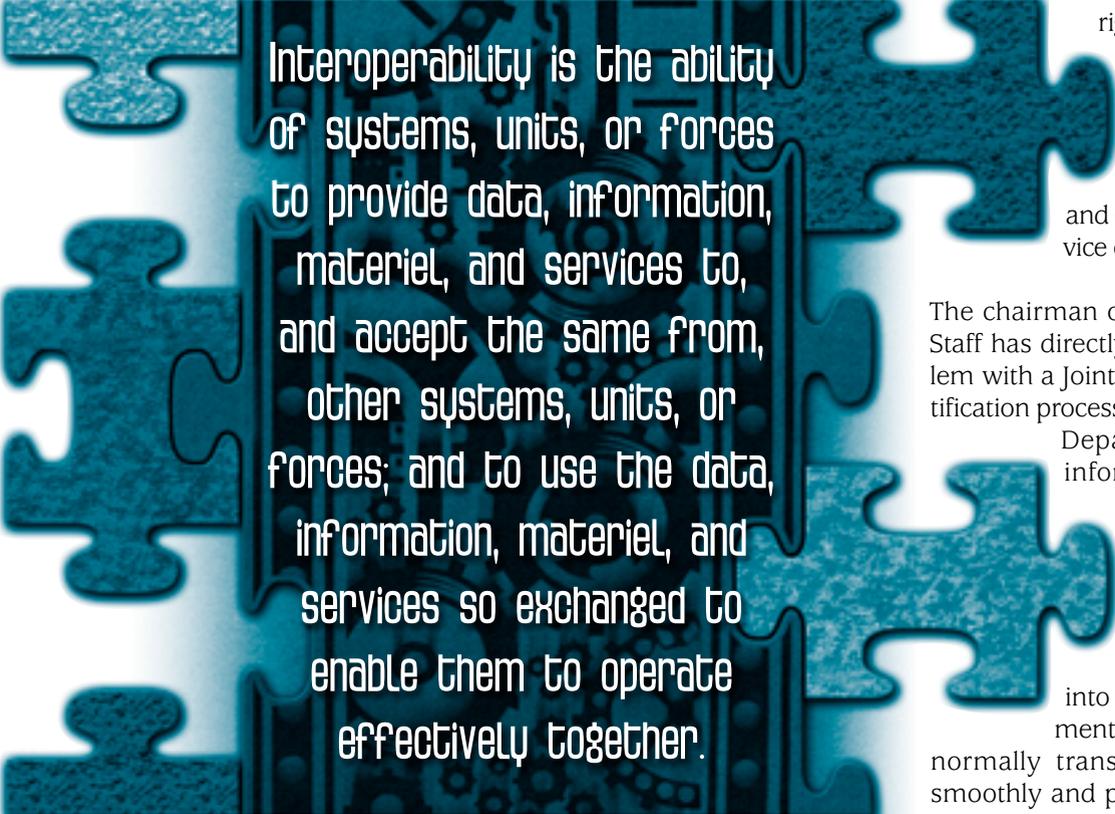


Joint Interoperability Certification

What the Program Manager Should Know

Phuong Tran ■ Gordon Douglas ■ Chris Watson



Interoperability is the ability of systems, units, or forces to provide data, information, materiel, and services to, and accept the same from, other systems, units, or forces; and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together.

right people at the right time. That often happens when systems don't share information and interoperate efficiently and effectively across Service or agency boundaries.

The chairman of the Joint Chiefs of Staff has directly attacked this problem with a Joint Interoperability Certification process that applies to every Department of Defense information technology (IT) system and national security system (NSS).

Systems that integrate this process into their overall development and testing schedule normally transition into the field smoothly and provide the best support to their users. Programs where

interoperability problems are discovered too late may suffer delays, cost overruns, or—worst of all—contribute to deadly mistakes at critical times.

Program managers need to understand the process and use it to their advantage; and in order to understand, a few basic questions need to be answered.

What is interoperability?

Interoperability is the ability of systems, units, or forces to provide data, information, materiel, and services to, and accept the same from, other systems, units, or forces; and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. IT

Would you agree that a program manager whose system meets performance requirements, is on schedule, and within budget, is in good shape? If your answer is “yes,” you might, in fact, be wrong if the system isn't interoperable with its surrounding systems or networks.

They Should Have Known

Whenever the public is made aware of an apparent military failure resulting from inaccurate or delayed information, critics say, “They should have known.” While human error, mechanical failure, and the fog of war all play their part, the critics are sometimes right. Some people *did* know, but the right information didn't get to the

Tran is the chief of the Plans and Policies Branch, Joint Interoperability Test Command. She is a graduate of the University of Arizona and University of Phoenix and has almost 20 years of government service in the T&E arena. *Douglas* is an operations research analyst with the Plans and Policies Branch, Joint Interoperability Test Command. He is a graduate of the University of Arizona, with more than 20 years of military, government, and private industry experience in research, engineering, and T&E. *Watson* serves as an information systems test director and corporate communications officer for the JITC organization. His experience encompasses over 20 years in the operation, training, and testing of military IT systems.

and NSS interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchanged information as required for mission accomplishment. Interoperability is more than just information exchange; it includes systems, processes, procedures, organizations, and missions over the life cycle, and it must be balanced with information assurance.

What is interoperability certification?

Interoperability certification is the process of ensuring that a system meets the joint interoperability requirements of its users. It includes the collection of the data necessary to determine whether or not the system conforms to applicable interoperability standards and can effectively exchange all required information with all pertinent systems.

Why is interoperability certification necessary?

Interoperability certification assures the warfighter that the combatant commander, the Services, and agency systems can interoperate in a joint, combined, and coalition environment.

Who certifies that a system is interoperable in a joint environment?

The Joint Interoperability Test Command (JITC—an organizational element of the Defense Information Systems Agency, Test & Evaluation Directorate) has responsibility for certifying joint and combined interoperability of all DoD IT systems and NSSs. JITC facilities are strategically located at Fort Huachuca, Ariz., and Indian Head, Md. The diverse capabilities and resources associated with each respective location allow the armed services to have access to a dynamic environment for laboratory tests and on-site field evaluations.

What systems need to be certified?

All IT systems and NSSs that exchange and use information to enable units or forces to operate effectively in joint, combined, coalition, and interagency operations and simulations.

When should systems be certified?

All systems must be certified before they are fielded. Fielded systems must be recertified every three years or after any changes that might affect interoperability. The system proponent should contact JITC early in the acquisition program to ensure that certification is timely and cost-effective.

What does certification involve?

JITC follows the processes outlined in *Chairman, Joint Chiefs of Staff Instruction 6212.01, Interoperability and Supportability of Information Technology and National Security Systems*, to perform the joint interoperability test and certification mission. This document establishes policies and procedures for developing, coordinating, reviewing, and

approving IT and NSS interoperability needs. It also establishes procedures for performing interoperability test certification using a new “net-ready” approach.

Generally, the Interoperability Test Certification process consists of four basic steps. Joint interoperability testing and evaluation can be a repetitive process as conditions change. The steps are to:

- Identify (interoperability) requirements
- Develop certification approach (planning)
- Perform interoperability evaluation
- Report certifications and statuses.

Identifying Interoperability Requirements

Establishing requirements is a critical step, and system sponsors must resolve any requirements/capabilities issues with the Joint Staff J-6. The Joint Staff J6 must certify specific requirements/capabilities if system validation is required. The JITC provides input to the J6 requirements/capabilities certification process and uses the results as the foundation for the remaining three steps of the Interoperability Test Certification process.

The requirements-generation process has been strengthened with the publication of the CJCSI 3170.01, Joint Capabilities Integration and Development System (JCIDS). The JCIDS supports the Joint Staff and the Joint Requirements Oversight Council (JROC) in identifying, assessing, and prioritizing joint military capability needs. As prescribed by the JCIDS process, JITC will participate in the technical assessment of all IT and NSS capability and requirements documents to ensure interoperability requirements are specified in measurable and testable forms. JITC assists in identifying requirements contained in such sources as the program’s capability development document (CDD), capability production document (CPD), and information support plan (ISP).

Once requirements are identified, JITC develops a joint interoperability requirements matrix and confirms it with the appropriate operational command or agency. This matrix then serves as the basis for development of the certification approach.

Developing the Certification Approach

JITC’s evaluation strategy will identify data necessary to support Joint Interoperability Test Certification as well as the test events/environments planned to produce those data. The current evaluation strategy is driven by DoD’s architectural shift towards a net-centric operational environment.

The foundation of DoD’s net-centric environment is the Global Information Grid. The GIG is the globally interconnected, end-to-end set of capabilities, processes, and resources for collecting, processing, storing, managing, and disseminating on-demand information to the

IN MEMORIAM



Dr. Franz A.P. Frisch died Nov. 20, 2005, in Jackson, Miss., at the age of 86. Witty, colorful, unique, and having lived the World War II history he often wrote about, Frisch remained a popular colleague, mentor, friend, and after his retirement, professor emeritus of the Defense Systems Management College (DSMC) at

Fort Belvoir, Va. He first joined the DSMC faculty in 1978 as chief of the Technical Management Division, left for employment with the Navy in 1981, and rejoined DSMC in 1987. After serving over 13 years as a DSMC professor and associate dean, he had retired from federal service in June 1998.

A private in the German Army for nine years, Frisch was an artillery *soldat*, or German simple (common) soldier, whose battalion participated in numerous Panzer assaults in the European war. Drafted from his home in Vienna in 1938, Frisch saw action in the German invasions of Poland in 1939, which began WWII; France in 1940; and the Soviet Union in 1941. In Russia, his unit reached the outskirts of Moscow before the Soviet counterattack and the extreme bitter winter cold forced the Germans backward.

In 1943, his artillery unit was assigned to defend Sicily against the invading Americans. Retreating to Italy, his battalion fought the American advance, including at the bloody Battle of Casino, northward up "the boot," where the Americans captured him

near the Austrian border in March 1945, two months before Germany surrendered. He spent the next two years in a prisoner of war camp in Italy before returning home.

Following the war, Frisch completed his education at the Technical University of Vienna, attaining a doctorate in engineering management. After a successful career in shipbuilding and shipyard management in Germany, he and his family emigrated to the United States in 1958.

Besides teaching on the DSMC faculty for more than 13 years, Frisch was also an adjunct professor for Virginia Polytechnic Institute and State University, as well as Massachusetts Institute of Technology, where he taught graduate courses in advanced engineering economy and management concepts.

Frisch published papers on transportation, naval architecture, economy, and management, among other subjects. In 2003, former DSMC professor Wilbur D. Jones collaborated with Frisch to research and write a book on Frisch's campaigns, *Condemned to Live: A Panzer Artilleryman's Five-Front War*.



Preceded in death two years ago by his wife Traudel, Frisch is survived by three daughters who will carry the ashes of both their parents to Europe next spring to be spread over the Danube in their native Austria.

warfighter. This environment compels a shift from "system-to-system" to "system-to-Service" exchange to enable on-demand discovery of and access to all available information resources.

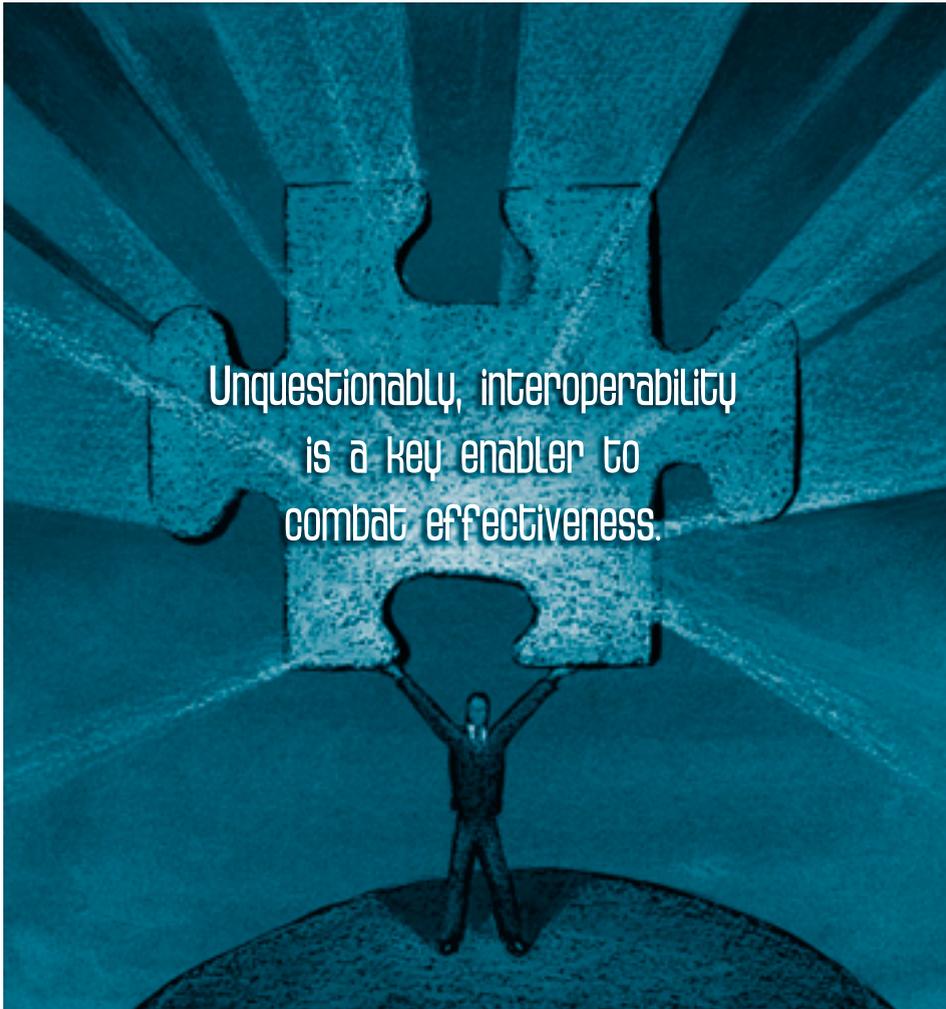
As the GIG evolves toward a net-centric architecture, interoperability testing must also evolve. Increasingly, the requirement will be to test a system's ability to successfully discover and employ the appropriate information resources within the context of the GIG.

The main component of this new approach to interoperability testing is the net-ready key performance parameter. The NR-KPP consists of measurable, testable, or

calculable characteristics and/or performance metrics required for the timely, accurate, and complete exchange and use of information expressed by the following four elements:

- Compliance with the Net-centric Operations and Warfare Reference Model (NCOW RM)
- Integrated architecture products
- Compliance with applicable key interface profiles (KIPs)
- Compliance with DoD information assurance (IA) requirements.

The NCOW RM describes the activities required to establish, use, operate, maintain, and manage the net-centric enterprise information environment. It also describes



gral part of net-readiness. All GIG information systems must implement IA elements, such as information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. Also included are system restoration and threat detection capabilities.

All CDDs, CPDs, and ISPs for systems that exchange information with external systems will be reviewed and certified based on adherence to NR-KPP criteria. In turn, JITC will use the NR-KPP thresholds and objectives to ensure that all system information exchange requirements have been satisfied during all applicable test events. These test events must be conducted in an operationally realistic environment. This includes employing production-representative systems, members of the user community as operators, and realistic messages and network loads.

a selected target set of key standards that will be needed as the NCOW capabilities of the GIG are realized.

Integrated architecture product descriptions assist DoD in understanding the linkages between capabilities and systems. An integrated architecture consists of three major perspectives or views—operational, system, and technical—that logically combine to describe a program's architecture. The architecture is integrated when the data elements defined in one view are the same as architecture data elements referenced in another view. Each of the three views depicts certain architecture attributes. Some attributes bridge two views and provide integrity, coherence, and consistency to architecture descriptions.

Because of the complexity of the GIG environment, a form of enterprise-level integration management is needed to facilitate interoperability testing at the seams of GIG components. GIG KIPs are used to communicate the technical specification of the applicable DoD IT Standards Registry (DISR) standards and the implementation of these standards as they apply to key interfaces.

All IT and NSSs must comply with applicable DoD information assurance policies and instructions. IA is an inte-

Performing the Interoperability Evaluation

Interoperability evaluation often spans developmental testing (DT) and operational test and evaluation (OT&E) and relies on multiple test events conducted by various organizations. The amount and type of testing will vary based on characteristics of the system being evaluated.

DT looks at how the system and its components meet the specifications to which the contractor/vendor signed up to build. With the new acquisition strategies, such as spiral development, testers are involved earlier; this helps JITC collect information and data to reduce risk and the time required for interoperability certification and operational testing or assessments. Verification of conformance to standards is one of the first steps in the interoperability testing process. As IT systems/NSSs are designed, the developer is required to implement standards or products contained within the DISR. Early on in the development/acquisition cycle, the particular IT system/NSS (or components of the system) is tested to ensure that the chosen standards are properly implemented. Conformance with DISR standards does not guarantee interoperability, but it is an important step toward achieving it. Developmental testing performed under govern-

LETTERS.

We Like Letters.



You've just finished reading an article in *Defense AT&L*, and you have something to add from your own experience. Or maybe you have an opposing viewpoint.

Don't keep it to yourself—share it with other *Defense AT&L* readers by sending a letter to the editor. We'll print your comments in our "From Our Readers" department and possibly ask the author to respond.

If you don't have time to write an entire article, a letter in *Defense AT&L* is a good way to get your point across to the acquisition, technology, and logistics workforce.

E-mail letters to the managing editor:
defenseat&l@dau.mil.

Defense AT&L reserves the right to edit letters for length and to refuse letters that are deemed unsuitable for publication.

ment supervision that generates reliable, valid data can be used to determine technical capabilities and standards-conformance status, and may supplement operational data for an interoperability evaluation.

As the only joint operational test agency (OTA) in accordance with Title 10 of the United States Code, JITC plays several key roles in the OT&E process as well. As DISA's OTA, JITC oversees and carries out all phases of OT&E pertaining to DISA-managed programs. Through policy and agreement, JITC also serves as the OTA for other DoD organizations that do not have their own dedicated test resources. JITC's OT&E strategy involves planning and conducting tests under realistic combat conditions to determine the effectiveness and suitability of the system/program. During these events, JITC views interoperability and net-readiness as operational effectiveness issues.

JITC works closely with the military service OTAs before or during a system's operational test readiness review (OTRR). When JITC is involved, it will provide input to the OTRR covering interoperability/net-ready aspects of the program based upon pertinent information. In many cases, JITC will be fully involved during a Service's OT&E event for the sole purpose of gathering the appropriate data necessary to certify the system for joint interoperability.

JITC also supports the objectives of the director of operational test & evaluation (DOT&E) by assisting the exercise staffs in planning, execution, data collection, analysis, and reporting on IA and interoperability of operational networks and architectures involved in combatant commander field exercises.

Throughout the acquisition cycle, JITC will use any valid data from DT, OT&E, demonstrations, field exercises, or other reliable sources for interoperability evaluations. Each potential data collection opportunity should be used in the overall certification process to get the best interoperability picture of the system in the most efficient manner possible.

Reporting Interoperability Status

Certification is based on Joint Staff-certified capabilities and requirements, the criticality of the requirements, and the expected operational impact of any deficiencies. Certification is applied to the overall system if all critical interfaces have been properly implemented and tested. Interoperability status represents the extent to which a system is interoperable with respect to the elements of the NR-KPP, information exchanges, and other defined interoperability requirements.

What will JITC do to get your system certified?

When contacted by a program manager early in the acquisition process, JITC will:

- Assist in identifying joint interoperability requirements during the concept development/design phase of the program
- Ensure that interoperability is built into the system from the start
- Plan for the most efficient use of resources
- Assist the program manager in identifying solutions to interoperability problems necessary to get the system certified.

JITC also has a range of tools available for system assessments and laboratory resources for testing virtually all types of IT system and NSS.

What will happen if a PM fails to participate in the Joint Interoperability Certification process?

The simple answer to this question comes straight from 6212.01:

2. *Failure to meet Certifications*
 - a. *If a program/system fails to meet certification requirements, the J-6 will:*
 - (1) *Not validate the program.*
 - (2) *Recommend the program not proceed to the next milestone.*
 - (3) *Recommend that funding be withheld until compliance is achieved and the program and/or system is validated.*
 - b. *The J-6 will make this recommendation to the USD (AT&L), USDP, USD (C), ASD (NII), DoD Executive Agent for Space, the Military Communications-Electronics Board (MCEB), and the JROC. The J-6 will also request that the program and/or system be added to the DODI 4630.8, Interoperability Watch List (IWL).*

Of course, real-world capability development and testing are rarely simple, and the DoD has provided several mechanisms for identifying and seeking solutions to current or foreseen interoperability problems. DoD policy clearly states that all IT and NSS, regardless of acquisition category (ACAT), must be tested and certified for interoperability before fielding. The Military Communications Electronics Board (MCEB) Interoperability Test Panel (ITP), identifies, coordinates, and resolves IT system/NSS interoperability policy and testing issues to ensure compliance with DoD policy regarding interoperability of IT system/NSS during the requirements validation process and throughout the remainder of the acquisition life cycle.

To further assist in monitoring compliance with DoD policy regarding interoperability certification, the ITP provides semi-annual interoperability status briefings to the MCEB. These typically provide the overall interoperability status of a functional area or family or system of systems to the MCEB, identifying capabilities that may require additional attention or assistance to achieve full

interoperability. When necessary, the ITP may nominate programs for inclusion on the Interoperability Watch List (IWL) of the Interoperability Senior Review Panel (ISRP) established in DoD Instruction 4630.8. Criteria for nominating programs to the IWL include, but are not limited to, the following:

- No plans for (JITC) Joint Interoperability Certification testing
- Failed (JITC) Joint Interoperability Certification tests and no plans for addressing identified deficiencies
- Lack of JCIDS or test documentation for defense technology projects and pre-acquisition demonstrations
- Known interoperability deficiencies observed during operational exercises or real world contingencies
- Noncompliance with approved integrated architectures.

Once a program is placed on the IWL, it is the PM's responsibility to undertake corrective action to address interoperability deficiencies and report progress to the principals represented on the ISRP. If interoperability issues are not adequately addressed or if deficiencies persist, the program or system may be recommended for transfer to the OSD T&E oversight list.

In certain cases, the ITP may grant an Interim Certificate to Operate that may not exceed one year. The ICTO provides the authority to field new systems or capabilities for a limited time with a limited number of platforms to support development efforts, demonstrations, exercises, or operational events, without an interoperability test certification. It is the PM's responsibility to submit the ICTO request. As the ITP executive agent, JITC provides recommendations to the ITP for or against the ICTO, based on available interoperability data and an evaluation of the possible risk to the user and other connected systems. After reviewing the PM's justification statements and JITC's recommendations, the ITP will vote to approve or disapprove the request.

Assurance of Interoperability for the Nation's Warfighter

Unquestionably, interoperability is a key enabler to combat effectiveness. JITC will continue to play an active role in the joint interoperability test and certification process. This proven process affords higher levels of assurance that warfighting systems will interoperate properly so that the battleground does not become the testing ground.

To obtain more information about the Joint Interoperability Certification process, call 800-LET-JITC (800-538-5482) or visit <<http://jitc.fhu.disa.mil>>.

The authors welcome comments and questions and can be contacted at phuong.tran@disa.mil, gordon.douglas@disa.mil, and chris.watson@disa.mil.