A Basis for Joint Interoperability

Lieutenant Colonel John A. Hamilton, Jr.
Office of the Chief Engineer, Code 05J
Space and Naval Warfare Systems Command
4301 Pacific Highway
San Diego, Calif. 92109
hamiltoj@spawar.navy.mil

Major Jeanne L. Murtagh
Software Professional Development Program
AFIT/LSS, 2950 P Street
Air Force Institute of Technology
Wright-Patterson AFB, OH 45433-7765
jeanne.murtagh@afit.af.mil

Colonel John C. Deal
Office of the Director for Command, Control, Communications and Computers
107 Army Pentagon
Washington, D.C. 20310-0107
dealjc@hqda.army.mil

Abstract

How can the Services benefit from a more detailed description of the basis for joint interoperability? Without interoperable systems, we cannot truly have "joint operations." Instead, we have a collection of forces from more than one service -- and possibly even from more than one country -- conducting independent operations in the same geographical area. We cannot work together in a cooperative, coordinated, mutually supportive effort to win on the battlefield if we cannot communicate, and communication is dependent on interoperable systems. The Joint Technical Architecture (JTA) was developed to provide DOD systems with the basis for the seamless interoperability necessary to ensure that we can truly conduct joint operations. This paper describes the three architectural components (views) of the JTA, and then proposes additional detail for one of these three components. Our goal is to help improve interoperability of joint forces by providing a more detailed description of the requirements which must be considered when new systems are being developed. This work is the result of engineering support conducted by the Joint Forces Program Office under the direction of the US Atlantic Command J6.[*]

[*] Brig. Gen. J. McElwee, USA, USACOM J6; Capt. R. Rushton, USN, USACOM J61; Lt.Col. T. Mansfield, USA; USACOM J612B, Lt. Cmdr. D. LeGoff, USN, SPAWAR; and Maj. Scot Ransbottom, USA, USMA made significant intellectual contributions to this work.

1. Introduction

Joint operations are essential to the success of our warfighters on today's battlefields. We must have truly joint operations; we cannot afford to merely have a collection of forces from different services operating independently in the same geographical area. We must be able to communicate in order to conduct operations which are truly joint operations, and this communication is dependent on interoperable systems. The Joint Technical Architecture (JTA) was developed to help meet this critical need.

This paper describes the three architectural components (views) of the JTA, and then proposes additional detail for one of these three components. Our goal is to help improve interoperability of joint forces by providing a more detailed description of the requirements that must be considered when new systems are being developed.

The JTA is an evolving document. It is helpful to briefly review its origins before we discuss the additional detail proposed in this paper.

In early fall of 1994, the Army Science Board released the results of its summer study of the Army's vision of the future.[1] The Army Science Board stated the need to develop a technical architecture based on commercial standards in order to achieve the level of interoperability envisioned by key Army planning documents, including Force XXI. This led to the development of the Army Technical Architecture. When the Assistant Secretary of Defense for Command, Control, Communications and Intelligence directed the implementation of a working set of standards applicable to all the services in 1995, the Army Technical Architecture was used as the basis for the Joint Technical Architecture.[2]

2. The Joint Technical Architecture: An Overview

The JTA is composed of three components (or views). These components and their interrelationships are summarized in Figure 1, and then discussed in more detail below.

[1] M. S. Frankel, et al., "Technical Information Architecture for Army Command, Control, Communications and Intelligence," Army Science oard Summer Study; January-July 1994, Final Report, April 95, pp i-ii.
[2] Joint Technical Architecture, Defense Information Systems Agency, Arlington, Va, 22 Aug 96, vers 1.0, p 1-2.

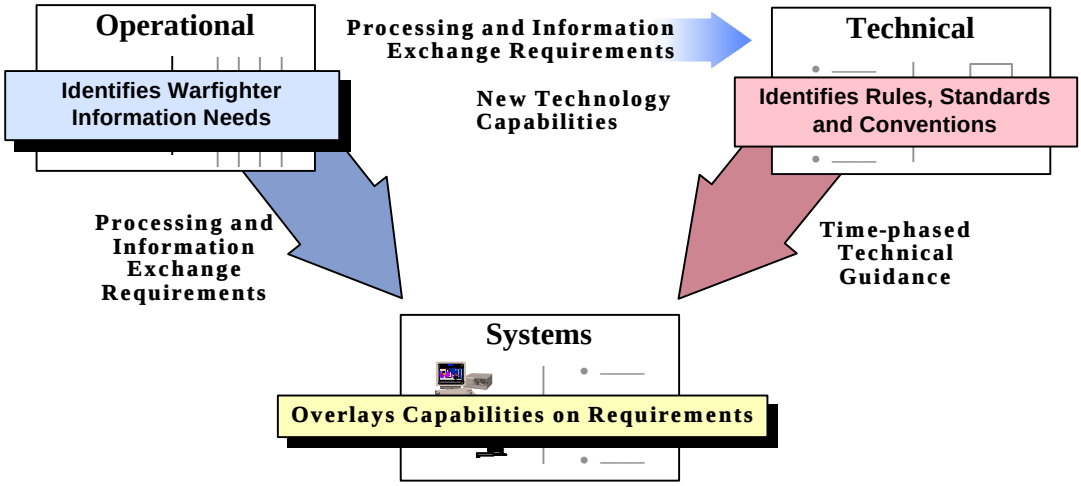


Figure 1. Interrelationships of the Operational, Systems, and Technical Views.[3]

Within the JTA, each of these components is called an "architecture view." It is important to understand the way the term "architecture" is used in this context. The JTA is not merely a "computer systems architecture;" instead, the use of the term "architecture" within the JTA is broader than that. It is consistent with the Institute for Electrical and Electronics Engineers (IEEE) definition:

> An architecture is composed of “the structures or components, their relationships, and the principles and guidelines governing their design and evolution over time.”

Let's examine each of the components of the JTA in more detail.

The Operational Architecture View is defined in JTA Version 3.0 Draft 1, dated 26 February 1999, as follows:

> "The operational architecture (OA) view is a description of the tasks and activities, operational elements, and information flows required to accomplish or support a military operation.
>
> It contains descriptions (often graphical) of the operational elements, assigned tasks and activities, and information flows required to support the warfighter. It defines the types of information exchanged, the frequency of exchange, which tasks and activities are supported by the information exchanges, and the nature of information exchanges in detail sufficient to ascertain specific interoperability requirements."

Simply stated, the operational view is a doctrinal template that illustrates which units communicate which data to which other units via which systems.

The Technical Architecture View is defined in JTA Version 3.0 Draft 1, dated 26 February 1999, as follows:

---

[3] Joint Technical Architecture - Army, version 5.0, Office of the Director, Information Systems for Command, Control, Communications, and Computers, 107 Army Pentagon, Washington, DC, 11 Sep 1997 pp 2-7.

> "The technical architecture (TA) view is the minimal set of rules governing the arrangement, interaction, and interdependence of the system parts or elements, whose purpose is to ensure that a conformant compliant system satisfies a specified set of requirements.
>
> The technical architecture view provides the technical systems-implementation guidelines upon which engineering specifications are based, common building blocks are established, and product lines are developed. The technical architecture view includes a collection of the technical standards, conventions, rules and criteria organized into profile(s) that govern system services, interfaces, and relationships for particular systems architecture views and that relate to particular operational views."

Simply stated, the technical architecture view could be regarded as a set of implementation guidance, and standards such as WIN32 API, TCP/IP and X-windows (X11R5). It is important to note the difference between this definition and what a computer systems engineer might envision as a "technical architecture."

The Systems Architecture View is defined in JTA Version 3.0 Draft 1, dated 26 February 1999, as follows:

> "The systems architecture (SA) view is a description of systems and interconnections providing for, or supporting, warfighting actions. For a domain, the systems architecture view shows how multiple systems link and interoperate, and may describe the internal construction and operations of particular systems within the architecture."

Simply stated, the systems architecture view answers the "how" question in response to the "why" from the operational architecture view. The systems architecture component of the JTA is close to -- but not identical to -- what a computer systems engineer (CSE) would consider as an "architecture."

3. Extension of the JTA's Systems Architecture View

3.1 Overview

We propose that the JTA's Systems Architecture View be extended to address these three categories of requirements:

a) Data Requirements
b) Hardware and Software Requirements (to a CSE, the "computer system architecture")
c) Communications Requirements.

It should be easier to develop system requirements to support joint interoperability when these three categories are specifically addressed. Without this level of detail, it is more difficult to develop system requirements that are rigorous and sound from an engineering viewpoint.

We will address each category in turn, starting with data requirements.

3.2 Data Requirements

Why should a discussion of system architecture to support interoperability start with data requirements? The answer to that is simple: data is at the heart of interoperability. Interoperability is accomplished by first identifying data needed by other users or systems, and then by arranging to share that data quickly enough that it is still useful upon receipt by those other users or systems.

What data is present in a battlefield scenario, and what information exchange must be accomplished in support of interoperability? This is represented graphically in Figure 2. Note that these information exchange requirements could be defined in terms of data (generally defined as a raw or minimally processed product) or information (generally considered to be the result of processing data). Dictating how these information exchange requirements are specified -- in terms of data or information -- is not the purpose of this diagram; therefore, the distinctions between the terms "data" and "information" are not significant in the context of this diagram, and those two terms are used interchangeably.

3.2.1 Information from the Four JV2010 Functional Areas

The categories of information depicted in Figure 2 are based on the four JV2010 Operational Concepts (Functional Areas).

Within a tactical battlespace, there will be information available for each of the four JV2010 functional areas:

a) Dominant Maneuver
b) Precision Engagement
c) Focused Logistics
d) Full Dimensional Protection

Within each functional area, this information is divided into two categories:

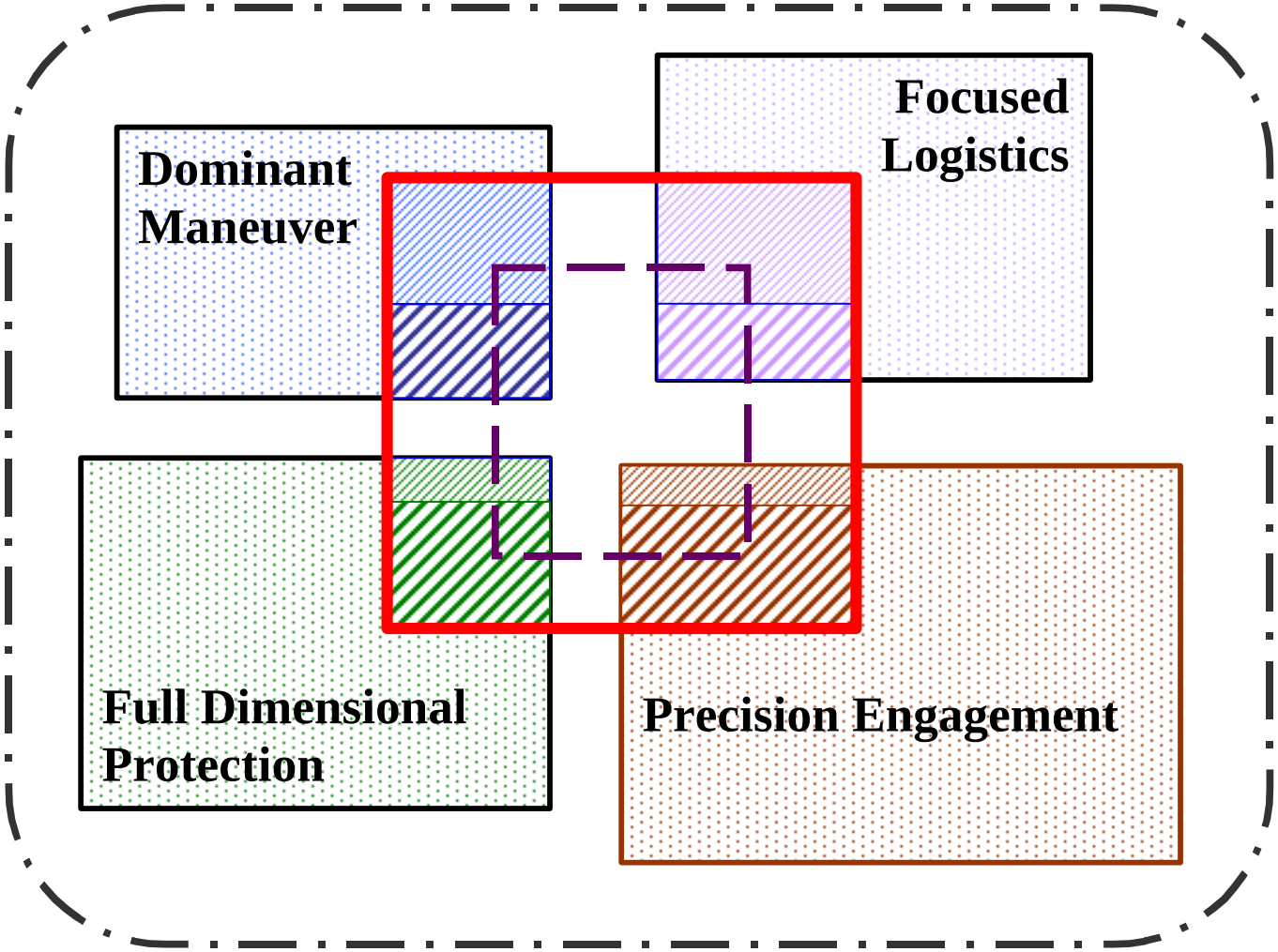
a) Planning Information
b) Survival Information

These two categories are defined in the Draft JV2010 Command, Control, Communications and Computers (C4) Capstone Requirements Document (CRD) being staffed in the US Atlantic Command.

> "Survival information requires immediate action such as to attack the enemy, avoid being attacked, and/or to prevent fratricide. It is, therefore, extremely time-sensitive."
>
> "Planning information is used as a basis for determining future action and is generally not as time-sensitive as survival information."

In Figure 2, the information from each of the four JV2010 functional areas is shown in rectangular boxes of different sizes. Several subsets of information are also identified; these

subsets will be discussed in more detail later in this narrative. Note that the diagram is not "drawn to scale." For example, it is not our intent to imply that Precision Engagement will require more information than the other areas; we are just trying to illustrate that different amounts of information may be required for each area. This same caveat applies to all data subsets represented on the diagram.



Key

Solid Thick Line: Joint Information Exchange Requirements (JIERs) necessary for interoperability. "MUST Share" Subset.

Thin Striped Section: "Planning" Information within each functional area
Thick Striped Section: "Survival" Information within each functional area

Large Dashed Line: Subset of information which can feasibly be shared between the new system and legacy system(s). "CAN Share" Subset.
Dash/Dot Line: Theoretical Boundary for information which might be shared

Figure 2. Joint Vision 2010 (JV2010) Data Interoperability Model.

3.2.2 Information Exchange Requirements for Interoperability

How much information must be shared in support of interoperability? Should we attempt to share *all* information, as shown by the set of data contained within the **dash-dot line** on the diagram? No. Full interoperability does not require that *every* piece of data available within a tactical battlespace be shared. This would be unnecessary and impractical:

1) Warfighters do not require access to all data within the battlespace in order to accomplish their missions.

2) We currently cannot build a "communications pipe" large enough to share all information with all warfighters, and we cannot count on removing this constraint through new technologies. While technology improvements are very likely to provide greater capacity in the future, our information exchange requirements may expand as well, consuming -- or even exceeding -- this new capacity.

3) We must avoid information overload. We do not want to "drown" other users with massive quantities of information that is not relevant for those other users.

If we are not going to share *all* the data available within a tactical battlespace, then we must carefully determine what data does, indeed, need to be shared in order to support interoperability. This "MUST share" data is represented by the subset contained within the **thick solid line** on the diagram. "Must share" *survival* information is depicted in the **thick striped sections** within the red "must share" box on the diagram; "must share" *planning* information is depicted in the **thin striped sections**. The distinction between survival and planning information is significant because of the different timing constraints (as discussed in the previous section) associated with each type of data. The remaining data for each of the four functional areas shown on the diagram does not need to be shared in support of interoperability. This remaining data, which includes both unshared planning and unshared survival information, is depicted in a light dot pattern. Note that some of the subsets depicted in the diagram might be empty sets. For example, your system might not process any Precision Engagement data, and it might not have to share any data from the Dominant Maneuver functional area.

In order to design interoperable systems, you must define the survival information and the planning information which will be processed by your system, and specify, for each piece of that information, whether it needs to be shared in support of interoperability.

3.2.3 Interoperability, Information Exchange and Legacy Systems

The *goal* for information exchange to support interoperability with legacy systems is the "MUST share" subset of information depicted within the **thick solid line**. After all, the warfighters information exchange *requirements* are a function of mission needs, not a function of the systems used to support these needs. However, information exchange *capabilities* are, indeed, a function of the systems being used. We must acknowledge that it might not be possible -- within the constraints imposed by the legacy system(s) -- to fully meet the requirements reflected by the

complete "MUST share" information subset. Therefore, we must realistically assess what information can feasibly be shared between the new system and the legacy system(s). We have called that subset the "CAN share" information subset. It is depicted graphically within the **large dashed line** on the diagram.

It is essential to identify the information elements in this "CAN share" data subset, so warfighting planners can address the interoperability difficulties caused by the differences between the warfighters' interoperability *needs* (the "MUST share" subset) and the legacy system(s) information exchange *capabilities* (the "CAN share" subset).

3.2.4 Data Requirements Summary

Figure 2 graphically depicts the different sets of information that must be identified when we are considering requirements for -- or development of -- any new Joint Tactical C4 system. These new systems must be interoperable; they must help all warfighters function together effectively in a tactical environment. Clearly identifying the data that must be shared in support of interoperability, in addition to any limitations imposed by legacy systems, is the critical first step toward achieving that interoperability goal.

After we understand the information exchange requirements for a new system, we can consider how we will accomplish this information exchange. This is addressed by the second and third requirements categories we propose:

- The Hardware and Software Requirements
- The Communications Requirements

3.3 Hardware and Software Requirements

The hardware and software requirements are what a computer systems engineer would view as an "architecture."

There are a number of considerations that are applicable to information systems that run on existing commercial hardware. An example of this type of system is the Global Command and Control System (GCCS), which runs on commercial off-the-shelf computers under a UNIX operating system. For these types of systems, consideration must be given to Defense Information Infrastructure - Common Operating Environment (DII-COE) compliance. Applications access the COE via application programming interfaces (APIs), which are routines used by an application program to request lower-level operating system services. Functionality is easily added to or removed from the target system in small, manageable units called segments. While the goal for this type of information system is clearly convergence upon a single hardware/software standard, that might not realizable in the foreseeable future.

The issues for hardware and software which are embedded within a weapon system -- and, therefore, are usually "custom made" for their particular applications -- are even more complex. It is exceptionally difficult to create "architectural" requirements which can be broadly applied to systems of this type.

3.4 Communication Requirements

The third key component to our proposed extension to the JTA's System Architecture View is communication requirements. The following two questions must be considered:

- With whom must this system communicate?
- What is the requisite bandwidth (or required capacity) for each destination?

The answers to those two questions will form the basis for several other communications requirements. What transmission medium is most appropriate? As a goal, we should make maximum use of a common multi-spectral communication system. This has the effect of "separating the radio from the application" -- with several significant benefits. It decreases the amount of "real estate" on the weapon system (e.g., ship or airplane) committed to antennas and to application-specific radios. It also avoids "wasted" bandwidth by allowing a number of applications to share one radio, rather than requiring each application to have a radio which is not in use during a significant portion of time.

It is also critical to use standardized transmission protocols (e.g., 1553 MUX buses in an embedded system or TCP/IP for an information system network) whenever possible.

3.5 Extension Summary

Specifically addressing these three categories of requirements (Data Requirements, Hardware and Software Requirements, and Communications Requirements) when you specify your JTA System Architecture View should make it easier to develop system requirements which will support joint interoperability

4. Conclusion

Joint operations are essential to battlefield success, and interoperability is essential to joint operations. We cannot interoperate if we cannot communicate with each other. Interoperability will result when joint information exchange requirements are clearly addressed early in every new system's development lifecycle.

The JTA was developed to provide a framework for the design and implementation of interoperable systems. This paper has briefly described the three components (or architectural views) of the JTA. We proposed additional detail for the system architectural view, in order to facilitate the development of engineering requirements which will ensure system interoperability.

Authors

Lieutenant Colonel John A. (Drew) Hamilton, Jr., US Army, is currently assigned to the US Navy Space and Naval Warfare Systems Command (SPAWAR). Previously he served as the Research Director for the Department of Electrical Engineering and Computer Science at the US Military Academy, as Chief of the Ada Joint Program Office, and as the Chief of the Officer Training Division at the Computer Science School, Fort Gordon. Lt.Col. Hamilton has a BA in Journalism from Texas Tech University, where he was commissioned in Field Artillery; an MS in Systems Management from the University of Southern California, an MS in Computer Science

from Vanderbilt University, and a Ph.D. in Computer Science from Texas A&M University. Lt.Col. Hamilton graduated from the Naval War College with distinction. CRC Press publishes his book, Distributed Simulation, written with Major D. A. Nash and Dr. Udo W. Pooch.

Major Jeanne L. Murtagh, USAF, is currently the Director of the Software Professional Development Program (SPDP) at the Air Force Institute of Technology, Wright-Patterson, AFB, OH. Major Murtagh's previous assignments include software development positions in an Air Force laboratory, real-time embedded weapon system software management positions in system program offices, and instructor duties in acquisition, professional continuing education and academic positions. Major Murtagh has a B.S. in Computer Science from Rensselaer Polytechnic Institute and an M.S in Computer Science from Boston University. She has completed Squadron Officer School and Air Command and Staff College. She is certified under the Acquisition Professional Development Program at Level III in Systems Planning, Research, Development & Engineering and at Level II in Program Management.

Colonel John C. Deal, US Army, is currently the Executive Officer to the Director of Information Systems for Command, Control, Communications and Computers (DISC4). Previously Colonel Deal served as a member of the Secretary of Defense Strategic Studies Group and as the Deputy Director of Standards in the Architecture Directorate, ODISC4. He played a critical role in the development of the Army Technical Architecture, the Army Systems Architecture, and the Army Operational Architecture. Colonel Deal is a graduate of the University of Alaska, the Naval Command and Staff College, and the Army War College Fellowship Program at the University of Pittsburgh. He has earned an MS in Electrical Engineering from the Naval Post Graduate School, an MA in National Security Studies from the Naval War College, and an MA in International Relations from Salve Regina University. Colonel Deal has been selected to command the US Army Information Systems Engineering Command.