

The Data Administration Newsletter (TDAN.com)

[Robert S. Seiner - Publisher](#)

[Main Menu](#)

[New Articles](#)

[Article Archive](#)

[Special Features](#)

[What's New](#)

[Contact the Publisher](#)

DATA, ARCHITECTURES AND THE INTEROPERABILITY CHALLENGE

Written by Michael Gorman - Whitemarsh Information Services Corp.

[\[Return to the Article Archive\]](#)

Published in TDAN.com July 2004

The ability of the Battle Commanders to execute the tenets of war with speed and precision comes from three factors: a shared situational understanding of the battlespace, the ability to collaboratively plan and knowing the commander's intent.

Sharing common situational understanding of the battlespace is essential for Army and Joint combat operations, but building that common picture is not a simple process. Everyone using the common picture must have the same understanding of the symbology, confide in its accuracy, and use the same data to build the picture. Such coordination requires common data, information requirements, a transport (communication) mechanism, and the display requirements for the mission. Additionally, authoritative data sources and doctrine-based business rules are required to ensure that the right information reaches the right person at the right time. As the Army moves from service specific operations to Joint, interagency, multinational, and Net-centric environments, this issue becomes more complex. That is why data engineering and management are essential to supporting the combat commander.

Situational awareness and the common picture is not a snapshot or a static image electronically mailed around the battlefield but a dynamic display of common information from multiple sources. The common picture is not called "common" because it is the same display (picture) at all locations but because everyone uses the same data — from the commander in chief to the soldier in a fighting vehicle. Users select required data (fuel status) and how they want it displayed (pie charts or bar graphs). Regardless of the display, the data remains common between all of the users. This data must be clearly defined as to format, names and meaning.

To illustrate the issue, imagine that information on a damaged bridge is transmitted in a Joint or net-centric environment. A ground force commander would want to know whether it is a four-lane concrete bridge that a tank could not cross, or is it a rickety wooden footbridge that a soldier could not cross. To an Army commander, this concept of "bridge" is self-evident. But to the commander of the 3rd Fleet, and his supporting command systems, the "damaged bridge" terminology is confusing. To him a bridge is where he commands a ship. A tank is either salt or fresh water. And why would a tank be on his bridge? Assuming universal acceptance of any information is dangerous unless it is standardized and has the same definition for all information users.

The issues of non-common naming conventions, definitions, and business rules impact current

operations on a daily basis, and will continue to impede interoperability and combat operations in the Joint, interagency, multinational, and net-centric environments unless addressed in the architecture and system engineering efforts of the Army and DoD.

SITUATIONAL AWARENESS AND DATA INTEROPERABILITY ENABLERS

Having all systems provide information is not adequate to generate a common picture. Likewise, unlimited bandwidth and the best electronic mail system in the world are not the answers either, although they contribute to the solution. Overloading users with mountains of unstructured information (such as electronic mail, pictures and web pages) could be as harmful as providing no information at all.

Structured data is information arranged so that it can be searched, sorted or organized for automatic processing. Using such data is essential to creating a common picture. Software can easily take a mountain of structured data, use operator-defined filters, sift through it quickly and provide exactly the information needed. This focuses information collection and processing to meet specific warfighter needs.

For example, MCS obtains friendly data from the FCB2 and converts it to units for display in the common picture. This conversion generates a basic military science problem—how does the computer know that bumper number A-11 belongs to 1st Squad, Alpha Section, 1st Platoon, Alpha Company, 3-9 Infantry? It does not. First, the computer must be fed unit organization in a form conducive to machine manipulation. The common picture needs five different types of structured information—organizational, personnel, materiel, facilities and features. This information is defined and documented in the data engineering and management process.

To enable the systematic development and documentation of combat essential data exchange specifications CIO/G6 has developed a net-centric data strategy that provides a framework and methodology that will allow the Army to migrate current systems to net-centric capabilities and provide interoperability with new systems in Joint and Net-centric operations. The essential elements of the strategy are:

1. Establishment of Communities of Interest (COI) in compliance with DoD policy.
2. Development of COI information exchange standard specifications (IESS) to establish and document the common COI vocabulary, authoritative data sources (ADS) and business rules for the exchange of information.
3. The use of Enterprise Identifiers (EID) for the unambiguous exchange of organizational information across disparate databases/systems.
4. The use of Authoritative Data Sources to ensure a common, trusted, information source for the sharing of critical combat information.
5. The use of Extensible Markup Language (XML) as a common format for the tagging of information assets and common data exchange format with appropriate GIG Services and subscribers.
6. The use of the Data Strategy Framework and Data Performance Planning methodology to ensure a common approach and quality data products addressing COI and Cross-COI interoperability.

TECHNICAL DISCUSSION ON THE IMPORTANCE OF

INTEROPERABLE DATA ASSET ENVIRONMENTS AND DATA ARCHITECTURE VIEWS

The DoD Net Centric Data Strategy refers to data, in all forms, as a data asset that includes, for example, system files, databases, documents, official electronic records, images, audio files, web sites, and data access services. Every data asset must be assessed against a set of mandatory DoD NII goals –is it visible, accessible, institutionalized, understood, interoperable, trusted, and responsive to user needs? Under the DoD Net-Centric approach, every data asset consists of two fundamental forms: its content, and the envelope that surrounds its content. The collective term for all specifications about a data asset, including its content envelope, is commonly known as metadata.

Every data asset requires an authoritative source so that it, when employed, is known to be the definitive instance. Many data assets will also require a unique enterprise identifier so that its instance is unambiguous (one example where this concept is being executed is in the Global Force Management System). Data assets will need to be configured (format, names and meaning) into a form, such that it meets the needs of communities of interest. Along with the associated business rules, the specifications of this commonly reusable form is called an information exchange standard specification. When data assets are accessed and/or exchanged, then its content may be transmitted “raw” or may be wrapped in “handles.” Handles include, for example, Electronic Data Interchange (EDI) or eXtensible Markup Language (XML)^[1]. Data asset content exchange format decisions are based on practicality and performance.

Data assets, then, which meet the DoD NII data goals by being represented authoritatively, identified uniquely, configured within a common exchange format, and interchanged via appropriate wrappers, are interoperable across the enterprise. Data assets lacking these attributes will not be interoperable enterprise-wide.

The data asset infrastructure underlying interoperability is accomplished through metadata management, standard data elements, and standard data segments that, in turn, consist of standard data elements.

The de jure standards, which are employed to make data assets technologically definable and exchangeable across the world, are ISO/ANSI SQL for data segment definition and access, WC3 for data asset XML construction, and ISO 11179 for data element standardization.

Data assets, constructed along the lines cited above, are thus able to be materialized, seen, understood, collected, interrelated, and exchanged both automatically within a weapon system’s component and also within and across collections of weapon systems within a battle space that may be deployed within service programs, joint-service programs, and coalition service programs.

However, if interoperable data asset environments are not created and managed across the battle command environment, then battle command operations and weapon system executions will either be severely degraded or fail outright. Thus, “data” is an essential architecture view and a battle command asset that must be managed across the life cycle of all battle command and weapon systems.

“DATA” VIEW AS CORNERSTONE OF DOD INTEROPERABILITY AND ARCHITECTURE INTEGRATION

The architecture initiative within the Department of Defense (DoD) is known as the DoD Architecture

Framework. The current specification for the creation and maintenance of DoD architecture products is contained in the DoD Architecture Framework, Version 1.0. According to this specification, all architectures should be formulated as belonging to one of three views or perspectives, namely Operational, Technical or Systems, and all architecture-related information should be captured through one or more of the 26 architecture products documented therein. One of the goals of the Architecture Framework is to ensure that architecture-related information can be more readily shared and re-used among the services, especially if the products are maintained in databases that support all the data needed automatically to generate these products.

While the DoD Architecture Framework specifies just three types of architectures views (operational, systems, and technical), there is an architecture view, the data view, that addresses issues, standards, guidelines, and analysis in the area of data exchange. This fourth area, the data view, critically impacts information compatibility, interoperability, and integration, in a way that the other views cannot. This is because the OV, SV, and TV views can be developed without being specific about data content. For instance, the Systems Architecture view primarily documents hardware and software configurations and information processing/database management system platform environments, while the Technical Architecture view specifies standards and protocols. The Operational Architecture view documents information requirements in the form of information flows (both need lines and content) without ensuring that data specifications are consistent, complete, and encompass all stated data requirements. In contrast, the “data” architecture view provides the means for data exchange and the underlying data specifications essential to these exchanges.

The “data” view, as described above, implicitly underlies each of the three DoD Framework architecture views (Figure 1). The “data” view is more than an integrated schema for the All-View (AV) architecture product AV-2, Integrated Data Dictionary. It also is more than a selection of entities from the Core Architecture Data Model (CADM), which specifies the data requirements for the 26 architecture products. Finally, it is more than a Service-specific or Agency-specific extension of the CADM. The “data” view provides the framework for and definition of common data structures (whether part of the Integrated Data Dictionary or not) from specific sets within the scope of a system of systems initiative.

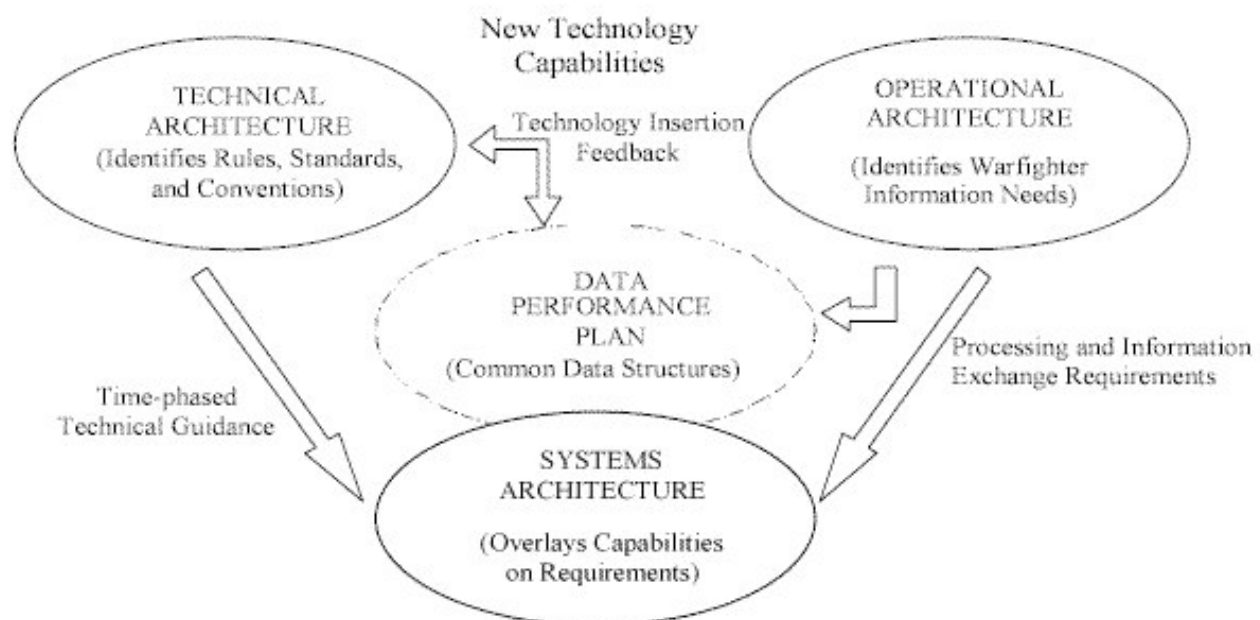


Figure 1. Relation of Enterprise Architecture Data to Architecture Views

Adopting the “data” view as part of the Army Enterprise Architecture approach would significantly increase the effectiveness of overall Army architectural efforts. In particular, Army information systems would share a consistent approach that addresses the capture, storage, management and distribution of data as an integral component of systems design. This would reduce system development and integration costs by reducing the per system (stovepipe) engineering for data. This also would promote timely identification of data issues along with operational and procedural issues impacting information interoperability.

The “data” view is a key aspect of ensuring the compliance and validation of architecture products. Whereas Operational Architecture products record information exchange requirements, and Technical Architecture products promote software and hardware interoperability, and Systems Architecture products set common links and communications networks, no portion of the DOD Architecture Framework, Version 1.0, specifically addresses the requirements of data interoperability at the level required to permit data reuse without loss of semantic and syntactic integrity.

“Data” view initiatives are primarily focused on data exchange and data reuse among databases, where data is highly structured, and its semantics—i.e., entity and attribute definitions, enumerated domains, etc.— and physical characteristics (e.g., data length, data type, etc.), need to be tightly controlled in order to permit information transfers with minimal or no human intervention. It is, therefore, more than what is contained in the JTA-A Combat Support and Sustainment Domain Profile based on the Technical Architecture Profile 1 (TV-1), and its results go towards the process improvement of information exchanges.

DATA INTEROPERABILITY CHALLENGE

Joint Vision 2020 clearly articulates the need for Information Superiority. This superiority is only an advantage when contextualized data can become information, which then can be converted into superior knowledge leading to better decisions. During the conduct of joint operations, “interoperability” is a mandate for the joint force of 2020, especially in terms of communications, common logistics items, and information sharing. Information systems and equipment that enable a relevant common operational picture (COP) must work from shared networks that can be accessed by any appropriately cleared participant (JV2020).

The challenge of DoD strategic information policy is for all Army and DoD information systems to be interoperable. One component of interoperability is data interoperability. Data interoperability is the ability to reuse data from another information system without any intermediate transformation and human intervention.

Two examples illustrate the lack of data interoperability in DoD. In stark contrast to data interoperability, these examples demonstrate the current way of doing business, which is point-to-point exchange of data via messages and translators. In this environment, every database configuration board (i.e., TADL-J, USMTF, VMF, MIDB, JCDB, etc.), considers the standards from their community of interest (COI) to be “the standard”.

As a first example, one of these COIs uses a complex digital message protocol, the Joint Variable Message Format (JVMF). According to Edgar Dalrymple (Crosstalk, February 2002, p. 25):

The specification for the JVMF message protocol is the Technical Instruction Design Plan that is maintained by the Army’s Communication and Electronics Command (CECOM). The specification is effectively maintained as a database that is known as the Variable Message Format (VMF) Integrated Database (VID). The VID defines the possible data fields and their associated parameters, structure, and the message cases and conditions. Cases and

conditions are assertions about the consistency of the fields in the messages, and the parser must implement them in order to encode and decode a valid message.

CECOM produces a new database release when either new messages have been added, or existing ones have been changed. The specification of the messages is nested up to six levels deep, and each level can have potentially thousands of data elements that may or may not be present. The current version of the VID has 121 messages, with millions of fields possibly present. The information that could be contained in the full message set if all fields were populated would cause the storage size for the messages to be in the terabytes range.

The Army Battle Command System (ABCS), a command and control system of systems, provides a second example of the lack of data interoperability. Without including Army systems, ABCS consists of over 80 Joint or other Service's systems. It has 226 external system interfaces (Army, Joint, other Services). In attempting to determine the cost of continuing to fund and maintain these interfaces, an Air Mobility Command FY95 Study reported that 80% of its software dollars went for interface maintenance (\$335,000/interface/year – 123 interfaces). One wonders how much the ABCS System of Systems is spending annually on funding and maintaining its interfaces, and one must definitely wonder whether there is not a better way to exchange data?

FEDERAL ENTERPRISE ARCHITECTURE AND CORPORATE INFORMATION MANAGEMENT

From the above examples, it is clear that to begin to address the challenge of achieving data interoperability while migrating to a net-centric, fully distributed, synchronized, knowledge-based solution in line with "Army Transformation" and "Vision 2020", the Army must develop a data interoperability strategy based on an Enterprise Architecture. In January 1999, the Federal Conceptual Model Subgroup drafted version 1.0 of a Federal Enterprise Architecture Framework and defined a Federal Enterprise Architecture as follows:

A strategic information asset base which defines the *business*, the *information* necessary to operate the business, the *technologies* necessary to support the business operations, and the *transitional processes* for implementing new technologies in response to the changing needs of the business. Stated differently, the Federal enterprise architecture is a strategic asset repository, which consists of models that define the current and target architecture environments, and the transitional processes for evolving from the current to the target. The focus of a Federal enterprise architecture is limited to *common federal architecture issues* (Subgroup, p. 7).

Ten years earlier in September 1989, Donald Atwood, then Deputy Secretary of Defense, formed the Executive Level Group (ELG) as a Federal Advisory Committee for Information Management to advise him on how to implement a Corporate Information Management (CIM) program (See Paul A. Strassmann, *The Politics of Information Management*, New Caanan, CT, 1995, pp. 396-397). The ELG disseminated a frame of reference and a set of priorities in what was called the Corporate Information Management (CIM) model.

On level one of the model was POLICY (What is the goal of our business?). Level two consisted of BUSINESS METHODS (How do we want to do business?) and BUSINESS MEASURES OF PERFORMANCE (How do we judge how well we do business?). Level three contained PROCESS MODELS (What will the activities of our business be?) and DATA MODELS (What will we need to know to do business?). On level four was INFORMATION SYSTEMS (How can technology help us do business?); and on level five was COMPUTING AND COMMUNICATION INFRASTRUCTURE

(What information technology will support our business?) (See GAO/AIMD-94-14 "Defense Data Administration," p. 3).

Paul Strassmann, one of the nine ELG members who in early 1991 became Director of Defense Information, interpreted the CIM model as follows (Strassmann, p. 400):

- Policy ahead of everything else;
- Business methods and performance measure ahead of modeling; and
- Information systems and technology decisions take place only after all the conditions for its success are in place.

Strassmann believed this "common sense approach" to the management of all information resources was diametrically opposed to the thinking of system developers and administrators. According to Strassmann: "DoD system managers usually first focused on the technology and only then looked for its justification. Hardly anyone had a comprehensive set of information management policies. When such policies were available, measurements concerned technical details. Typically, business models were incomprehensible to everyone except to their originators" (Strassmann, p. 401).

CONCLUSION: AN ARMY DATA INTEROPERABILITY STRATEGY

As noted earlier, data interoperability is the ability to reuse data from another information system without any intermediate transformation and human intervention. The data interoperability strategy and transition plan for moving from a point-to-point current architecture to a target architecture enabling COI and cross-COI information exchanges within the Army and the Net-Centric environment depends on the six-component strategy enumerated above. This strategy is based on:

- Creating first the policy in Level One (i.e., AR 25-1, paragraphs 4-7 through 4-12);
- Developing Authoritative Data Sources (ADS) in Level Two by identifying high-risk data elements;
- Creating Information Exchange Standards Specifications (IESS) in Level Three consisting of common information exchange data models and standard data elements and other related products (i.e., activity models);
- Mandating the use of XML technologies in Level Four to promote data exchanges among automated information systems;
- Mandating the use of globally unique enterprise identifiers (EIDs) in Level Five to transform the various and disparate databases in the current infrastructure into a distributed, enterprise-wide, single virtual database; and
- Using the Data Strategy Framework and Data Performance Planning methodology to ensure a common approach and quality data products for addressing COI and Cross-COI interoperability.

Each of the components is needed to create a data engineering and data exchange environment where COI and cross-COI interoperability can be defined and achieved. This six-component

strategy for achieving data interoperability is foundational for defining and specifying an integrated set of processes and services for accomplishing the target architecture of information exchange. To achieve information exchange in the Army, there is a need for both a services or materiel solution, and a non-materiel set of (1) policy, (2) objectives, (3) goals, and (4) metrics to provide discipline. The six-component strategy for achieving data interoperability provides a framework and methodology for accomplishing net-centric operations where information producers and consumers work effectively and efficiently to accomplish Army missions.

[1] XML is a set of syntax rules for creating semantically rich markup languages in a particular community of interest (COI). A markup language's primary concern is how to add semantic information about the raw content in a document; thus, the vocabulary of a markup language is the external "tags" to be attached or embedded in a document. Associated with XML is the XML Schema. XML schema is a definition language that enables COIs to constrain conforming XML documents to a specific vocabulary and a specific hierarchical structure. XML schema is analogous to a database schema, which defines the column names and data types in database tables.

Michael M. Gorman, President of Whitemarsh Information Systems Corporation, has been involved in database and DBMS for almost 35 years. Mr. Gorman has been the Secretary of the ANSI Database Languages Committee, X3H2 for 25 years. X3H2 standardizes SQL. A full list of Whitemarsh's clients and products can be found on the web site, www.wiscorp.com. The goal of the web site, WisWeb, is to make data management books, courses, methodologies, software, and metrics available to the database community through electronic publishing and downloading. WisWeb memberships are very reasonable and are designed for the individual, the ISD organization, universities/colleges, and professional training organizations.

[\[Return to the Article Archive\]](#)

The Data Administration Newsletter (TDAN.com)

Robert S. Seiner - Publisher - rseiner@tdan.com

© Copyright 1997-2004 - The Data Administration Newsletter (TDAN.com)

-