System of Systems Interoperability (SOSI): Final Report

Edwin Morris
Linda Levine
Craig Meyers
Pat Place
Dan Plakosh

April 2004

TECHNICAL REPORT
CMU/SEI-2004-TR-004
ESC-TR-2004-004

Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

System of Systems Interoperability (SOSI): Final Report

CMU/SEI-2004-TR-004
ESC-TR-2004-004

Edwin Morris
Linda Levine
Craig Meyers
Pat Place
Dan Plakosh

April 2004

Integration of Software-Intensive Systems Initiative

This report was prepared for the

SEI Joint Program Office
HQ ESC/DIB
5 Eglin Street
Hanscom AFB, MA 01731-2116

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

FOR THE COMMANDER

Christos Scondras
Chief of Programs, XPK

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (http://www.sei.cmu.edu/publications/pubweb.html).

Table of Contents

List of Figures

Abstract

This technical report documents the findings of an internal research and development effort on system of systems interoperability (SOSI). The study was based on the belief that interoperability must occur at multiple levels within and across programs, and not solely in the context of a system construction. The Software Engineering Institute looked at the full range of barriers to achieving interoperability between systems, including programmatic, constructive, and operational barriers. An initial SOSI model representing this perspective was developed. The research method consisted of three activities: review of related research, conducting of small workshops, and interviews with experts. The literature survey focused on Department of Defense and related initiatives dedicated to achieving interoperability. Workshops were held in Washington, D.C. in February and May 2003. Interviews were conducted with experts representing each of the services, the National Reconnaissance Organization, and industry. Results from these activities are presented here.

1 Purpose of the Research and Development Effort

As technology becomes more far-reaching and interconnected, interoperability has become critical. Interoperability to achieve information superiority is the keystone on which future combat systems (e.g., Air Operations Center, Future Combat Systems), logistic systems (e.g., Global Combat Support System), and other government systems (e.g., interoperability between organizations for homeland security) will be constructed. *Joint Vision 2020*, which guides the continuing transformation of America's armed forces, states "Interoperability is the foundation of effective joint, multinational, and interagency operations" [Joint 00].

Currently, there is a tendency to concentrate on the mechanisms that various systems use to interoperate. However, focusing solely on mechanisms misses a larger problem. Creating and maintaining interoperable systems of systems requires interoperation not only at the mechanistic level, but also at the levels of system construction and program management. Improved interoperation will not happen by accident and will require changes at many levels.

While many systems produced by Department of Defense (DoD) programs can, in fact, interoperate with varying degrees of success, the manner in which this interoperation is achieved is piecemeal. In the worst case, interoperability is achieved by manually entering data produced by one system into another—a time consuming and error-prone process. Clearly, if America's armed forces are to achieve *Joint Vision 2020*, and if cross-organizational homeland security capabilities are to be developed, a better way forward must be found:

> *Although technical interoperability is essential, it is not sufficient to ensure effective operations. There must be a suitable focus on procedural and organizational elements, and decision makers at all levels must understand each other's capabilities and constraints. Training and education, experience and exercises, cooperative planning, and skilled liaison at all levels of the joint force will not only overcome the barriers of organizational culture and differing priorities, but will teach members of the joint team to appreciate the full range of Service capabilities available to them* [Joint 00].

The purpose of this independent research and development (IR&D) effort was to respond to the need for the Carnegie Mellon® Software Engineering Institute (SEI) to address the issue of interoperability. The study was based on the hypothesis interoperability must occur at multiple levels within a program and not solely in the context of an operational system. We looked at the full range of barriers to achieving interoperability between systems, including programmatic, constructive, and operational barriers.

The goals for the System of Systems Interoperability (SOSI) IR&D can be summarized as the following:

- Identify interoperability problems for which solutions or partial solutions are possible.
- Corroborate our model of interoperability, or identify an alternate model of interoperability supported by lessons learned.
- Identify ways in which the SEI can contribute solutions to the interoperability problem.

® Carnegie Mellon is registered in the U.S. Patent and Trademark Office.

2 Defining Interoperability

There is a need for precise definition of *interoperability*, because the term can have various interpretations in different contexts. For example, interoperability between a field commander's planning systems and a weather system may be addressed via a simple broadcast email. In contrast, radar reports of objects in the environment that must be shared between complex systems like AWACS and Aegis may require frequent, automated updates of complex information.

Experts suggest that there are different interpretations of terms such as *system of systems* and *interoperability*, based on divergent needs: "What someone considers to be a system of systems, someone else considers a system." This becomes particularly apparent when discussing hugely complex systems like the Army Future Combat System that are really multiple systems of systems.

Some of the difficulty associated with defining interoperability is reflected in the many definitions that exist. For example, the IEEE has four definitions of interoperability [IEEE 00]:

- the ability of two or more systems or elements to exchange information and to use the information that has been exchanged.
- the capability for units of equipment to work together to do useful functions.
- the capability, promoted but not guaranteed by joint conformance with a given set of standards, that enables heterogeneous equipment, generally built by various vendors, to work together in a network environment.
- the ability of two or more systems or components to exchange information in a heterogeneous network and use that information.

The DoD also uses multiple definitions of interoperability, several of which incorporate IEEE definitions:

> *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 01a].
>
> *The condition achieved among communications-electronics systems or items of communications-electronics systems 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. For the purposes of this instruction, the degree of interoperability will be determined by the accomplishment of the proposed Information Exchange Requirement (IER) fields* [DoD 01b].
>
> *(a) Ability of information systems to communicate with each other and exchange information. (b) Conditions, achieved in varying levels, when information systems and/or their components can exchange information directly and satisfactorily among them. (c) The ability to operate software and exchange information in a heterogeneous network (i.e., one large network made up of several different local area networks). (d) Systems or programs capable of exchanging information and operating together effectively* [GIG 01].

We may never have agreement on a precise definition due to differing expectations that are constantly changing. New capabilities and functions (e.g., netcentric warfare) continue to offer new opportunities for interactions between systems. For the purposes of this report, we define interoperability as: The ability of a set of communicating entities to (1) exchange specified state data and (2) operate on that state data according to specified, agreed-upon, operational semantics.

3 Models of Interoperability

Part of our research involved investigation of existing models of interoperability. These models are described in this section. In addition, we also discuss the SOSI model.

3.1 Levels of Information System Interoperability

A widely recognized model for system of systems interoperability is Levels of Information System Interoperability (LISI) [C4ISR 98]. LISI (see Figure 1) focuses on the increasing levels of sophistication of system of systems interoperability.

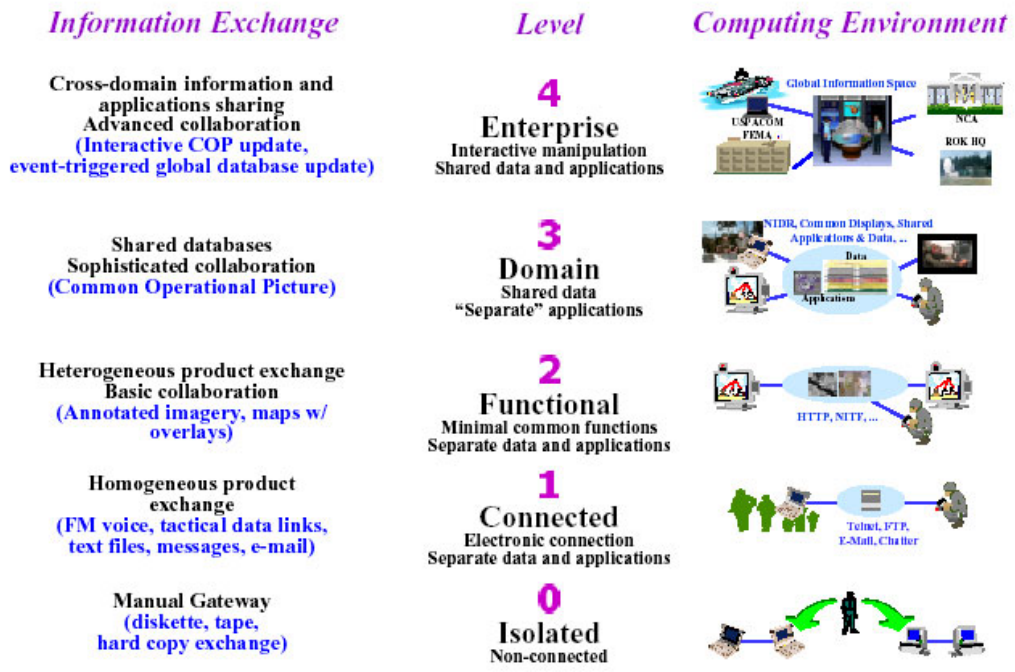

Figure 1: The LISI Interoperability Maturity Model

[taken from LISI 1998]

Five levels are defined:

Level 0 – Isolated interoperability in a manual environment between stand-alone systems: Interoperability at this level consists of the manual extraction and integration of data from multiple systems. This is sometimes called "sneaker-net."

Level 1 – Connected interoperability in a peer-to-peer environment: This relies on electronic links with some form of simple electronic exchange of data. Simple, homogeneous data types, such as voice, text email, and graphics (e.g., Graphic Interface Format files) are shared. There is little capacity to fuse information.

Level 2 – Functional interoperability in a distributed environment: Systems reside on local area networks that allow data to be passed from system to system. This level provides for increasingly complex media exchanges. Logical data models are shared across systems. Data is generally heterogeneous-containing information from many simple formats fused together (e.g., images with annotations).

Level 3 – Domain based interoperability in an integrated environment. Systems are connected via wide area networks. Information is exchanged between independent applications using shared domain-based data models. This level enables common business rules and processes as well as direct database-to-database interactions. It also supports group collaboration on fused information.

Level 4 – Enterprise-based interoperability in a universal environment: Systems are capable of using a global information space across multiple domains. Multiple users can access complex data simultaneously. Data and applications are fully shared and distributed. Advanced forms of collaboration are possible. Data has a common interpretation regardless of format.

Within a level, LISI identifies additional factors that influence the ability of systems to interoperate. These factors comprise four attributes: Procedures, Applications, Infrastructure, and Data (PAID). PAID provides a method for defining the set of characteristics required for exchanging information and services at each level. It defines a process that leads to interoperability profiles and other products. Scenarios depict the possible uses of LISI in different circumstances throughout the system life cycle.

LISI focuses on technical interoperability and the complexity of interoperations between systems. The model does not address the environmental and organizational issues that contribute to the construction and maintenance of interoperable systems (e.g., shared processes for defining interoperability requirements and maintaining interoperability across versions).

3.2 Organizational Interoperability Maturity Model

Acknowledging this limitation, Clark and Jones proposed the Organizational Interoperability Maturity Model (OIM), which extends the LISI model into the more abstract layers of command and control support [Clark 99]. Five levels of organizational maturity, describing the ability to interoperate, are defined. These include

Level 0: independent

Level 1: ad hoc

Level 2: collaborative

Level 3: integrated (also called combined)

Level 4: unified

On one end of the spectrum, at Level 0, no formal framework is in place for interoperation, whereas at Level 4, common goals, value systems, command structure and knowledge bases exist. OIM is not concerned with organizations that are building systems; rather, the focus is on the human-activity and user aspects of military operations. The model has been used to identify problems and to conduct evaluations in coalition operations such as the International Force in East Timor [INTERFET] and the Australia–U.S. Interoperability Review [Fewell 03]. A mapping between OIM and LISI taken from Clark is provided in Figure 2 [Clark 99].

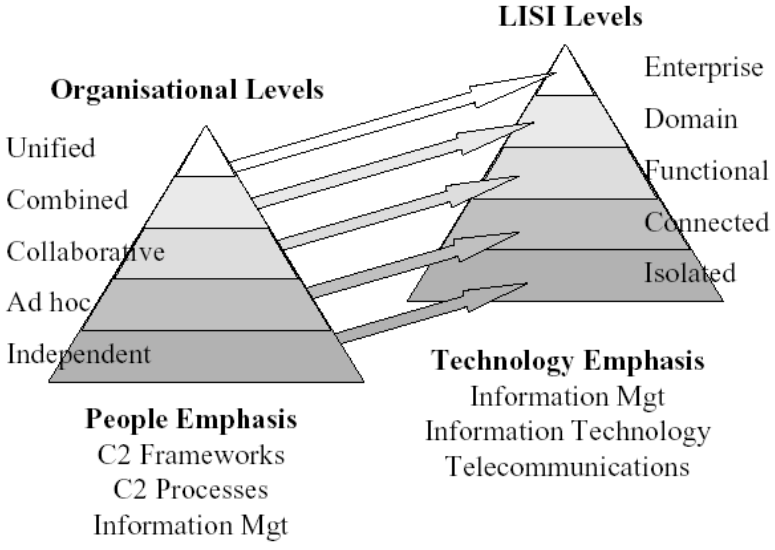

Figure 2: Alignment Between Organizational Model and LISI

3.3 NATO C3 Technical Architecture (NC3TA) Reference Model for Interoperability

Previously, the NATO model focused on technical interoperability and established interoperability degrees and sub-degrees. The four degrees of interoperability were defined as follows:

Degree 1 - Unstructured Data Exchange: exchange of human-interpretable unstructured data such as the text found in operational estimates, analyses and papers.

Degree 2 - Structured Data Exchange: exchange of human-interpretable structured data intended for manual and/or automated handling, but requires manual compilation, receipt and/or message dispatch.

Degree 3 - Seamless Sharing of Data: automated sharing of data amongst systems based on a common exchange model.

Degree 4 - Seamless Sharing of Information: universal interpretation of information through data processing based on cooperating applications.

The degrees were intended to categorize how operational effectiveness could be enhanced by structuring and automating the exchange and interpretation of data. These were further refined into sub-degrees that identified specific interoperability services.

In December 2003, the NC3TA was updated to closely reflect the LISI model.

3.4 Levels of Conceptual Interoperability (LCIM) Model

Tolk has developed the Levels of Conceptual Interoperability (LCIM) Model that addresses levels of conceptual interoperability that go beyond technical models like LISI [Tolk 03a]. The model is intended to be a bridge between conceptual design and technical design. The focus lies in the data to be interchanged and the interface documentation that is available. The layers of the LCIM model include

Level 0: System specific data: black box components with no interoperability or shared data

Level 1: Documented data: shared protocols between systems with data accessible via interfaces

Level 2: Aligned static data: common reference model with the meaning of data unambiguously described. Systems are black boxes with standard interfaces. However, even with a common reference model, the same data can be interpreted differently in different systems.

Level 3: Aligned dynamic data: Use of data is defined using software engineering methods like Unified Modeling Language. This allows visibility into how data is managed in the system. But even systems with the same interfaces and data can have different assumptions and expectations about the data.

Level 4: Harmonized data: Non-obvious semantic connections are made apparent via a documented conceptual model underlying components. This goes beyond Level 3 because the assumptions concerning the data are made apparent.

As LCIM points out, in order to achieve the highest levels of interoperability, the assumptions underlying how systems interpret data must be made transparent. Tolk observes that the model has been developed for the simulation domain but the basic premises apply to many complex sets of interoperating systems.

3.5 Layers of Coalition Interoperability

Tolk surveys a number of models including LISI and the NC3TA Reference Model for Interoperability and establishes a reference model for coalition interoperability [Tolk 03b].

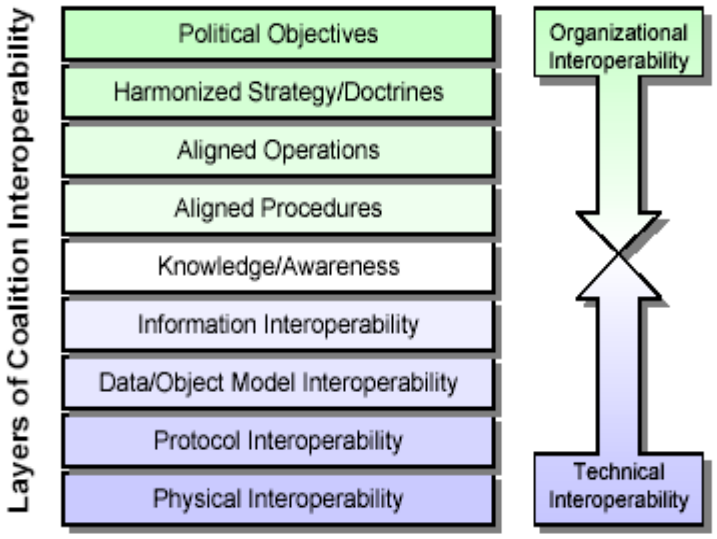

Figure 3: The Layers of Coalition Interoperability

[from Tolk 2003b]

This model (which we call LCI) is intended to facilitate discussion on technical and organizational (political and military) support required for interoperable solutions. It is not intended to be a substitute for other models. The four lower levels of the model deal with technical interoperability. The knowledge/awareness level provides a transition between technical interoperability and organizational interoperability, which is represented by the top four levels.

3.6 The System of Systems Interoperability (SOSI) Model

The models previously discussed address a range of interoperability issues from technical to coalition organizational. We have developed the SOSI model, which addresses technical interoperability (also covered by LISI, LCI, and NATO) and operational interoperability (also covered by OIM and LCI). However, SOSI goes a step further to address programmatic concerns between organizations building and maintaining interoperable systems.

Interoperation among systems is typically achieved through significant effort and expense. Too often, the approaches used lead to interoperability that is specific to the targeted systems (sometimes called “point-to-point interoperability”) and that does not facilitate extension to other systems. Even then, the technical approaches employed, such as the Defense Information Initiative Common Operating Environment (DII/COE) and the Extensible Markup Language (XML), offer only partial interoperability.

Achieving large-scale and consistent interoperation among systems will require a consistently applied set of management, constructive, and operational practices that support the addition of new and upgraded systems to a growing interoperability web. Improvements in technology alone (whether XML or any other) will not be sufficient. There must be parallel improvements in the ways that current and future interoperability needs are identified, and how organizations pursue interoperability.

Figure 4 depicts the broad range of activities that are necessary to achieve interoperability.

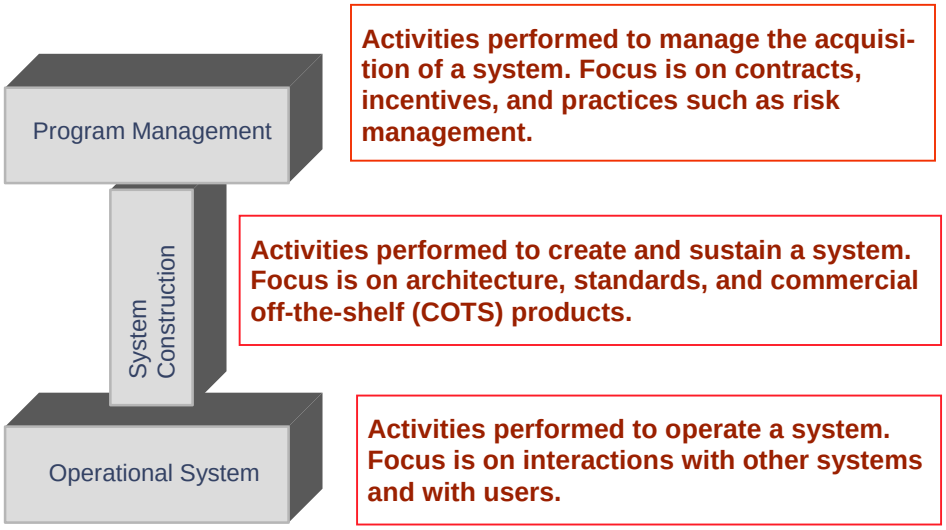

Figure 4: System Activities Model

As shown in Figure 4, *Program Management* defines the activities that manage the acquisition of a system. *System Construction* defines the activities that develop or evolve a system (e.g., use of standards and COTS products, architecture). *Operational System* defines the activities within the executing system and between the executing system and its environment, including the interoperation with other systems. The end user is considered part of the operational system.

Figure 4 represents activities within a single acquisition organization. When we consider the interaction between two programs the result is shown in Figure 5. It is through this figure that we introduce the following types of interoperability:

- programmatic: interoperability between different program offices
- constructive: interoperability between the organizations that are responsible for the construction (and maintenance) of a system
- operational: interoperability between the systems

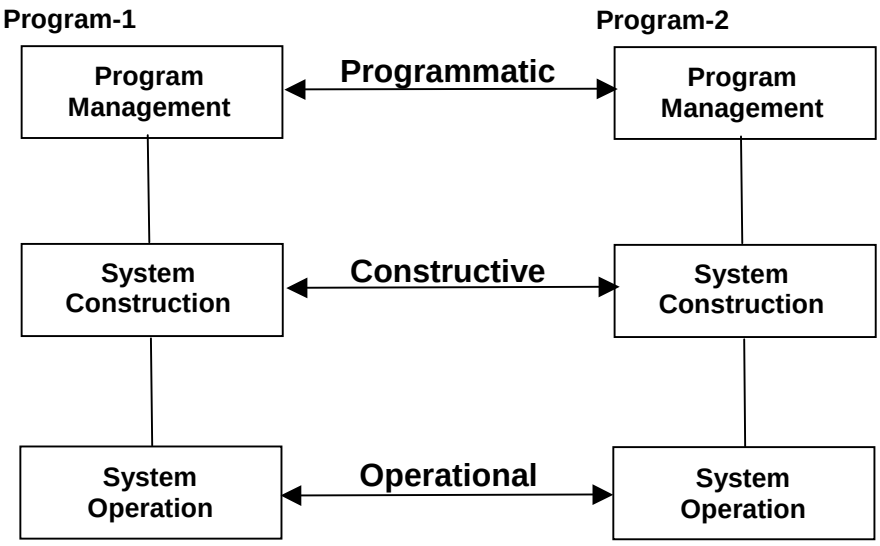

Figure 5: Different Types of Interoperability

Figure 5 illustrates a key premise of the SOSI work: In order to have interoperability between operational systems, one must introduce—and address—the full scope of interoperability between those organizations that participate in the acquisition of systems. It is this premise that leads us to introduce the notions of programmatic interoperability and constructive interoperability. The scale of interoperability can be much greater than between two programs. In general, one needs to consider interoperability issues between all relevant organizations responsible for any part of a system of systems. The SOSI model suggests that the concept of an *interoperability backplane* is needed.

All of the models described here are successful in that they provide a partial representation of some aspect of interoperability. The SOSI model extends the existing models by adding a focus on programmatics (e.g., activities performed to manage the acquisition of a system). In the SOSI model, programmatic, constructive, and operational issues must be managed across

the life cycle. What is needed is a set of compatible models that collectively address all of the dimensions of interoperability.

4 Approach

4.1 Method

The research method for this IR&D consisted of three activities: review of the related research, small workshops, and interviews with experts. Each activity is discussed below.

Our survey of the literature focused on DoD and related commercial initiatives dedicated to achieving interoperability. Briefings from recent conferences were investigated. A Web-based search was performed to identify related technical literature. Throughout the search process, new leads were identified and pursued, and numerous briefings and papers were reviewed.

Workshops were held in Washington, D.C. in February and May 2003. The first workshop was held with the SOSI advisory board of DoD experts. The preliminary SOSI model of interoperability was presented and feedback was requested in the following areas:

- critical interoperability issues
- insight into programs that are solving critical interoperability problems
- recommendations and best approaches for conducting research on the current state of the practice

A technical note (CMU/SEI-2003-TN-016) documented the model of interoperability presented and the findings from the workshop [Levine 03].

Finally, a small set of interviews was conducted with experts representing each of the services, several other government agencies, and a single contractor. These individuals primarily represented a technical-management perspective. Notes from the interviews were analyzed and coded according to the parameters of the SOSI model. Five general themes emerged which are discussed in Section 5. For the interview script, see the Appendix.

While the interviews were generally successful, one shortcoming emerged: a difficulty in identifying end-users to provide good feedback from an operational perspective.

4.2 Collaborators

An advisory board of DoD experts was convened for the study. Members include

Dr. Stan Levine

Dr. James Linnehan, U.S. Army G8

Ms. Beth Lynch

Mr. Chuck Gibson

Col. Mike Therrien

Other experts contributed to this work through their attendance at workshops or by participating in interviews. To ensure confidentiality, these individuals are not identified by name.

5 Results: Current State

In spite of the large number of organizations involved in addressing interoperability, problems continue to be significant, even across releases of a single system. Any solution will require addressing organizational and technical issues. For example, achieving interoperability between two distinct systems will require changes to management planning and system implementation.

To address these issues, we consider general observations on the utility of the SOSI model, a discussion of DoD-related interoperability initiatives and strategies, and findings from interviews and workshops.

5.1 Observations on the SOSI Model

We found that, on the whole, the three-tiered model (programmatic, constructive, and operational) was a useful way to organize our investigation and observations. However, the model is not complete, because it does not provide a comfortable fit for issues beyond the scope of programs, such as vision, high-level policy, and standards development. As a result, the model was modified to include environmental factors (see Figure 6). Note that some issues can be placed into more than one category. For example, communication is relevant at multiple levels.

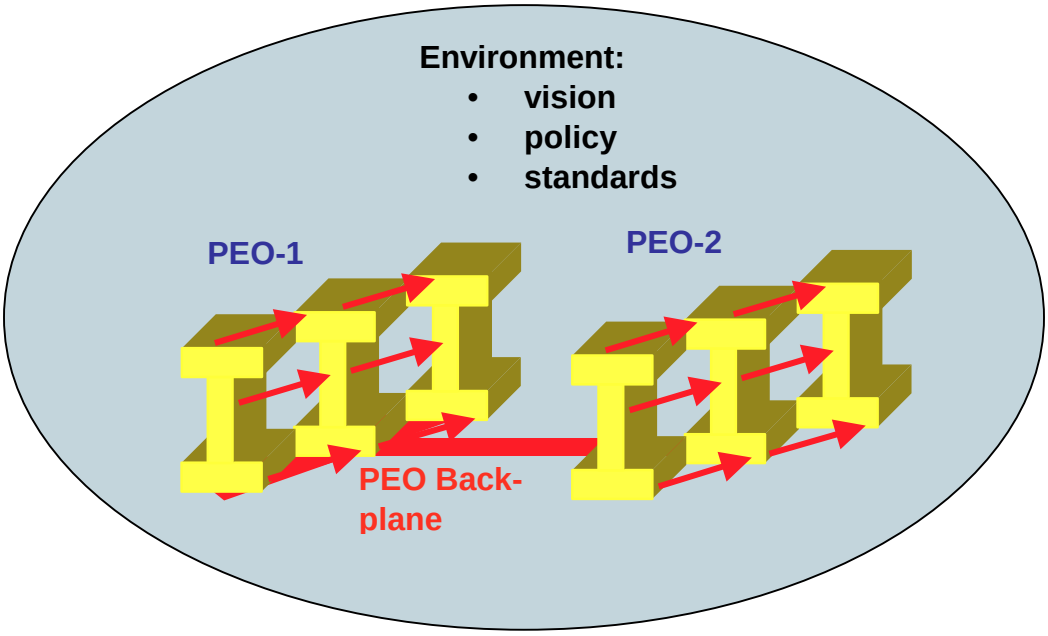

Figure 6: Modified SOSI Model

Feedback we received identified other perspectives orthogonal to the model (e.g., people oriented, life-cycle oriented). One recommendation from the first workshop was to present the interoperability message from the standpoint of the end users of interoperable systems. This perspective suggests putting the end user first—implying that the effect of interoperability decisions on the end user should be central to the model. A second recommendation centered on the specific activities that must occur in each life-cycle phase in order to achieve interoperability. In keeping with a people-centered perspective, the life cycle must be extended to include training, fielding, and end users.

6 DoD Interoperability Initiatives

In keeping with Joint Vision 2020, interoperability is receiving increasing and widespread attention. Our research identified a range of DoD and related organizations that are attempting to define the problem, provide solutions, and build interoperable systems. Some of these entities include commands, directorates, and centers; bodies creating standards and strategies; demonstrations and testbeds; joint force integration initiatives; and DoD-sponsored research. These entities comprise the efforts and organizations described below. Web site addresses are listed for those desiring more information.

6.1 Commands, Directorates and Centers

Note: URLs are accurate as of the publication date of this report.

Combatant Command Interoperability Program Office: The goals of this office include: advancing the Combatant Command C2 capability through enhanced integration /interoperability of current command, control, communications, computer intelligence, surveillance, and reconnaissance (C4ISR) systems; assuring joint and service force modernization initiatives are aligned with Combatant Command C2 concept of operations; exploiting the integration/interoperability opportunities discovered through experimentation. http://esc.hanscom.af.mil/ Esc-PA /NEWS /2003 /Jun%202003/ESC%2003-15.HTM

Defense Information Systems Agency (DISA) Center for Joint & Coalition Interoperability: The mission of the Center for Joint & Coalition Interoperability is to foster interoperability among our joint and coalition partners worldwide; provide technical guidance to facilitate the effective exchange of information across multilateral environments; serve as the DoD IT life-cycle interoperability advocate to all joint, allied, and combined activities internationally. http://in.disa.mil/in3.html

DISA Interoperability Directorate: The goals of this directorate are the following: to enhance joint and coalition combat effectiveness through development, promotion and use of IT standards, architectures, and tools to enable end-to-end interoperability of the Global Information Grid (GIG); provide life cycle test, assessment, evaluation, certification, and technical support for the National Security Systems and Information Technology Systems; serve as the

Operational Test Agency to determine operational effectiveness and suitability of systems managed and procured by DISA. http://in.disa.mil/

Institute for Defense Analysis (IDA) Joint Advanced Warfighting Program (JAWP): JAWP was established in 1998 to serve as a catalyst for transforming U.S. military capabilities, with particular focus on joint concept development and experimentation. The JAWP provides an independent source for formulating and assessing advanced concepts for joint warfighting experimentation. Its mission is to assist the DoD in developing the capabilities envisioned in Joint Vision 2010 by leveraging advanced technology, innovative operational concepts, and new organizational structures.
http://www.ida.org/IDAnew/Divisions/jawp.html

JFCOM Interoperability Technology Demonstration Center (ITDC): (Stood-up in September 2003) ITDC will give JFCOM a vital new interoperability advocacy role in the DoD's acquisition process. The ITDC will serve as a DoD checkpoint capable of demonstrating whether prospective computer and information technologies can operate with the networks in the military's emerging joint command and control environment.

Joint Interoperability and Integration Directorate (JI&I): JI&I supports the Joint Warfighter as the champion of the Joint Force Integrator process; improves the review effort for new joint Capstone Requirements Documents and Operational Requirements Documents to ensure systems are born joint; provides Doctrine, Organization, Training, Materiel, Leadership, Personnel and Facilities (DOTMLPF) synchronized solutions to select operational deficiencies http://www.teao.saic.com/jfcom/html/charter.html

Joint Interoperability Test Command (JITC): JITC identifies and solves C4I and Combat Support Systems interoperability deficiencies; provides C4I joint and combined interoperability testing, evaluation and certification; brings C4I interoperability support, operational field assessments, and technical assistance for Combatant Commands, Services, and Agencies. http://jitc.fhu.disa.mil

Joint C4ISR Battle Center: Joint C4ISR Battle Center (JBC) leads near-term transformation of joint force C4ISR capabilities through assessing new technology. The JBC provides objective recommendations for rapid insertion of solutions to support identified combatant commands' needs for a joint task force (JTF). http://www.jbc.jfcom.mil/Common/index.htm

Joint Experimentation Directorate (J 9): J9 develops, explores, tests, and validates 21st-century warfighting concepts. Joint warfighting transformational concepts developed here will be integrated into future joint forces training. J9 offers improvements in doctrine, interoperability, and integration, all of which lay the foundation for defense transformation.
http://www.jfcom.mil/about/abt_j9.htm

Joint Forces Command (JFCOM): JFCOM is the “Transformation laboratory" of the United States military that serves to enhance the unified commanders' capabilities to implement that strategy. Develop concepts, test these concepts through rigorous experimentation, educate joint leaders, train joint forces, and make recommendations on how the Army, Navy, Air Force and Marines can better integrate their warfighting capabilities. http://www.jfcom.mil/index.htm

Joint Logistic Transformation Center (JLTC): JLTC serves as a U.S. Joint Forces Command rapid logistics concept and prototype development unit within the Joint Experimentation Directorate. It provides the joint logistics community with a conduit to the joint experimentation process. JLTC also connects various Department of Defense, Joint Staff, and Joint Forces Command activities to experimentation. http://www.jfcom.mil/about/fact_jltc.htm

Joint Requirements and Integration Directorate (J8): The director for requirements and integration (J8) serves as the lead joint integration expert, ensuring the various services and defense agencies can combine their capabilities into a single successful effort. This allows us to fight both “joint” (integrated capabilities between the Marines, Air Force, Army, Navy, etc.) as well as “combined” (U.S. forces and allied militaries fighting as a cohesive package). http://www.jfcom.mil/about/abt_j8.htm

Joint Warfighting Center (JWFC): represents the action arm supporting the JFCOM joint force training effort. The JWFC commander also serves as the JFCOM director for joint force training (J7) to ensure the coordination of the overall joint training program through the J7, and its subsequent execution by the JWFC. The JWFC is located at the Joint Training, Analysis, and Simulations Center (JTASC) at the JFCOM Suffolk campus. The JTASC represents a state-of-the-art technology center that supports joint training simulations for the JWFC, interoperability testing by the requirements and integration director’s Joint C4ISR Battle Center, and joint experiments by the joint experimentation director. http://www.jwfc.jfcom.mil/

Naval Network Warfare Command (NETWARCOM): NETWARCOM is the central operational authority responsible for coordinating all information technology, information operations, and space requirements and operations within the Navy. NETWARCOM aligns the various staffs needed to support the concept of one naval network and to support that network's end-to-end operational management. http://www.news.navy.mil/search/display.asp?story_id=1156

OSD OT&E Foundation Initiative 2010 (FI 2010): FI2010 is a joint interoperability initiative of the Director, Operational Test and Evaluation. The vision of FI 2010 is to enable interoperability among ranges, facilities and simulations in a quick and cost-efficient manner, and to foster reuse of range assets and future range system developments. To achieve this vision, FI 2010 is developing and validating a common architecture, a core set of tools, inter-

range communication capabilities, interfaces to existing range assets, interfaces to weapon systems, and recommended procedures for conducting synthetic test events or training exercises. http://www.dtic.mil/ndia/marketplace/rumford.pdf

6.2 Standards

C4ISR Architecture Framework/DoDAF: The C4ISR Architecture Framework is intended to ensure that the architecture descriptions developed by the Commands, Services, and Agencies are interrelatable between and among each organization's operational, systems, and technical architecture views, and are comparable and integrable across Joint and combined organizational boundaries. The DoD Architecture Framework (DoDAF) is an evolution of the C4ISR Architecture Framework. In late 2003, the DoDAF superceded the C4ISR framework. Its intent remains ensuring that architecture descriptions can be interrelated and that resulting systems can interoperate.
http://www.opengroup.org/public/member/proceedings/q403/dandashi.pdf
http://aitc.aitcnet.org/dodfw/

DII/COE (also called COE): DII/COE is a framework for interoperability that encompasses guidelines for software construction, packaging, behavior, operating environment and accompanying documentation; guidelines and a repository for the reuse and sharing of software and data; tools and procedures for registering, verifying, submitting, and certifying mission applications as being DII COE compliant. http://diicoe.disa.mil/coe/
http://www.dis.anl.gov/is/DIICOE.html

Joint Technical Architecture (JTA): JTA provides the minimum set of standards that, when implemented, facilitates the flow of information among DoD's sensors, processing and command centers, shooters, and support activities; provides the foundation for interoperability among all tactical, strategic, and combat support systems; mandates IT standards and guidelines for DoD system development and acquisition that will facilitate interoperability in joint and coalition force operations. http://jta.disa.mil/

6.3 Strategies

Air Force Warfighter Integration (AF/XI) Headquarters: This office is responsible for the following: forming and executing policy and strategy to integrate command, control; communications, computers, intelligence, surveillance and reconnaissance capabilities; providing guidance and direction to field-operating agencies.
http://www.hanscom.af.mil/Hansconian/Articles/2002Arts/03222002-01.htm

Army Software Blocking (SWB): A policy for harmonizing requirements and development that leads to fielding and support of software-intensive systems. With limited exception, the policy applies to all new and upgraded systems that exchange information. Business systems that do not exchange information directly with tactical C4ISR systems are excluded at this time. This approach transitions away from a stovepipe acquisition process by identifying Integrated Capability Packages. Each software block is certified and operationally evaluated before being made available for use. http://www.dtic.mil/ndia/2002systems/levine1c2.pdf

Global Information Grid (GIG): The Global Information Grid is the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. The GIG supports all Department of Defense, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DoD users and systems. http://www.disa.mil/ns/gig.html

Military Restructuring and Transformation: The Secretary of Defense Mandate Management Initiative Decision 912 (MID 912) expanded the role of JFCOM. In this expanded role, JFCOM is charged with (1) discovering promising alternatives through joint concept development and experimentation; (2) defining enhancements to joint warfighting requirements; (3) developing joint warfighting capabilities through joint training and solutions; (4) delivering joint forces and capabilities to warfighting commanders.
http://www.chips.navy.mil/archives/03_summer/PDF/transformation.pdf

6.4 Demonstrations, Exercises and Testbeds

Distributed Engineering Plant (DEP): The Navy Distributed Engineering Plant (DEP) was established in 1998 to address critical fleet interoperability issues. The primary mission of the DEP and its associated testing processes is to characterize the interoperability of each deploying Battle Group and provide this information to the Battle Group staff.
http://www.navsea.navy.mil/featurestories_summary.asp?txtDataID=4551

Joint Distributed Engineering Plant (JDEP): JDEP is a DoD- and service-funded initiative created to support interoperability. JDEP facilitates access, coordination, scheduling, and technical support to replicate joint operational environments through the reuse of existing hardware capabilities and software capabilities across the DoD and industry. http://jitc.fhu.disa.mil/jdep/

Joint Warrior Interoperability Demonstration (JWID): Annual event with the international community to investigate C4ISR solutions to near-term coalition interoperability challenges. The event provides an opportunity for government, private industry and coalition partners to demonstrate new and emerging technologies in a simulated warfighting environment. http://www.jwid.js.mil/

Pinnacle Vision (formerly called Olympic Challenge): In 2004, JFCOM plans to hold a large experiment called Pinnacle Vision in which the focus will be on the technological architecture needed to build the systems that the military must have to operate jointly on future battlefields. The results of that experiment will represent JFCOM's debut into the acquisition business, as the lessons learned in 2004 could have significant impact on the decisions to pursue a variety of DoD programs.
http://www.dtic.mil/descriptivesum/Y2004/OSD/0603727D8Z.pdf

6.5 Joint and Coalition Force Integration Initiatives

Blue Force Tracking (BFT): A single, interoperable system designed to reduce the number of fratricide incidents, sustain forward-deployed forces, and maintain contact with them. The system will consist of global positioning applications, communications, logistics and supply, and tactical overlays. The system is designed to put electronics on major moving parts, such as tanks, armored personnel carriers, aircraft, and infantry fighting vehicles.
http://www.fcw.com/fcw/articles/2003/0526/web-blue-05-30-03.asp

Combat Identification (CID): a framework for a program of technology experiments, modeling, simulation, and analytical efforts, culminating in an operational demonstration of air-to-ground and ground-to-ground CID system alternatives. CID will demonstrate system alternatives that can enhance the capability of our combat forces to positively identify friendly and hostile platforms during air-to-ground and ground-to-ground operations, in order to reduce fratricide due to misidentification, and to maximize combat effectiveness.
http://www.fas.org/spp/military/docops/defense/actd_mp/CID.htm

Common Tactical Picture (CTP): The common tactical picture refers to the current depiction of the battlespace for a single operation within a Commander-in-chief's (CINC) area of responsibility, including current, anticipated or projected, and planned disposition of hostile, neutral, and friendly forces as they pertain to US and multinational operations ranging from peace-time through crisis and war.
http://www.tpub.com/content/USMC/mcwp3402/css/mcwp3402_49.htm

Deployable Joint Command and Control (DJC2): This is a mobile command post that will support the operations of a Standing Joint Force Headquarters at each regional combatant command by 2005. DJC2 will provide both the infrastructure at the command post and com-

mand and control information systems for the Standing Joint Force. http://www.gcn.com/22_10/dodcomputing/21945-1.html

Family of Interoperable Operational Pictures (FIOP): A plan to achieve a coherent view of the battlespace from the CINC to the soldier/sailor/airman/marine. It goes beyond situational awareness to include battlespace management, fire support, intelligence, logistics, and so on. Currently, systems with poor interoperability hinder the ability to achieve a fully coordinated strategy. http://www.dtic.mil/ndia/systems/Quinlan.pdf

ForceNet: The operational construct and architectural framework for Naval Warfare in the information age that integrates warriors, sensors, networks, command and control, platforms and weapons into a networked, distributed combat system, scalable across the spectrum of conflict from seabed to space and sea to land. http://www.afcea-sd.org/briefs/2002-10_afceasd_forcenet.ppt

Global Command and Control System – Joint (GCCS-J): The military's system for the command and control of joint and coalition forces. It incorporates the force planning and readiness assessment applications required by battlefield commanders to effectively plan and execute military operations. Its Common Operational Picture correlates and fuses data from multiple sensors and intelligence sources to provide warfighters the situational awareness needed to be able to act and react decisively. It also provides an extensive suite of integrated office automation, messaging, and collaborative applications. http://gccs.disa.mil/gccs/

Global Combat Support System (GCSS): a family of interconnected systems that will provide the Combatant Command/JTF Commanders a high-level, fused view of information through a fully integrated information system. GCSS will be a seamless, integrated combat support information data source to the Global Command and Control System (GCCS) and will integrate combat support information in a user-friendly format that will enable the Combatant Command/JTF Commanders to make timely informed decisions. http://www.disa.mil/pao/products/ccjtf.html

Joint Battle Management/Command & Control (JBMC2): Based on findings of a 2002 study conducted by USJFCOM, the Joint Staff and other military commands and agencies, Secretary of Defense Donald Rumsfeld directed USJFCOM to improve coordination of DoD's JBMC2 efforts JBMC2 brings together several different programs to work toward joint interoperability and integration. http://www.jfcom.mil/about/fact_jbmc2.htm

Joint Close Air Support (JCAS): A DoD Joint Test and Evaluation (JT&E) program chartered by OSD to assess the current capabilities of U.S. forces to conduct joint close air support (CAS) in both day and night conditions. The JCAS Joint Test Force (JTF) will also test and recommend potential enhancements to improve joint CAS effectiveness. The JTF will

employ multi-service air and ground equipment and personnel in realistic combat training scenarios. The test will address two critical issues: (1) What is the joint CAS baseline effectiveness? (2) What changes to Joint CAS tactics, techniques, procedures, equipment/systems, and training increase effectiveness compared to the baseline?
http://www.globalsecurity.org/military/library/budget/fy2001/dot-e/jte/01jcas.html

Joint Fires Network (JFN): JFN provides near real-time intelligence correlation, sensor control and planning, target generation, precise target coordinates, moving target tracks and battle-damage-assessment capabilities to support more timely engagement of time-critical targets. This capability allows a ship with the full JFN suite to share a greatly improved battlespace picture very quickly with other ships in the area of operations.
http://www.news.navy.mil/search/display.asp?story_id=5569

Joint Global Command and Control System (GCCS-J): System for the command and control of joint and coalition forces. It incorporates the force planning and readiness assessment applications required by battlefield commanders to effectively plan and execute military operations. Its Common Operational Picture correlates and fuses data from multiple sensors and intelligence sources to provide warfighters the situational awareness. GCCS-J allows greater software flexibility, reliability, and interoperability with other computer systems.
http://gccs.disa.mil/gccs/

Joint Intelligence Surveillance Reconnaissance ACTD: The DoD and Joint Chiefs of Staff have identified the need for improved intelligence, surveillance and reconnaissance (ISR) and operational information integration to enhance situational awareness in support of an Early Entry Force (EEF) and supporting components. The JISR Advance Concept Technology Demonstrations (ACTD) solves this critical problem by providing an enhanced tactical picture which includes: (1) Timely integration of traditional sensor and non-traditional sensor data (e.g., LAMPS, Firefinder, Longbow, Scouts, UGS, TARPS, SPY radar); (2) Friendly force and other operational information; (3) Intuitive, user-friendly battlespace visualization capability; and (4) Accessibility to joint and coalition forces and the CINC.
https://peoiewswebinfo.monmouth.army.mil/JPSD/jisr.htm

Precision Engagement/Time Sensitive Tracking (PE/TST): In summer 2001, the Defense Science Board (DSB) performed a study on precision targeting. Recommendations were vetted and endorsed in September 2002. The next step is to continue review of PE/TST acquisition programs and initiatives. A second mission area review will also be conducted to determine the “right things to do” and help lay out a capability roadmap.
http://www.dtic.mil/ndia/2002systems/quinlan1c2.pdf

Shared Tactical Ground Picture (STGP): The STGP is an initiative by seven NATO Nations to improve sharing of information in a coalition environment. The effort includes development of concepts, methods, and standards to make better use of existing information,

share data, leverage national operational picture capabilities, and enable development of interoperability of data, databases, applications, systems, and networks. www.itcm.org/ppt/Retzer_NATO.ppt

Single Integrated Air Picture (SIAP): The air component of the Common Tactical Picture (CTP) that is generated and distributed by the sensors and command-and control systems that make up the Joint Data Network (JDN). The anticipated improvements produced by SIAP will enhance the capabilities of current and future command-and-control systems and aviation platforms. A CTP that is reliable and accurate will provide a significant improvement in the ability to employ aviation assets and increase combat effectiveness while preserving war-fighting assets. http://siap.navsea.navy.mil/public/index.cfm

Single Integrated Ground Picture (SIGP): The SIGP is the collection, correlation and visualization of force-level data that depicts current locations, battlefield geometries, resources and status of red, blue, gray and other ground battlefield forces and systems. SIGP uses non-real-time and real-time information that is correlated, scalable, and filterable to support the tactical commanders C4ISR requirements
http://www.dtic.mil/ndia/2003interop/Tony.pdf

Single Integrated Maritime Picture (SIMP): SIMP is now part of ForceNet.

Single Integrated Space Picture (SISP): SISP provides complete situation awareness and the ability to command and control assigned space forces and the capabilities and effects they bring to the fight. http://www.mat-kmi.com/archive_article.cfm?DocID=89

Standing Joint Force Head Quarters (SJFHQ): The SJFHQ is organized cross-functionally with four joint teams – plans, operations, information management, and information superiority – that form the core of a joint task force command structure. It is a commander centric, effects-based command and control element. The SJFHQ focuses on the non-materiel issues such as doctrine, training, organization and procedures (Joint Task Force readiness) and their interaction with technology in a collaborative information environment. http://www.jfcom.mil/newslink/storyarchive/2003/pa050903.htm

6.6 DoD-Sponsored Research

DARPA Control of Agent Based Systems (CoABS): The CoABS program has focused on technology for run-time interoperability of heterogeneous systems by creating the CoABS Grid and toolkits for rapid creation of interoperable agents to automatically perform integration. From: FACT FILE: A Compendium of DARPA Programs, Defense Advanced Research Projects Agency, August 2003, Page 76.
http://www.darpa.mil/body/pdf/FINAL2003FactFilerev1.pdf

6.7 Other Initiatives

Levels of Information System Interoperability (LISI)： LISI is a maturity model and process for profiling a system's capabilities and implementations in context with various levels of information-exchange interoperability; and a metric for measuring the level of interoperability at which systems are able to interact. http://www.defenselink.mil/nii/org/cio/i3/lisirpt.pdf

Interoperability Clearing House (ICH): ICH is a not-for-profit collaboratory of standards/industry groups, solution providers, testing/research organizations, and IT practitioners helping to advance the capability and integrity of information and communication infrastructures. http://www.ichnet.org/about.html

7 Interview and Workshop Findings

The findings presented here communicate the major themes regarding the problem of interoperability and, where possible, identify promising directions. The findings are drawn from observations and presentations made during the workshops, from the interviews conducted with experts, and from related literature. These are discussed at two levels. First, we consider general themes that emerged during the investigation. Second, we present more specific results according to the dimensions of the SOSI model (i.e., programmatic, constructive, and operational).

7.1 General Themes

The following five general themes emerged during our research. These themes are discussed below:

1. Complexity and combinatorics: many problems and many players
2. Interoperability: more than a technical problem
3. Funding and control: not aligned
4. Leadership, direction, and policy: not effective
5. Legacy: a persistent problem

7.1.1 Complexity and Combinatorics: Many Problems and Many Players

Interoperability is a difficult challenge. This is true whether the goal is to increase interoperability between systems that originally did not interact, or to build new systems designed to interoperate. Unfortunately, very little is known about interoperability requirements at the start of a program. In some cases, the systems that will interoperate are not yet conceived. Thus, new strategies must be developed to anticipate future needs and cope with current uncertainty. In other cases, the constraints imposed by existing systems make approaches to achieving interoperability equally complex.

Some specific issues are described below:

- Backwards compatibility: Maintaining compatibility with older systems sometimes conflicts with achieving greater levels of interoperability between newer systems. This conflict can lead to decisions to accept reduced interoperability between old and new systems. Unfunded mandates that force resources away from patching and upgrading old systems exacerbate the problem. Here, funding/control and legacy issues are intertwined.
- Transitive interoperability: Interoperability between systems is sometimes specified in the following form:
  A is interoperable with B
  B is interoperable with C
  This does not imply that A will be interoperable with C, as is sometimes inferred due to false assumptions.
- Inconsistent standards: A number of attempts have been made to increase interoperability by developing standards and models for architecture (Joint Technical Architecture—JTA) and system components (Defense Information Initiative Common Operating Environment—DII/COE). Unfortunately, using the same standard can give a false sense of assurance. The standards and models alone are insufficient for achieving interoperability, and inconsistencies within standards are sometimes a problem.
- Contractors' processes: Interoperability is hindered by the size and diversity of the systems built and the number of contractors necessary to build those systems. Processes have not been established between contractors to guarantee the required level of interoperability. Further, our experts suggest this problem exists even within a single contractor. As one interviewee stated, "Even with one contractor, we must [define] some processes—you will still have this need."
- Ambiguous terminology: Differences in the use of terms across organizations can be troublesome. The terms used are sometimes mutually exclusive or conflicting. This ambiguity extends down to the operational level. For example, even American armed forces use different terms for cease-fire (e.g., hold fire, weapons hold).
- Rules of engagement and doctrine: The operational context must address the way that a system is used. This is often described in terms of "rules of engagement" or doctrine. In development controlled by one acquisition organization, all information—including doctrine—is controlled in the user-acquisition context. However, when we address interoperability among multiple systems, doctrine also must be interoperable.

The difficulty of the interoperability problem is complicated by the number of organizations and initiatives that are attempting to provide solutions (see Section 6 on DoD initiatives). While it is gratifying to see these resources applied to the problem, the large cast of characters increases the challenges for communication, coordination, and sharing of knowledge and lessons.

7.1.2 Interoperability: More than a Technical Problem

There is common acceptance among our DoD experts that interoperability is not solely a technical problem. Interoperability requires appropriate processes for identifying and communicating requirements, working in concert on enabling technologies, strategy and schedule; and managing joint risks.

Within the technical realm—where new technology solutions are being developed—common agreements are still needed with respect to the meaning (semantics) of shared data and messages. A lesson learned from CASE tool integration tells us that a primary barrier to increased interoperability is the difficulty of reaching such agreements.[1]

Our experts pointed out that reaching agreement about messages and data semantics means that programs will have to compromise, and some systems will have to be reworked or completely rebuilt to achieve and implement consensus. There are reasons why program managers resist making these compromises that relate to matters of funding, control, and incentives, topics that are discussed below. Finally, even in situations where there is great potential for agreement at the programmatic and constructive level, underlying assumptions and expectations related to operations may still obstruct efforts to achieve interoperability.

7.1.3 Funding and Control: Not Aligned

Our experts stressed the contradictions between the objectives for interoperability and current funding models and incentives, which emphasize individual program success for a specific system. They pointed out that interoperability is almost never funded, and reaching agreement between programs is dependent on money: A key factor "for interoperability is who controls the funds." "PEOs [Program Executive Officers] are reluctant to collaborate because then they will have to share or give up some of their funding." The following additional observations were made:

- Interoperability (including overhead) must be planned for, funded, and resourced. One workshop attendee's estimate places the costs to build interoperable systems at 140% of the costs to build similar, non-interoperable systems. "We get [the money] religion real quick. [After all we wouldn't] have done SIAP [Single Integrated Air Picture] without money." Consequently, the current funding paradigm will need to change in order to achieve success.

[1] In the early 1990's, competing industry standards groups (CASE Communiqué and CASE Interoperability Alliance) were separately attempting to reach agreement regarding common services for computer-aided software engineering (CASE) tools. These groups eventually merged and produced a draft standard. However, by the time this occurred, the technology base had already moved on and the standard was no longer applicable.

- DoD program staff is often inexperienced in estimating the costs associated with interoperability. We are not aware of any guidelines for estimating the level of effort necessary to achieve a given level of interoperability.
- Contractors will need to receive incentives to tie a program's success or profit to another program's success.

Beyond money issues, program staff is reluctant to relinquish control. One expert illustrated the problem: "I will be forced to change my perfect implementation … for your imperfect [implementation]." Another added, "Don't take away my control of my stuff."

7.1.4 Leadership Direction and Policy

A barrier to interoperability is a lack of centralized or coordinated ownership of the problem. Shortsighted decisions promote a single system's view at the expense of other systems. Our experts also expressed concern about interoperability with regard to policy making. Some felt that policies were drafted in a vacuum without a full understanding of the problems and the people affected. They observed that: "policy for policy's sake is bad"; "policy needs to be sensitive to the implementer's controls and constraints"; and "policy needs some flexibility." The following additional ideas and comments were presented regarding policy:

- Policy decisions often reflect only a single domain, whereas interoperability concerns may differ across domains, and it may require consideration of special constraints (e.g., environment, safety).
- "Writing policy is the easy step. Implementing it is hard." "No one is collecting data to determine which policies are effective." The timing of policy implementation is also critical: "Just because you put out a policy on interoperability does not mean that all the preexisting systems under development are going to be interoperable."
- Experts suggested that "Contractors sometimes prefer standards/policies like DII/COE or the Joint Technical Architecture (JTA) because they are easier to satisfy by 'checking a box' instead of having to solve the interoperability problem." Sometimes, even when contractors understand the real interoperability problem, they may prefer not to acknowledge it because then they will have to provide a complex and labor-intensive solution. Ironically, in this case, standards/policy can work against doing the right thing.

7.1.5 Legacy: a Persistent Problem

Satisfying expectations for interoperability poses a dilemma: can existing systems be altered to achieve sufficient interoperability? Or, must legacy systems be abandoned to ensure new capabilities? One expert expressed the opinion that, in order for us to achieve the desired levels of interoperability, we would need to eliminate legacy systems and technologies (e.g., legacy communication links). He continued, "At some point you need to start over and raise the technology floor. New technologies tend to break old technologies."

While this perspective is attractive and has utility in isolated cases, it cannot be extended to the broad range of interoperability problems. Today's systems (the ones that must be replaced) are the result of decades of development. It is not feasible in terms of either schedule or cost to redevelop many systems quickly and simultaneously. Moreover, these systems, once constructed, will represent tomorrow's legacy—employing old technologies. In tandem, DoD demands for interoperability will continue to accelerate. "There will always be legacy and any solution that ignores the problem is bound to fail—even if that legacy is represented not in U.S. systems but in allied systems."

7.2 Detailed Results

This section captures the essence of more detailed findings gathered from the interviews, presentations and surveyed literature. The findings were coded according to the category in the SOSI model. The analysis identified the need to enlarge the model to represent factors that extend beyond the purview of a PEO (e.g., vision, policy and standards). As a result, we created a fourth category to represent these environmental factors (see Figure 6).

Most of the findings here speak to constructive concerns. The majority of programmatic concerns have been discussed previously in the General Themes Section. The lack of data on operational issues may be reflective of the long-standing gulf between organizations building DoD systems and those using these systems in the field. The experts we consulted worked in the acquisition stream rather than in operations, and so the emphasis on programmatics and construction is not surprising.

In each of the broad categories (programmatic, constructive, operational and environmental), we identified areas of focus.

8 Programmatic Interoperability

8.1 Requirements

Experts expressed the belief that the emphasis on interoperability is relatively new and easily abandoned in the face of adversity. Until recently, few interoperability requirements were identified, and often only after the system was deployed. Now, programs must expect to depend on others. As a result of compromises, some systems must settle for reduced capability in order to achieve interoperability.

There are currently inconsistent and limited structures for enforcing hard interoperability choices across programs. The Joint Requirements Oversight Council (JROC) represents one attempt to coordinate requirements. Other reorganizations are aligning programs under JFCOM—a single central authority. However, it is not clear whether these attempts at coordination and reorganization will change the day-to-day reality for programs: "The first thing that goes when things get tight is interoperability with non-critical components … Once these requirements for interoperability are removed, the tendency is for the builders to go for solutions that are not as interoperable in order to get increased performance or capability."

8.2 Motivation, Incentives, and Processes

Program offices and contractors are encouraged but not consistently incentivized and rewarded to deliver interoperable solutions. In the past, they have found success by constructing and maintaining their own parochial, proprietary solution. "The problem becomes intractable if the organizations have agendas. It comes down to a big stick and money."

Trials and demonstrations of new approaches for achieving interoperability such as Navy Distributed Engineering Plant (DEP) and the Army Blocking Policy appear to be achieving some success. However, it is not clear how these efforts will translate into everyday acquisition, development, and maintenance activities. The way the Navy handled incentives for Link 16 may provide a model. The Navy created a PMO and funded it with money from affected programs. These monies were returned to programs specifically to work toward Link 16 capability. However, even this approach has limitations. For example, Link 16-compliant programs have implemented different message sets, limiting their interoperability.

Program Offices and contractors often remain stove-piped, with each program doing its own thing and nobody willing to spend more to achieve interoperability. If an organization breaks the mold, spending money to achieve interoperability, things work better. “What is needed are processes that help to reach agreements, blinders to avoid getting distracted by things that are not related (e.g., portability), and to be agnostic about specific technologies (e.g., CORBA or Message Oriented Middleware).”

9 Constructive Interoperability

9.1 Technology

Experts claimed that much of the technology needed to support current interoperability needs already exists. Two exceptions involved real-time applications and multilevel security. First, "Internet Protocol Version 6 fixes many network interoperability problems, but it does not sufficiently address high-speed issues." Second, "Multilevel security appears to be a critical technical problem, although there are some budding solutions like Meridian and Authentica."

The market has converged on data transmission protocols. While this basic technology is present there's been no convergence on common semantics for messages or data. "Systems simply don't operate the same way. They use different time concepts, different tagging of information, and different expectations regarding the order of information, and so on. We currently use complicated rule sets and algorithms to kludge it together—fix it now and hope it doesn't break something."

On reflection, it appears that the experts were stating that they were able to make do with available technologies. However, there is still a great deal of room for improvement: the existing technologies are awkward to use and don't easily lend themselves to simple, maintainable interoperability solutions. Even the best of the technology ingredients, including XML, still require that programs reach agreement on the semantic value of information to be exchanged.

Experts were more uncertain about the technologies needed for the future. Organizations are struggling with Information Exchange Requirements (IERs) in a netcentric context. They claim that "IERs make best sense point to point but if the system is providing a service to a general audience, it is not clear the unique needs of systems are specified. New IER approaches must build in flexibility to expect the unexpected."

9.2 Communication

One critical problem to be resolved is communication between the management, technical, and operational communities. Some experts believed that the technical community does what it can with available technology and funding, but does not do a good job informing

management of the technical implications and consequences. Some issues are understood but poorly communicated and other issues are not understood. As previously indicated, communications and information flow with the operational community are poor.

Interoperability depends on the quality of communication within and between organizations. Intra- and inter-organizational communication is complicated by a lack of

- understanding regarding whom to communicate with
- methodology for how to communicate
- early specification of interoperation ("I built a great little system. I was told to do that piece. I wasn't told about the interface.")
- incentive to pursue interoperability when it makes the work more complex and creates internal and external dependencies that can affect the program

9.3 Data Models

Experts expressed three views regarding approaches to achieving interoperability of data. These approaches are represented in Table 1.

Table 1: Views of Data Interoperability

View	**But …**
Establish a common data model and enforce it: "We really need an underlying data model that everyone uses."	• Data model alone is insufficient; defined functional boundaries between systems are also required. This additional information is necessary to identify which systems use which data in which ways. • Agreeing on common data models is hard. (Different organizations within "a single contractor are experiencing disagreements on common schemas.")
Establish a common data model within a domain and *do not* generalize across other domains.	• See above. • There is a growing tendency to identify interoperability opportunities *across* domains—which is not supported by this view.
Let each program choose its own approach and use technologies like XML to bridge the gap.	• One contractor experimenting with XML has concerns over performance, maintenance, and extension of schemas. • XML still requires agreement on data semantics.

It is important to recognize that even common data models and schemas do not carry the complete semantic value of data. For example, they do not convey timing information, sequencing, and assumptions about how and when the data should be used or interpreted. Furthermore, even if a data model/schema could carry complete semantic information and new systems could be designed to take advantage of that, interoperation will still be limited by non-standard or differing expectations of legacy systems.

9.4 Architecture

In general, the lack of system of systems architectures makes it nearly impossible to understand how systems will interoperate. Some groups within the defense community are trying to create these architectures for various domains (e.g., Global Combat Support System-AF, Global Command and Control System-AF). However, creating architectures will mean that there are winners and losers—some systems will fit cleanly within the boundaries prescribed by the architecture, while others will require extensive and expensive rework.

DoD experts believe that once a system of systems architecture exists, it will be possible to isolate components and services. This will promote interoperability and reuse but also requires planning and flexibility in the definition and use of services and agreements on common semantics for messages and data.

Consensus on common semantics has been difficult to achieve. Our experts suggested that the problem needed to be attacked hierarchically. First, work should focus on interfaces that require broad agreement within specific application domains, such as common representations and semantics for track position and time for radars. Second, small subgroups should be enabled to work on the specifics of domains. Finally, only after progress has been made within domains, groups should be formed to expand to areas beyond. These issues relate both to data models and architecture.

No discussion of DoD architectural standards can be complete without consideration of the C4ISR Architectural Framework and the Joint Technical Architecture (JTA). Synopses excerpted from applicable documents are provided below.

> *The C4ISR Architecture Framework is intended to ensure that the architectures developed by the geographic and functional unified commands, military services, and defense agencies are interrelatable between and among the organization's operational, systems, and technical architecture views, and are comparable and integratable across joint and multi-national organizational boundaries* [DoD 97]. http://www.afcea.org/education/courses/archfwk2.pdf

> *The JTA provides DoD systems with the basis for seamless interoperability. The JTA defines the service areas, interfaces, and standards (JTA elements) applicable to all DoD systems, and its adoption is mandated for the management, development and acquisition of new or improved systems throughout the DoD … The JTA consists of two main parts: the JTA Core and the JTA domains. The JTA Core contains the minimum set of JTA elements applicable to all DoD systems to support interoperability. The JTA subdomains contain additional JTA elements applicable to specific functional domains (families of systems). These elements are needed to ensure interoperability of systems within each domain but may be inappropriate for systems in other domains* [DoD 99].
> http://jta.disa.mil/jta/jtav3-final-19991115/jta30_15nov99.pdf

While these standards may represent a step in the right direction, they are limited in the extent to which they facilitate interoperability. At best, they define a minimal infrastructure that consists of products and other standards on which systems can be based. They do not define the common message semantics, operational protocols, and system execution scenarios that are needed for interoperation. They should not be considered system architectures. For example, the C4ISR domain-specific information (within the JTA) identifies acceptable standards for fiber channels and radio transmission interfaces, but does not specify the common semantics of messages to be communicated between C4ISR systems, nor does it define an architecture for a specific C4ISR system or set of systems.

Additional discussion of standards follows in Section 11.

10 Operational Interoperability

As previously noted, our findings in the area of operational interoperability are limited. This is due to a lack of access to system users.

The experts we interviewed expressed the opinion that little information is shared between systems. Even when sharing occurs, the user interface is not intuitive for users. Much richer interoperability could be achieved if the users played a larger role from inception to deployment of the system. Currently, data owners (i.e., system owners), rather than a combination of owners and users are defining the interfaces, data, and messages.

Nevertheless, our experts were impressed by the opportunistic interoperability that has been achieved. This has occurred as a result of users in the field identifying problems and responding by creating innovative solutions. For example, to enable interoperability between a radio and cryptographic equipment, users reconfigured settings on both devices. Unfortunately, this led to interoperability problems with other systems.

11 Interoperability Environment

11.1 Standards

Our experts suggested that standards are necessary, but not sufficient for guaranteeing interoperability. They believe that the right standards have not yet been developed. They also referred to the contractor's dilemma in having to satisfy performance and other non-functional requirements while adhering to relevant standards. This results in the following phenomenon: "People get waivers; they won't implement the standard without getting paid for it; they will only implement what you directly pay for. Nobody wants to pay for interoperability." In some cases, systems implement the same standard, but still fail to interoperate due to flexibility in the standard and implementation.

There are also problems with application of standards. For example, the Joint Technical Architecture is useful but presents a problem because the level of differentiation by domain is not sufficiently detailed. Our experts argued that even within specific domains and subdomains (e.g., Weapons Systems domain and Aviation subdomain) different systems require different standards profiles. They warn that mandates must not be applied outside of appropriate system context.

Our experts also claimed that "Mandates don't work because they are enforced by tests that miss the point. (For example, two ships pass link certification but can't interoperate.) Or they don't test everything because it is too expensive to test all the rules." In general, our experts suggest that the interoperability certification process is broken. Systems fail but are deployed anyway.

Developing useful standards is extremely difficult. Standards bodies are compromised by unique and sometimes petty demands of different parties, including the services and contractors trying to standardize their solution. Efforts at standardization will always be a delicate balancing act between the desire for commonality, achieving optimal system capability (e.g., performance, space efficiency, security), and changing expectations and technologies.

11.2 Policy

Recent efforts to establish oversight bodies, including expansion of the role of the Joint Forces Command, have been helpful. However, these bodies do not control the funding stream. Our experts observed that: "He who has the gold rules. High rank without control of funding doesn't guarantee that individuals have the authority to enforce interoperability," and "Even with direct orders, debates occur and people go their own ways."

Our experts expressed concern about the limitations of established policies. They claim that policies don't reach down below contractors to subcontractors. They also say that there is little faith in Pentagon policies. "Standards are overgeneralized and overapplied, such as JTA and DII/COE applied to radar."

Policies have moved strongly in favor of performance-based analysis of contractors. It is not clear if this is the right approach for interoperating systems. "The acquisition process for interoperating systems is inappropriate. We never get it right the first time, [we] aren't given time to get it right, [we] are forced to deploy before it is ready. No experiments, no beta time, you can't fail at anything. Acquisition policy doesn't allow for failure."

11.3 Vision

Our experts acknowledged the existence of "grand plans" for interoperability. Simultaneously, they expressed the opinion that there is little understanding of what the services are trying to achieve. The solutions tend to be local. They are concerned that there is no "controlling organization that says what they are going to do and how to architect it."

Part of the challenge in achieving interoperability requires that we reconcile multiple visions from the past, present, and future. The vision for interoperability at any time must include some notion of continuous evolution. Our experts told us that "Today's next generation is the Cooperative Engagement Capability (CEC). We don't know how to do that, but we need to figure out how to do it at the same time we begin thinking about tomorrow's netcentric generation." As discussed previously [see Section 7.1.5 on legacy], it is naïve to assume that there can be a solution for interoperability without addressing the critical role that legacy will play in tomorrow's systems.

There is a basic choice that the DoD must make between centralized (top-down) and decentralized (bottom-up) approaches to acquisition of interoperable systems [Polzer 03]. A centralized, top down approach favors tight constraint of system architectures, design, and operations. This can lead to highly interoperable systems with tightly coupled components. Such systems are also less flexible and harder to change. This approach requires complete analysis and specification up front—often before doctrinal and technological unknowns are resolved.

A decentralized approach to achieving interoperability will rely on looser coupling between components and provide greater freedom in component architecture, design, and operation. Loosely coupled systems are flexible, responsive to change, and often provide opportunities for integrations "on the fly." This approach requires less complete analysis up front but may result in reduced interoperability. Network-accessible services tend to be associated with this approach.

Both approaches have value, but neither guarantees deep semantic information will be shared between systems. The vision of netcentric warfare aspires to maximum interoperability and the greatest flexibility to adapt to new situations. These goals are laudable but not necessarily achievable given the limitations inherent in the basic choices we have outlined.

12 Conclusions and Implications for the Future

The current state of interoperable systems can be summarized as a combination of tight and loose coupling between various system of systems components. Tight coupling tends to occur between systems that perform closely related functions. In Figure 7, systems are represented as circles, and functions provided by systems are indicated by diamonds. Tight coupling is indicated by a solid line. Looser coupling is represented by dotted lines. Tight coupling tends to occur between systems that have been developed by a single military service, or by joint services for a common purpose. Looser coupling occurs where opportunities for inter-operation arise between systems not originally developed to interoperate.

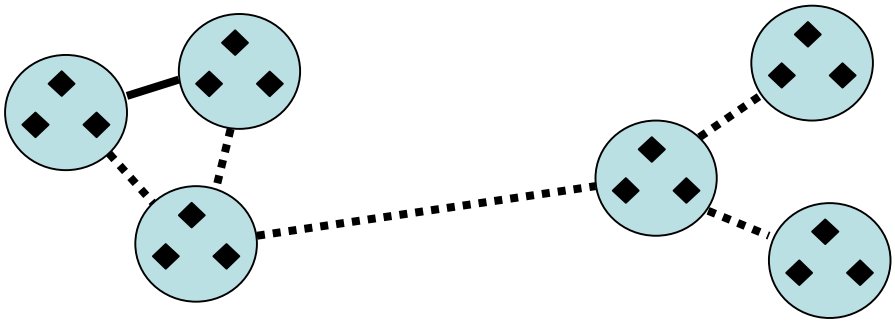

Figure 7: Current State: Tight and Loose Coupling Within Systems of Systems

A practical way to achieve enhanced interoperability may involve a series of intermediate stages providing increasing degrees of connectivity and flexibility (see Figure 8: Interim State). This approach is represented by joint efforts such as FIOP and SIAP. These systems can be characterized as tightly connected clusters of systems. These clusters are likely to be loosely connected to other, independently developed clusters.

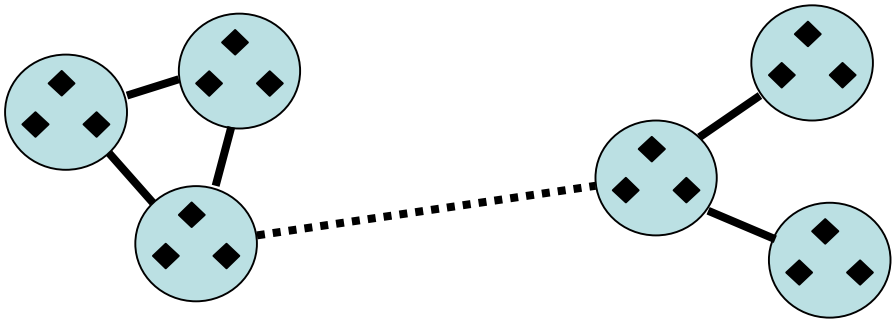

Figure 8: Interim State: Tightly Coupled Clusters Loosely Connected to Other Clusters

Many new programs are grappling with joint requirements generation, shared architectures, and coordinated oversight. However, it remains unclear whether corresponding adjustments have been made to policies and incentives to provide the motivation for change (e.g., funding models). What's really required here is an understanding of what is enabling the current state, and what must change to create incentives for future interoperable systems.

The interoperable environments required to implement Joint Vision 2020 represent a radical departure from the approaches depicted in Figures 7 and 8. In Figure 9, the boundaries representing systems have been erased providing access to individual functions. These functions can be dynamically recombined to comprise new systems. Two different systems are represented by the dashed and solid lines.

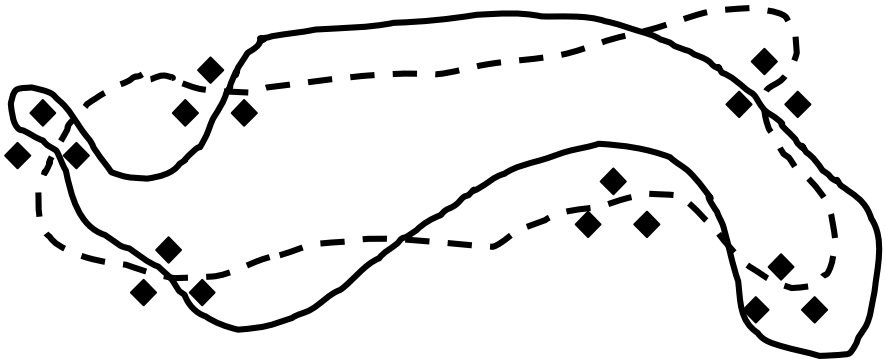

Figure 9: Network of Interoperable Services

We are years away from being able to implement a network of interoperable services. The first ingredients must be a common, consistent problem definition and a concept of operations for netcentric warfare. Necessary technology advances must follow in these areas:

- basic research on network behavior; "emergent properties" of networks

- network fundamentals (e.g., routing, forwarding); adaptive dynamic networking
- modeling and simulation of component interactions
- effect of component architectures on quality attributes (e.g., security, reliability, survivability and reconfigurability) of systems of systems
- service-oriented architectures defining basic and higher level capabilities for system composition
- capability to specify semantic assumptions and expectations about shared data
- approaches for legacy system integration and migration

Even with these necessary technology advances, success will not be achieved without corresponding changes in policy, funding and incentives, and the development of complementary acquisition approaches.

The complexity of the transition to netcentric warfare should not be underestimated. Not only must interim solutions such as SIAP be developed (Figure 8), they must be developed in such a way as not to preclude working in a network of interoperable services (Figure 9). Joint efforts of today represent the legacy of tomorrow. As we have observed, legacy systems will remain regardless of new approaches and strategies. Any solution that ignores the problem of legacy, in U.S. systems or those of our allies, is destined to fail.

The SOSI IRAD took initial steps to study the problem of interoperability now and in the future. The SEI has also formed a new initiative focused on exploring Integration of Software-Intensive Systems (ISIS).

The SEI is well positioned to analyze existing technologies and identify missing technologies to achieve the vision of netcentric warfare. As appropriate technologies are identified, the SEI can facilitate the transition of these technologies to DoD programs.

The SEI has experience in driving process and technology change. We can exploit this experience with process and maturity models to affect the way organizations interact with respect to programmatics. We have been successful with process improvement on the intra-organizational level. Inter-organizational issues represent a new challenge.

Some specific activities that the SEI might become involved in include

- classification of the interoperability problem space
- work with others toward a complete and consistent set of interoperability models
- understanding of ramifications of netcentric warfare from a software and systems perspective

- analysis of emerging technologies
- planning for migration and incorporation of legacy systems
- analysis of existing and new acquisition regulations and policies; identification of barriers

Achieving interoperability involves changes to the way the DoD does business, including: acquisition practices and guidance, technologies, engineering and management practices, operational doctrine for both the warfighter and those who support the systems. Joint Vision 2020 provides further challenges for the future. Realizing this vision requires that we begin to define approaches and models in more concrete terms.

Appendix: Interview Script

As part of the System of Systems Interoperability (SOSI) IR&D at the SEI, we are interviewing people who understand interoperability issues well. We would like to spend about 1-1.5 hours on the phone with you to pick your brain. We have attached a short introduction explaining what we are trying to accomplish. We would like to set up an interview at some other time convenient to you. We will be asking you to address some of the following questions.

System Information

- How do you define interoperability?
- Describe your system.
- With what other systems must your system interoperate?
- What are the primary functions of the other systems?
- How is your system expected to interoperate with these other systems?
- How complex is this interoperability?

Programmatic

- What organizations manage/control the systems?
- Where in the life cycle are the systems?
- What organizational characteristics helped interoperability? Hurt?
- What cross-organizational mechanisms were established to support interoperability? What helped?
- What regulations and policies govern system development? Do these help or hinder interoperability? How?
- Is this a joint program?
- Who controls the direction of programs constructing/supporting systems with which your system must interoperate?
- What was the relative importance of achieving interoperability in decisions regarding architecture, design, and implementation?

- Where in the hierarchy is joint control applied?
- How are risks managed internally?
- How are risks relative to interoperability managed? How is this information shared?
- How is scheduling managed when there are interoperability dependencies on other systems?
- What early insight do programs get regarding capabilities in releases and interfaces?
- To what degree did your program have influence on technical direction, documentation, standards, construction, testing, and so on?
- What guidance did you have regarding such decisions that were made by others?
- To what extent did advocates for systems with which your system was required to interoperate participate in the decision process?
- What was the relative importance of achieving interoperability in user acceptance, rewards and incentives, cost and schedule, and so on?
- Were joint incentives available? Were they earned by the parties involved? Were they successful in stimulating the expected results?
- What is the nature of your relationship with interoperation counterparts (contractual, practical, etc.)?

Constructive

- What mechanisms are used to provide interoperability?
- Where did these mechanisms work well? Where were they deficient?
- What other mechanisms are needed?
- What were the major interoperability successes? failures?
- Have there been difficulties interpreting data from other systems?
- What types of system-of-system modeling of interoperability were done?
- How much did this help? Why?
- When and where were interoperability problems identified?
- How were they resolved?
- What standards are intended to support interoperability? Are they sufficient? Where could they be made better?
- What standards are you using? What other mechanisms – home grown and other?
- Did existing systems with which you were required to interoperate support these?

- How is system testing accomplished? Does system testing include interoperability testing? How is this accomplished?
- How is system of systems testing accomplished?
- What types of interoperability problems became evident during system testing? System-of-system testing?
- How were configurations of systems of systems managed during development?
- How were shared interfaces and other interoperability characteristics identified?
- How were decisions regarding security, performance, reliability, safety, and so on, made so that they reflected interoperability?

Operational

- Was a common conop developed? When and how?
- Were common user protocols and instructions developed? When and how?
- How were configurations of systems of systems managed during deployment?

References/Bibliography

URLs are valid as of the publication date of this document.

[C4ISR 98] C4ISR Interoperability Working Group, Department of Defense. *Levels of Information Systems Interoperability (LISI)*. Washington, DC: 1998. <http://www.defenselink.mil/nii/org/cio/i3/lisirpt.pdf> (1998).

[Clark 99] Clark, T. & Jones, R. "Organisational Interoperability Maturity Model for C2." *Proceedings of the 1999 Command and Control Research and Technology Symposium*. United States Naval War College, Newport, RI, June 29-July 1, 1999. Washington, DC: Command and Control Research Program (CCRP), 1999. <http://www.dodccrp.org/events/1999/1999CCRTS/pdf_files/track_5/049clark.pdf >(1999).

[DoD 97] Department of Defense. *C4ISR Architecture Framework Version 2.0.* Architecture Working Group Washington, DC: 1997. <http://www.afcea.org/education/courses/archfwk2.pdf >(1997).

[DoD 99] Department of Defense. *Joint Technical Architecture Version 3.0.* Washington, DC: 1999. <http://jta.disa.mil/jta/jtav3-final-19991115/jta30_15nov99.pdf > (1999).

[DoD 01a] Department of Defense. Joint Pub 1-02, DoD *Dictionary of Military and Associated Terms.* Washington, DC: 2001. <http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf> (2001).

[DoD 01b] Department of Defense. Chairman of the Joint Chief of Staff (CJCS) Instruction 3710.01B, *Requirements Generation System*. Washington, DC: 2001. <http://www.dtic.mil/doctrine/jel/cjcsd/cjcsi/3170_01b.pdf> (2001).

[Fewell 03] Fewell, S. & Clark, T. "Organisational Interoperability: Evaluation and Further Development of the OIM Model." *8th International Command and Control Research and Technology Symposium (ICCRTS)*, Washington, DC, June 17-19, 2003. Washington DC: Command and Control Research Program (CCRP), 2003. <http://www.dodccrp.org/8thICCRTS/pdf/028.pdf> (2003).

[GIG 01] *Global Information Grid (GIG) Capstone Requirements Document* (*CRD),* Flag Draft. Washington, DC: March 28, 2001.<http://www.dfas.mil/technology/pal/regs /gigcrdflaglevelreview.pdf> (2001).

[IEEE 00] IEEE Standards Information Network. *IEEE 100, The Authoritative Dictionary of IEEE Standards Terms*, Seventh Edition. New York, NY: IEEE, 2000.

[Joint 00] Joint Chiefs of Staff. *Joint Vision 2020*. Washington, DC: U.S. Government Printing Office. <http://www.dtic.mil/jointvision/jvpub2.htm> (2000).

[Levine 03] Levine, L.; Meyers, B. Craig.; Morris, E.; Place, P.; & Plakosh, D. *Proceedings of The System of Systems Interoperability Workshop (February 2003)* (CMU/SEI-2003-TN-016). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003. <http://www.sei.cmu.edu/publications/documents/03.reports /03tn016.html> (2003).

[NATO 03] NATO C3 Technical Architecture (NC3TA) *Reference Model for Interoperability.* The Hague, The Netherlands: 2003. <http://www.nc3a.nato.int/index.html> (2003).

[Polzer 03] Polzer, Hans. *Systems Integration: Creating an Evolutionary Environment to Foster Capability-Oriented Interoperability*. Bethseda, MD: Lockheed Martin, 2002. <http://www.dtic.mil/ndia/2002interop/polzer.pdf> (2002).

[Tolk 03a] Tolk, Andreas & Muguira, James *A.* "The Levels of Conceptual Interoperability Model." *2003 Fall Simulation Interoperability Workshop* Orlando, Florida, September 2003. <http://www.vmasc.odu.edu/publications/Tolk/03F-SIW-007.pdf> (2003).

[Tolk 03b] Tolk, Andreas. "Beyond Technical Interoperability – Introducing a Reference Model for Measures of Merit for Coalition Interoperability." *8th International Command and Control Research and Technology Symposium (ICCRTS)*, Washington, DC, June 17-19, 2003. Washington DC: Command and Control Research Program (CCRP), 2003. <http://www.dodccrp.org/8thICCRTS/pdf/084.pdf> (2003).

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	April 2004	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
System of Systems Interoperability (SOSI): Final Report	F19628-00-C-0003

6. AUTHOR(S)

Edwin Morris, Linda Levine, Craig Meyers, Pat Place, Dan Plakosh

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2004-TR-004

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116	ESC-2004-TR-004

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	56

13. ABSTRACT (MAXIMUM 200 WORDS)

This technical report documents the findings of an internal research and development effort on system of systems interoperability (SOSI). The study was based on the belief that interoperability must occur at multiple levels within and across programs, and not solely in the context of a system construction. The Software Engineering Institute looked at the full range of barriers to achieving interoperability between systems, including programmatic, constructive, and operational barriers. An initial SOSI model representing this perspective was developed. The research method consisted of three activities: review of related research, conducting of small workshops, and interviews with experts. The literature survey focused on Department of Defense and related initiatives dedicated to achieving interoperability. Workshops were held in Washington, D.C. in February and May 2003. Interviews were conducted with experts representing each of the services, the National Reconnaissance Organization, and industry. Results from these activities are presented here.

14. SUBJECT TERMS	15. NUMBER OF PAGES
interoperability, system of systems, Organizational Interoperability Model, Levels of Information Systems Interoperability Model, Levels of Conceptual Interoperability Model, NATO 3 Technical Architecture Model, Levels of Conceptual Interoperability Model	63

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	UL