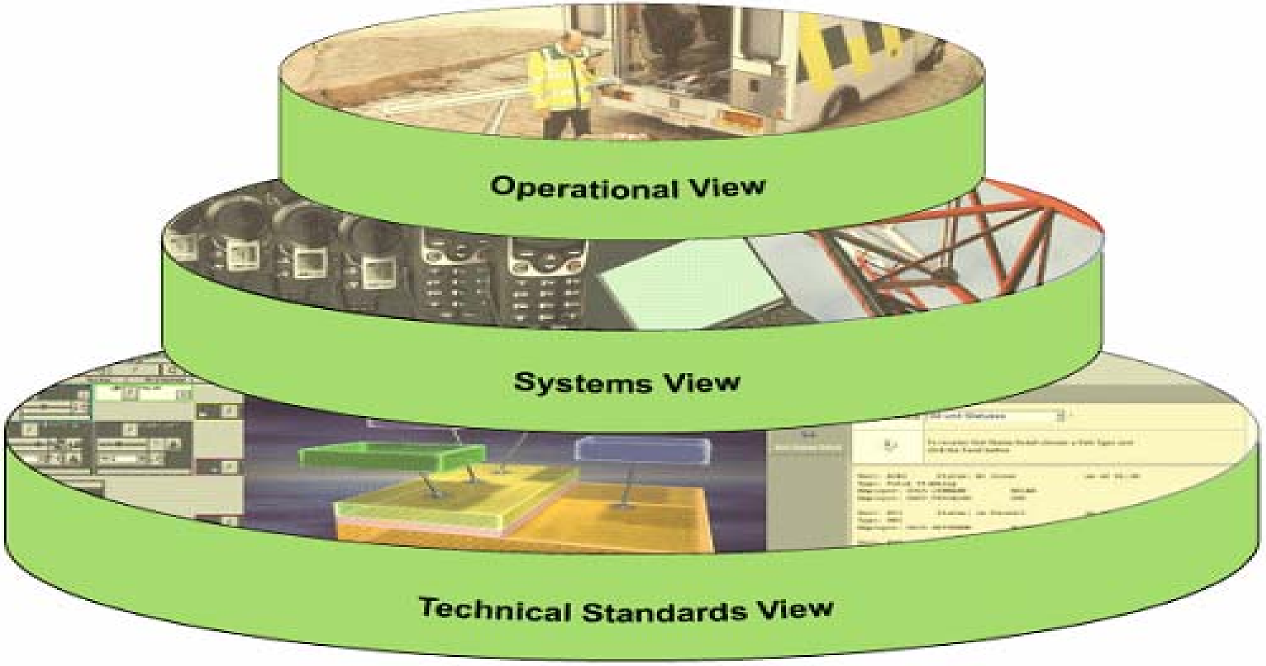
Systems View

Relates Capabilities and Characteristics to Operational Requirements

Technical Standards View

Prescribes Standards and Conventions

PSAF’s Three Primary Views



Each View Contains Specific Products

All Views

- Integrated Dictionary
- Overview and Summary Info

Operational View Products

- High-level Operational Concept Description
- Operational Node Connectivity Description
- Operational Information Exchange Matrix
- Organizational Relationships Chart
- Activity Model
- Operational Rules Model
- Operational State Transition Description
- Operational Event/Trace Description
- Logical Data Model

Systems View Products

- System Interface Description
- Systems Communications Description
- Systems Matrix
- Systems Functionality Description
- Operational Activity to System Function Traceability Matrix
- System Data Exchange Matrix
- System Performance Parameters Matrix
- System Evolution Description
- System Technology Forecast
- Systems Rules Model
- Systems State Transition Description
- Systems Event/Trace Description
- Physical Schema

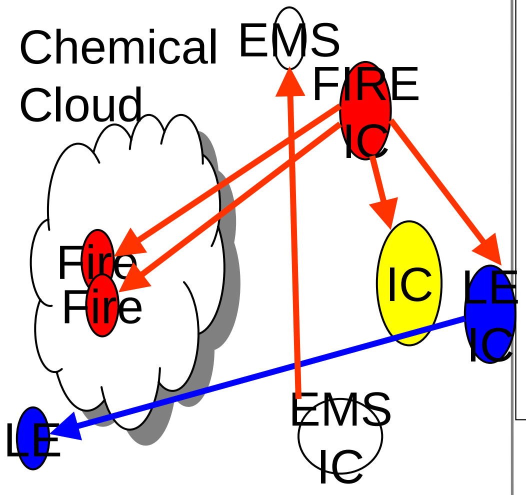
Technical Standards View Products

- Technical Standards Profile
- Standards Technology Forecast

“Operational View” Products

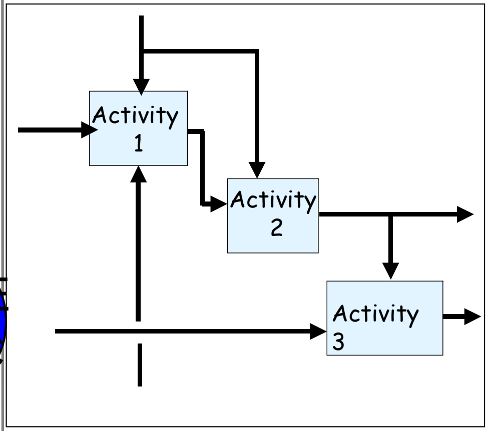
Captures Critical Mission Relationships and Information Exchanges

High-Level Operational Concept Description



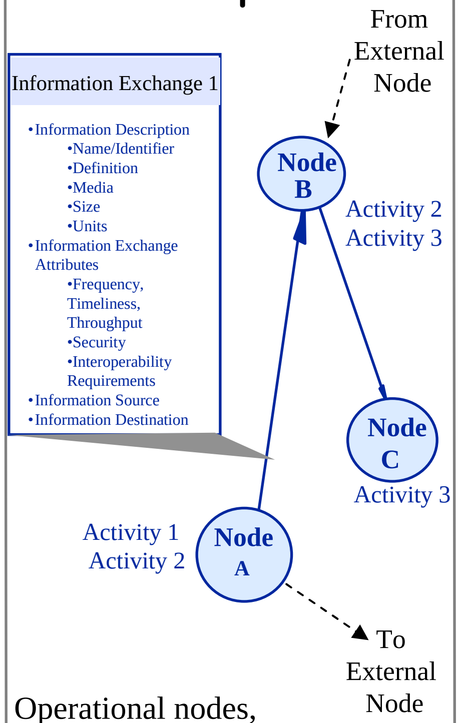
High-level graphical description of the operational concept of interest

Activity Model



Operational activities performed and their input/output relationships

Operational Node Connectivity Description



Information Exchange 1

- Information Description
  - Name/Identifier
  - Definition
  - Media
  - Size
  - Units
- Information Exchange Attributes
  - Frequency, Timeliness, Throughput
  - Security
  - Interoperability Requirements
- Information Source
- Information Destination

Operational nodes, activities performed at each node, node-to-node relationships, and information needlines

Operational Information Exchange Matrix

INFORMATION DESCRIPTION				INFORMATION SOURCE			INFORMATION DESTINATION		INFORMATION EXCHANGE ATTRIBUTES		
OPERATIONAL INFORMATION ELEMENT	DESCRIPTION	MEDIA	SIZE	UNITS	OPERATIONAL ELEMENT & ACTIVITY		OPERATIONAL ELEMENT & ACTIVITY		FREQUENCY, TIMELINESS, THROUGHPUT	SECURITY	INTEROPER-ABILITY REQUIREMENTS
NAME/IDENTIFIER	DEFINITION	DIGITAL, VOICE, TEXT, IMAGE, ETC.	RANGE LIMITS	FEET, LITERS, INCHES, ETC.	IDENTIFIER OF PRODUCING OE	PRODUCING ACTIVITY	IDENTIFIER OF CONSUMING OE	CONSUMING ACTIVITY			

Information exchanged between nodes and the relevant attributes of the exchanges

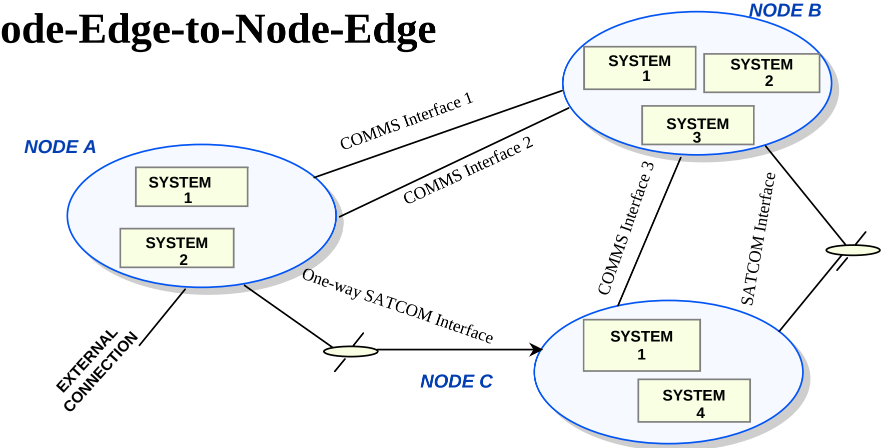
“Systems View” Products

Examines Current and Postulated Capabilities in Context with Operations

Core Product: System Interface Description

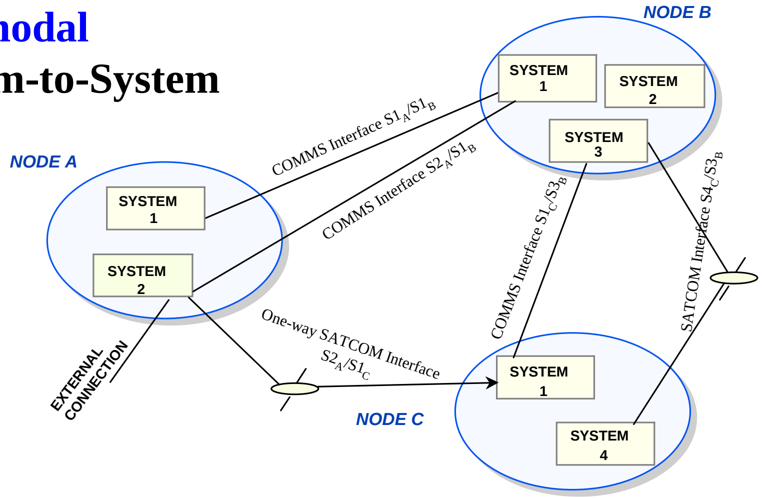
Internodal

Node-Edge-to-Node-Edge

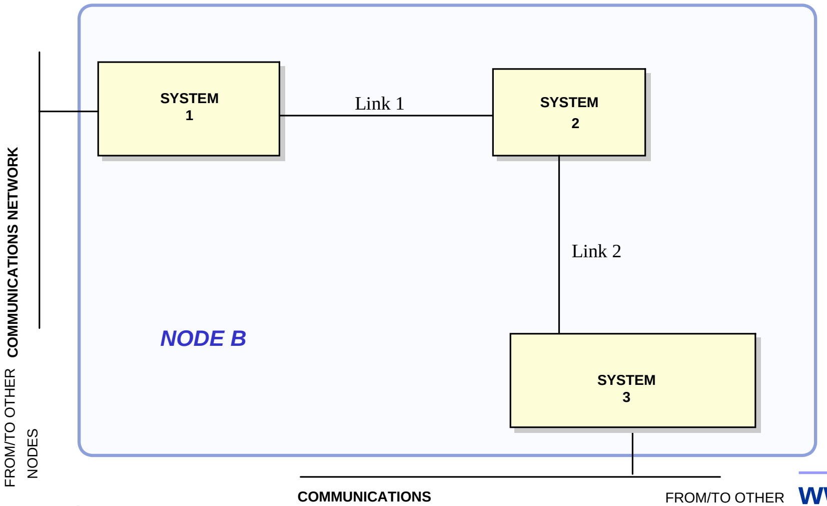


Internodal

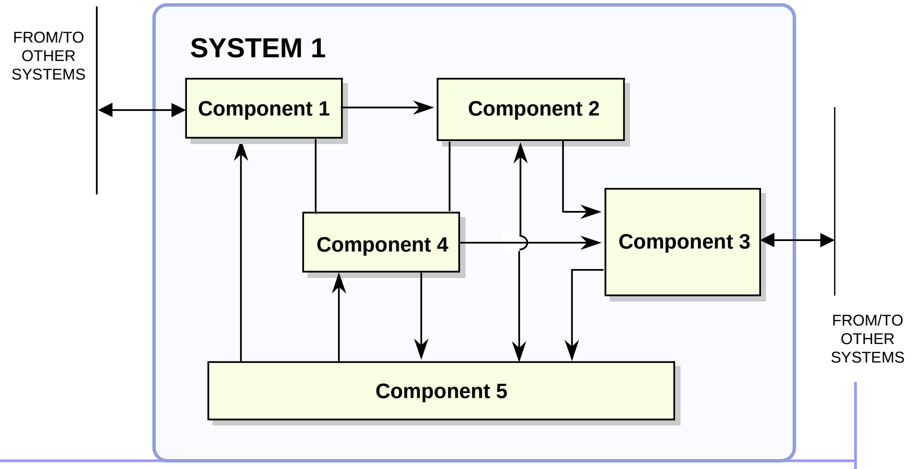
System-to-System


NODE B
SYSTEM 1
SYSTEM 2
SYSTEM 3
NODE A
SYSTEM 1
SYSTEM 2
COMMS Interface $S1_A/S1_B$
COMMS Interface $S2_A/S1_B$
COMMS Interface $S1_C/S3_B$
SATCOM Interface $S4_C/S3_B$
One-way SATCOM Interface $S2_A/S1_C$
EXTERNAL CONNECTION
NODE C
SYSTEM 1
SYSTEM 4

Intranodal

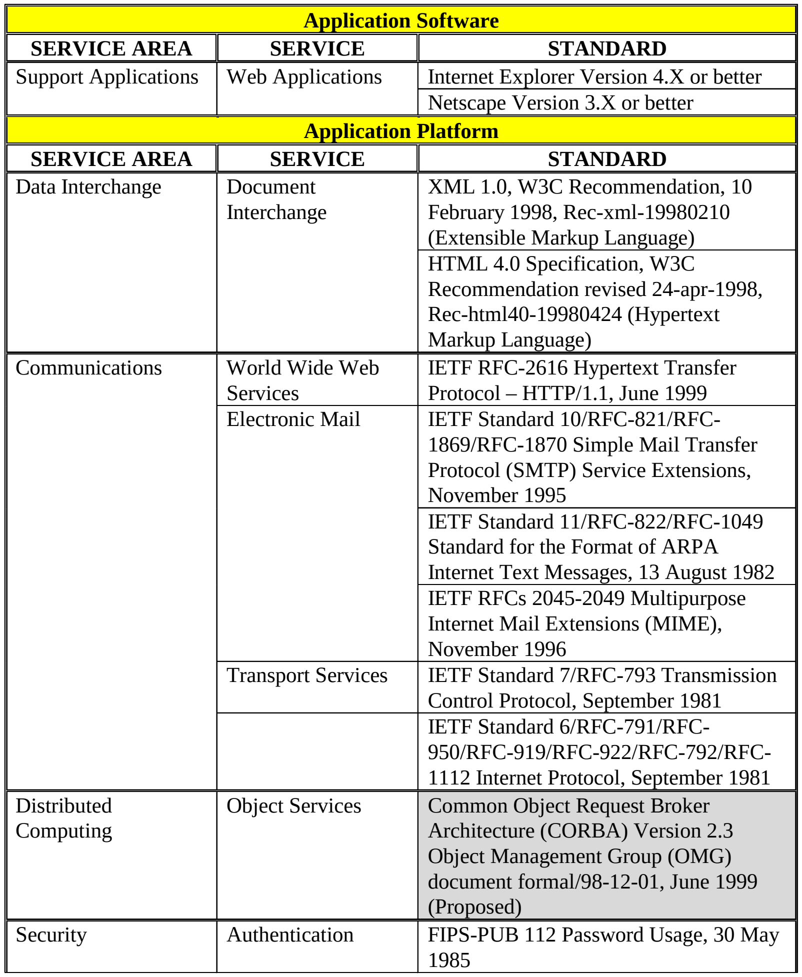


Intrasystem

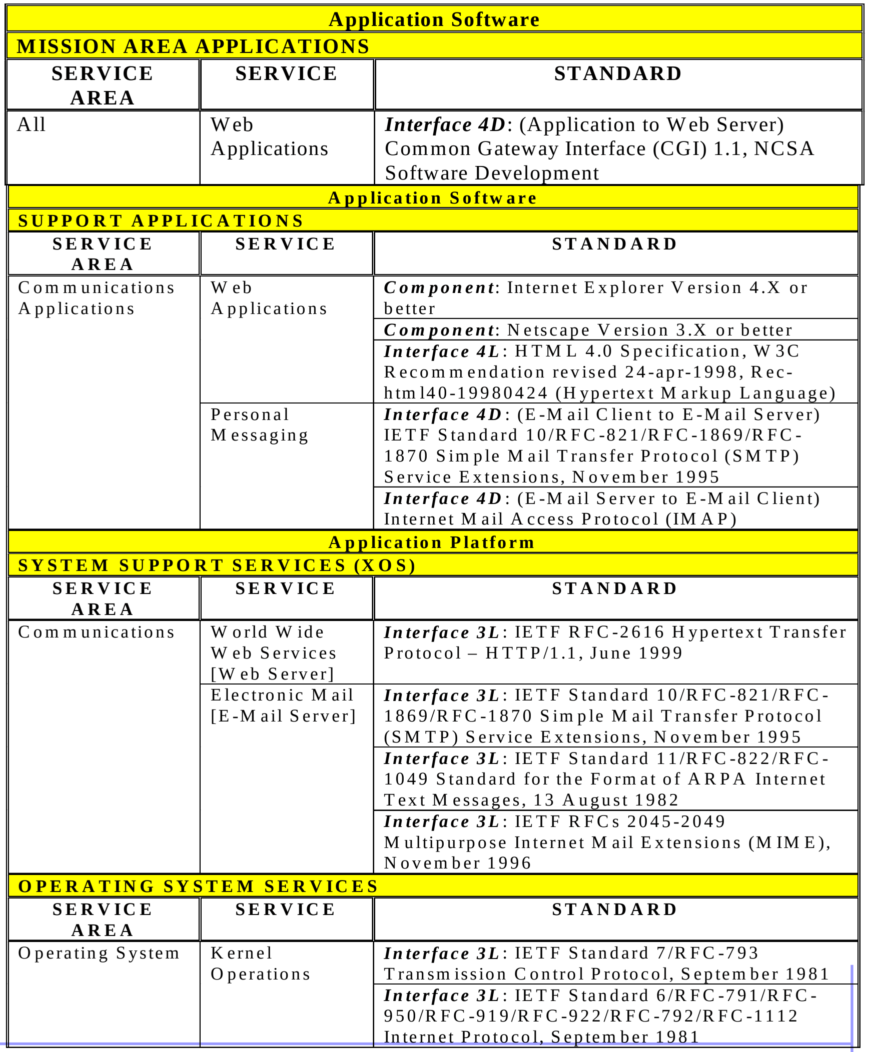


“Technical Standards View” Products

Identifies the Standards That Govern the Given Architecture



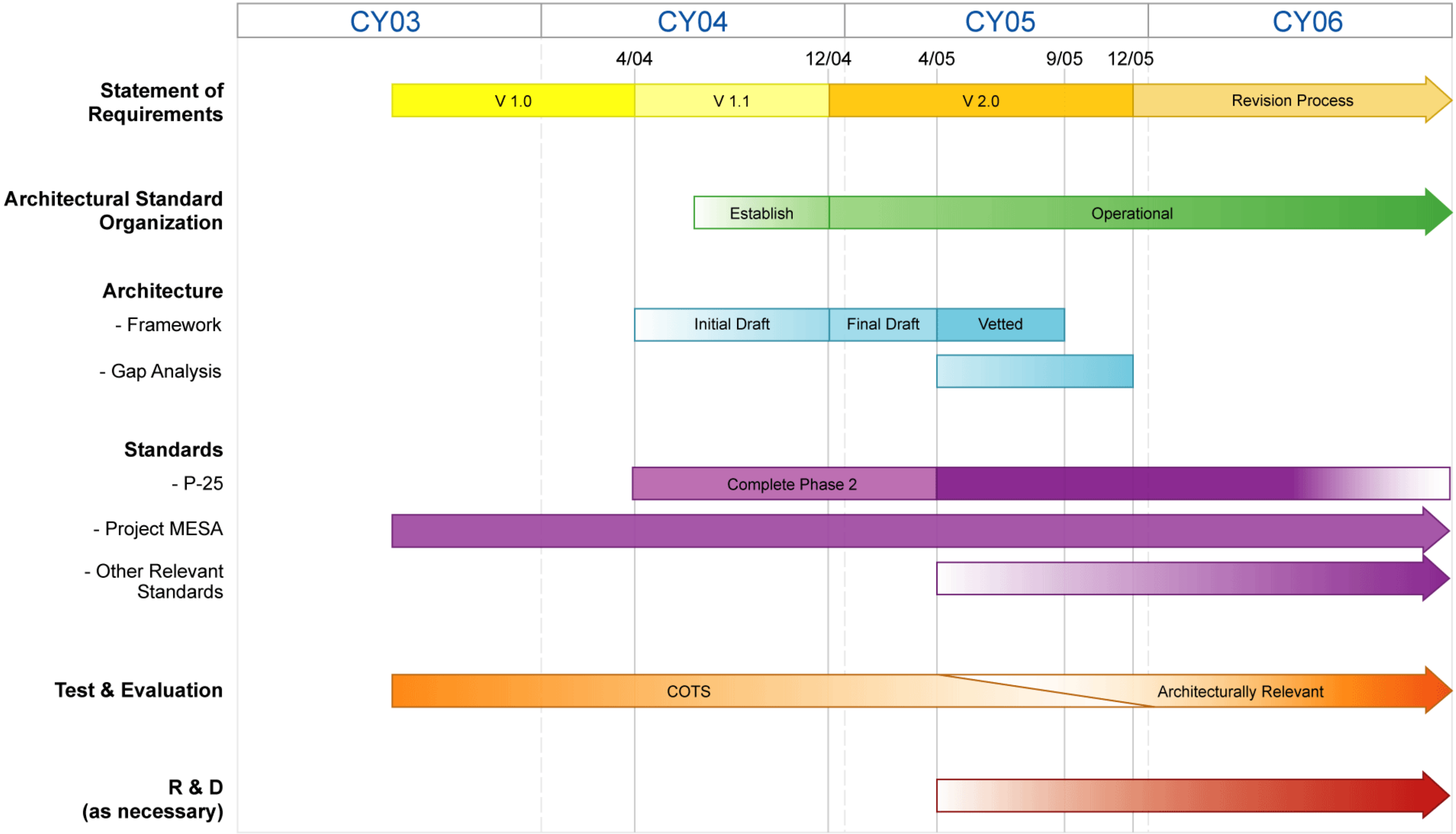
Application Software		
SERVICE AREA	**SERVICE**	**STANDARD**
Support Applications	Web Applications	Internet Explorer Version 4.X or better
		Netscape Version 3.X or better
Application Platform		
SERVICE AREA	**SERVICE**	**STANDARD**
Data Interchange	Document Interchange	XML 1.0, W3C Recommendation, 10 February 1998, Rec-xml-19980210 (Extensible Markup Language)
		HTML 4.0 Specification, W3C Recommendation revised 24-apr-1998, Rec-html40-19980424 (Hypertext Markup Language)
Communications	World Wide Web Services	IETF RFC-2616 Hypertext Transfer Protocol – HTTP/1.1, June 1999
	Electronic Mail	IETF Standard 10/RFC-821/RFC-1869/RFC-1870 Simple Mail Transfer Protocol (SMTP) Service Extensions, November 1995
		IETF Standard 11/RFC-822/RFC-1049 Standard for the Format of ARPA Internet Text Messages, 13 August 1982
		IETF RFCs 2045-2049 Multipurpose Internet Mail Extensions (MIME), November 1996
	Transport Services	IETF Standard 7/RFC-793 Transmission Control Protocol, September 1981
		IETF Standard 6/RFC-791/RFC-950/RFC-919/RFC-922/RFC-792/RFC-1112 Internet Protocol, September 1981
Distributed Computing	Object Services	Common Object Request Broker Architecture (CORBA) Version 2.3 Object Management Group (OMG) document formal/98-12-01, June 1999 (Proposed)
Security	Authentication	FIPS-PUB 112 Password Usage, 30 May 1985



Application Software		
MISSION AREA APPLICATIONS		
SERVICE AREA	**SERVICE**	**STANDARD**
All	Web Applications	***Interface 4D***: (Application to Web Server) Common Gateway Interface (CGI) 1.1, NCSA Software Development
Application Software		
SUPPORT APPLICATIONS		
SERVICE AREA	**SERVICE**	**STANDARD**
Communications Applications	Web Applications	***Component***: Internet Explorer Version 4.X or better
		Component: Netscape Version 3.X or better
		Interface 4L: HTML 4.0 Specification, W3C Recommendation revised 24-apr-1998, Rec-html40-19980424 (Hypertext Markup Language)
	Personal Messaging	***Interface 4D***: (E-Mail Client to E-Mail Server) IETF Standard 10/RFC-821/RFC-1869/RFC-1870 Simple Mail Transfer Protocol (SMTP) Service Extensions, November 1995
		Interface 4D: (E-Mail Server to E-Mail Client) Internet Mail Access Protocol (IMAP)
Application Platform		
SYSTEM SUPPORT SERVICES (XOS)		
SERVICE AREA	**SERVICE**	**STANDARD**
Communications	World Wide Web Services [Web Server]	***Interface 3L***: IETF RFC-2616 Hypertext Transfer Protocol – HTTP/1.1, June 1999
	Electronic Mail [E-Mail Server]	***Interface 3L***: IETF Standard 10/RFC-821/RFC-1869/RFC-1870 Simple Mail Transfer Protocol (SMTP) Service Extensions, November 1995
		Interface 3L: IETF Standard 11/RFC-822/RFC-1049 Standard for the Format of ARPA Internet Text Messages, 13 August 1982
		Interface 3L: IETF RFCs 2045-2049 Multipurpose Internet Mail Extensions (MIME), November 1996
OPERATING SYSTEM SERVICES		
SERVICE AREA	**SERVICE**	**STANDARD**
Operating System	Kernel Operations	***Interface 3L***: IETF Standard 7/RFC-793 Transmission Control Protocol, September 1981
		Interface 3L: IETF Standard 6/RFC-791/RFC-950/RFC-919/RFC-922/RFC-792/RFC-1112 Internet Protocol, September 1981

SAFECOM Wrap-Up

Architectural Standards Timeline



Anticipated Products and Activities

- Revise the SoR
- Develop an Architecture Framework
- Gap Analysis
- Support, adopt, and develop Interface Standards *(in conjunction with SDOs)*
- Test & Evaluation recommendations
- RDT&E recommendations
- Grant Guidance recommendations

The 120-Day Congressional Standards Report

- The House Report (H. Rep. 108-796) Intelligence Reform Bill requires the Department of Homeland Security (DHS) within 120 days to report on plans for accelerating the development of national voluntary consensus standards for public safety interoperable communications, a schedule of milestones for such development, and achievements of such development.
- SAFECOM will ensure that this plan
  - Is practitioner-driven,
  - Applies a comprehensive framework to communications interoperability,
  - Utilizes a structured lifecycle approach to standards development,
  - Employs common grant guidance to assist communities in planning and implementing their interoperability solutions,
  - Integrates new and legacy systems using a system-of-systems,
  - And establishes industry and government partnerships.
- This Report will be released in April 2005 timeframe.

Spectrum Needs Assessment and Plan

- The President directed DHS in Presidential Memorandum, “Improving Spectrum Management for the 21st Century”, dated November 30th 2004, to identify public safety spectrum needs within 6 months.

- DHS was also tasked to incorporate these needs in a comprehensive spectrum needs plan, within 1 year.

- The Assessment will be vetted through the SAFECOM EC and other public safety practitioners

Questions?

www.safecomprogram.gov

info@safecomprogram.gov

1-866-969-SAFE