Measuring Systems Interoperability

Challenges and Opportunities

Version 1.0

Mark Kasunic
Software Engineering Institute
Carnegie Mellon University

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
01-01-2001		xx-xx-2001 to xx-xx-2001

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Measuring Systems Interoperability Version 1.0 Unclassified	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Kasunic, Mark ;	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME AND ADDRESS Booz Allen & Hamilton 8283 Greensboro Drive McLean, VA22102	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS Software Engineering Institute ,	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This paper is one of a series commissioned by the DoD that characterizes the status of measurement associated with a particular aspect of software engineering. The specific focus of this paper is on measures for interoperability. Interoperability is the ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together The intent of this paper is to identify current practices related to measuring systems interoperability and to recommend a set of measures that will assist military planners in the acquisition, development and implementation of C4I systems that are interoperable.

15. SUBJECT TERMS
IATAC Collection; systems; interoperability

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
			Public Release	40	Fenster, Lynn lfenster@dtic.mil
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	1/1/2001	Report 1/1/2001

4. TITLE AND SUBTITLE
Measuring Systems Interoperability Version 1.0

5. FUNDING NUMBERS

6. AUTHOR(S)
Mark Kasunic

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Software Engineering Institute

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

This paper is one of a series commissioned by the DoD that characterizes the status of measurement associated with a particular aspect of software engineering. The specific focus of this paper is on measures for interoperability. Interoperability is the ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together The intent of this paper is to identify current practices related to measuring systems interoperability and to recommend a set of measures that will assist military planners in the acquisition, development and implementation of C4I systems that are interoperable.

14. SUBJECT TERMS
IATAC Collection, systems, interoperability

15. NUMBER OF PAGES
39

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

Table of Contents

Executive Overview

This paper is one of a series commissioned by the DoD that characterizes the status of measurement associated with a particular aspect of software engineering. The specific focus of this paper is on measures for interoperability.

Interoperability is the ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together The intent of this paper is to identify current practices related to measuring systems interoperability and to recommend a set of measures that will assist military planners in the acquisition, development and implementation of C4I systems that are interoperable.

In an April 1998 report to Congress, the Secretary of Defense noted that "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" [Hamilton 2000]. Serious interoperability deficiencies exist today. They have been perpetuated across all the services and have been identified in all recent, allied, joint and combined operations and exercises. Interoperability is often considered to be a desired, but unattainable, goal rather than a condition that can be quantified [Leite 98].

Interoperability is a broad and complex subject rather than a binary attribute of a system. Developing and applying precise measurements in an area as multidimensional and complex as interoperability is difficult. However, measurement, assessment and reporting of interoperability results in a visible way are essential to continued focus and to setting the right priorities. The increasing importance of, and reliance on C4I support of military operations suggests that the state and health of C4I interoperability be characterized, as much as possible, in a more explicit, objective and *measurable* way.

Measurement and assessment—and reporting of results in a visible way—are essential to continued focus and to setting the right priorities. As noted by Presson 18 years ago, "interoperability will never be an analytically useful field of study until it is defined in a quantitative way" [Presson 83]. Despite laudable case-by-case efforts, today there is no method for tracking interoperability on a comprehensive or systematic basis [Committee 99].

In this paper, we review the state of the practice in interoperability. We introduce and discuss an evolving and promising approach called the Levels of System Interoperability (LISI) Model. We feel that this model, although immature, provides a structured and systematic approach for assessing and measuring interoperability throughout the system life cycle. After describing the LISI Model and its measurement approach, we conclude this section with a summary of recommended measures that we feel will promote systems interoperability in the DoD.

Measuring Systems Interoperability

Challenges and Opportunities

> *"Information Superiority is the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same … The unqualified importance of information will not change in 2010. What will differ is the increased access to information and improvements in the speed and accuracy of prioritizing and transferring data brought about by advances in technology. While the friction and the fog of war can never be eliminated, new technology promises to mitigate their impact."*
>
> *– Joint Vision 2010*
> *Chairman of the Joint Chiefs of Staff*

1. Introduction

Command, control, communications, computers, and intelligence (C4I) systems relay critical information to U.S. forces during joint operations.

In an April 1998 report to Congress, the Secretary of Defense noted that "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" [Hamilton 2000].

Parts of DoD are well aware of a defense-wide problem in exploiting rapidly changing information technologies. A DoD strategy and ongoing efforts are in place to promote interoperability, resting on technical standards such as the Joint Technical Architecture and the use of a defense-wide common infrastructure. While much has been accomplished, the goal of a C4I system of systems with interoperability for the U.S. military continues to be unachieved. Despite increased attention and management awareness, much more must be done before C4I interoperability is sufficient to provide adequate end-to-end support of military missions and are no longer a major constraint on the execution of military operations.

The popular perception is that interoperability is synonymous with connectivity. However, true interoperability is much more than just connectivity. It is also a function of operational concepts and scenarios, policies, processes and procedures. For this reason, developing and applying precise measurements in an area as multidimensional and complex as interoperability is difficult and problematic. Interoperability is often considered to be a desired, but unattainable, goal rather than a condition that can be quantified [Leite 98]. Serious interoperability deficiencies exist today. They have been perpetuated across all the services and have been identified in all recent, allied, joint and combined operations and exercises. Measurement and assessment—and reporting of results in a visible way—are essential to continued focus and to setting the right priorities. As noted by Presson 18 years ago, "interoperability will never be an analytically useful field of study until it is defined in a quantitative way" [Presson 83]. Despite laudable case-by-case efforts, there is today no method for tracking interoperability on a comprehensive or systematic basis [Committee 99].

The intent of this paper is to identify best practices related to measuring systems interoperability and to recommend a set of measures that will assist military planners in the acquisition, development and implementation of C4I systems that are interoperable. We begin the next section by reviewing the multi-dimensional scope of the interoperability issue and what interoperability *means* in the DoD systems context. We describe a major initiative that takes the form of a three-part architecture[1]. We believe that

[1] The three-part architecture consists of: (1) Joint Technical Architecture, (2) Joint Systems Architecture, and (3) Joint Operational Architecture.

measurement of C4I interoperability requires such a unifying framework or architecture with a body of implementing guidance. Many DoD enterprise-wide efforts are underway to improve information systems interoperability. In sections 3 and 4, we describe polices related to interoperability and the information needs that are distributed across the DoD. In section 5, we introduce an evolving and promising approach called the Levels of System Interoperability (LISI) Model. We feel that this model, although immature, provides a structured and systematic approach for assessing and measuring interoperability throughout the system life cycle. After describing the LISI Model and its measurement approach, we conclude this section with a summary of recommended measures that we feel will promote an effective approach to interoperability. In section 6, we recommend specific next steps for promoting a deeper understanding of interoperability issues so that effective remedies can be pursued.

2. What is Interoperability?

A number of reports and technical papers have defined interoperability in different ways[2]. More recently, the Joint Chiefs of Staff Publication 1-02 defines interoperability in a way that acknowledges both the technical and operational components that contribute to a meaningful interpretation.

Operational Interoperability	The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together [DoD 95, DoD 98].
	The ability of systems, units, or forces to provide services to or access services from other systems, units, or forces, and use the services to operate effectively together [DoD 96].
Technical Interoperability	The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases [DoD 98].
	Interoperability is the ability of systems to provide dynamic interactive information and data exchange among C4I nodes for planning, coordination, integration, and execution of Theater Air Missile Defense operations [JTAMDO 97].

Operational interoperability addresses support to military operations and, as such, goes beyond systems to include people and procedures, interacting on an end-to-end basis. Implementation of operational interoperability therefore implies not only the traditional approach of defining standards but also enabling and assuring activities such as testing and certification, configuration and version management, and training [Committee 99].

Interoperability at the *technical* level is essential to achieving operational interoperability. Technical interoperability arises between systems rather than between organizations and must be considered in a variety of contexts and scopes. Dimensions of technical interoperability include

- sensors generating bits of information
- communication channels transmitting the bits of information
- computers processing the bits of information
- weapons directed by messages composed of bits

For two C4I systems to effectively interoperate, they must be able to exchange relevant bitstreams as well as interpret the bits they exchange according to consistent definitions.

Thus, technical interoperability places detailed demands at multiple levels, which range from physical interconnection to correct interpretation by applications of data that is provided by other applications.

[2] See appendix A titled, "Some historical definitions of interoperability."

2.1 An Architectural Approach to Technical Interoperability

The architecture of a system is the structure or structures of the system, which comprise components, the externally visible properties of those components, and the relationships among them [Bass 98]. Measurement of C4I interoperability requires such a unifying framework or architecture with a body of implementing guidance.

Architectures are a hierarchical description for the design of a system and in many cases how it will be developed, evolved, and operated. Architectures provide the underlying blueprint for the more detailed design and implementation decisions about components of a system. When well-defined architectures exist, engineers can design individual components and builders can implement them with a high degree of confidence that the end results will work as expected and meet user needs.

There are a number of architectural characteristics that can be used as a basis for reasoning about what might be considered appropriate quality attributes that can be measured. These include: interfaces and layers, standards, and data interoperability.

When reasoning about architecture, it makes sense to strive for an information systems environment that is based on (1) well-defined requirements specification, (2) common data structures, (3) common interface requirements, and (4) well-specified high-level information flows. Systems constructed in accordance with such an architecture are much more likely to be adequately interoperable than those that are not.

2.1.1 Interfaces and Layers

The modular decomposition of systems is typically both horizontal and vertical. Vertical decomposition refers to *interfaces* between discrete systems within the same layer (e.g., a standard message format used by different applications to exchange information). Horizontal decomposition of functions is known as *layering* (e.g., the separation of bit transport technologies, transport protocol, and applications).

Interfaces

Systems that perform a variety of functions are normally composed of multiple subsystems or components. Interfaces arise whenever one subsystem or component interacts with another. An architect that is designing and partitioning a system must consider the importance of:

Interface design	Well-designed interfaces permit development programs to be divided into more manageable pieces, which can result in faster development because the work of different players can proceed in parallel.
Encapsulation	This permits modular change in version and implementation technology. By encapsulating the internal details of a system component which may change over time, interfaces allow changes in internal implementation of portions of a system to be transparent to other portions.
Reducing interaction	Reducing the complexity of intersystem dependencies facilitates more rapid reconfiguration of systems to meet operational requirements.

Layers

Layers facilitate making C4I systems interoperable in the presence of rapidly changing technologies and/or multiple technology choices. Layering makes it possible to design a system of systems that has technology independence, scalability, decentralized operation, appropriate architecture and supporting standards, security, and flexibility. Layering can also accommodate heterogeneity, accounting, and cost recovery [CSTB 94]. Excellent examples of layering include (1) the use of TCP/IP to decouple communications link technologies from applications that use communications and (2) the use of hypertext transport protocol (HTTP) and hypertext markup language (HTML) to separate presentation from storage and retrieval functions.

Middleware is one instance of the layering principle. It provides a separation between applications and the operating systems platforms that the application run on [SEI 00, Bernstein 96]. As outlined in Figure 1, middleware services are sets of distributed software that exist between the application and the operating system and network services on a system node in the network.

By decreasing the dependence of applications on a particular operating system, middleware increases the ease of moving applications to new computer or systems and decreases dependence on operating systems that might fall out of favor in the commercial marketplace.

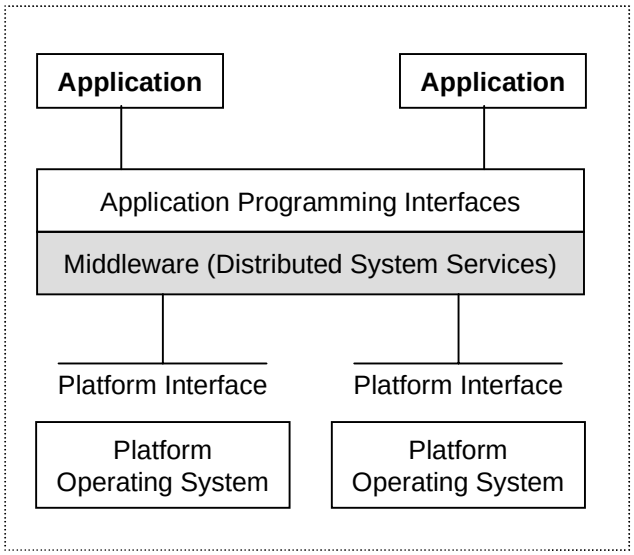


Figure 1. Use of Middleware.

CORBA (Common Object Request Broker Architecture) is widely perceived as an emerging middleware platform for distributed systems development [OMG 98]. CORBA specifies a system that provides interoperability between objects in a heterogeneous, distributed environment and in a way transparent to the programmer. It enables applications to cross the boundaries of different computing machines, operating systems, and programming languages. It specifies how client applications can invoke operations on server objects. Abundant information about CORBA is available from various resources [Cetus 00].

2.1.2 Standards

An essential aspect of architecture is the establishment of technical standards. (We have already alluded to some important standards in the section above when we introduced TCP/IP, HTML, HTTP, and CORBA.) In general, standards define common elements, such as user interfaces, system interfaces, representations of data, protocols for the exchange of data, and interfaces accessing data or system functions.

Technical standards provide a number of advantages for the system architect. With regard to interoperability, standards are important because they are accepted by multiple vendors, thereby increasing the likelihood that a collection of systems from diverse sources will be able to interoperate. It has become generally accepted by now that, although standards are certainly beneficial, simple adherence to standards is not sufficient to guarantee interoperability [NIMA 98]. Even when there are accepted standards and products compliant with these, interoperability is facilitated but not assured (because there are options within standards and different releases and version of products).

Finally, it is important to realize that technical standards are, by themselves, necessarily incomplete from the standpoint of a system or component designer. The operational scenarios that a system is expected

to support play an integral role. This range of scenarios defines the context in which a system is to perform specific desired functions and thus provides a meaningful reference for testing and evaluation.

2.1.3 Data Interoperability

Experience suggests that left to their own devices, the designers of individual systems will often make locally optimal decisions about data definitions and formats [Committee 99]. Data formats resulting from such local decisions may not be compatible when operational requirements dictate that a network of systems be called upon to interoperate. Thus architectural design must provide guidance to developers to minimize the applications-layer incompatibilities that inevitably arise when systems with different purposes must communicate with each other.

Examples of approaches to data interoperability include:

- Single data definition for all systems

  This approach can be problematic when applied on a large scale to a complex, evolving system or system of systems. The task of agreeing on definitions consumes a great deal of effort and time that might be better used elsewhere. Also, when a single set of definitions is mandated for all applications, definitions are no longer locally optimal, and thus such mandates often encounter substantial resistance in implementation.

- Object orientation

  This is a technically promising approach for developing data definitions by encapsulating the internal details of the data [Committee 99].

- Extensible data model

  This approach uses an extensible data model and standardized interface. The Simple Network Management Protocol is an example [Cherkaoui 99].

Legacy systems, which have been built around frequently unique data definitions, pose a major challenge to interoperability. Industry has developed a number of approaches by which systems not designed up-front for interoperability can interoperate to exchange information. These include (1) data “bus” approach, (2) data dictionary approach, (3) data translator approach, and (4) data server approach.

2.2 Elements of DoD’s Strategy for Addressing Interoperability

In recognition of the importance of interoperability to realizing its C4I goals (Joint Vision 2010 [Chairman 96]and Joint Vision 2020 [Chairman 00]), the DoD has adopted a joint/defense-wide strategy for promoting interoperability. Specifically, there are three major elements that have emerged

- a triad of interrelated architectures
- a common defense-wide infrastructure with a common applications platform
- applications-level efforts to promote interoperability

The three-part architecture is conceptually presented in Figure 2 and described in Figure 3. It’s important to note that the architectures are not all at the same level of development. DoD architectural development to date has focused on the Joint Technical Architecture (JTA) and it is by far the most mature architecture of the three.

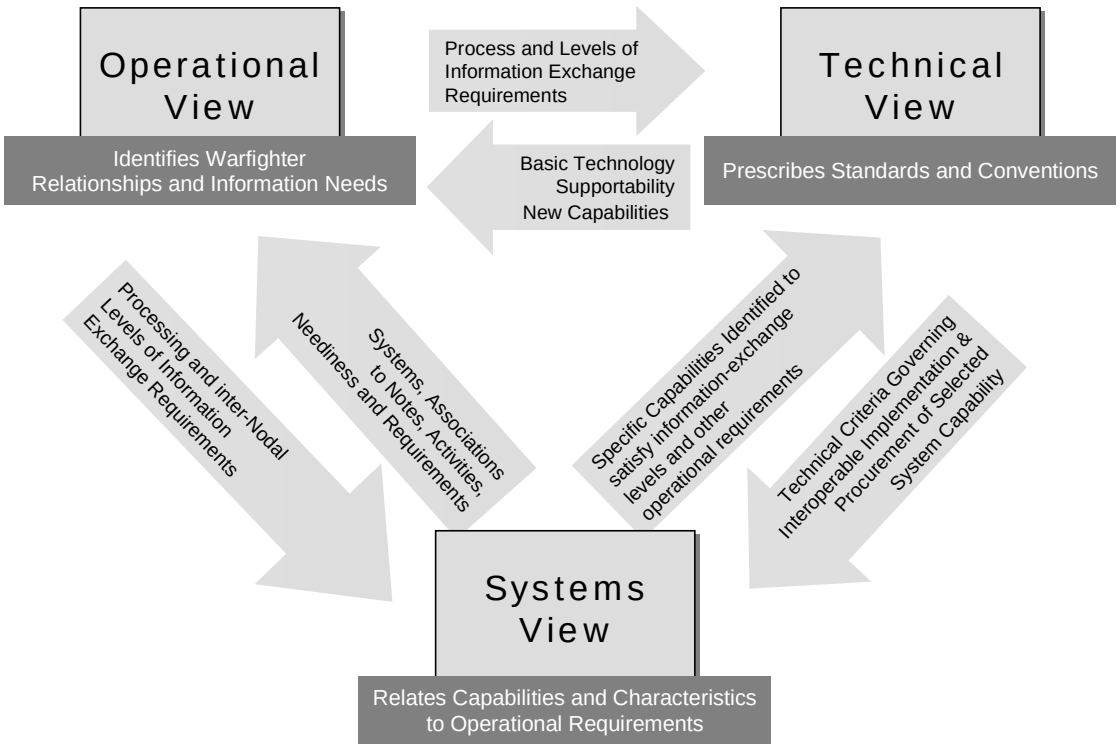


Figure 2. The three views of an architecture (Adapted from [Chatfield 98]).

Part of Triad	Description
Joint Operational Architecture	A description (often graphical) of the operational elements, assigned tasks, and information flows required to support the warfighter. It defines the type of information [exchanged], the frequency of the exchange, and what tasks are supported by these information exchanges. The operational architecture is thus the doctrine-driven representation of C4ISR nodes, roles, processes, interrelationships, and data/information exchanges. This representation relates to specific scenarios and joint/combined/coalition mission functions and forms the basis for realistic process and information flow representation and prioritization.
Joint Systems Architecture	A description, including graphics, of the systems and interconnections providing for or supporting a warfighting function. The systems architecture [view] defines the physical connection, location, and identification of the key nodes, circuits, networks, warfighting platforms, etc. associated with information exchange and specifies system performance parameters. The systems architecture [view] is constructed to satisfy operational architecture component requirements per the standards defined in the technical architecture.
Joint Technical Architecture	A minimal set of rules governing the arrangement, interaction, and interdependence of the parts or elements whose purpose is to ensure that a conformant system satisfies a specific set of requirements. It identifies system services, interfaces, standards, and their relationships. It provides the framework upon which engineering specifications can be derived, guiding the implementation of systems.

Figure 3. Elements of the DoD Architectural Triad [C4ISR 97].

The JTA is intended to provide a set of correct and mutually consistent technical standards, application interfaces (APIs), and protocols, along with the decision rules for using them.

The Joint Operational Architecture was originally intended to be a construct covering all military operations. The Information Superiority Campaign Plan of the Joint Chiefs of Staff calls for "the development of a high-level, C4 Joint Operational Architecture that integrates the joint warfare functions, from national level through operational level, into implementations of the JV2010 (Joint Vision 2010) operational concepts" [JCS 00].

An additional piece of the DoD strategy for C4I interoperability is the building of a common, defense-wide information infrastructure called the Defense Information Infrastructure (DII). The DII includes a set of common software, the DII-Common Operating Environment (COE). The DII-COE includes increasingly capable middleware, on top of which service/mission-specific application can be built. Use of the DII-COE and achieving compliance at certain levels is specified in the Joint Technical Architecture.

With regard to data interoperability, the DoD understands the importance of data integration and has launched two major efforts in this area:

- The Enterprise Data Model Initiative [DoD 91]
- Shared Data Environment (SHADE) program [DISA 96]

The Enterprise Data Model Initiative sets forth a DoD process through which standard data definitions in C4I functional areas are developed. As part of the process, they are then subjected to a cross-functional review process prior to being adopted as DoD standards. The goal of this process is to develop a complete set of standard data elements for DoD applications.

The Shared Data Environment (SHADE) program relies on a "bottom-up" approach to enable different C4I systems to share data segments and to use standardized access methods. SHADE has demonstrated some success in enabling legacy systems to interoperate. This program has recently been subsumed by DII-COE.

3. Policies related to interoperability

Current systems are increasingly being built to meet explicit requirements for interoperability and flexibility. The DoD's vision of the future—Joint Vision 2010 is one of information superiority [Chairman of the Joint Chiefs 96]. The cornerstone of information superiority is advanced C4I technology and systems, which can provide a robust, continuous, common operating picture of the battlespace to all tactical levels of command[3]. The common operating picture is a central element in a number of initiatives, including

- The Army Digitization Master Plan (Force XXI) [Army 96]
- The Theater Air and Missile Defense Program [TMD Plan 98]
- The Battle field Awareness and Data Dissemination (BADD) advanced concept technology demonstration (ACTD) [Office of Under Sec1 99]
- The "Extending the Littoral Battlespace" (ELB) ACTD [Office of Under Sec2 99]

Joint Vision 2010 and Joint Vision 2020 reflect the top-level vision in the DoD of what is possible though the exploitation of technology to solve the interoperability problem [Chairman 96, Chairman 00]. Each of the services has translated this top-level vision into a service-specific vision [Dept. of Army 96, Dept. of Air Force 96, Dept. of Navy 96, Marine 96]. Each of these services is exploring the implications of Joint 2010 and Joint 2020 for itself, taking steps with experimental studies, wargames, research and development activity and simulation gaming to develop and test concepts and capabilities that will ensure military preparedness for the 21st century. Additionally, as an extension of individual service experimentation, and in response to congressional pressures, a joint experimentation activity is being established at the U.S. Atlantic Command to address the co-evolution of doctrines, tactics, and new technological capabilities [Committee 99].

[3] The term "common operating picture" refers to a view of the battlespace that is near-real-time.

The DoD has a number of other initiatives underway that address various aspects of interoperability including

- C4I for the Warrior Concept
- Command, Control Communications, Computers, Intelligence, Surveillance, and Reconnaissance Architecture Framework
- Defense Information Infrastructure strategy
- Levels of Information Systems Interoperability initiative

All of these initiatives are about improving the interoperability of C4I Systems [GAO 98].

4. Information Needs

Historically, DoD approaches to interoperability have ranged from handling it on a program-by-program basis to making limited-scope efforts on a joint, community-wide basis (e.g., the Joint Interoperability of Tactical Command and Control Systems activity to address joint message standards) or a functional community basis (e.g., air defense). In addition, some programs to develop defense-wide infrastructure, dating back to at least the 1960s, have been followed more recently by a few sizable, centrally managed application development programs (e.g., the Global Command and Control System as a replacement for the Worldwide Military Command and Control System [Committee 99].

However, the responsibility for interoperability is now distributed across the DoD, and each of the higher ranks of command has at least one entity charged with responsibility for interoperability issues[4]. See Figure 4.

Agency or Command	Entity responsible for Interoperability
U.S. Atlantic Command	Joint Battle Center
Joint Staff	Military communications and Electronics Board
Assistant Secretary of Defense for C3I	Information, Integration, and Interoperability Directorate
Defense Information Systems Agency	Joint Interoperability Test Command

Figure 4. Interoperability entities for agencies and commands in the DoD.

DoD guidance requires that a system be tested and certified before approval to produce and field it. Depending on the acquisition category and dollar threshold of the program, the approval authority may be one of the following [GAO 98]:

- Under Secretary of Defense (Acquisition and Technology), with advice from the Defense Acquisition Board
- Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), with advice from the Major Automated information System Review Council
- DoD component head (such as the commander in chief of a unified combatant command, the head of a military service, or a DoD agency head)

To ensure interoperability, the Defense Information Systems Agency (DISA)—under the direction of the Joint Chiefs of Staff—established the current C4I interoperability certification process in 1992. According to Joint Staff guidance, commanders in chief, the four services, and Department of Defense (DoD) agencies are required to use this process to test and certify existing and newly developed systems for interoperability.

[4] The listing of organizations is far from complete. There is a multiplicity of organizations and offices with some responsibility for C4I matters, and organizational structures for C4I (in general) have been rapidly evolving.

The Joint Staff's Director for C4 systems (J-6) is assigned primary responsibility for ensuring compliance with the certification requirement. DISA's Joint Interoperability Test Command is the sole certifier of C4I systems. According to Joint Staff guidance, commanders in chief, the services, and DoD agencies are required to adequately budget for certification testing [GAO 98].

When thinking about these stakeholders, one may note the different perspectives that are working based on the role of the stakeholder. Some entities are operational while others are more focused on planning. Operational units (in the DoD context, this would be the CINCs as the warfighting authorities) have a perspective concerned with the capabilities of today's systems (in the short term). Planning units[5] are concerned with the capabilities of tomorrow's systems, over the longer term.

5. Recommended Measures for Interoperability

Currently, interoperability is typically assessed by DoD through non-comprehensive perspectives that are focused, for example, on standards (e.g., Joint Technical Architecture), COE (Common Operating Environment) compliance, data models, or certification criteria, and how individual systems match up to such criteria or standards. It is generally recognized that much more needs to be accomplished in this area (e.g., see [Committee 99]).

The popular perception is that interoperability is synonymous with connectivity. However, as we discussed previously, true interoperability is much more than just connectivity. It is also a function of operational concepts and scenarios, policies, processes and procedures. For this reason, developing and applying precise measurements in an area as multidimensional and complex as interoperability is difficult. However, the increasing importance of, and reliance on, C4I support of military operations suggests that the state and health of C4I interoperability be characterized in a more explicit, objective and *measurable* way.

To account for the multi-faceted nature of the interoperability domain, we propose four sets of measures that address the following aspects of this challenging problem space:

- Technical compliance measures
- Systems interoperability measures
- Operational interoperability measures
- Organizational and cultural measures

The first three sets of measures are discussed in the context of the Levels of Systems Interoperability (LISI) Model. This evolving model is described below in section 5.1, and sections 5.1.1 to 5.1.2 describe proposed approaches for addressing the measurement areas listed in the first three bulleted items above.

In addition, it is now generally accepted that management must be able to measure what they wish to change. Achieving large-scale cultural change (that is required to bring about interoperability) requires commensurate change in management and the organizational measures of performance. In section 5.2, we recommend a starter set of important management measures for assessing progress related to interoperability. Finally in section 5.3, we briefly discuss tradeoff considerations that must be factored in as part of the challenge to promote systems interoperability.

5.1 Levels of Information Systems Interoperability

The Levels of Information Systems Interoperability (LISI) project was initiated in 1993 by MITRE, the C4ISR Integration Task Force, and the ACC Architecture Working Group [C4ISR 98]. LISI is a reference model and process for assessing information systems' interoperability required. It is a discipline and a process for defining, measuring, assessing, and certifying the degree of interoperability required or achieved between organizations or systems.

[5] For example, Office of the Secretary of Defense, Joint Chiefs of Staff, and the service chiefs as the policy makers, allocators of resources, and acquirers.

LISI assesses the level of interoperability attained between systems (not between users). Once system-to-system interoperability issues have been isolated, the ability to address user interoperability issues is vastly improved (e.g., can now effectively measure which user problems are related to: functional training needs/shortfalls, differing operational methods & procedures, and difficulties in user-to-computer interactions). See Figure 5 (adapted from [Hamilton 2000]).

LISI uses a common frame of reference and measure of performance. LISI applies throughout the information system life cycle, i.e., from requirements analysis through systems development, acquisition, fielding, and subsequent improvement and modification. In this context, LISI

- facilitates a common understanding of interoperability and the suite of capabilities that enable each logical level of system-to-system interaction
- provides an interoperability maturity model and associated requisite capabilities as the basis for making comparisons between heterogeneous systems and maturing individual systems
- provides a methodology for assessing and improving interoperability by guiding requirements and architecture analysis, systems development, acquisition, fielding, and technology insertion

Figure 6 presents an overview of the LISI Interoperability Maturity Model. This Model identifies the stages through which a system should logically progress, or "mature," in order to improve their capabilities to interoperate. LISI considers five increasing levels of sophistication regarding system interaction and the ability of the system to exchange and share information and services. Each higher level represents a demonstrable increase in capabilities over the previous level of system-to-system iteration.

A critical element of interoperability assurance is a clear prescription of the common suite of requisite capabilities that must be inherent in *all* information systems that desire to interoperate at a selected level of sophistication.

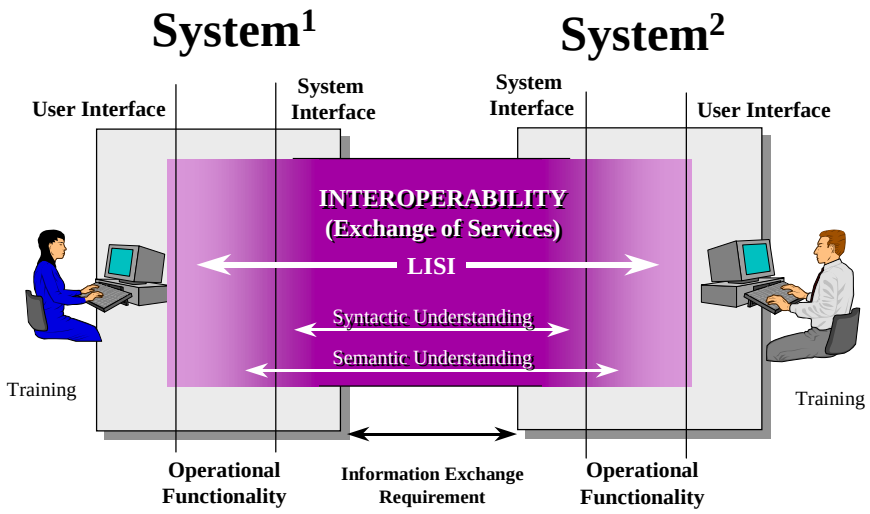


Figure 5. LISI scope of analysis.

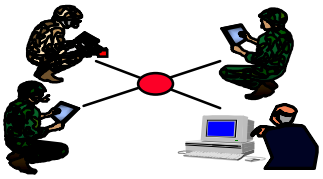
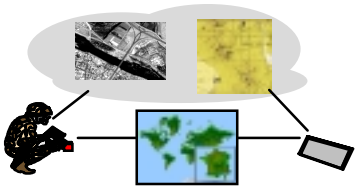
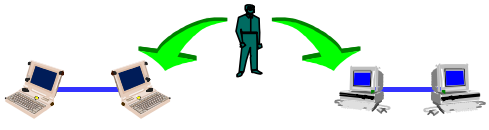
Information Exchange	Level	Computing Environment
• Distributed global information and applications • Simultaneous interactions with complex data • Advanced collaboration, e.g. interactive COP update • Event-triggered global database update	4 Enterprise Interactive manipulation; shared data and applications	
• Shared databases • Sophisticated collaboration, e.g., Common Operating Picture	3 Domain Shared data; "separate" applications	
• Heterogeneous product exchange • Basic collaboration • Group collaboration, e.g., exchange of annotated imagery, maps with overlays	2 Functional Minimal common functions; separate data and applications	
• Homogeneous product exchange, e.g., FM voice, tactical data links, text files, transfers, message, e-mail	1 Connected Electronic connection; separate data & applications	
• Manual gateway, e.g., diskette, tape, hard copy exchange	0 Isolated Non-connected	

Figure 6. Overview of the LISI Interoperability Maturity Model.

Each level's prescription of capabilities must cover all four enabling attributes of interoperability, namely:

P	Procedures	Policies and procedures govern a systems development through established standards and the procedures and processes which influence system integration and functional operational requirements
A	Applications	The functions a system is intended to perform. These functions reside most often in the form of user-based application programs which perform or support a specific set of processes or procedures.
I	Infrastructure	The infrastructure required to support the systems operations. Contains four sub-components which are also defined in terms of increasing levels of sophistication.
D	Data	The data and information structures used to support both the functional applications and system infrastructure.

In addition, for each prescribed capability, system developers need to know what implementation options are available, and which options conform with prevailing DoD criteria. The LISI Capabilities Model and its associated Implementation Options Tables identify the full suite of capabilities and available technical implementations, for attaining each level of interoperability. Figure 7 summarizes the LISI Reference Model and shows the relationship of the PAID attributes.

			Interoperability Attributes			
Description	**Computing environment**	**Level**	P	A	I	D
Enterprise	Universal	4	Enterprise level	Interactive	Multiple dimensional topologies	Enterprise model
Domain	Integrated	3	Domain level	GroupWare	World wide network	Domain model
Functional	Distributed	2	Program level	Desktop automation	Local networks	Program model
Connected	Peer-to-Peer	1	Local/site level	Standard system drivers	Simple connection	Local
Isolated	Manual	0	Access control	N/A	Independent	Private

Figure 7. LISI Reference Model.

Figure 8 (below) presents a general overview of the major elements that comprise LISI. LISI provides an assessment process for determining the interoperability maturity level or "measure" of a given system or system pair. (Note in Figure 8 that *Interoperability Metrics* is included as one of the LISI assessment products.)

	LISI Element	Description
LISI Assessment Basis	Interoperability Maturity Model	Defines the five levels of interoperability expressed within LISI. The LISI interoperability Maturity Model describes the increasing sophistication of system-to-system interactions as one progresses from one level to the next.
	Reference Model	Characterizes the five levels of interoperability in terms of four comprehensive, integrated attributes: procedures, applications, infrastructure, and data (**PAID**). At any particular level of interoperability, a set of specific capabilities must be present for each attribute in order to achieve the degree of interoperability maturity defined by that level.
	Capabilities Model	Defines the specific capability thresholds, i.e., capability suites across **PAID,** required for attaining each level of interoperability. This model provides the level of detail needed to determine systems interoperability profiles and measures, and provides the basis for conducting LISI assessments.
	Implementation Options Tables	Captures the full range of possible implementation choices that are available to developers for implementing each of the capabilities identified in the Capabilities Model.
LISI Assessment Products	Interoperability Profiles	The interoperability profile for a particular system is produced as a results of completing the LISI questionnaire. This profile contains the specific implementation choices made by a particular developer regarding a specific system or application.
	Interoperability Metrics	Calculated by applying the Capabilities Model to the data collected from the questionnaire. Through this mapping, a profile emerges which depicts the organized set of capabilities exhibited by a system in terms of the LISI levels. The result is a “measure” which captures the level of interoperability that a system possesses.
	Comparison Tables	These LISI products are developed via comparison and assessment of the interoperability profiles and measures for a given suite of systems.
	Architecture Products	

Figure 8. Overview of the LISI Elements (Adapted from [C4ISR 98]).

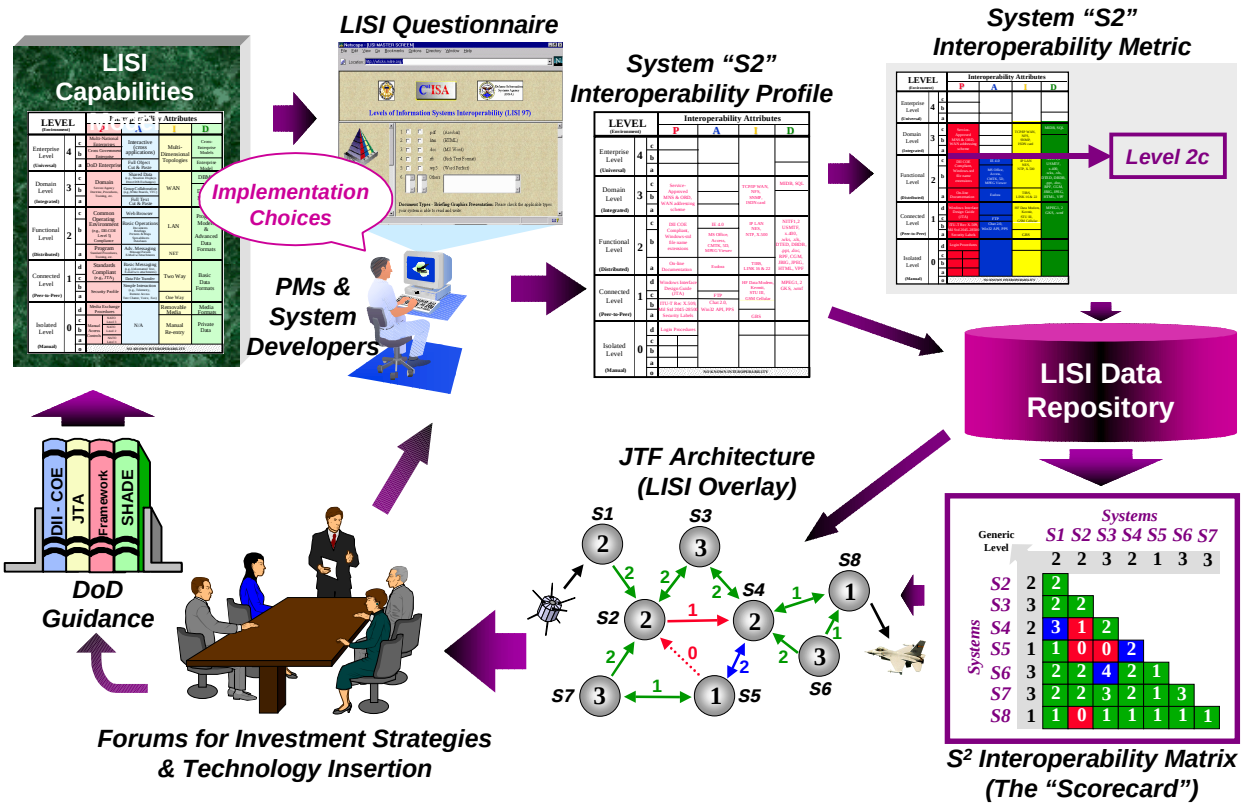


Figure 9. The LISI Interoperability Assessment Process (Adapted from [C4ISR 98]).

Using the LISI approach, interoperability measures could be deduced using a scorecard method. (See Figure 9 that shows a contextual diagram of the LISI Interoperability Process.) In the absence of precise measures and recognizing the multidimensionality of interoperability, it is reasonable to use scorecard techniques based on human judgment to capture how well a unit (or DoD as a whole) is doing with respect to

- technical compliance (represented in Figure 4 as 'the System "S2" interoperability)
- system-to-system interactions (represented in Figure 4 as the "S^2 Interoperability Matrix")
- operational mission effectiveness (represented in Figure 4 as the "JTF Architecture [LISI Overlay"])

5.1.1 Measuring Technical Compliance

The technical view of an architecture focuses on the criteria governing the implementation of specific system capabilities or attributes. From an assessment perspective, the concern is whether a given system's implementation complies with the applicable standards and guidelines. Therefore, a technical scorecard could be viewed as a list of systems with ratings (pass/marginal/fail) of compliance with the relevant standards and guidelines.

The purpose of the LISI measure is to capture the essence of potential interactions available between systems, as registered through the implementation choices made by developers. The measure is therefore a direct reflection of the comparison of interoperability provided between systems.

The LISI measure provides a shorthand definition of the particular form of interoperability as expressed in the LISI maturity model. The measure comes in various flavors based on the nature, purpose, and

approach to performing and displaying the results of the comparisons. An example of the various options for describing LISI measures is shown in Figure 10 (Adapted from [C4ISR 98, p. 4-3].).

The main distinction among the three types of LISI measures is the comparison of a single system against the capabilities model (***generic***) and the two different cases where two or more systems are compared to each other (*expected* and *specific*). The ***expected*** level of interoperability between two systems is simply the lesser of the two systems' generic levels, i.e., the level at which one would *expect* the two systems to interoperate. The ***specific*** level of interoperability is the calculated measure between two systems as a results of comparing the specific implementation choices that each system has made regarding the registered PAID capabilities. The *specific* level may be different than the expected level based on the added use of the LISI Options Tables and the consideration of the technical implementation criteria. These are more formally defined elsewhere [C4ISR 98, p. 4-4].

		Code
Metric type	Generic	G
	Expected	E
	Specific	S
Level	Enterprise	4
	Domain	3
	Functional	2
	Connected	1
	Isolated	0
Sublevel	Varies by levels; defined as "a" through "z"	a-z

Figure 10. The LISI interoperability measures.

As an example[6], using the measures in Figure 10, consider that a system assessment was conducted and the LISI measure obtained was "G2c." Such a rating of the inherent characteristics of this system would mean the system or application has a *generic level* of "2c." Therefore

- It complies with JTA and DII-COE
- It can operate on a LAN
- Its environment is built within a GUI
- It supports common office functions
- Its database information is compliant with a particular functional program.

The LISI measure obtained from these comparisons can be represented in several formats, including those described in Figure 11. Figure 12 shows the example populated interoperability profile for this system. In this example, the system's generic interoperability level is 2c, the highest level at which a capability is implemented for each of the **PAID** attributes.

Format	Description	Examples
Summary LISI measure	Only the major level and/or sublevel is shown.	G2, E3, G2b, S3C
Detailed LISI measure	Individual values of PAID are each portrayed as separate components within the measure	G2(P3A2I3D2) S1b(P3a, A2c, I2b, D1b)

Figure 11. Possible formats for LISI measure.

[6] Adapted from [C4ISR 98, p. 4-3].

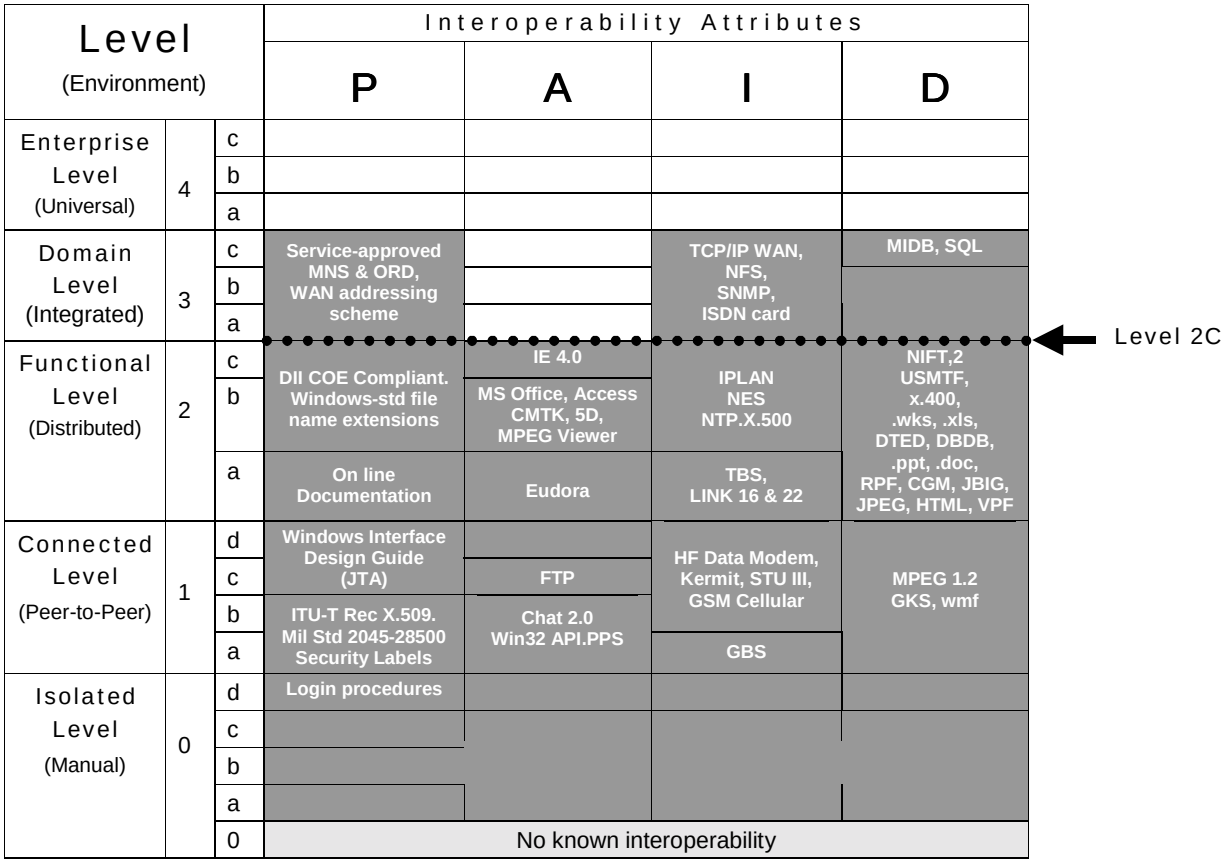


Figure 12. Example populated interoperability profile for a system that's rated 2c.

In addition to the LISI measure, others have defined architectural attributes that could serve as indicators of interoperability. These appear in Figure 17 in the appendix on page 33.

5.1.2 A Potential Systems Interoperability Scorecard

The systems view of an architecture focuses on the information and communications systems that are brought to bear to support the information flows required to accomplish operational missions. The Systems Interoperability Scorecard attempts to measure the degree to which the various system pairs can effectively interoperate in context to meet these information flow requirements.

A potential interoperability matrix can be generated for a group of systems based on the generic interoperability level of each system and the specific interoperability level for each system pair with the group (See Figure 13 below). In this view, a scorecard used to measure interoperability from a systems perspective would derive from a codified (or de facto) system architecture, and would focus on the ability of the systems in each pair to interact with one another. The scorecard could be viewed as a matrix with the systems represented in both the rows and columns and entries indicating system-to-system interoperability as inadequate (red), marginal (yellow), or adequate (green).

	S1	S2	S3	S4	S5	···	S_n
S1							
S2	G						
S3	Y	R					
S4	Y	G	N/A				
S5	G	G	R	Y			
.	⋮	⋮	⋮	⋮	⋮		
S_n	G	Y		G	G		

Figure 13. Example systems operability scorecard (Adapted from [Committee 99]).

5.1.3 Measuring Operational Interoperability

The operational view of an architecture addresses particular mission slices, such as targeting, close air support, force sustainment, or the like, of a broader operational setting. Within each slice, it could capture the players involved and their interactions, their functions, decisions, actions, and the flows of information postulated to support their particular roles in achieving overall mission effectiveness.

The review of a system's Operational Requirements Document will determine the existence of system interoperability requirements. (Note: system interoperability is discussed in the last section.) The first step in measuring compliance of these requirements is to trace the requirements through the system functions. This may be accomplished by the development of "operational threads" (system node connectivity or link/node diagrams) or paths between the systems. The threads are identified, traced, and developed in order to measure and quantify system interoperability [Leite 98].

A scorecard used to assess interoperability (see Figure 14) from an operational architecture perspective would focus on the ability to satisfy specific node-to-node information flow requirements (that describe the nature of the information and services needed, its directional flow, and the constraints and demands imposed by the operational environment. The assessed degree to which each flow requirement is met can be scored using green/yellow/red ratings. These measures are often derived from lessons learned through crises or exercises including observed events and anecdotal feedback [Committee 99].

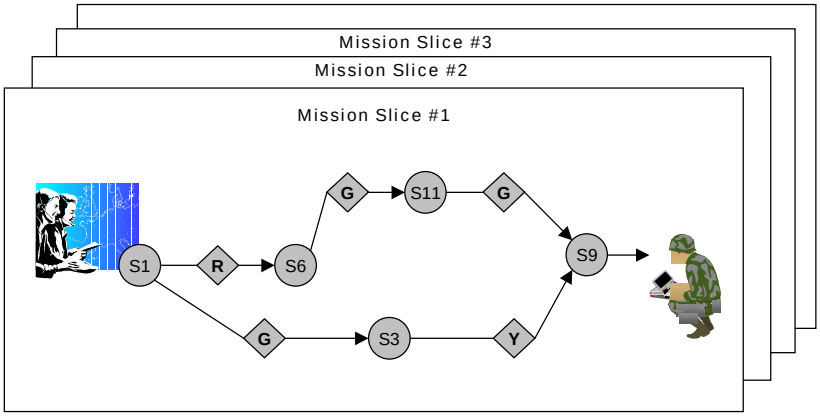


Figure 14. Example of an operational interoperability scorecard (Adapted from [Committee 99]).

It is possible to estimate and measure important quality attributes associated with interoperability at this level. Leite has defined these relationships and they are summarized below [Leite 98]. The mathematical relationships for each of these measures are defined in the Appendix, beginning on page 34.

Attribute Measure	Description
Connectivity	Connectivity can be directly measured by counting the number of messages initiated by all participating units and the number of messages received for the network or data link. To the extent that the link is in continuous operation, the connectivity sampled in this manner is representative of network connectivity. If the network is operated intermittently, then the sample must be carefully selected and tested to ensure that the required confidence level is attained.
Capacity	The capacity of a system is the rate at which data may be passed over time. Given its operating parameters, a maximum data rate can be calculated for any system or group of systems.
System overload	A system overload occurs when more data must be exchanged than the system is able to transmit. Typically, the overload is placed in a queue and is then transmitted when capacity is available. Therefore, the measure of system overload is the sum of the messages remaining in queues after their assigned transmission period for all system nodes.
Underutilization	This occurs when the system data rate/message load is less than its full capacity but messages are waiting in queues to be transmitted. This occurs when the item slot or transmission allocation to selected nodes is less than that required to clear the queue by the end of a transmission period. Similarly other nodes do not use all of their allocated time.
Undercapacity	Undercapacity occurs when messages remain in queues and the system data rate is at the maximum.
Data latency	Data latency is the elapsed time from the time of the event to the time of receipt by the user (tactical data processor). For analytical purposes, the latency is often divided into smaller segments. Several common time periods are the following: • time of event to time of observation • time of observation to completion of processing • completion of processing to time of receipt at the tactical data processor This division is useful in situations involving a remote sensor and intermediate processing to reduce the data to a usable form (track message) prior to passing the data to the user. These relationships are expressed as follows.
Information interpretation and utilization	Having passed the data and correctly interpreted it, the next step would be to verify that the proper action is taken. Verification of the action taken involves a review of the logic associated with every option that is possible in response to a message or operator action. These deal, of course, with questions of interoperability and not with the difficult, higher-level topic of measuring mission effectiveness.

5.2 Management Measures Associated With interoperability

The magnitude of the technology-driven transformation required to achieve interoperability points to the enormity of the institutional challenges associated with the transformation. The Committee to Review DoD C4I Plans and Programs found that "achieving C4I interoperability is more a matter of organizational commitment and management[7] than one of technology."

Adequate C4I interoperability is inherently a distributed, horizontal challenge that must be addressed in a largely vertical world. Enabling fast and effective responses to this challenge requires that interoperability be built into the force structure across service and unit boundaries. This means that there must be incentives and rewards for investments and actions across organizational boundaries. Crossing these boundaries is particularly important to the development and fielding of systems that support joint operations. The DoD must search for practical ways to reward interoperability.

Measures are important to senior decision-makers. The Information Technology Reform Act (ITMRA) of 1996 (Public Law 104-106), also known as the Clinger-Cohen Act, requires the Federal government to develop

> "a process and procedure for establishing goals for improving the efficiency and effectiveness of government agencies operations and the ability to deliver goods and services to the public using Information Technology. The goals must be measurable."

Achieving large-scale cultural change in an organization to achieve C4I interoperability requires commensurate change in management and the organizational measures. In large organizations, the behavior of personnel is strongly influenced by the measures that management uses to assess performance, whether those measures are part of a formal assessment or are more perceived than formal. People are keenly aware of what matters in terms of rewards, promotion, credit, etc., and they behave in a manner consistent with their perceptions. Good management measures help to drive organizational behavior that supports areas of operational significance. In general, management measures focus on organizational performance or characteristics and are used by senior management to assess the effectiveness of the organization and its leadership.

The Committee to Review DoD C4I Plans and Programs has identified the following list of possible management measures to promote interoperability across the board:

- Number of C4I systems that conform to the Joint Technical Architecture
- Number of individuals trained in the use of specific C4I systems
- Number of C4I systems "certified" to be interoperable
- Time or personnel required to develop time-phased force and deployment data or an air tasking order
- Time needed to stand up a tactical network for a joint task force

[7] Including allocation of resources, attention to detail, and continuing diligence.

5.3 Summary of Recommended Measures

In this section, we provide a summary of recommended measures that have been organized into the Practical Software Measures (PSM) Issue-Category-Measure (ICM) structure [PSM 98].

Specific Issues	Common Issue Area	Measurement Category	Recommended Measure
Compliance with standards	Technical Adequacy	Technical Performance	LISI ***generic*** level of interoperability
Systems interoperability	Technical Adequacy	Technical Performance	LISI ***expected*** level of interoperability
Operational interoperability	Technical Adequacy	Technical Performance	LISI ***specific*** level of interoperability
Operational interoperability	Technical Adequacy	Technical Performance	Connectivity[†]
Operational interoperability	Technical Adequacy	Technical Performance	Capacity[†]
Operational interoperability	Technical Adequacy	Technical Performance	System Overload[†]
Operational interoperability	Technical Adequacy	Technical Performance	Underutilization[†]
Operational interoperability	Technical Adequacy	Technical Performance	Undercapacity[†]
Operational interoperability	Technical Adequacy	Technical Performance	Data latency[†]
Operational interoperability	Technical Adequacy	Technical Performance	Information interpretation and utilization
Management commitment	Schedule and Progress	Milestone Performance	Number of C4I systems that conform to the Joint Technical Architecture
Management commitment	Schedule and Progress	Milestone Performance	Number of C4I systems "certified" to be interoperable
Management commitment	Development Performance	Productivity	Time needed to stand up a tactical network for a joint task force
Management commitment	Development Performance	Productivity	Time or personnel required to develop time-phased force and deployment data or an air tasking order
Management commitment	Resources and Cost	Personnel	Number of individuals trained in the use of specific C4I systems

[†] For a formal definition of this measure, refer to Appendix D beginning on page 34.

5.4 Tradeoff Analysis

Although interoperability is a critical enabler for military operations, interoperability must be recognized as just one of several technical attributes of any system of systems. Military commanders need many things from their C4I systems besides interoperability, and trade-offs among these needs are often required. Other attributes will sometimes be in competition with interoperability and with each other. In thinking about overall system functionality or performance, security requirements such as confidentiality, authentication, non-repudiation, integrity, and system availability must be considered together with interoperability. An appropriate balance must be sought. (For example, there are trade-offs between security and interoperability. Interoperability can promote an attacker's access to diverse systems, thus facilitating the rapid spread of attacks.)

6. Recommendations

The following recommendations are made for further exploring into this area:

- Fully investigate the efforts that are being undertaken to track interoperability on a comprehensive basis[8]. This includes investigating the maturity and use of LISI as a framework to assess interoperability.
- Careful analysis of results from well-instrumented simulations and exercises is needed to evaluate trade-offs between interoperability and other fundamental attributes of C4I systems, including security, availability, flexibility, survivability, and performance.
- Examine scenario-based assessment and architectural style based assessment as a way to better understand interoperability measures and the trade-offs involved between other quality attributes of a system.[9] Investigate appropriate interoperability measures using the Architecture Tradeoff Analysis Method (ATAM) [Kazman 00].
- Explore the use of multivariate analysis to take into account the likely interdependence of various interoperability measures and competing system quality attributes.
- Assess the current use of statistically designed experiments that are being used to assess interoperability. Possibly explore ways to improve upon the current state of practice (e.g., the use of 2^n factorial experimental designs to expose masking and confounding by multiple system attributes).

[8] The Committee to Review DoD C4I Plans and Programs determined that despite laudable case-by-case efforts to track interoperability, there is today no method for tracking interoperability on a comprehensive or systematic basis [Committee 99].

[9] Investigations in this area would be based on foundational work described by Bass et al, Barbacci et al. and Taylor. [Bass 93, Barbacci 95, Taylor 00].

7. References

[Army 96] Army Digitization Office. “Army Digitization Master Plan, 1996.” Army Digitization Office, Washington, D.C. March 1996.

[Bernstein 96] Bernstein, Philip A. “Middleware: A Model for Distributed Services.” Communications of the ACM 39, 2 (February 1996): 86-97.

[Barbacci 95] Barbacci M., Klein, M., Longstaff, T., Weinstock, C. “Quality Attributes.” Technical Report CMU/SEI-95-TR-021. December 1995.

[Bass 98] Bass, L., Clements P., Kazman R. “Software Architecture in Practice.” Addison Wesley Longman, Inc. 1998.

[Cetus 00] Cetus Links, CORBA Links. Available at <http//:www.cetus-links.org/oo_corba.html>

[Chairman 96] Chairman of the Joint Chiefs. “Joint Vision 2010.” Joint Chiefs of Staff, Washington D.C. 1996.

[Chairman 00] Chairman of the Joint Chiefs. “Joint Vision 2020.” Joint Chiefs of Staff, Washington D.C. 2000. Available online at <http://www.dtic.mil/jv2020/jvpub2.htm>

[Chatfield 98] Chatfield, J., Enyeart, C., and Ficks, W. “New Architecture Directions.” *The Edge Newsletter*. January,1998. Available online at <http://www.mitre.org/pubs/edge/january_98/fifth.htm>

[Cherkaoui 99] Cherkaoui, O., Rico, N., Serhrouchni, A. “SNMPv3 can still be simple?” pp 201-515. In *Integrated Network Management*, 1999.” Distributed Manager Networked Millennium. Proceedings of the Sixth IFIP/IEEE International Symposium. May 1999.

[C4ISR 97] C4ISR Integration Task Force. 1997. “C4ISR Integration Task Force Executive Report.” p. 27. Department of Defense, Washington, D.C.1997.

[C4ISR 98] C4ISR Architecture Working Group, “Levels of Information Systems Interoperability (LISI).” 1998. Available online at <http://www.c3i.osd.mil/org/cio/i3/AWG_Digital_Library/>.

[Committee 99] Committee to Review DoD C4I Plans and Programs. “Realizing the Potential of C4I.” National Academy Press. Washington, D.C. 1999.

[CSTB 94] Computer Science and Telecommunications Board, National Research Council. “Realizing the Information Future: The Internet and Beyond.” National Academy Press, Washington, D.C. 1994.

[Dept. AF 96] Department of the Air Force. “Global Engagement: A Vision for the 21st Century.” Department of the Air Force, Washington, D.C.; Air Force Experimentation Office EFX Public Web Site, available online at <http://efx.acc.af.mil>. 1996.

[Dept. Army 96] Department of the Army. “Army Vision 2010.” Department of the Army, Washington, D.C. 1996.

[Dept. Navy 96] Department of the Navy. “Forward...From the Sea.” Department of the Navy, Washington, D.C. 1996.

[DISA 96] The Defense Information System Agency. “Defense Information Infrastructure (DII) Shared Data Environment (SHADE) Capstone Document.” 1996. Available online at <http://diides.ncr.disa.mil/shade>.

[DoD 91] Department of Defense Directive 8230.1-M. “DoD Data Administration.” 1991.

[DoD 95] Chairman of the Joint Chiefs of Staff, Instruction 6212.01A: “Compatibility, Interoperability, and Integration of Command, Control, Communications, Computers, and Intelligence Systems.” June 1995.

[DoD 96] DOD Directive 5000.1, “Defense Acquisition,” March 15, 1996.

[DoD 98] Joint Chiefs of Staff. “Department of Defense Dictionary of Military and Associated Terms, as amended through December 7, 1998” (Joint Publication 1-02)

[DoDD 2010.6 77] “DODD 2010.6 Standardization and Interoperability of Weapon Systems and Equipment Within the North Atlantic Treaty Organization (NATO).” 11 March 1977.

[Eldridge 78] Eldridge, Ingrid A. “Interoperability Via Emulation.” Proceedings of the 1978 Summer Computer Simulation Conference July 24-26, 1978, Los Angeles, California.

[GAO 98] General Accounting Office. “Joint Military Operations: Weaknesses in DoD’s Process for Certifying C4I Systems’ Interoperability.” GAO/AIMD-98-257, General Accounting Office, Washington, D.C. 1998.

[Hamilton 2000] Hamilton, John A. “Joint Interoperability from the Service C4I Systems Command.” Proceedings of the Software Technology Conference 2000. Salt Lake City, Utah, April, 2000.

[IEEE 90] “IEEE Standard Glossary of Software Engineering Terminology,” IEEE Std 610.12-1990.

[JCS 00] Joint Chiefs of Staff. “Information Superiority Campaign Plan.” Washington D.C. Available online at <http://www.dtic.mil/execsec/adr98/apdx_k.html>

[JINTACCS 74] “JINTACCS Interoperability.” ref-PM99 21 DEC 1974 HQDA.

[JITC 00] Available online at <http://jitc/fhu.disa.mil/testing/interop/interop.html>

[JTAMDO 97] Joint Theater Air Missile Defense Organization (JTAMDO). “JTAMDO Master Plan.” JTAMDO, Joint Staff, Department of Defense, Washington, D.C., Chapter 7. 1997.

[Kalyanasundaram 98] Kalyanasundaram, S., Ponnambalam, K., Singh, A, Stacey, B, Munikoti, R. “Metrics for Software Architecture: A Case Study in the Telecommunication Domain.” Proceedings of IEEE Canadian Conference on Electrical and Computer Engineering. May 24-28, 1998. pp. 715-718, Volume 2. 1998.

[Kang 98] Kang, Sungwon. “Relating Interoperability Testing With Conformance Testing.” Global Telecommunications Conference, 1998. GLOBECOM Global Integration. IEEE. 1998.

[Kazman 00] Kazman, R., Klein, M., Clements, P. “ATAM: Method for Architecture Evaluation.” SEI Technical Report CMU/SEI-2000-TR-004. Pittsburgh, PA. 2000.

[Koyak 99] Koyak, Robert A. “Research Opportunities in Joint Interoperability Testing.” Defense Information Systems Agency. Joint Interoperability Test Command. Fort Huachuca, AZ. September 1999.

[Marine 96] U.S. Marine Corps. “Operational Maneuver from the Sea.” Headquarters, Marine Corps, Washington, D.C. 1996.

[McCall 80] McCall, James A. “An Assessment of Current Software Metric Research.” EASCON ’80. 1980. pp 323-333.

[NIMA 98] National Imagery and Mapping Agency, “USIGS Technical Architecture, Revision A.” September 1998.

[Office of Under Sec1 99] Office of the Under Secretary for Acquisition and Technology. “Battlefield Awareness and Data Dissemination.” Office of the Under Secretary for Acquisition and Technology, Department of Defense, Washington, D.C. 1999. Available online from <http://www.acq.osd.mil/at/badd.htm>.

[Office of Under Sec2 99] Office of the Under Secretary for Acquisition and Technology. “Extending the Littoral Battlespace.” Office of the Under Secretary for Acquisition and Technology, Department of Defense, Washington, D.C. 1999. Available online from <http://www.acq.osd.mil/at/eld.htm>.

[OMG 98] Object Managagement Group. “CORBAIIOP 2.2 Specification.” Updated July 1998. <http://www.omg.org/corba/corbaiiop.html>. 1998.

[Presson 83] Presson, Edward P. “Software metrics and interoperability.” Proceedings of AIAA Computers in Aerospace IV Conference. Hartford, Connecticut. 1983.

[PSM 98] Office of the Under Secretary of Defense for Acquisition and Technology. “Practical Software Measurement: A Foundation for Objective Project Management” Office of the Under Secretary for Acquisiiton and Technology, Department of Defense, Washington, D.C. 1998. Available online from <http://www.psmsc.com/>

[SEI 00] Software Engineering Web page: “Software Technology Review: Middleware.” Available at <http://www.sei.cmu.edu/str/descriptions/middleware.html>

[Taylor 00] Taylor R. “Identification of Emergent Properties in a Federation.” DERA/CIS/CIS3/TR000143. Defence Evaluation and Research Agency, UK. February, 2000.

[TMD Plan 98] Deputy for Theater Air & Missile Defense, Ballistic Missile Defense Office. “Theater Missile Defense (TMD) Family of Systems (FoS) Interoperability Program Plan (IPP). Office of the Secretary of Defense, Ballistic Missile Defense Organization. Washington, D.C. 1998

8. Acronym List

ACTD	Advanced Concept Technology Demonstration
AOI	Area of Interest
ATAM	Architecture Tradeoff Analysis Method
BADD	Battle Field Awareness and Data Dissemination
C3I	Command, Control, Communications and Intelligence
C4I	Command, control, communications, computers, and intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CINC	Commander-in-Chief
CORBA	Common Object Request Broker Architecture
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DoD	Department of Defense
ELB	Extending the Littoral Battlespace
HTML	hypertext markup language
HTTP	hypertext transfer protocol
ICM	Issue, Category, Measure
ITMRA	Information Technology Reform Act
JINTACCS	Joint Interoperability of Tactical Command and Control System
JTA	Joint Technical Architecture
JTF	Joint Task Force
JV2010	Joint Vision 2010
JV2020	Joint Vision 2020
LISI	Levels of Systems Interoperability
PSM	Practical Software Measures
TCP/IP	Transmission Control Protocol/Internet Protocol

Appendix

Appendix A: Some historical definitions of *interoperability*

A number of reports and technical papers have defined interoperability in different ways:

> "The effort required to couple one system with another" [McCall 80].
>
> "The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together" [DoDD 2010.6 77].
>
> "The ability of one services' system to receive and process intelligible information of mutual interest transmitted by another service's system" [JINTACCS 74].
>
> "The ability of one system to receive and process intelligible information of mutual interest transmitted by another system" [Eldridge 78].
>
> "The ability of two or more systems or components to exchange information and to use the information that has been exchanged" [IEEE 90].

There are problems with McCall's definition. Here, "coupling" includes linking two programs to interoperate on a single computer or linking programs on separate computers to interoperate. The quality factor, interoperability, is therefore important when:

1) retrofitting two or more previously developed systems into one system;
2) developing new systems independently that will interoperate with each other; or when
3) developing a system with the expectation that it will eventually interoperate with an, as yet, undefined future system.

The definition, taken literally, includes only the connectivity and compatibility issues of interoperability; it implies only equipment-level considerations. But hardware compatibility does not assure interoperability. For example, two persons using exactly the same transmitters on the same frequency may not be able to interoperate, particularly if one person speaks only English, the other speaks only Arabic. Interoperability is achieved when both persons can transmit and receive information of mutual use and understandability.

Eldridge's definition of interoperability is also unsatisfactory because it stresses standardization. The emphasis on standardization of hardware and software overlooks the content of the messages and the differing operational requirements that affect interoperability.

The JINTACCS and DoDD 2010.6 definitions are preferable. These definitions seem to most accurately define the ultimate meaning of interoperability—as a broad and complex subject rather than a binary attribute of systems.

More recently, the Joint Chiefs of Staff Publication 1-02 defines interoperability in a way that acknowledges the technical and operational components that contribute to a more meaningful interpretation.

Appendix B: Testing Interoperability

A essential underpinning of C4I interoperability is architecture and the resultant requirements specification. Testing compares actual performance with requirements. Ensuring that the architecture and requirements are in fact successfully implemented, and that the required level of interoperability is achieved requires comprehensive testing and evaluation.

Testing can take place in a laboratory, a field location, or at an individual's workstation (with early system designs). Typically, systems are tested at different stages in their life cycle, during (1) development, (2) preproduction, and (3) in the field.

Developmental testing	Assesses progress in meeting system-level requirements ranging from functionality to performance. To ensure correct intent, a system's "paper" requirements may be tested against user-stated needs.
Preproduction testing	*Conformance testing* focuses on the stand-alone functionality and performance of a particular system in terms of stated requirements (through a paper or laboratory test). *System-to-system testing* determines how well a system interoperates with other systems. It is typically performed in a laboratory where two or more systems can be interconnected. Its scope can range from "lower-layer" (e.g., communications) to "higher-layer" (e.g., applications and data) interoperability.
Field testing	Assesses the extent to which a system satisfies users' operational needs in a "real-world" setting. *Functional testing* involves configuring systems to meet the unique demands of particular customers, integrating products with the embedded base of systems, and evaluating the resulting system of systems from the end-to-end functional perspective. *Follow-on testing* assesses a system's performance after it has been fielded, reverifying interoperability periodically or as changes occur and providing a mechanism for tracking progress in addressing known problems.

Leite proposes the test assessment method that is summarized in Figure 15 [Leite 98] on page 31.

Testing should be seen as an integral part of requirements definition and system development. Thus testing must be essentially continuous, and "stability" is a state that is never reached in any meaningful sense. Without ongoing feedback, initial implementations of processes and systems may interoperate satisfactorily at first, but not later [Committee 99].

Often, requirements are strong in specifying behavior under ideal conditions but weak about what should happen under adverse situations (e.g., what the response of a system to a failure somewhere should be).

Many interoperability problems are subtle, manifesting themselves only in certain sets of circumstances, and so are hard to uncover, and they demand a great deal of empirical work and testing to resolve. Research on the theory and practice of interoperability testing has begun only very recently and it is scarce [Kang 98].

Appendix B: Testing Interoperability, continued

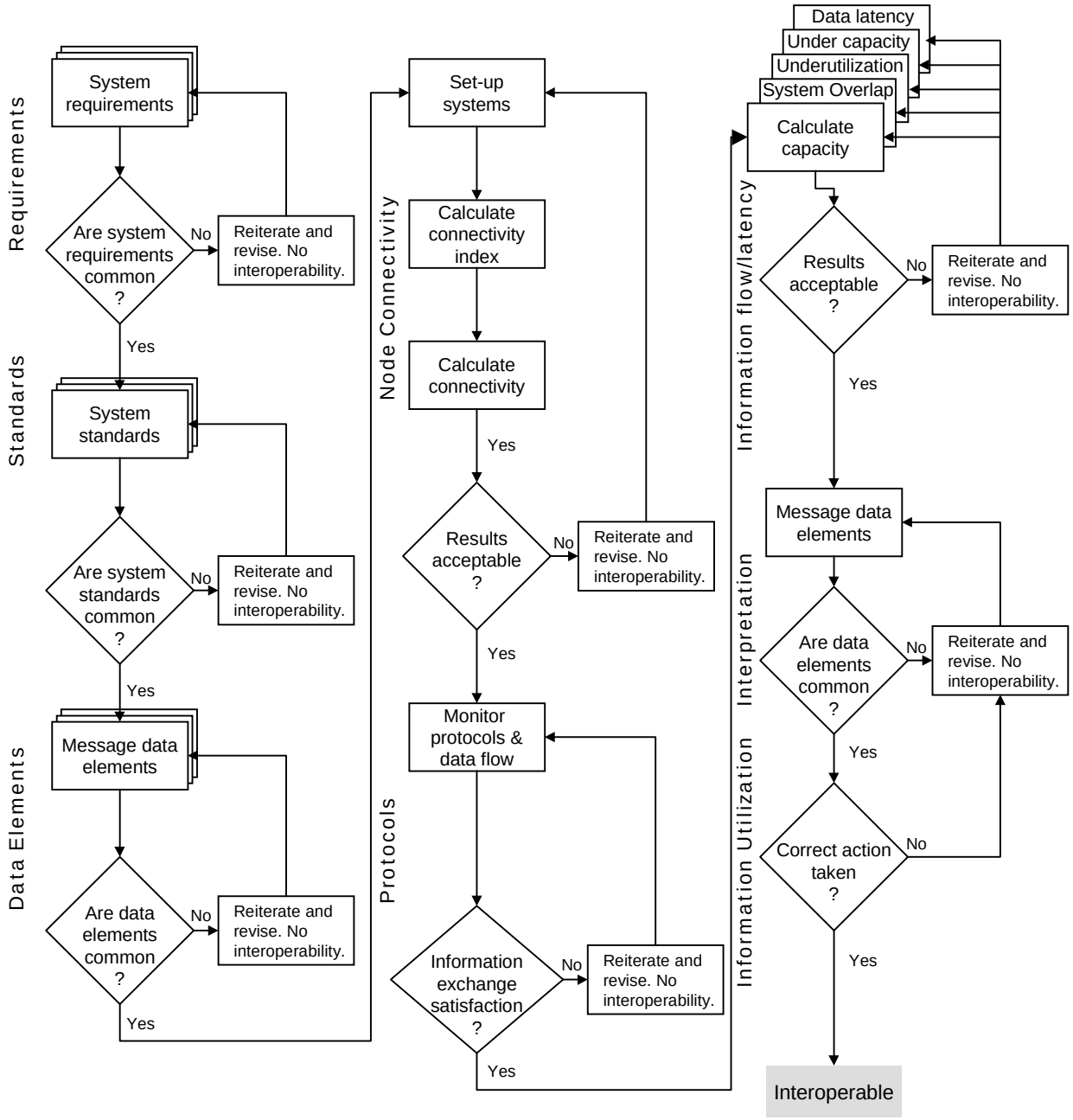


Figure 15. Interoperability Assessment Process (Adapted from [Leite 98]).

Appendix C: Potential Measures of Interoperability

Figure 16 and Figure 17 list potential measures (proposed by other authors) that may provide insight into interoperability.

Category	Measures
Standards	standards explicitness
	standards maturity
	standards vendors supporting
	standards feature coverage
	standards sufficiency
Profiles	profile explicitness
	profile width
	profile coverage
	profile extensions
	us during product selection
	profile sufficiency
	profile documentation
Products	products available supporting
	product performance
	platforms supported
Conformance	degree of conformance
	product-to-product interoperability

Figure 16. Software interoperability categorical measures[10].

[10]This list was generated during a workshop at the Practical Software Measurement (PSM) Annual User's Conference on July 26, 2000.

Appendix C: Potential Measures of Interoperability, continued

Measure	Code	Description
Number of 3rd party components	No3C	The count of the number of components that have been acquired from outside vendors. This measure is a reflection of the 'openness' of the architecture.
Number of components	NoC	The total number of architectural units that can be found in the system of interest. (A measure of the size of the system.)
Number of control components	NoCC	Number of total components that provide logical operations on a given set of input data. An example of control component is a software structure that acts as an iterator. This number is a subset of NOC.
Number of data components	NoDC	Total number of components that are passive in nature. Examples are databases, stacks, shared memory units, etc.
Total number of external interfaces	NoDC	Number of connectors that allow the component to interact with other components outside the system or subsystem. This is an indirect measure that tries to capture the coupling in the system.
Total number of internal interfaces	TNII	The number of connectors that allow components to interact with other components within a subsystem or layer.
Number of specialized components	NoSC	A count of components that are considered to have a high level of system specificity. These components offer specific services, which prohibit their use in any other context. This measure is based on a subjective measure provided by the architects and designers.
Number of functionally critical components	NFCC	Counts the number of components whose failure would affect the systems' functionality drastically. This is a subjective measure provided by the designers.
Number of shared memory components	NSMC	Shared memory is a critical component in large-scale systems with a high level of criticality associated with it.
Number of architectural revisions	NoAR	Represents the number of changes that the architecture has gone though before reaching the current productization level.
Number of interface types	NoIT	In large system, several types of interactions are available. This is a measure of the various interface techniques in the system. The more the NoIT, the higher the complexity.
Number of generic components	NoGC	This is a measure of components, which are 'general' in nature. These components are not domain specific. (The designer would label each component as generic or specialized.)
Number of redundant components	NoRC	In some systems, hardware components as well as software components are replicated to recover during component failures. Redundant components are components that are generally not exercised by the system during normal operation and the components usually mirror functionality of other components in the system that are used extensively. This measure is provided by the system documentation.
Number of concurrent components	NCC	The number of components that operate concurrently. Concurrency is prevalent in real-time telecommunications systems and its effect on the quality of the system is significant.
Number of subsystems	NoSS	Represents the number of units that are logical or physical clusters or components.
Number of services	NoS	The number of different services that are offered by a telecommunication system.

Figure 17. Architecture measures related to interoperability (Adapted from [Kalyanasundaram 98]).

Appendix D: Equations for quality attributes associated with the interoperability scorecard[11]

Connectivity

A connectivity index can be calculated for any communications system. It is a relationship between the number of system nodes and the available paths. The connectivity index is defined by the equation:

$$C_i = \frac{k}{n * (n-1)} \quad (1)$$

Where:

C_i= Connectivity index
k = Number of connections (paths between nodes)
n = Number of nodes (participating units)

Connectivity can be measured directly by counting the number of messages initiated by all participating units and the number of messages received for the network or data link. To the extent that the link is in continuous operation, the connectivity sampled in this manner is representative of network connectivity. If the network is operated intermittently, then the sample must be carefully selected and tested to ensure that the required confidence level is attained.

The general relationship for measuring the connectivity is the following:

$$C = (1/n_r) \times \frac{\sum_{y=1}^{n_r} (M_r)_y}{\sum_{x=1}^{n_t} (M_t)_x} \quad (2)$$

Where:

C = Node Connectivity (during measurement period
n_r = Number of receiving nodes
n_t = Number of transmitting nodes
M_t = Messages transmitted by a node
M_r = Messages received by a node

Information Flow

The volume of data is typically a function of the tempo of operations and the area of interest. The area of interest (AOI) is defined by the operational commander. The tempo of operation is event-driven; however, estimates are possible based on historical and exercise results.

Capacity is a function of the available data links. In practice, multiple links or paths are available. For weapon and combat systems, there is a requirement for primary and back-up paths. The redundancy of data flow limits the total capacity to an amount that is less than the sum of the individual systems.

Several items may be measured or calculated with respect to system performance. They are capacity, system overload and data latency. The relationships for these measures follow:

[11] See Section 5.1.3, “Measuring Operational interoperability” for a discussion of this topic.

❖ Capacity

The capacity of a system is the rate at which data may be passed over time. Given its operating parameters, a maximum data rate can be calculated for any system or group of systems. These relationships are described as follows:

$$Q_{eff} = (Q_{\max} - Q_{oh}) \times (t_f - t_p) \quad (3)$$

Where:

Q_{eff} = Effective system capacity (data rate)
Q_{max} = Maximum data rate
Q_{oh} = System overhead data rate
t_f = Time slot duration (unit transmission)
t_p = Unit propagation time

❖ System Overload

A system overload occurs when more data must be exchanged than the system is able to transmit. Typically, the overload is placed in a queue and is then transmitted when capacity is available. Therefore, the measure of system overload is the sum of the messages remaining in queues after their assigned transmission period for all system nodes.

$$M_{OL} = n_t \times \sum_{y=1}^{n_r} (M_q)_y \quad (4)$$

Where:

M_{OL} = System message overload
n_t = Number of transmitting nodes
M_q = Messages in queue to be transmitted by node

❖ Underutilization

This occurs when the system data rate/message load is less than its full capacity but messages are waiting in queues to be transmitted. This occurs when the item slot or transmission allocation to selected nodes is less than that required to clear the queue by the end of a transmission period. Similarly other nodes do not use all of their allocated time.

$$Q_{uu} = M_{OL} \quad (5)$$

For $M_{OL} \le (Q_{eff} - Q)$

AND

$$Q_{uu} = Q_{eff} - Q \quad (6)$$

For $M_{OL} > (Q_{eff} - Q)$

Where:

Q_{uu} = System Underutilization (data rate)
Q = Measured/observed data rate

(Other terms as previously defined.)

❖ Undercapacity

Undercapacity occurs when messages remain in queues and the system data rate is at the maximum.

$$Q_{uc} = (Q + M_{OL}) - Q_{eff} \quad (7)$$

Must be > 0

Where:

Q_{uc} = System undercapacity (data rate)

(Other terms as previously defined.)

Data Latency

Data latency is the elapsed time from the time of the event to the time of receipt by the user (tactical data processor). For analytical purposes, the latency is often divided into smaller segments. Several common time periods are the following:

- time of event to time of observation
- time of observation to completion of processing
- completion of processing to time of receipt at the tactical data processor

This division is useful in situations involving a remote sensor and intermediate processing to reduce the data to a usable form (track message) prior to passing the data to the user. These relationships are expressed as follows.

$$\overline{\Delta t} = t_r - t_e \quad (8)$$

$$\overline{\Delta t_o} = t_o - t_e \quad (9)$$

$$\overline{\Delta t_m} = t_m - t_o \quad (10)$$

$$\overline{\Delta t_r} = t_r - t_m \quad (11)$$

Equation 8 may be rewritten as:

$$\overline{\Delta t} = \overline{\Delta t_o} + \overline{\Delta t_m} + \overline{\Delta t_r} \quad (12)$$

Where:

Δt = Time latency
Δt_o = Latency of observation
Δt_m = Latency of measurement/processing
Δt_r = Latency of transmission/receipt
t_e = Time of event
t_o = Time of observation
t_m = Time of completion of processing
t_r = Time of receipt

Information Interpretation and Utilization

Having passed the data and correctly interpreted it, the next step would be to verify that the proper action is taken. Verification of the action taken involves a review of the logic associated with every option that is possible in response to a message or operator action. These deal with questions of interoperability and not with the difficult, higher-level topic of measuring mission effectiveness. These data would be qualitative in nature, perhaps binary (i.e., successful vs. failed). Some suggested measures in this area include

- Percentage of initial transmission messages received correctly by shooters
- Percentage of consistency/disparity of redundant data sources
- Number of tries needed to establish connections
- Delay in sending critical command messages and time to receive acknowledge messages

