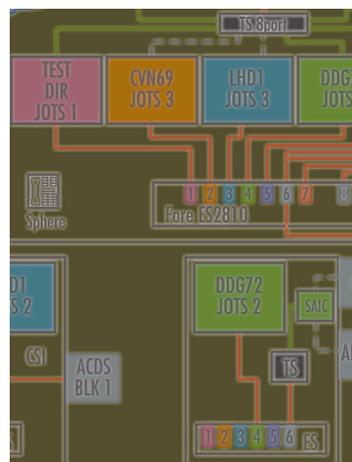


C⁴ISR Systems Integration and Interoperability ■



C⁴ISR Involvement with the Distributed Engineering Plant (DEP)	135
BeEm V. Le (SSC San Diego)	
The Over-the-Horizon Targeting (OTH-T) Program and the Reconfigurable Land-Based Test Site (RLBTS) Laboratory	141
Gary E. McCown (SSC San Diego)	
Automation in Software Testing for Military Information Systems	148
Jack Chandler (SSC San Diego)	
Systems Integration Facility: Past, Present, and Future	155
David P. Andersen (SSC San Diego) Karen D. Thomas (Digital Wizards, Inc.)	

C⁴ISR Involvement with the Distributed Engineering Plant (DEP)

BeEm V. Le
SSC San Diego

BACKGROUND

In February 1998, the Fleet was concerned about interoperability failures among combat systems recently installed in deploying fleet units. These failures led to two modern combatants being tied to the pier during their Battle Group deployment. During the final 6 months before Battle Group deployment, shipboard and Battle Group "debugging" of systems consumed valuable fleet training time. In March 1998, the Chief of Naval Operations assigned to Naval Sea Systems Command (NAVSEA) the responsibility to address combat systems interoperability problems across Battle Management Command, Control, Communications, Computers, and Intelligence (BMC⁴I)/combat systems, and to coordinate resolution with the Fleet. In April 1998, NAVSEA formed the Task Force on Combat System Interoperability to study the interoperability crisis and provide recommendations for solutions. In May 1998, the Task Force was formally tasked to determine the feasibility and cost of using a land-based Distributed Engineering Plant (DEP) to support the design, development, test, and evaluation of interoperability of Battle Force systems. In June 1998, the Task Force on Combat System Interoperability reported that the establishment of a DEP was technically possible, but organizationally difficult because of the diverse group of organizations and elements. The Task Force also stressed that a DEP is only a tool to enable good design decisions early in the acquisition process. Following the Task Force Report, the collection of government activities represented in Table 1 formed a cooperative effort known as the Navy Alliance.

The Navy Alliance, made up of surface, air, subsurface, and command, control, communications, computers, intelligence, surveillance, and reconnaissance (C⁴ISR) components, crosses all Navy Systems Commands (SYSCOMS). The Navy Alliance developed a proposal for the establishment and implementation of a Navy DEP. The following sections

ABSTRACT

The Navy's requirement for interoperability between systems and Battle Groups led to the development of the Distributed Engineering Plant (DEP). The DEP Battle Group Interoperability Test (BGIT) was a combination of several Navy laboratories in which command, control, communications, computers, intelligence, surveillance, and reconnaissance (C⁴ISR) systems were tested within the DEP. This paper focuses on C⁴ISR integration and interoperability testing accomplished by the DEP BGIT program. It also discusses the support that C⁴ISR systems provide the Fleet and problems found during the DEP BGIT.

TABLE 1. Navy Alliance.

Naval Surface Warfare Center/Dahlgren Division—Dahlgren, VA
Aegis Combat Systems Center—Wallops Island, VA
Naval Warfare Analysis Station—Corona, CA
Naval Undersea Warfare Center—Newport, RI
Naval Surface Warfare Center/Port Hueneme Division (PHD)—Oxnard, CA
SSC San Diego—San Diego, CA
Naval Surface Warfare Center/PHD—Dam Neck, VA
SSC Charleston—Charleston, SC
Naval Surface Warfare Center/PHD—San Diego, CA
Aegis Training and Readiness Center—Dahlgren, VA
Naval Research Laboratory—Arlington, VA
Johns Hopkins University (JHU) Applied Physics Laboratory—Laurel, MD
Naval Air Warfare Center/Aircraft Division—Patuxent River, MD
Naval Air Warfare Center/ Weapons Division—China Lake, CA

describe the DEP concept as drafted by the Task Force, and developed and engineered by the Navy Alliance. The DEP was founded on the existence of shore-based combat system sites. These combat system sites were built to replicate the hardware, computer programs, connectivity, and environment of the ship and aircraft combat systems as much as possible. The DEP extends this concept to the Battle Group level by interconnecting these combat system sites to replicate a Battle Group. Given that the DEP is founded on shore-based combat systems, understanding the DEP begins with an understanding of a basic combat system. The combat system consists of many important elements integrated to form a system.

Space and Naval Warfare Systems Command (SPAWAR) and DEP

The plan from SSC San Diego and Space and Naval Warfare Systems Center, Charleston (SSC Charleston) was to incorporate the C⁴ISR family of systems into the DEP. This plan complemented the Battle Group/Battle Force (BG/BF) interoperability Navy Alliance proposal, but focused on implementing the DEP C⁴ISR component. The plan also detailed the roles of major Space and Naval Warfare Systems Command (SPAWAR) participants and provided a technical approach for integration of SPAWAR test resources with the DEP.

SPAWAR's mission was to deliver integrated interoperable C⁴ISR systems to the operational Fleet. SPAWAR had implemented an initial capability to build, integrate, test, and support systems by establishing the Systems Integration Environment (SIE), a robust engineering infrastructure that supported this evolution. The success of the DEP was also essential to horizontal integration, not only of the SPAWAR product lines, but also between Department of the Navy (DoN) combat systems and information systems. Many combat systems and C⁴ISR integration issues (singly and collectively) existed and needed to be identified and resolved with the DEP BG/BF integration and test process. It was SPAWAR's plan that commitment and participation in DEP by SSC San Diego and SSC Charleston would more quickly identify, quantify, and resolve fleet interoperability issues. SPAWAR's first approach was to use the SIE as a DEP extension while evaluating C⁴ISR capability. SSC San Diego and SSC Charleston would do this by adopting a management approach that complemented the Alliance approach and by leveraging infrastructure and resources as much as possible. SPAWAR would phase in implementation of its C⁴ISR site to complement the DEP process.

SPAWAR is the Navy's C⁴ISR product and service provider, supplying advanced information systems technology to the Fleet. Programs such as the Joint Maritime Communications System (JMCOMS), Automated Digital Network System (ADNS), Global Command and Control System–Maritime (GCCS–M), Information Technology for the 21st Century (IT-21), and Navy Wide Intranet (NWI) are initiatives that are critical to the implementation of network-centric warfare. SPAWAR is initially integrating command resources to provide a virtual environment for C⁴ISR development and testing initiatives around the globe. SPAWAR provides integrated information hardware and software systems to the Navy, other branches of the military, other agencies of the federal government, and prospective nations. The command organizational structure has three fleet-focused "Pillars"—Engineering, Installations, and Operations.

Since technology and systems change about every 16 months, training sailors and Marines on new technology becomes paramount. By focusing on deploying battle and amphibious-ready groups, SPAWAR works to ensure that new capabilities are provided to fleet units likely to need them the most—deploying Battle and Amphibious Ready Groups. SPAWAR 05 sets goals for systems engineering and for the use and management of the SIE to reduce risk, measure results, and ensure delivery of tested and validated capability to the Fleet. SPAWAR 051 is the systems engineer responsible for the development of end-to-end C⁴ISR systems designed to provide required capabilities for each deploying Battle Group. SPAWAR 053 acts as the primary manager/test directorate for complex highly integrated C⁴ISR integration test and evaluation. SPAWAR 053 establishes and maintains the test and evaluation processes, policies, and test infrastructure, including the SIE for the claimancy. These factors are tailored to fit specific program needs. Because the complexity of the program and its requirements vary, the management structure must have varying depth. SPAWAR 053 tailors the integration test organization to fit the complexity of each program. As a major player in the Alliance, SPAWAR 053 is a member of the Technical Advisory Board, the Systems Engineering Group (SEG), the Network Engineering Group (NEG), and the Collaborative Engineering Group (CEG). NAVSEA is assigned central responsibility to address BMC⁴I/Combat Systems interoperability problems within the SYSCOMs/Program Evaluation Offices (PEOs) and to coordinate resolution with the Fleet.

ACCOMPLISHMENTS

The first Battle Group that SPAWAR participated in was USS *Dwight D. Eisenhower* (CVN 69) (IKE) (Figure 1). During IKE BGIT, SSC San Diego and SSC Charleston accomplished the following:

- Executed limited Y2K testing between C⁴ISR systems and combat systems in accordance with the Navy Y2K Master Plan
- Added the ability to test a mix-match of real-time and non-real-time tracks
- Added the ability to mix live/simulated C⁴ISR tracks
- Added the limited ability to test joint C⁴ISR assets
- Added the ability to test C⁴ISR interfaces to several Naval Air Systems Command (NAVAIR) platforms (E2-C, F14D (Joint Tactical Information Distribution System [JTIDS]), F18 (Multifunction Information Distribution System [MIDS]), P-3, and S-3 aircraft)
- Developed/incorporated initial Common Simulation (SIM)/Stimulation (STIM) capabilities required to test C⁴ISR systems
- Developed/incorporated initial Data Extraction (DX)/analysis capabilities to test C⁴ISR systems
- Led efforts to enhance and implement full collaborative engineering capabilities for the Alliance
- Provided leads in C⁴ISR systems engineering functions in the DEP
- SPAWAR leveraged SIE test requirements and assets to address DEP goals during IKE BGIT
- Established an interface between SPAWAR C⁴ISR SIE and DEP, which replicated the ship configurations for the Automated Digital Network System (ADNS), GCCS-M, and the Officer in Tactical Command Information Exchange Subsystem (OTCIXS) for the IKE BGIT

- Planned and conducted a Battle Group Interoperability (BGI) Test Program that included C⁴ISR, combat systems, and several select "multi-source inputs"
- Supported the Navy Y2K Master Test Plan Level 2 and Level 3 test for C⁴ISR systems that interfaced to combat systems
- Supported the development of a "common" SIM/STIM C⁴ISR component for use in the DEP and SIE SIM/STIM environment.

Besides the IKE BGIT, SPAWAR has been a participant in the USS *George Washington* (CVN 73), USS *Abraham Lincoln* (CVN 72)/USS *Harry S. Truman* (CVN 75), USS *Constellation* (CV 64)/USS *Enterprise* (CVN 65), and USS *Carl Vinson* (CVN 70) BGITs. During these BGITs, several technical reports were written to document fleet findings for the C⁴ISR systems, particularly GCCS-M and Common Operational Picture (COP) Sync Tools (CST). These problems have been documented and reported to the Fleet and Program Office for correction.

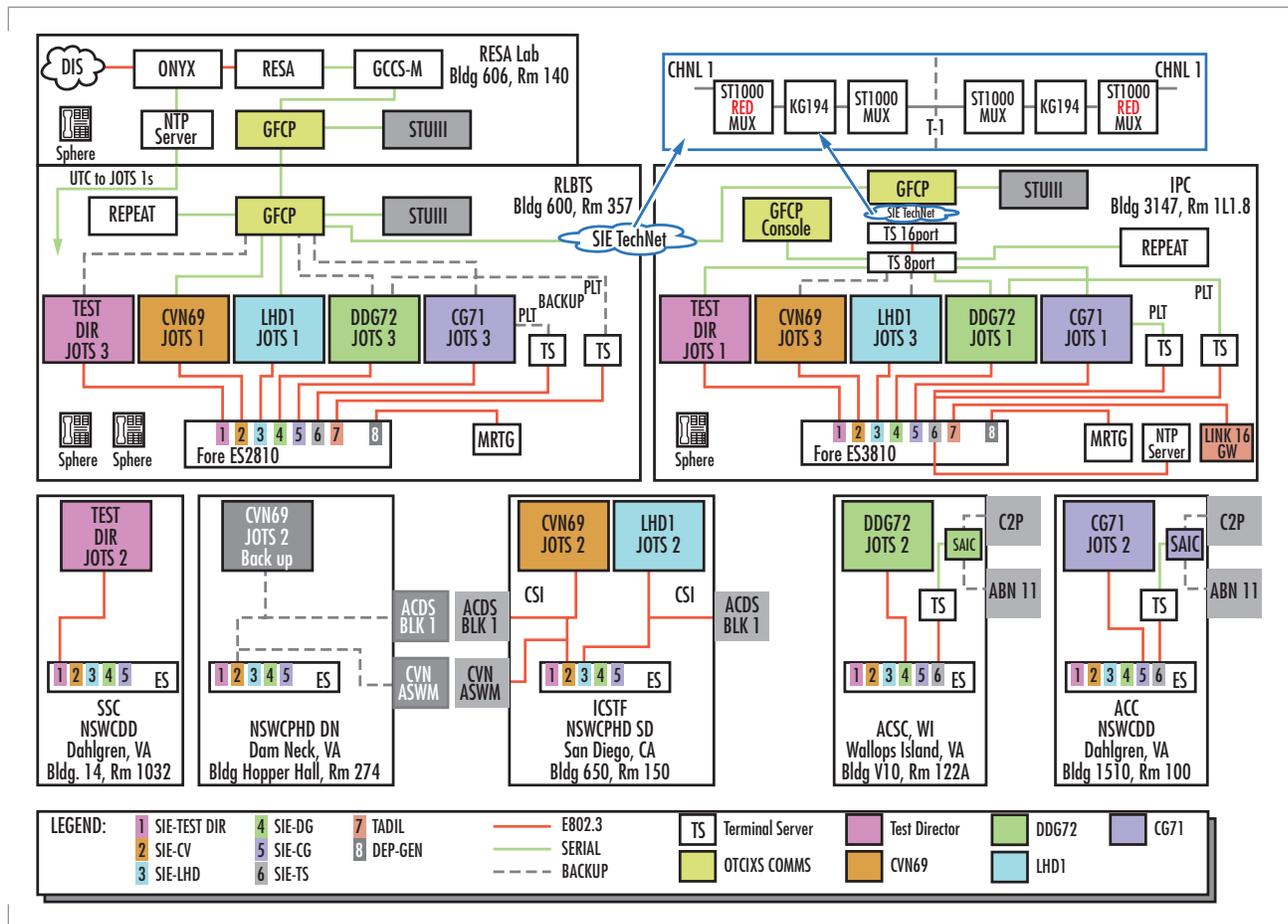


FIGURE 1. IKE DEP/SIE architecture.

LOOKING FORWARD—THE FUTURE

For the intermediate future, SPAWAR is planning to participate in USS *John F. Kennedy* (CV 67) BGIT, which is scheduled in June and July

2001. For this BGIT, GCCS–M will interface with the Advanced Combat Direction System (ACDS) Block 1 (two-way Combat System Integration [CSI] interface) and will interface with the Air Defense Systems Integrator (ADSI).

Looking ahead to FY 2002 and beyond, SPAWAR is planning to support and can include Joint Systems and Coalition Systems into the DEP. The overall focus of the original DEP Systems Engineering effort was to set up a disciplined and robust systems engineering process that leads to the development of a more interoperable joint force and the development of the DEP required to support that process. SPAWAR's system engineering process supports the concept in which the BF is the warfighting system rather than an individual platform. SIE offers a proven capability to build and test valid C⁴ISR architectures, which represent the complex operational C⁴ISR environment. The C⁴ISR SIE will further develop the DEP's ability to support overall force requirements to have interoperability "engineered-in." The direct interfaces between C⁴ISR and combat systems are limited today; however, highly integrated C⁴ISR systems on the other side of the direct interface system (e.g., GCCS–M) provide multi-source inputs that are fused together, providing vital information to the warfighter. Interoperability testing requires that many components besides the direct interface system be tied into the test architecture. Network-centric warfare and NWI will provide important timely information, extending the battlespace and supporting advanced mission planning. SPAWAR's commitment to the DEP will also support future efforts, including a closer integration of real-time and non-real-time command and control (C²), development of a common information base for C², and integration of the Tactical Digital Information Links (TADILs) into the common backbone. A valid C⁴ISR architecture has elements that operate at UNCLASSIFIED, SECRET, and Sensitive Compartmented Information (SCI) classification levels. All three are crucial for accurate integration and valid interoperability testing for BG C⁴ISR architecture and the integrated network security.

The original DEP effort was designed to support the important interoperability requirements of:

- A common tactical picture across all force elements
- The control and coordination of engagements at the force level
- Force-level planning

SPAWAR's specific goals, with other SYSCOMS, are to add the following important interoperability requirements of C⁴ISR:

- A common operational or tactical picture across all force elements
- Inclusion of the intelligence, information warfare (IW), cryptologic, and mission planning elements of BMC⁴I
- Inclusion of the meteorological, navigation, logistics elements of BMC⁴I
- Ability to simulate the NWI and Global Networked Information Enterprise (GNIE)
- Inclusion of real and simulated C⁴ISR networks (e.g., radio frequency [RF] and Internet Protocol [IP] networks)
- Integration of real-time and non-real time C² to include an integrated information base (IIB)

- Integration of the TADIL data into the common backbone
- GCCS–M for Submarine Combat Systems
- The COP Test will verify the capability to provide a common operational picture environment for interoperability testing. Several protocol scripts will be used to drive multiple SIMs/STIMs at various DEP sites. Data will be recorded. Track databases from C⁴ISR C² system base lines will be compared to ensure replication of known and/or expected performance.
- Link capabilities related to C⁴ISR will be tested to ensure the C⁴ISR DEP's capability to test interoperability. These capabilities include ADSI, multi-TADIL capability (MTC), and GCCS–M Tactical/Mobile, Coast Guard Link 11, and other related capabilities.



BeEm V. Le

BS in Electrical Engineering, Bradley University, 1987; BS in Mathematics, Bradley University, 1987

Current Research: Interoperable C⁴ISR systems; IT-21.

The Over-the-Horizon Targeting (OTH-T) Program and the Reconfigurable Land-Based Test Site (RLBTS) Laboratory

Gary E. McCown
SSC San Diego

INTRODUCTION

The Over-the-Horizon Targeting (OTH-T) program conducts interoperability certification testing in accordance with Office of the Chief of Naval Operations instruction (OPNAVINST) 9410.5. OPNAVINST 9410.5 requires interoperability certification for new/upgraded systems to proceed to Operational Evaluation (OPEVAL). This instruction provides for configuration management, process and plan development, and requirements development for U.S. Navy and Joint interoperability testing.

To fulfill the charter of OPNAVINST 9410.5, the OTH-T program provides a virtual, global systems integration and test facility for Information Technology for the 21st Century (IT-21) command, control, communications, computers, intelligence, surveillance, and reconnaissance (C⁴ISR) technology. This technology collects, transmits, correlates, and displays track data into a Common Operational Picture (COP) to support warfighting requirements. The common view of the battle space that the COP provides the warfighter has been applied across the spectrum of warfare missions areas; however, the technology and doctrine have changed radically in recent years and continue to change rapidly. Thus, the primary goal of the OTH-T program is to transition architectures and systems from older military standard (MIL-STD) technologies to commercial/government off-the-shelf (COTS/GOTS) technologies.

Another goal of the OTH-T program is to support the integration of all C⁴I systems into warfighting capabilities; this support included Year 2000 (Y2K) interoperability and integration testing and direct fleet support. Fleet support also includes providing technical expertise afloat and ashore through highly trained experienced Fleet Systems Engineers (FSEs) who ensure smooth integration of new C⁴ISR capabilities during major fleet exercises and demonstrations that validate and evaluate developed portions of configurations. The OTH-T program performs integration and interoperability testing to support warfighting capabilities for MIL-STD and IT-21 COTS/GOTS equipment for submarines, surface, and land-based components. The Fleet System Engineering Team (FSET) provides system engineers to support command centers and numbered fleet commanders; Officer in Tactical Command Information Exchange Subsystem/Tactical Data Information Exchange System (OTCIXS/TADIXS) network monitoring and troubleshooting support to Pacific Fleet/Atlantic Fleet (PACFLT/LANTFLT) command centers; data collection and analysis

ABSTRACT

This paper focuses on command, control, communications, computers, intelligence, surveillance, and reconnaissance (C⁴ISR) integration and interoperability testing accomplished by the Over-the-Horizon Targeting (OTH-T) program and the support that the OTH-T program provides the Fleet, including technical expertise afloat and ashore for submarines, surface, and land-based components. Test scalability from recent small-scale tests such as Web replication (Fleet-requested) to large-scale projects such as the Distributed Engineering Plant (DEP) are also discussed. This paper also addresses the Fleet Systems Engineering Team (FSET). FSET support provides system engineering to command centers and numbered fleet commanders, daily network monitoring and troubleshooting of the Officer in Tactical Command Information Exchange Subsystem/Tactical Data Information Exchange System to Pacific Fleet/Atlantic Fleet command centers, and data collection and analysis tools.

tools for FSEs (ashore and afloat); test coordination/direction for system integration testing; and coordination with other certification agencies.

BACKGROUND

Experiments in the 1970s showed the difficulty and problems associated with maintaining command and control across platforms with many individual platforms developing their own tactical picture and sharing that picture. The Office of the Chief of Naval Operations (OPNAV) established the OTH-T program in 1985 to address these problems. The OTH-T program was originally tasked to develop communications specifications and Battle Group Data Base Management (BGDBM). The objective of the OTH-T program is to produce a complete, accurate, timely, precise, tactical picture suitable for getting ordnance on target where all participants have access to the correct information. The OTH-T program established the Reconfigurable Land-Based Test Site (RLBTS) in 1989 to allow interoperability and integration testing. The OTH-T program is funded through OPNAV N6 and receives Operational Maintenance, Navy (OM&N) funding to support the RLBTS Laboratory and facilities. Other major sponsors include Space and Naval Warfare Systems Command (SPAWAR) PMW 157 and 165, and PACFLT.

THE RECONFIGURABLE LAND-BASED TEST SITE (RLBTS) LABORATORY

In the early 1990s, the Navy designated the RLBTS Laboratory as the lead OTH-T laboratory. RLBTS was established as a facility to support the development of tactics and procedures for targeting systems and weapons, concept demonstrations of prototype systems, and the definition of architectures intended to ease future acquisition decisions. RLBTS provides the Navy with a facility that maintains command, control, and communication systems expertise to ensure technical and scientific excellence that provides the corporate knowledge, technical networking innovation, and real-world understanding to support operationally effective fleet warfare mission area systems. The OTH-T program operates RLBTS as a full-service facility for conducting Joint Distributed Tests and Evaluations (DEP and Joint DEP) and OTH-T system integration interoperability tests and certifications. RLBTS is expandable to support command and control configurations from the platform level to the afloat/ashore Command Center level. RLBTS provides a test control center hub, network operations center (NOC), a focal point for all test data collection and analysis, a classified test environment, architecture development and validation, and network engineering to support Fleet Command Centers.

Figure 1 shows a combined view of Joint Operation Test Site (JOTS) workstations and the multimedia center. The large screen display (Figure 1) can be connected to any workstation and various videoteleconferencing (VTC) units. A whiteboard and VTC unit are permanently connected to SPAWAR Headquarters (SPAWAR HQ) and SSC Charleston for collaborative real-time test planning and test execution. Figure 2 shows the Tactical Analysis Section of the laboratory. These machines house the Repeatability Performance Evaluation and Analysis Tool (REPEAT) used for tactical data recording, analysis, and playback. Figure 3 shows



FIGURE 1. The RLBTS Laboratory.



FIGURE 2. The Tactical Analysis Section of the RLBTS Laboratory.



FIGURE 3. View of REPEAT machines and JOTS1 tactical workstations.

REPEAT machines and JOTS tactical workstations in the Tactical Data Section.

Network infrastructure supported by the RLBTB Laboratory (Figure 4) includes secure fiber connections to other laboratories, including the Integrated Shipboard Network System–Test Facility (ISNS–TF) (NOCC); Integrated Test Facility (ITF); Integrated Combat System Test Facility (ICSTF, NAVSEA); Research, Evaluation, and Systems Analysis (RESA); Global Command and Control System–Maritime (GCCS–M), and Systems Integration Facility (SIF), with T1 and Asynchronous Transfer Mode (ATM) connectivity to SPAWAR–HQ, SSC Chesapeake, and SSC Charleston. Network connectivity also includes the Systems Integration Environment (SIE) Upgrade (T1)/Defense Information Systems Network–Leading Edge Services (DISN–LES, ATM); DEP/DISN–LES; Defense Research and Engineering Network (DREN); Ship Wide–Area Network/Secret Internet Protocol Router Network (SWAN/SIPRNET); and SSC San Diego networks. The RLBTB Laboratory also maintains a satellite communications capability to PACFLT and LANTFLT assets. RLBTB Laboratory assets include routers, packet shapers, ATM switches, firewalls, cryptos, multiplexers, and satellite simulators. Additionally, a capability to emulate the Integrated Shipboard Network System (ISNS) shipboard network has been developed by the OTH–T Program.

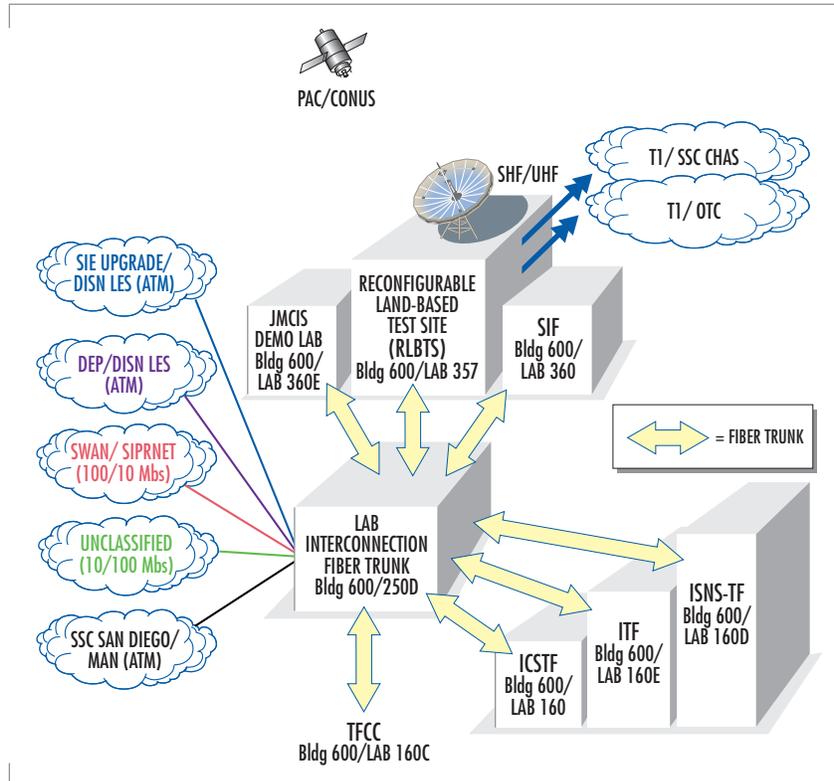


FIGURE 4. RLBTB networking communication and laboratory interconnection.

TESTING AND OTHER ACCOMPLISHMENTS

The OTH–T program has certified the interoperability of systems and software including OASIS, GCCS–M, Combat Control System (CCS) MK II, and the Advanced Tomahawk Weapon Control System (ATWCS). These certifications are performed annually or as new versions or software patches are developed for the Fleet to meet OPNAVINST 9410.5 requirements.

During FY 1999, the OTH–T program conducted systems integration, interoperability, and Y2K testing using the facilities of the Land-Based Test Network (LBTN), and expanded RLBTB to validate IT-21 technologies prior to shipboard installation. The OTH–T program conducted 27 tests, recommended certification of 3 systems during 59 test weeks, produced 229 documents, and provided 43 Software Trouble Reports (STRs) to program managers and system developers. OTH–T team members also

participated in the DEP Battle Group Interoperability Test (BGIT) for USS *Dwight D. Eisenhower* (CVN 69) and USS *George Washington* (CVN 73), and developed and tested the COP Synchronization Tools (CST) functional requirements.

During FY 2000, the OTH-T program conducted integration and interoperability testing using the LBTN, SIE, and the IT-21 infrastructure in the RLBTLS Laboratory connected to various facilities around the U.S. The OTH-T program conducted 29 tests, recommended certification of GCCS-M 3.1.2.1 and CCS MK II during 149 test weeks, produced 191 documents, and provided 91 STRs to program managers and system developers. Forty briefs were given in the RLBTLS Laboratory.

The OTH-T team supported the DEP BGIT of *Eisenhower*, *George Washington*, USS *Carl Vinson* (CVN 70), and USS *Constellation* (CV 64) BG C4ISR configurations. The OTH-T team's participation in the test readiness reviews, test execution BGIT analysis review panels, and scheduling meetings for SPAWAR led to the identification of 24 Test Observation Reports (TORs). TORs are used to isolate problems and provide a fix or work-around recommendation.

Interoperability and Integration Testing

Specific interoperability and integration testing was accomplished for the CST segment in GCCS-M and GCCS-M version 3.1.2.1. Fifty-six STRs were recorded with 30 high, 18 medium, and 8 low. These STRs were passed to the developer and sponsor and recorded in the OTH-T database. Certification was recommended with Interim Authority to Operate (IATO) in the Fleet. As a follow-on to the certification testing, OTH-T test engineers participated in developmental testing / operational testing (DT/OT) and OPEVAL with USS *Enterprise* (CVN 65) at sea. The DT/OT demonstrated the capabilities of the GCCS-M/CST software. The OTH-T program also provided test procedures and lessons-learned reports. As this software is installed in the Fleet, the OTH-T program provides technical support and additional testing as requested by users.

Interoperability certification tests were conducted for the submarine weapons CCS MK II. Interoperability certification was recommended for the CCS MK II system. During DT, eight STRs were identified. These STRs were identified before certification, and fixes or work-arounds were implemented.

Additional interoperability/integration testing included joint testing with the Joint Interoperability Test Command (JITC). The RLBTLS Laboratory participated as a node on a wide-area network (WAN) on SIPRNET testing of GCCS-M and GCCS-J (Joint). Additional participants were the Naval Center for Tactical Systems Interoperability (NCTSI) and the Defense Information Systems Agency (DISA).

Repeatable Performance Evaluation Analysis Tool (REPEAT)

The OTH-T program initiated the development of REPEAT and supports its maintenance, use, distribution, and continued development. REPEAT monitors and tests all C4I synchronous and asynchronous serial devices. REPEAT monitoring and testing allows the user to conduct statistical analyses on volume and type of data, system throughput and timeliness, tactical data network loading, correlation accuracy, system data loss, common tactical picture, and comparison of data transmitted and received at various locations. Message formats that are currently supported include OTH-Gold, TACREP, TADIL-A, TADIL-B,

TADIL-J, RAINFORM, Tactical Information Broadcast System/Tactical related application Data Distribution System (TIBS/TDDS), Tactical Electronic Intelligence (TACELINT), LOCATOR, Tactical Receive Equipment (TRE), Tactical Fire Direction System (TACFIRE), and Sensor Tactical Contact Report (SENSOREP). REPEAT tests OTCIXS/TADIXS/SIU/V6 interfaces. The OTH-T team provides software support, training, and upgrades. REPEAT is available in MS-DOS and Windows versions. REPEAT is currently installed and used for data analysis and recording at over 300 military sites at more than 55 commands and allied militaries. More than 300 help calls are handled each year. REPEAT software is available to all U.S. military at <http://repeat.spawar.navy.mil>. REPEAT provides scenario development and data/platform injection for Joint Warrior Interoperability Demonstration (JWID) exercises. During FY 2000, REPEAT supported the Global Positioning System (GPS) Inter-Service Agreement (ISA) Demonstration (sponsored by Fleet Battle Laboratory), specifically injection of GPS messages into GCCS-M. REPEAT is currently installed on many Navy platforms and is used by the Fleet to identify problems.

Test Process Web-Enabled

The OTH-T program maintains a password-protected Web site at <http://otht.spawar.navy.mil> to support the OTH-T team and promote process documentation, process improvement, and configuration management. The Web site allows documentation development, a tester log, engineering notes, test planning, and process documentation.

FLEET SYSTEMS ENGINEERING TEAM (FSET)

The OTH-T program supports the Fleet Systems Engineering Team (FSET), which is the main technical advisor to carrier Battle Group (CVBG)/amphibious ready group (ARG) staffs in matters related to the IT-21 architecture, associated C⁴ISR/information operations (IO) systems, and supporting networks and infrastructures. Besides serving as a technical liaison on system management issues, the FSET also interfaces with those baseband systems that provide connectivity between the shore and shipboard networks. This connectivity includes Challenge Athena, super high frequency (SHF), Automated Digital Network System (ADNS), and other line-of-sight systems. Integrated with LANTFLT and PACFLT Commander-in-Chief (CINC) N6 organizations, the FSET also monitors all CVBG/ARG C⁴ISR installations and liaisons with ship C⁴ installation supervisors to verify that all required connectivity is in place to support tactical operations.

Coordinated with the RLBTB Laboratory, the FSE team provides system engineering support for experiments and tests that support the introduction of new SPAWAR Common Operational Picture (COP) software/hardware or system capabilities. Systems engineering will support pre-test coordination, test design, installation test and coordination, and onsite support when required at remote facilities, data collection and analysis, injection of synthetic data, and post-test lessons-learned reports. FSETs provide daily support to the numbered commanders and CINC staff and their command Assist CINC in developing C⁴I architectures and requirements. Support includes system-level support for C⁴I non-real-time systems during BG work, Battle Group Systems Integration Test (BGSIT), and exercises (for example, Joint Task Force Exercise [JTFFEX], Cobra Gold, Kernel Blitz, Tandem Thrust, and Magellan).

As representatives of SPAWAR and the Fleet CINC, the FSET ensures that deploying forces have ready access to technical experts familiar with the IT-21 architecture from an installation and operational point of view. FSET support is available upon request to major staffs throughout their deployment workup cycle. The FSET provides the ship, staff, and Battle Force an "on-scene" representative, uniquely experienced in the afloat architectures. Information on how to request FSET support is available by contacting either the LANTFLT or PACFLT program managers. In coordination with the OTH-T program, the FSET provides rapid response problem solving for issues encountered in the Fleet.

LOOKING FORWARD—THE FUTURE

With the infrastructure that has been established in the RBLTS Laboratory and connections to many other facilities from the RLBT Laboratory, the future looks busy and full of new opportunities. These opportunities are described in the following subsections.

Multiple Large-Deck BG Interoperability Testing

Multiple large-deck BG interoperability testing ensures that multiple large-deck BGs can communicate and share data for collaborative planning, COP, and dissemination of (air) tasking orders on virtual local-area networks (VLANs), LANs, or WANs. This testing is required as a result of previous fleet observations of conflicts that involved multiple BGs converging in an operational theater with interoperability problems that forced technical experts to quickly respond to the BGs and implement work-arounds to ease operations—a costly occurrence. Multiple large-deck interoperability testing of C⁴ISR systems has never been executed in preparation for multiple large-deck contingencies.

Prioritized Products List (PPL) Testing

Prioritized Products List (PPL) testing for intensified rapid-response interoperability testing is required because of changing shipboard infrastructure and networks, the use of multiple vendors, increased complexity of systems and software, an increased number of nodes/participants, increased geographic extent, and the complexity of required networks. Equipment upgrades and evolutions require more regression testing, verification, and validation to ensure and certify that new and legacy software function according to specification and interoperate with other equipment and platforms. Critical issues include WAN/bandwidth management and the extent of impact of applications when WAN bandwidth is constrained or dirty satellite conditions exist. Interoperability problems will become evident when hardware and software are installed in the Fleet and during fleet operations rather than in the laboratory. Mission capabilities will be reduced. Costs to repair problems and develop *ad hoc* fixes found in the Fleet will greatly exceed costs to identify and fix problems found in an ashore test environment. The OTH-T program with the RLBT Laboratory is ideal for this PPL testing because of existing NOC, Integrated Shipboard Network System (ISNS), satellite simulation, and WAN facilities and expertise.

CONCLUSION

The OTH-T program will continue to provide the Fleet with high-quality products in the conduct of integration and interoperability testing of OTH-T and combat systems with tactical data exchanged over CST networks and other networks. Integration testing will include testing of GCCS-M and Combat Decision Systems (CDS) two-way interfaces. The OTH-T program will continue to support FSET integration tests and fleet test requests, horizontal integration, relevance verification, modification recommendations, and OTH-T specification maintenance to support distribution of C⁴ISR systems to the Fleet, and participate in DT, OT, and OPEVAL as required. OTH-T will also provide certification testing as required by OPNAVINST 9410.5.



Gary E. McCown

Ph.D. in Atomic/Surface Physics,
Oregon State University, 1990
Current Work: Program Manager
for the Over-The-Horizon
Targeting (OTH-T) Program.

Automation in Software Testing for Military Information Systems

Jack Chandler
SSC San Diego

INTRODUCTION

This paper shows how automation can improve test results. At the beginning of this effort, a search was conducted to survey the status of automated testing. The survey revealed white papers and some commercial products that help automate testing (see Dustin [1] and Pettichord [2]). Many of the commercial products are key and cursor recorders that capture the keystrokes and cursor movements produced by test engineers during the testing process. This testing works well for testing revisions of the same product. It is not as appropriate for testing multiple pieces of software for compliance to a standard.

Dustin's paper on introducing automation to a test team states that the first phase of designing testing automation is analyzing the testing process [1]. To be of value, software testing must be a repeatable process that is definable, measurable, consistent, and objective. If the process is deficient in any of these areas, the testing will not be repeatable. This paper examines various factors in the testing process (including the human factor), describes the results of a case study on military information systems, reviews the steps required for successful automation, and provides a conclusion.

COMPONENTS OF THE SOFTWARE TESTING PROCESS

Software under Test

The most essential and basic component of the testing process is the software under test. This component cannot be changed to any great extent. The two basic categories of software under test, depending on the type of testing, are as follows: (1) testing a software product to determine whether the product is ready for release or to validate error corrections, and (2) testing multiple components of software for compliance to a standard. Both types of testing are valid; they have different requirements and different automation strategies.

Hardware for Software Testing

The second component of the testing process is the hardware platform on which the software is loaded. Improvements may be possible in this area. For example, a different hardware platform may increase the speed of software testing. Increasing the number of "seats" in use simultaneously

ABSTRACT

Software testing must be definable, measurable, consistent, and objective to be a repeatable process. This paper examines the components of the testing process, including software, hardware, the human element, and the data-collection process. It also includes a case study in test automation derived from the Defense Information Infrastructure Common Operating Environment (DII COE). A reduction in the number of human-controlled steps in the software process significantly improved test results during this case study. Automation was successful because the many different components of software were tested for compliance to a well-defined standard. Automation was straightforward because the test methodology did not require any specific assumptions about the software tested.

during the testing scenario or increasing the performance of the individual "seats" is another way hardware can improve testing. The disadvantage of substituting different hardware during the testing process is the risk of testing on a non-representative platform, which would make test results questionable. To overcome this potential problem, some testing must be done on a typical user platform.

Human Testers

The third component of the testing process is the engineer or group of engineers testing the software. Test engineers make a substantial contribution to the testing process, but the possibility of human error makes them the weakest factor in the testing process. Even more important is the fact that the process is not consistent because test engineers do not consistently make the same mistake. The most dedicated and competent engineer can err under some circumstances. Thus, eliminating the "human in the loop" can significantly improve the testing process. Reducing the number of human-controlled steps can dramatically improve software testing. An example of how to reduce the human interface areas in a testing process is described below.

Data Collection

Another major component of the software testing process is the data-collection function, which often can be improved. The data-collection function often consists of the test engineer manually filling out a paper data-collection form. The test engineer will have a test notebook or a data form in which the test data are recorded. Often, the test data are re-entered into a spreadsheet or a word processor for report generation or into an e-mail message for distribution of the test results. Forms, which provide ample opportunity for errors, could be significantly improved. For example, if the form is structured in a multiple-alternative, forced-choice paradigm rather than a less-structured essay format, subjectivity can be reduced.

Another common test procedure consists of the test engineer manually filling out an electronic data-collection form. The electronic form is better than the manual form because data are manipulated only once, thus reducing transcription errors if the data are input into a report generator or an e-mail system. Using an electronic form can require investing in more hardware to support the collection. More time may be needed to fill out the forms initially, but this method saves time by reducing or eliminating the need to transpose data.

As with paper forms, the design of the electronic form is critical. One way to improve the design is to minimize the number of probable answers while still allowing all possible answers. This is done by prompting the user to consider certain likely choices while grouping other possible answers under "other" with a space to insert a comment. A periodic review of the use of the "other" category is recommended, with the objective of providing common "other" answers with specific choices of their own.

Another useful mechanism is to collect data automatically and manually by enabling software to perform the test. Efficient results are achieved by automating to the fullest practical extent the test data acquisition process. The parts of the process that do not lend themselves to automation still

can be performed manually. A useful, proven procedure is to provide in the testing software a mechanism to input the manually derived test information. The "form" that is provided for collecting this manual information should be designed using the criteria discussed previously.

The most advanced and desirable phase of automation consists of collecting the testing data with a computer program that involves little or no human involvement. Only when the testing process is completely automated is a repeatable process achieved. Whenever a person manually performs a test, there is a chance that the test cannot be consistently repeated. Human beings are predictable in a group, but unpredictable individually.

Other Components

The other two major components of software testing are the education of the test engineers and the testing process itself.

TEST AUTOMATION: A CASE STUDY

Background

This section describes an example of end-to-end testing where the testing itself has been mostly automated and the areas that cannot be automated have been analyzed to reduce or eliminate subjectivity. The Department of Defense (DoD) has created the Defense Information Infrastructure Common Operating Environment (DII COE). Many DoD systems are being built using this "plug and play" infrastructure. The components of software for this system are called segments. A compliance specification has been created to enhance the "plug and play" capability of this infrastructure. This specification consists of over 300 requirements. A segment must pass at least the first 200+ requirements to be considered for inclusion in the DII COE.

DII COE compliance involves a time-consuming and human-intensive testing process. In one instance, about 18 person-hours were required to test a single, simple segment. Significantly greater test durations have been common in other cases. Compliance testing was a likely candidate for automation because it is common to all segments. The procedure that was used to automate this testing process is described below.

Document the Testing Process

In this step, the engineer will discover the current method of testing, including the acceptable test methods and the methods that are unsatisfactory. In many cases, the test engineer will be able to learn the test processes and procedure and to expose many inconsistencies in this step. The information that needs to be recorded during the test procedure is documented. From this experience, the test team learned that there were many "homegrown" solutions to the automation, a situation that had advantages and disadvantages. On the positive side, some work already had been completed. Unfortunately, these solutions were not consistent. After gleaning the currently automated processes, the test team captured the steps involved in those areas that were not automated.

The test team learned that not all DII COE requirements were tested. This was not because the untested requirements did not provide any added value, but rather to reduce the time required for testing. This prompted the test team to create a "best practices" spreadsheet in which

to capture the test algorithms, not the test "programs." To provide better DII COE compliance, the test team also created algorithms for the requirements that were not being tested.

Identify Common Processes

The test team identified the common processes from the algorithm spreadsheet. These will be used later to ensure that a single testing method will be used. Too often, common testing processes are coded multiple times because engineers are unaware that some of these processes are in common use. This causes inconsistencies in the use, application, and maintenance of these processes, especially if the processes need debugging or upgrade.

Design the Automation (Software)

The first steps of the automation design consisted of gathering and defining requirements. Then, the software had to be designed to meet those requirements. The design called for an object language with a compliance engine and an individual object for each requirement. Since the DII COE software is supported on multiple platforms, the test team elected to use Java as the programming language. In theory, this was expected to decrease the inconsistencies by providing a common baseline. The test team wanted to keep the design generic to accommodate any required testing process where the requirements were structured in hierarchical levels. To pass at level 5, for example, would require that all tests in levels 1 through 4 be passed as well as all tests in level 5. With this in mind, the test team designed a compliance engine with a test manager, an applicability filter, and some common data-collection agents. We defined an interface to the compliance engine that the test objects will use. The design included a report generator and a graphical user interface (GUI) that allows the test engineer to view the data-collection form and to access the various options. These components are described below in more detail.

Because many of the DII COE requirements apply only to certain types of segments, the test team needed an applicability filter to determine the applicable tests based on the segment type. Each test object specifies to the applicability filter the segment types to which it applies. The default was specified as applicable to all segment types.

The test manager launches the test objects at the appropriate times. For example, certain tests must be run while the segment is installed, whereas others cannot run until the segment is deinstalled. The test manager also runs some data-collection agents, which also must be run at certain times. The relative timing of each test is important to specify clearly when documenting the testing process.

The data-collection agents determine information about the segment under test and that segment's effect on the underlying system. The test-unique data-collection agents (if any) are common processes that collect other data from the underlying system. This feature was included in the design, not for the specific purposes of the test team, but only for the generic case.

The questionnaire object(s) obtain additional information from the test engineer. Questionnaires are presented twice in the testing process. (Figure 1 shows the testing process.) The first time the questionnaires are presented

is before the segment is installed; software developers provide this information. The second time is after installation to obtain information that the test engineer can determine easily, but that the automated software would not be able to determine (or be able to determine uniquely). The questionnaires present multiple-choice questions, including an "other" choice, where applicable. These objects read from formatted text data files and are therefore dynamic and easily modified.

The data-collection form and the menus presented are also dynamic. They are created by the compliance engine at runtime. The report generator merely specifies the state of each test object. This facilitates the additional tests as well as additional report formats. The testing process also tracks the test engineer's name and reports separately any tests that were waived or overridden. The test team found that the software to automate first should be that which provides the most efficient and largest payoff [2]. A phased approach to automation has proven most successful.

Designing the Automation Process

The requirements gathering described above also will yield one or more processes. In the beginning of software testing, all processes may not yet be in place. It is equally important to design the process. The automation software works within a process. This process will depend on the automation, which, in turn, will depend on the process recursively; often, both should be designed at the same time.

If testing has not been automated previously, the process will need a major rework. When automated testing is in place, personnel may be available to be tasked elsewhere. This will not be true in the beginning since the automation will also be undergoing testing. It is important to account for the testing assets that will be displaced by the automation. After some time, however, resource management will have to account for where to move these displaced testing assets.

Personnel Management Considerations

Test engineers, who will need to be trained how to use the automation, may have significant technical expertise. The main concern is to induce the test team to accept the new paradigm in which automation is replacing some of their expertise. It is not uncommon to see a reluctance to accept or attempts to discredit the automation.

In the author's experience, the best way to prevent this reluctance is to have the more experienced test engineers help with programming the

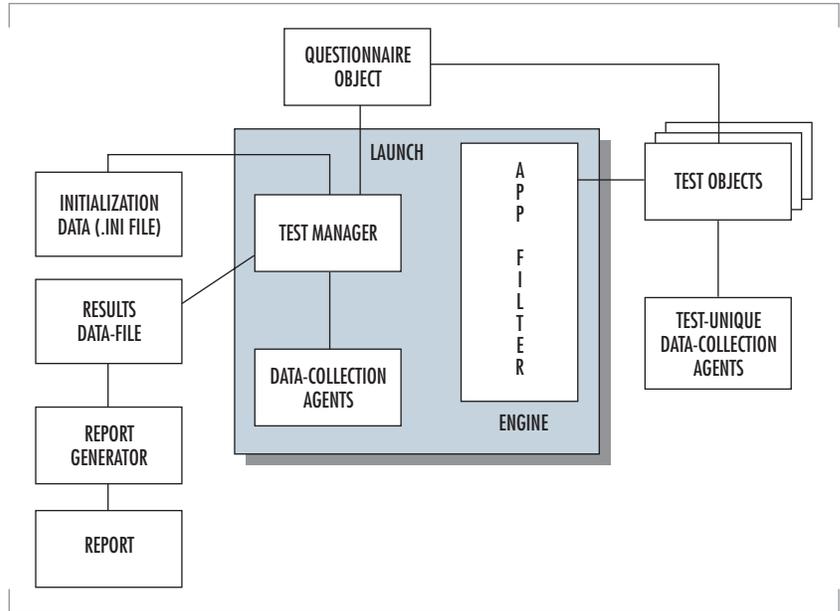


FIGURE 1. Block diagram of testing process.

algorithm-design phase if they are capable. It is important to get them to "take ownership" of the new paradigm. At least a small team of programmers will be required to help with the debugging and enhancing of the automation. The consistency and time savings will pay for these personnel.

The program manager also can redirect some personnel into a quality-assurance role to ensure that the output of the testing is of the required quality. Quality assurance is especially important if the results will be used outside of the test laboratory.

REVIEW

To achieve success in replacing the manual software testing process with an automated testing process, the test engineer must complete the following actions:

1. Document the current testing process.
2. Identify common processes.
3. Complete the following steps in parallel
 - a. Design the automation software.
 - b. Design the automation process.
 - c. Encourage acceptance by the test engineers by inducing them to "take ownership" of the new process.
 - d. If appropriate, consider using an object-design for the automation. Think about using a separate object for each test. Using objects helps when individual tests need to be modified.
 - e. Think about a design that allows new tests and new reports to be added with few or no changes to the underlying data-collection (engine) process.
 - f. When designing the software, think of the "big picture." How can this "machine" be used as part of a bigger system? Perhaps, instead of generating a report, the output could be used as input to a database. In this case, the report capabilities of the database could be used or the defects could be tracked automatically.

CONCLUSION

Replacing manual software testing with automated software testing can yield numerous rewards. A repeatable test process is the major advantage, leading to improved software quality and avoidance of a non-repeatable test. The depth of test coverage also can be increased, and the time requirements can be reduced. The combination of these two factors will improve the quality and cost savings of the software that supports DoD systems compliant with DII COE requirements. This testing methodology could be applied to testing software for government agencies outside DoD, such as the Department of Transportation Federal Aviation Administration and the Department of the Energy, both of which have exacting standards related to safety and security.

ACKNOWLEDGMENTS

This work was sponsored by the Defense Information Systems Agency–Defense Advanced Projects Research Agency (DISA–DARPA) Joint



Jack Chandler

BS in Computer Engineering,
University of New Mexico, May 1991
Current Research: Automation of
repetitive tasks and removal/reduction
of subjectivity; collaboration research.

Program Office. The author thanks the entire test team, especially Pho Le, Steve Bitant, Will Greenway, Todd Webb, Randy Schiffman, MAJ Greg Csehoski and CAPT Stuart Kurkowski.

REFERENCES

1. Dustin, E. 1997. "Process of Introducing Automated Test Tools to a New Project Team," *Proceedings of the Rational User Conference*. URL: <http://www.autotestco.com/html/sld001.htm>
2. Pettichord, B. 1996. "Success with Test Automation," *Proceedings of Quality Week 96*, URL: <http://www.io.com/~wazmo/succpap.htm>



Systems Integration Facility: Past, Present, and Future

David P. Andersen
SSC San Diego

Karen D. Thomas
Digital Wizards, Inc.

The Systems Integration Facility (SIF) opened in 1990 in Building 600 at SSC San Diego to support the Navy's first Joint Tactical Information Distribution System (JTIDS) developmental test program. Developed out of a need for a controlled, repeatable test environment to verify JTIDS terminal performance and combat systems interoperability, the SIF has become the Navy's leading laboratory for tactical data link interoperability testing.

Sharing near-real-time tactical data in a distributed, interoperable, and secure environment is a critical segment of warfighter universal information access. Tactical data links, specifically Link-11 and Link-16, now the Department of Defense's primary data link, and the future Link-22, provide this capability to Navy, Joint, and Allied forces.

SSC San Diego has been involved with tactical data link development, test, evaluation, integration, and life-cycle support since the early 1960s. Under sponsorship of the Space and Naval Warfare Systems Command's Advanced Tactical Data Links Program Office (PMW 159), the SIF has played an integral role as the central node of a complex stimulation/simulation environment for land-based testing and evaluation of Link-16 components and systems and integration with other data link systems. SIF operations are part of SSC San Diego D45, the Tactical Systems Integration and Interoperability Division.

The first- and second-generation Link-16 uses the JTIDS data terminal, which provides multiple-access, high-capacity, jam-resistant digital data and secure voice communication, navigation, and identification information to various command and control and weapons host platforms. The JTIDS terminals encompass software, radio frequency (RF) equipment, and the waveform they generate. Link-16 requires JTIDS terminals and host combat systems such as the Advanced Combat Direction System (ACDS) or Aegis Command and Decision (C&D), processors such as the shipboard Command and Control Processor (C²P) or the F14-D Mission Computer, Link-16 antennas, other hardware, software, and displays. The C²P was developed at SSC San Diego to provide data forwarding and translation between Link-16, Link-11, and Link-4A.

Using Time Division Multiple Access communications architecture, Link-16 terminals transmit information in the Tactical Digital Information Link-Joint (TADIL-J) message format. A common communications net is thus provided to a large community of airborne and surface elements within line of sight, and the network can be extended to platforms beyond line

ABSTRACT

This paper traces the development of SSC San Diego's Systems Integration Facility (SIF) and the Combined Test Bed (CTB) that, together, provide a flexible, fully integrated multi-platform test capability used by dozens of multi-service and multinational testing organizations to ensure the interoperability of tactical data link systems. The paper describes unique PC-based Data Link Test Tools vital to Link-16 testing components. It also chronicles work of the major command, control, communications, computers, and intelligence (C⁴I) interoperability testing organizations, such as Naval Sea Systems Command's Distributed Engineering Plant (DEP), and describes how the SIF/CTB will continue to support future tactical data link testing.

of sight by using one or more members of the net, or any Link-16 terminal, as relays.

When the Navy JTIDS developmental test program was established to verify the technical adequacy of the JTIDS terminal and the integration of Link-16 into designated Navy host combat platforms, a land-based laboratory environment for terminal specification testing and multi-platform integration/interoperability testing was needed as a cost-effective precursor to live platform testing and to allow problem resolution.

The SIF was designed to utilize a complex multi-computer simulator/stimulator connected to eight JTIDS terminals linked together by an RF network that introduced propagation delays and attenuation into tactical message traffic. The test bed also included external communications equipment, an antenna, test scripting, data storage, reduction, and analysis equipment, and various interfaces.

By September 1991, the SIF provided a fully integrated multi-platform functional testing capability. The SIF/Combined Test Bed (CTB) used intermediate processors to tie together the SIF and the Combat Direction System Development and Evaluation Site (CDES) laboratory in the same building, the E-2C Software Support Activity (SSA) laboratory in Building C-60, and the F-14D Mission Computer Subsystems Software Development Laboratory at Pt. Mugu, California. The CDES contains shipboard combat system configurations and programs for testing CV, LHD, Aegis CG/DDG, and LHA platforms. It also serves as the primary development and testing laboratory for the C²P. The E-2C laboratory consists of actual E-2C Airborne Tactical Data System (ATDS) software and hardware components. The F-14D facility consists of actual F-14D software and hardware components.

By early 1993, the CTB was extended to the Aegis Combat Systems Center, Wallops Island, Virginia, for testing and integrating Aegis combat systems. Later, to support developmental testing of the new generation of Link-16 terminals, the Multifunctional Information Distribution System (MIDS), the F/A-18 Advanced Weapons Laboratory at the Naval Air Warfare Center, China Lake, California, was added to the CTB.

The SIF is the central node of the CTB, providing a central script controller to run the test information and direct it to real or simulated host systems that control the appropriate terminal type in the SIF terminal farm. The unique JTIDS RF simulation environment in the SIF provides connectivity between the SIF terminals, with digital propagation delays and attenuation matched to a scripted scenario. To support exercises that require live transmission rather than SIF RF network simulations, two



The early SIF. Many of the original components of the Systems Integration Facility shown in this 1992 photo have since been replaced by "New SIF" distributed components hosted on personal computers, enabling an infinite number of system configurations that can be tailored to support a large number of test and training scenarios.

JTIDS antennas were installed on the roof of Building 600. Mobile JTIDS vans and portable JTIDS units, called mini-racks, were developed by the SIF team for deployment in other test locations or for installation on surface vessels. As tests were conducted, other SIF systems enabled collection of the test data for later replay and analysis.

The concept for JTIDS development and integration was to proceed through increasingly complex testing, from technical evaluation of the terminal to integration with the C²P, then with the ACDS, and, finally, with air programs. Following the initial terminal testing program in the early 1990s, the SIF/CTB and D45 test and evaluation team members played major roles in the JTIDS and C²P technical evaluation (TECHEVAL) processes that paved the way to a major milestone in the Link-16 program—the successful completion in 1994 of the required operational evaluation (OPEVAL) of the JTIDS and C²P development program during the USS *Carl Vinson* (CVN 70) Battle Group's deployment to the Persian Gulf. This important step in the introduction of Link-16 and the C²P into the Fleet was the culmination of years of development work by Navy activities and supporting contractors. It was also the beginning of new challenges for the SIF/CTB.

Early in the development of the SIF test bed, it was realized that significant modifications would be needed to support emerging test requirements. New capabilities were being added to Link-16 terminals. The new MIDS program was being planned, and the SIF would be the lead laboratory for terminal testing and integrating MIDS into Navy platforms, under sponsors PMW 159 and the MIDS International Program Office (PMW 101). The MIDS is a smaller, lighter weight terminal that maintains all JTIDS functionality. C⁴I interoperability testing needed to expand to support Joint service and multinational interoperability scenarios, and interoperability testing needed to support operations in multi-link environments.

While the SIF/CTB had provided valuable feedback to the Navy's JTIDS Program Office concerning the functional performance of Link-16 terminals and integration of the terminals with combat systems, its capability to support multi-service and multinational integration and interoperability testing was somewhat limited. A method of easily interfacing multi-service and multinational host combat systems was needed, as well as a system for addressing multi-link issues. These requirements led to the next developmental phase of the test bed.

Cost/benefit studies conducted by systems engineers from SSC San Diego and supporting contractors concluded that while the equipment in the



Shipboard combat system equipment in the Combat Direction System Development and Evaluation Site (CDES) laboratory in 1992. The CDES is an integral part of the Systems Integration Facility/Combined Test Bed for data link testing.

SIF was capable, it was costly to maintain and difficult to modify. The long-range functional requirements for the SIF/CTB could best be met by a complete re-engineering of the test bed's systems.

In the mid-1990s, development began on "New SIF" architecture. Its goal was to be a system with greater capability that could respond quickly and cost-effectively to the rapid evolution in functional requirements and could provide cost-effective test and evaluation support to any tactical platform, regardless of location or terminal availability. The "New SIF" would use commercial-off-the-shelf IBM-compatible personal computers and the OS/2 operating system that accommodated the robust multi-tasking required by the systems and provided a friendly graphical user interface. "New SIF" systems would be based on common software architecture to allow rapid development and flexibility when requirements changed.

By 1995, the Link-16 Gateway, now known as the Data Link Gateway (DLGW) system, was developed by D45 with contractor support to connect hosts at remote laboratories to the JTIDS and MIDS terminals in the SIF. The versatile PC-based Gateway system permitted the interfacing of multiple terminal farms, development laboratories, software support activities, live assets, and certification and simulation activities, forming a single extended Link-16 network for testing and integration. The Gateway system is composed of multiple DLGW units linked by secure dial-up phone lines or higher speed communications systems. Each DLGW can function as a host emulator, as a terminal emulator, or as a network monitor. The Gateway software provides a suite of functions that allows users to participate in data link exercises, and monitor, control, record, and analyze data from the exercises.

Other PC-based Data Link Test Tools were developed, including the following:

- Script Controller for executing test scripts on the SIF script network.
- Simulation Interface Units (SIUs) for translating scenario data in SIF format to the format and protocol needed by specific simulation systems.
- TADIL-J Host Simulator, a scenario-driven or real-time tactical data system emulator that creates realistic participants for testing and training.
- Link-16 Engine to support interconnection of non-Link-16-capable systems to the Gateway system.
- Script Generator for creating test scripts that pass events to various Data Link Test Tools for processing on a Link-16 network.
- Data Analysis and Reduction Tool (DART) for post-test analysis.

The original SIF systems were replaced by the "New SIF" distributed components hosted on PCs and communicating through Transmission Control Protocol/Internet Protocol (TCP/IP) on an Ethernet local area network (LAN). Because the new systems were interconnected to operate as a single distributed system, the re-engineered test bed offered an infinite number of system configurations that could be tailored to support a large number of test and training scenarios.

Each of the systems comprising the "New SIF" is a complex system in its own right, and each has evolved and continues to evolve to meet various new functional requirements. The SIF/CTB is a meta-system whose components are interconnected and mutually supporting. Within the SIF itself, systems communicate over the Script Net LAN. The remote sites are connected in a wide area network by the DLGW system, which

multiplexes Link-16 and scenario data between sites. At the remote sites, SIUs convert the scenario data into the form needed by the site-specific simulation system so that all systems are not only communicating in the same link environment, but also participating in a single coordinated scenario.

By 1996, the "New SIF" began to evolve into a major hub for Joint and multinational C⁴I interoperability testing and training, as well as a facility for testing new Link-16 terminal types such as the MIDS. Today, Data Link Test Tools provide Link-16 connectivity between the SIF and more than 100 Joint and international test and software support facilities, as well as all SSC San Diego C⁴I laboratories, including the Research, Evaluation and Systems Analysis (RESA), the Reconfigurable Land-Based Test Site (RLBTS), and the Global Command and Control System (GCCS). By installing a DLGW system at each of the remote facilities and linking them by telephone lines or high-speed circuits, a Gateway network is created. This connectivity enables a worldwide TADIL and systems interoperability test capability.

In addition to the unique combination of assets in the SIF/CTB, key to the success of the TADIL testing programs is one of the most experienced and knowledgeable Link-16 engineering and test and evaluation (T&E) teams in the world. The D45 T&E team has supported at-sea testing and engineering programs since the early 1990s. The team's extensive hands-on engineering experience from early Navy JTIDS terminal testing to the complex interoperability test programs of today has provided a valuable resource for testing and integration programs.

Today, a wide variety of JTIDS and MIDS testing activities are offered by the SIF/CTB, including terminal functionality and specification testing, pre-installation testing and checkout, relative navigation performance evaluation, JTIDS terminal network load testing, TDS-to-TDS interoperability testing, multi-TADIL/multi-platform interoperability testing, TADIL network performance evaluation, TADIL trouble report testing, TADIL standards certification testing, new TADIL "proof-of-concept" analysis, and live fleet service support. In addition, the test bed supports production testing of JTIDS terminal firmware upgrades for the Command and Control Fleet Engineering Division's JTIDS/MIDS SSA (SSC San Diego D64), and Product Acceptance Testing (PAT) and Functional Interoperability Testing (FIT) for the C²P SSA.

Scores of testing organizations have used the SIF/CTB resources. One of the first to use the DLGW systems and the "New SIF" for integration and interoperability was the Theater Missile



The SIF today. PC-hosted Data Link Test Tools communicating via TCP/IP protocols on an Ethernet local area network have replaced the original systems in the SIF, which is now the Navy's leading laboratory for tactical data link interoperability testing.

Defense System Exerciser (TMDSE), a program of the Ballistic Missile Defense Organization (BMDO) to integrate the entire TMD family of systems and test interoperability issues between the various TMD systems. The SIF/CTB supports certification testing programs conducted by the Joint Interoperability Test (JIT) network directed by the Joint Interoperability Test Command (JITC) and by the Navy Center for Tactical Systems Interoperability (NCTSI). The SIF is the lead laboratory for the ongoing MIDS Low Volume Terminal (MIDS-LVT) and MIDS on Ship (MOS) test and evaluation programs. The SIF/CTB and the D45 T&E teams have played a significant role in the North Atlantic Treaty Organization (NATO) program to test the Standard Interface for Multiple Platform Link Evaluation (SIMPLE), and the test bed has been used in many of the Navy's Commander, Operational Test and Evaluation Force (COMOPTEVFOR) testing programs. The SIF has been accredited by COMOPTEVFOR for operational testing of the rehosted C²P and the MOS terminal.

The SIF/CTB is a development and land-based testing and evaluation environment for the C²P, the rehosted C²P, the Common Data Link Management System (CDLMS) and, most recently, for the Multi-TADIL Capability (MTC) Global Command and Control System-Maritime (GCCS-M) program. The MTC will provide a standard and interoperable data link capability for exchanging information on TADIL-A, TADIL-B, TADIL-J, and Satellite TADIL-J (S-TADIL-J) across the entire Joint environment. The SIF has been equipped with computer systems dedicated to the MTC program, currently developed for use with GCCS-M. To support interoperability and integration testing of Aegis ship classes and related subsystems, the Integrated Combat System Test Facility (ICSTF), a field activity of Naval Sea Systems Command (NAVSEA) located at SSC San Diego, has located its Aegis 5.3.7 test bed in the CDES.

The SIF/CTB has supported the Cooperative Engagement Capability (CEC) "Road to OPEVAL" integrated testing program since 1996. The world's most technically advanced air defense system, the CEC has been a top priority for the Navy to achieve its vision of network-centric warfare, and has involved many systems interoperability issues during its development. Support is also provided for the JTIDS Range Extension (JRE) program, which involves transferring Link-16 live satellite and S-TADIL J transmissions through the C²P. S-TADIL-J was developed by the Navy to provide Link-16 connectivity when that connectivity is lost or affected by range limitations.

The SIF/CTB and Data Link Test Tools have become integral components of the extensive land-based Battle Group test bed of the Distributed Engineering Plant (DEP), a NAVSEA program designed to improve fleet readiness by identifying and resolving interoperability issues before deployments. The DEP connects, in real-time, land-based combat and



The team today. The D45 government and contractor teams for SIF/CTB operations, Data Link Test Tools development and support, and data link testing and evaluation.

battle management systems located in various Navy testing facilities across the U.S. The SIF is now home to the DEP's TADIL Operations Center (TOC). Information is exchanged among battle groups through Link-16 and Link-11, and DLGW Terminal Emulators located at each DEP Link-16 host site provide the Link-16 message exchange capability for the test bed. D45 provides the DEP TADIL team leaders.

To support government qualification testing of MIDS-LVT (PMW 101) production terminals, an environmental testing chamber is being installed in the SIF. First Article Qualification Testing (FAQT) of MIDS-LVT vendor terminals will include functional performance, interchangeability, and terminal compatibility tests. Following successful FAQT testing, the vendors will be allowed to competitively bid on full-rate production of the MIDS-LVT.

Today, more than 100 operational, test, training, and development sites around the world use the unique combination of interconnected Link-16 terminals, operational hardware and software, Data Link Test Tools, simulation systems, ship and air laboratory connectivity, live transmit/receive facilities, robust Link-11 capability, and the SIF's engineering, evaluation, and integration expertise to assist in the development and operational evaluation of tactical data systems.

Once begun as a single centralized JTIDS test bed with three remote development and test sites, the SIF/CTB has now become a powerful distributed network providing comprehensive operational testing and training support to the C⁴I community worldwide. As additional data links are developed and as interoperability programs are expanded and new programs begin, this unique test bed is well prepared to accommodate the future needs of the Navy, Joint, and Allied nation testing communities it serves.



David P. Andersen

BS in Mathematics, San Diego State University, 1985

Current Work: Link-16 (Joint Tactical Information Distribution System [JTIDS]/Multifunction Information Distribution System [MIDS]) Test and Evaluation Business Area Manager.



Karen D. Thomas

BA in Journalism, San Diego State University

Current Work: Principal Analyst/Writer; computer systems engineering.