Chapter 3
JTAV Architectures

INTRODUCTION

The JTAV system architecture is the foundation on which the JTAV capability depends. Successful migration to the JTAV "to be" architecture is a critical component of this strategic plan. The functionally oriented architectural basis for the initial JTAV implementation was superseded by the operationally oriented architectural framework issued as the *Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Integrated Support Activity's Architectural Framework*.[1] However, the JTAV functional architecture provided a basis for developing the JTAV operational architecture.

In 1997 the JTAV Office developed the JTAV operational and system architectures to support the joint warfighting process. (The life-cycle support and force preparedness architectures will be developed later.) The C4ISR document provides the following definitions for operational and system architectures:

- *Operational architecture.* Descriptions of the tasks, operational elements, and information flows to accomplish or support a warfighting function.

- *System architecture*. Descriptions, including graphics, of systems and interconnections that support warfighting functions.

The definitions clarify the distinctions between the two types of architectures. An operational architecture develops functional requirements, and a system architecture describes the physical capabilities that meet operational needs. A subtle but important point should be made concerning the JTAV operational architecture. As discussed in Appendix C, JTAV is a capability that facilitates improved performance for many functional or business processes, but owns no processes. Consequently, it is not feasible for the JTAV Office to develop a "to be" operational process; this task would be the responsibility of the organization or function responsible for the process. However, mapping JTAV capabilities to processes that the JTAV capability supports is a logical responsibility of the JTAV Office. A system architecture can be developed to support the processes.

[1] *C4ISR Integrated Support Activity Architectural Framework*, Version 1.0, 7 June 1996.

The JTAV architectures are documented in *Volume I, JTAV Operational Architecture,* and *Volume II, JTAV System Architecture*.[2] Both volumes will be modified to incorporate additional core processes and emerging technologies.

OPERATIONAL ARCHITECTURE

The JTAV Office developed an operational architecture to determine joint warfighting asset visibility requirements and capabilities, verify functional requirements, and identify automated systems that provide asset visibility. This architecture is compatible with the GCSS operational architecture and includes operational tasks identified by the Universal Joint Task List (UJTL).

The operational architecture consists of a narrative, process flow maps, information exchange requirements (IERs) matrices, and lists of source and receiver nodes. The process maps document the tasks that require asset visibility information to support joint warfighting. The maps also identify the high-level organizations involved in the joint warfighting process and describe the relationships among those organizations as well as a general information flow. The high-level joint warfighting tasks were derived from joint doctrine and the UJTL. These tasks were examined to identify subtasks and information flows supporting each phase. Each subactivity was directly linked to a JTAV requirement.

In developing the operational architecture, a standard process (Figure Chapter 3 - 1) was used to analyze all phases of the warfighting process.[3] Taking deployment as an example, step 1 consisted of identifying the core tasks that make up deployment. In step 2 each core task was then divided into its component activities. The activities were further decomposed in step 3 into subactivities. At this level it is possible to begin determining the JTAV information requirements necessary to accomplish each subactivity. These JTAV information requirements were documented in an IER matrix for each subactivity in step 4.

The operational architecture products were used to develop the JTAV system architecture. The IER matrix is the most critical product of the operational architecture because it expresses the relationships among the tasks, operational elements, and information flow. The IER format of the C4ISR document was tailored to link the information exchange requirements directly to the JTAV definition.[4] This approach allowed IERs to be grouped in a logical array to include all requirements and eliminate duplication.

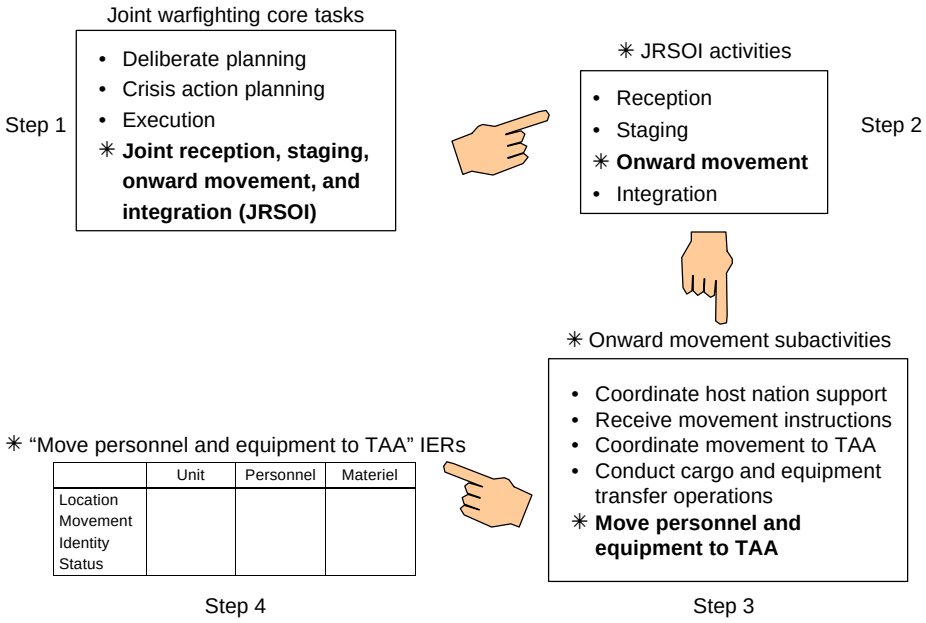
---

[2] *Volume I, JTAV Operational Architecture*, June 1997, and *Volume II, JTAV System Architecture*, August 1997.

[3] The operational architecture does not include the core processes of life-cycle management and force preparedness.

[4] Chapter 1 provides the JTAV definition.

Figure Chapter 3 -1. Deployment Operational Architecture Process



Note: TAA = theater assembly area.

JTAV data-access priorities are determined by this process. The data elements are used to develop the data-sharing request that the JTAV Office provides to the organization responsible for the data. Priorities for data access are determined based on the need identified in the operational architecture and IERs.

SYSTEM ARCHITECTURE

A system architecture is a description, including graphics, of systems and interconnections that support functions. In addition to a general description, it consists of system overlay diagrams and node descriptions. The initial JTAV system configuration is known as the "as is" system and depends on a database of JTAV information. The "to be" system architecture is based on providing access to data "in place" at the source as much as possible. The beta test of the architecture started in December 1998. The first operational release is scheduled for 1 April 1999.

JTAV "As Is" Architecture

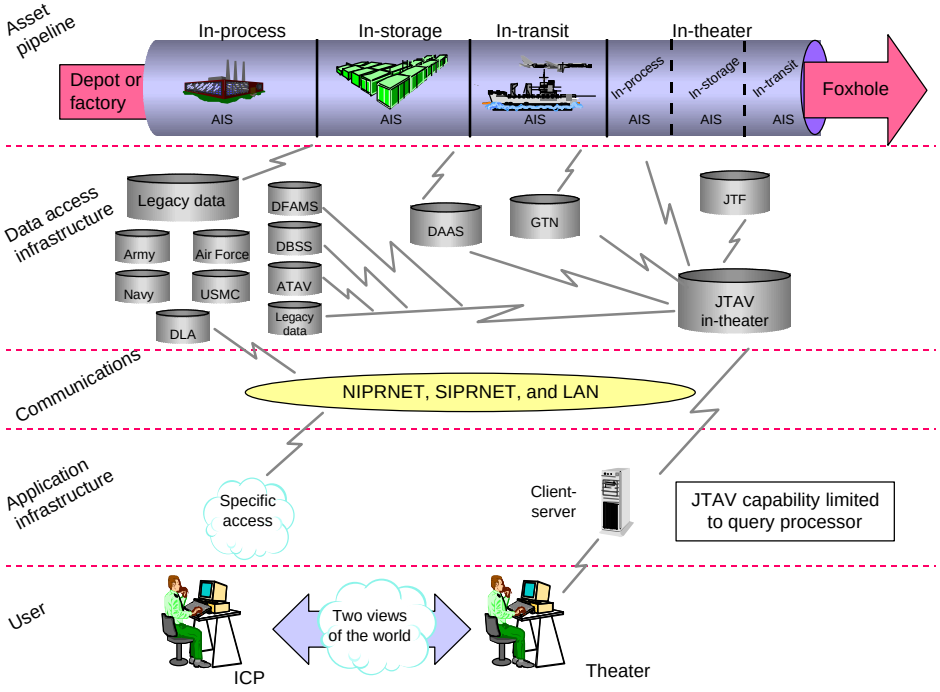
The JTAV "as is" architecture has the following significant architectural characteristics:

- Application software resides on a workstation, making configuration management and support difficult while allowing only one type of workstation to be used (single user and single box).

- The architecture does not take full advantage of Web technology.
- Information is fused when a database is loaded. As a result, ad hoc queries cannot be adequately accommodated.[5]

Figure Chapter 3 -2 depicts the JTAV "as is" system architecture. It consists of two differing world views by users. One is the theater, or operational, view—the view by a CINC or JTF—and the other is from an inventory control point (ICP), or sustainment base, perspective. JTAV supports both views by providing one account to access information previously contained in numerous data systems. Theater users access asset visibility information from the JTAV database.

Figure Chapter 3 -2. JTAV "As Is" System Architecture



Note: ATAV = Army total asset visibility; DAAS = Defense Automatic Addressing System; DBSS = Defense Blood Standard System; DFAMS = Defense Fuels Automated Management System; LAN = local area network; NIPRNET = Nonsecure Internet Protocol Router Network; SIPRNET = Secure Internet Protocol Router Network; USMC = U.S. Marine Corps.

[5] Information is fused when it is brought together from separate sources and presented in a single picture.

JTAV "To Be" Architecture

The JTAV "to be" architecture has the following significant architectural characteristics:

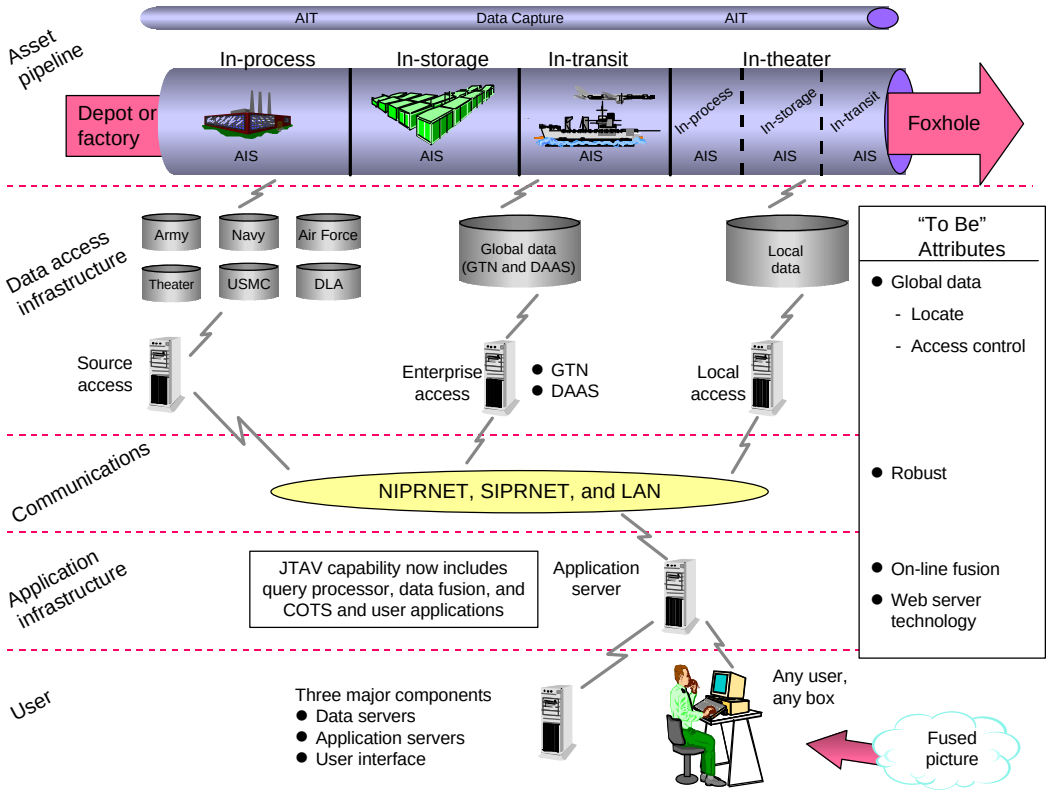
- Access to the JTAV capability is provided by a Web browser that allows a user to communicate with the JTAV application.
- Queries and responses are processed through a mediator that is configured with a dictionary that identifies the data available in the JTAV data environment and a directory that defines the location of the available data sources and their associated data elements.
- The mediator, using data translation information provided in the directory, fuses the responses into a single response for the user and passes it to the JTAV application.
- The JTAV application prepares the appropriate screen and passes the response through the Web server to the user's Web browser that displays the response.

Implementing the JTAV "to be" system architecture requires the following five conditions or qualifications:

- *Accurate operational architecture products.* Operational architecture products, particularly the IER matrices, need to be timely and accurate.
- *Fulfillment of development assumptions* Several assumptions were made to develop the JTAV "to be" system architecture. Two major assumptions are that communications capacity and response times are not constrained and that technology supporting access control and other security functions will be available.
- *Compatibility with GCSS design.* The architecture should be designed to allow JTAV extension to GCSS, support data access from commercial off-the-shelf (COTS) and user applications, comply with the Defense Information Infrastructure (DII) and Common Operating Environment (COE) framework, and serve as a baseline for COP support.
- *Migration of JTAV system architecture.* The architecture should support a migration path from the existing JTAV system architecture.
- *Responsibility for data quality.* The data provider is responsible for ensuring that data are accurate and timely.

Figure Chapter 3 -3 depicts the JTAV "to be" system architecture. It does not depend on building new databases, but relies on accessing data in place at the source as much as possible.

Figure Chapter 3 -3. JTAV "To Be" System Architecture



GENERAL OPERATING CONCEPT

The operational and system architectures are designed to support the joint warfighting process. Consequently, any general operating concept derived from those architectures maintains that perspective. The basic JTAV operating concept is simple. The JTAV capability needs to gain access to the data, fuse the data, and present the fused data to a user in a timely manner and useful format.

Data Access

The JTAV capability accesses data through data servers, the primary mechanisms that collect data and provide information. JTAV uses data resident in several databases and logistics information systems developed primarily to support functional processes. Each server accesses and aggregates data according to user needs.

The JTAV operating concept depends on three types of servers: local, global, and enterprise.

- Local servers provide access to *local* data.[6] For an overseas user, the local server allows access to theater data (e.g., data concerning assets under control of a CINC, JTF, or service component commander). Likewise, for a CONUS user, a local server allows access to CONUS data.

- Global servers provide access to data outside the theater or geographical area of a user. For example, an overseas user can use a global server to access wholesale assets. Likewise, a CONUS user can use a global server to access stocks in an overseas theater.

- Enterprise servers do not depend on a user's location and contain national-level joint information. GTN and LIPS are examples of enterprise servers. GTN collects, fuses, and integrates information concerning the Defense Transportation System.

Mediator

The mediator is the key for providing a reach-back capability directly to an authoritative data source. This concept replaces the current store-forward concept of JTAV-IT. The principal functions of the mediator are to

- respond to a data query request from an application or system,

- translate the queries into calls to the authoritative database,

- use a data dictionary and directory to determine the authoritative source, and

- fuse the database responses and return the fused response to the requestor.

The mediator should fit within the strategic vision; in other words, it should provide solutions that add value. An example is the time-critical nature of some data; (e.g., air mission data in GTN). In this case, data more than a few minutes old may be out-of-date and have no further value. A mediated solution provides near real-time updated data to ensure the most accurate and timely data possible.

Data Fusion

The JTAV capability retrieves data elements from many sources and consolidates the elements in the mediator. JTAV's capability to consolidate, or fuse, data is dependent on two primary functions—communications and data population. Un-

[6] Local data resides in a geographical area or theater.

classified communications is accomplished using the NIPRNET and classified communications is accomplished using the SIPRNET.

In the JTAV "as is" architecture, data are obtained through a data *pull* or *push* process that, in most instances, uses a file transfer protocol. In the JTAV "to be" architecture, data will be obtained using the following five-step process:

- The data dictionary defines all potential data in the environment.
- The directory identifies where the data reside and explains how to translate the data into the view defined by the dictionary.
- The dictionary and directory are installed in the mediator.
- The terminology in the dictionary is used to request data from the environment.
- The mediator uses the directory to submit requests to the data source and present the data to the user.

In addition to accessing data from numerous sources and making the data available on a single platform, the JTAV capability provides the consolidation of data into useful information. This consolidation is accomplished through the query process capability and reference tables in the server. Based on the data elements requested in the query, intelligent middleware accesses the correct database and retrieves, stores, and consolidates the data with other data to respond to a query. The reference tables are indispensable as they relate the data elements to specific queries and allow the fusion of data.

SECURITY

The JTAV Security Management Program encompasses all aspects of providing confidentiality, integrity, and availability for JTAV data accessed via JTAV applications. It supports the DoD information assurance efforts, particularly the DoD Information Technology Systems Certification and Accreditation Process in accordance with MIL-STD-5200.4D.

The objective of the JTAV Security Management Program is to provide security techniques and procedures to protect classified and unclassified information that is at least sensitive. The JTAV Security Management Program includes security for all current and future versions of JTAV, including JTAV-IT, "to be," ammunition, medical, and personnel applications. It includes technical and administrative interfaces with approval authorities, common security requirements, and security requirements of other joint AIS programs. The program encompasses all phases of development and operational deployment.

Most JTAV applications fall into the secret and below interoperability (SABI) category. The SABI process evaluates systems consisting of classified and unclassified data. The SABI process has separate approval requirements. The JTAV Office is following SABI procedures and has received fielding approval for USEUCOM, USPACOM, and USACOM.

The JTAV Office has conducted two formal risk assessments; both were on the "as is" configuration. The results of the tests provide a complete list of potential risks for the configuration. Architectural modifications have been introduced and risks have been mitigated. The first major change was the introduction of a guard to move data from unclassified to classified servers. The second change was the deletion of the graphical user interface (GUI) and the introduction of a Web-based interface using Netscape software. The development contractor will conduct a formal risk assessment for the JTAV "to be" architecture.

JTAV security procedures have been established in the following documents:

- JTAV risk management program
- JTAV concept of operations
- System administrators' manuals
- Users manuals.

SUMMARY

Operational and system architectures are the foundation for a concept of operations and should be reviewed periodically for currency and relevancy. The JTAV operational architecture provides common terms of reference, establishes common definitions, and documents asset visibility information requirements to support joint warfighting. The information requirements are documented in IER matrices that express the relationships among tasks, operational elements, and information flow.

The JTAV "to be" system architecture identifies and describes the infrastructure and components, as determined by the information exchange requirements, to support the joint warfighting process effectively. The keynote of the JTAV "to be" system architecture is access to data in place at the source and provide near real-time data access to users.