

Chapter 1

Interoperability Introduction and Overview

By
Dr. John A. Hamilton, Jr., Auburn University

The views expressed in this chapter are the opinions of the author, and do not reflect the official opinions of any U.S. government agency.

CHAPTER 1: THE TOPIC OF THIS BOOK: INTEROPERABILITY

Interoperability crosses two dimensions: organizational dimensions and time dimensions. In the here and now, interoperability across organization boundaries with their diverse communications devices is ultimately achieved through software. In planning for interoperability in the future, this is done via requirements engineering. So from a technical standpoint, command and control system interoperability is achieved via software engineering and requirements engineering.

A lot has to happen before the engineers are turned loose on interoperability problems. But it is important for everyone involved that there are hard technical issues at the end of the process. This book presents C2 system interoperability from both a systems viewpoint and a systemic viewpoint. Interoperability is a critical enabler of network centric warfare and it is not enough to simply engineer one-of band-aids to connect systems. A systemic approach to interoperability is required and it is the purpose of this book to show how that objective may be achieved.

What do we mean by interoperability? Definitions abound, but definitions do not equate to understanding. The definition of interoperability requires two systems to be able to exchange data with no loss of precision or other attributes, in an unambiguous manner, in a format understood by both systems, and in such a way

that interpretation of the data is functionally equivalent. External synthesizing functions will be computationally too complex, so architectural standards are required for data and the software that manipulates that data. In this volume, we limit our discussion of interoperability to the military command and control domain. Next, we recognize that standards are not sufficient to ensure command system interoperability.

We proceed as follows:

CHAPTER 2: THE DOMAIN OF INTEROPERABILITY IN THE US DEPARTMENT OF DEFENSE

By Rosen, Parenti and Hamilton

This chapter describes and defines the framework in which DoD systems are acquired and used, beginning with requirements definition, proceeding through acquisition, fielding into the sustaining base, and, ultimately, employment in military operations. It describes how interoperability is perceived by each of the players in this process, and how a rational use of architectural principles can support each of these players and the interactions between them – putting the interoperability horse before the architecture cart. By employing this model, we comment on some of the organizational issues affecting the DoD’s interoperability efforts, and show how relatively minor changes might be expected to improve our success in developing, acquiring, and employing interoperable systems. In addition, since the relationship to architecture is better understood, we conclude by providing a perspective on ongoing architecture efforts and their ability to support this process.

CHAPTER 3: INTEROPERABILITY FROM THE MATERIEL DEVELOPER POINT OF VIEW

By Hamilton, Melear and Endicott

The service C2 acquisition centers have an important role to play in breaking service stovepipes. Software engineering research consistently shows that software issues are most quickly and inexpensively resolved early in the lifecycle. Resolving interoperability issues in the acquisition centers before fielding will be the most cost-effective and will deliver interoperable capability to the field fastest. In an April 1998 report to Congress responding to some of those requirements, the Secretary of Defense noted “joint operations have been hindered by the inability of forces to share critical information at the rate and at the locations demanded by

modern warfare.” To attack this problem, the Secretary directed the creation of a study group to examine ways to establish a joint command and control (C2) integrated system development process.

As a result of this study, the commanders of the service C2 acquisition centers formed the Joint Command and Control Integration Interoperability Group (JC2I2G). Although this initiative was launched from a previous administration, its impact is still being felt. The assignment of officers from other services to the Army’s Communications and Electronics Command, Fort Monmouth (CECOM), the Navy’s Space and Naval Warfare Systems Command, San Diego (SPAWAR) and the Air Force’s Electronic Systems Center, Hanscom AFB (ESC) forced a joint perspective on those organizations. This was later augmented by detachments from DISA being assigned to each command. Further, these officers and civil servants established a presence in the Combatant Commands, for the first time giving the Combatant Command staffs direct access with the material developer. This initiative is clearly a precursor to the time when command and control requirements will be developed by the joint community rather than the individual service communities.

Through this initiative, it becomes clear that a software-based architecture approach is required for C2 interoperability and that introduces a basis for interoperability discussed in the next chapter.

CHAPTER 4: A BASIS FOR JOINT INTEROPERABILITY

By Hamilton and Murtagh

One of the first tasks given to the Joint Forces Program Office was to define a data model to support US Joint Forces Command’s work on Global Information Grid requirements definition. This work is based on the original definitions of the Operational, System and Technical Views by the Army Science Board and later codified in the Army Technical Architecture. Currently, the C4ISR Architecture Framework Document is regarded as the definitive guide for architecture, but the essence of the three architectural views is still consistent with the original roots in the Army. 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 chapter describes the three architectural components (views) described in the JTA (the JTA itself being a Technical View), and then proposes additional detail for one of these three components.

The Joint Vision 2010 Data Model defined in this chapter divides data requirements into survival data with hard real-time deadlines and planning data,

with near real-time deadlines. 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.

CHAPTER 5: BILATERAL INTEROPERABILITY THROUGH ENTERPRISE ARCHITECTURE

By Catania, Hamilton, Francia, Rosen, Melear and Burns

This chapter will address the important role of architecture planning for ensuring system interoperability in a network-centric coalition environment. As US forces become more dependent upon coalition partners to support crises around the globe, systems interoperability becomes a major concern. This problem is more acute in the Pacific theater, where the US has no equivalent to NATO to address such issues. In the Pacific, the US has numerous bilateral agreements with allied nations and therefore the degree of interoperability varies from country to country. A key to understanding interoperability shortfalls is documenting the “as is” architecture for each primary allied nation to facilitate identification of key information exchange requirements for critical command and control nodes.

The Alaskan Command (ALCOM) architecture study, using a prototype version of the Joint C4I Architecture Planning System (JCAPS), illustrated the utility of having a clearer picture of the enterprise architecture described in common lexicon. With this information, the CIO can make more informed decisions concerning resource requirements and contingency planning, to ensure information technology adequately supports Alaskan Command’s mission threads. Another result of the Alaskan Command study was the need to consolidate the numerous architectures that have been developed in recent years. These independent, non-collaborative efforts have resulted in information resources that often are of little use and are, consequently, shelfware.

During a survey at HQ US Pacific Command conducted by a CINC Interoperability / Joint Forces Program Office team, approximately sixteen documented or ongoing architecture efforts were revealed across the PACOM J2, J3, and J6. Each effort is separate and distinct. No centralized data repository exists. The existence of a relational architecture database that could be easily updated, maintained and reused would reduce duplication of efforts and multiple data requests and improve contingency and resource planning and allocations.

Finally, the authors propose a way forward in the development of a useful coalition interoperability architecture based on best practice experiences of the Australian Defence Force and the US Pacific Command.

CHAPTER 6: DEVELOPING INTEROPERABILITY METRICS

By Hamilton, Rosen and Summers

While interoperability issues are persistent and visible, the number of interoperability successes is easily overlooked. Most systems that are developed today meet the interoperability requirements that were specified in their Operational Requirements Document (ORD). The application of a set of metrics addressing this domain would shed more light on the situation and highlight the successes of the many agencies that have labored to produce interoperable systems. Effective metrics would enable the services and agencies to make more informed decisions about the allocation of scarce resources to solve interoperability in already fielded systems. This chapter begins by discussing some of the challenges involved in developing effective interoperability metrics. Next, it proposes a set of metrics that, the authors believe, would help realize the objectives described above. Finally, institutional and programmatic issues surrounding metrics are discussed.

CHAPTER 7: SUMMARY OF US PACOM'S INFORMATION CAPABILITIES FRAMEWORK

By Cieslak

The Information Capabilities Framework (ICF) provides a requirement grid, which systems and efforts must overlay to portray their contribution to end-to-end capability. This is markedly different than process diagrams that lead to systems for point (stovepiped) solutions. The ICF works in conjunction with the C4ISR Architecture Framework that calls for operational, system, and technical views of the architecture. The ICF organizes and relates efforts as well as systems. It supports the evolution of architectures over time and provides the structure needed for change management. The ICF is based upon the combination of the Global Information Grid (GIG), the Defense Information Infrastructure (DII) and a standard process organization model.

CHAPTER 8: A PROCESS FOR INTEROPERABILITY

By Sanders and Hamilton

The authors propose a C4ISR Architecture Framework Document-based System Interoperability Process Model. In the System Interoperability Process Model, the

C4ISR Architecture Views focus upon all stages of development involving system interoperability, specifically any software or hardware issues. Legacy systems will continue to dominate the initiation choice for a process model of development and enforce the idea that the C4ISR Architecture Views will be heavily relied upon in relation to software issues handling existing hardware and software incompatibilities.

CHAPTER 9: SECURITY ISSUES RESULTING FROM INTEROPERABILITY

By Hamilton, Chatham, Eoff, Imsand and Sachitano

There are multiple ill-defined relationships between interoperability and network security. It is clear the computer network defense measures can present challenges to interoperability in terms of national policy, physical system implementation and trusted system relationships. It is unclear whether greater interoperability between national assets makes them more vulnerable to computer network attack. As joint and combined interoperability becomes a reality, the potential for added security risks must be addressed. This chapter will outline the security issues raised by interoperability and list strategies to deal with them.

CHAPTER 10: APPLYING THE INFORMATION CAPABILITIES FRAMEWORK AT HQ, USPACOM

By Cieslak

How to proceed? Implementing system, operational and technical architectures in the US Alaskan Command provided a lot of insight on what was and was not useful and scalable to the authors. Randy Cieslak adds additional means and methods for achieving architecture-based interoperability. This chapter, written by the Chief Information Officer of the US Pacific Command, outlines how to apply the Information Capabilities Framework to support joint interoperability in the US Pacific Command.

CHAPTER 11: A SYSTEM DESIGN ARCHETYPE FOR C4ISR SYSTEMS OF THE 21ST CENTURY

By Reid and Johnson

It is simplistic to assume that interoperability problems exist only in requirements definition. Designing interoperable systems is a challenge and our colleagues

from Australia's Defence Science and Technology Office address this challenge with a prescription for a way ahead in this chapter.

The authors discuss the difficult issue of how to reliably design and build systems that are fundamentally suited to interoperate with one another. Ideally, all these systems would be constructed using the proposed design principles, but the requirement to interoperate with legacy systems is also recognized. It is not a traditional systems engineering or technology based approach. Rather, a set of key design principles is enumerated. They are, (i) *interoperability and system integration*, (ii) *decoupling of architecture layers*, (iii) *decoupling of system components*. There is also an emphasis placed on a design methodology embodying these design principles, which allows a flexible system design that changes infrequently, and a system implementation that changes constantly.

CHAPTER 12: CUTTING THE GORDIAN KNOT

By Hamilton

There are hard technical issues associated with interoperability. There are also funding, organizational and process challenges. US Forces have proven adept at using existing technology in new ways. This means that materiel developers will never be able to foresee all possible interoperability requirements.

Just as the knot of Gordius was never successfully untied, the current C2 interoperability situation in the US Department of Defense is similarly intractable using current solutions. The author proposes radical simplification of the problem space. There are too many agencies procuring too many systems. Finally, in summation, the author attempts to address and correct some of the myths and misconceptions associated with command and control interoperability.