JITC M&S Applications to National Security Systems/Information Technology Systems (NSS/ITS) Test and Evaluation

Author: Denny Beugureau, Kenneth G. Thomas, Chief, Modeling & Simulation, JITC

Abstract:

The application of modeling and simulation (M&S) is particularly appropriate to the test and evaluation of NSS/ITS and NSS/ITS interoperability. NSS/ITS typically operate in distributed network environments with many system and human interfaces. NSS/ITS may perform adequately in a small-scale operational context but degrade in conditions of high traffic volumes typical of actual contingency operations. It is often infeasible or cost prohibitive to assemble the representative number of human operators and live interfacing systems to adequately provide a relevant operational environment context. The Joint Interoperability Test Command (JITC) has a long history of using M&S to support NSS/ITS testing. This article presents several specific examples of the application of M&S to NSS/ITS testing to provide relevant context to NSS/ITS networks.

BACKGROUND

The JITC is the Operational Test Agency (OTA) for Joint NSS/ITS programs developed by the Defense Information Systems Agency (DISA) and other joint agencies and provides developmental testing services as well. JITC is the only agency with authority to recommend joint interoperability certification of NSS/ITS, also known as Command, Control, Communications, Computers and Intelligence (C4I), to the Joint Staff. Additionally, JITC has a mission to directly support the warfighter during exercises and contingencies with NSS/ITS interoperability lessons learned, troubleshooting and ongoing evaluations of interoperability in the field. JITC can frequently model NSS/ITS operational configurations, using similar equipments located at Fort Huachuca or available through distributed networks, to replicate problems encountered in the field and subsequently provide recommendations. JITC has used M&S for many years to supplement the live operators and systems available to establish a relevant operational context for evaluation of NSS/ITS and networks of NSS/ITS under test. The use of M&S often provides better control, repeatability and instrumentation than a strictly live environment for some evaluations. JITC cannot use simulations of the system(s) under test as the sole basis for operational or interoperability evaluations. This paper discusses specific examples of how JITC uses M&S applications for NSS/ITS and NSS/ITS interoperability testing.

The Joint OT&E Simulation Environment Facility (JOSEF) was developed to address operational testing of NSS/ITS generally, but primarily focused on overcoming testing shortfalls of two DISA pillar programs. These are the Defense Messaging System (DMS) and the Global Command and Control System (GCCS). JOSEF was established largely with funds provided through the Central Test and Evaluation Investment Program (CTEIP) Resource Enhancement Project (REP). The JOSEF has been used regularly in

developmental, operational and interoperability testing. Many NSS/ITS, including DMS and GCCS, are developed as evolutionary or incremental releases to reduce risks, costs and schedules; leverage latest emerging technology; and solidify requirements by providing early user involvement and input. The M&S test environment is reused for each new evolutionary or incremental product release and evolved to meet future releases.

JOSEF AND DMS

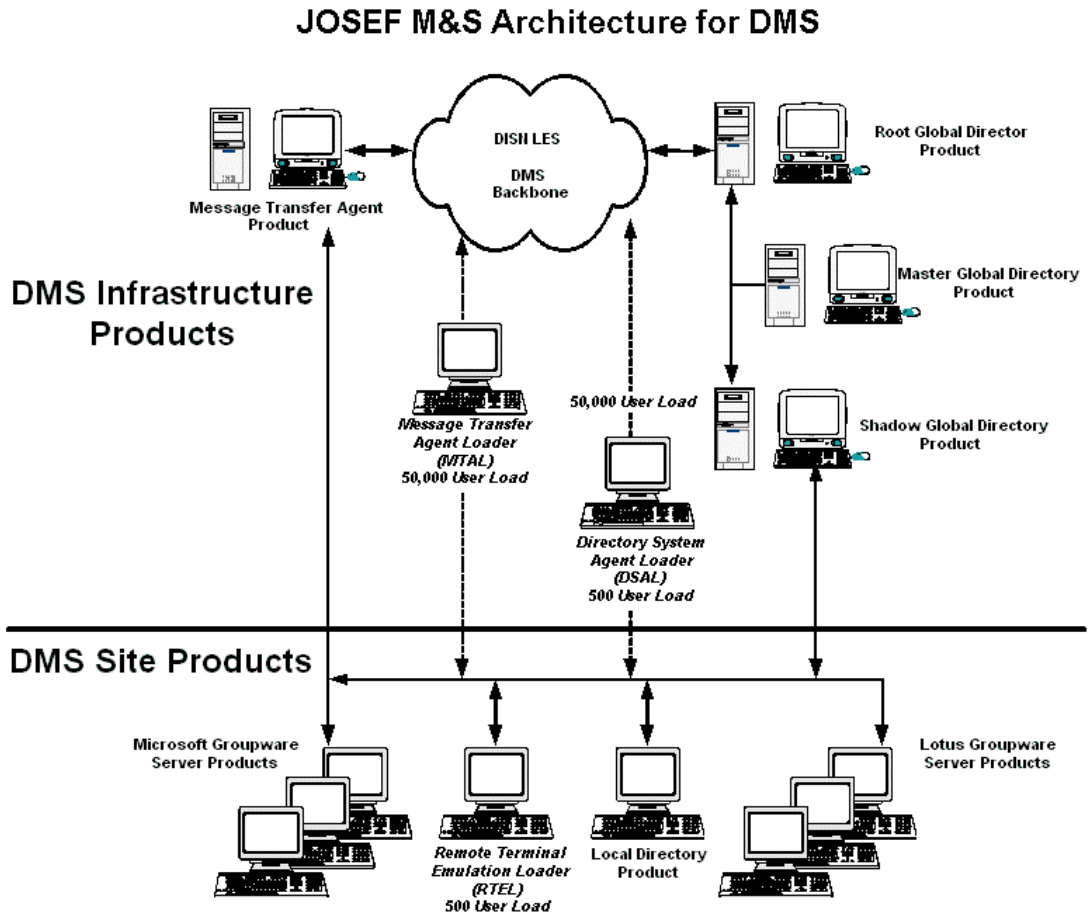

Figure 1

The JOSEF DMS configuration is displayed in Figure 1. The LAN Remote Terminal Emulation Loader (RTEL) provides the capability to emulate up to 500 DMS users generating messages under varying load levels established for peacetime, mobilization, and wartime. A user agent is the software interface that interacts directly with a user while he is constructing a message on his personal system. The RTEL emulates DMS user agent software outputs. A groupware server handles a group of user agent inputs. A groupware server sends completed messages to a message transfer agent. A message transfer agent (MTA) is similar to a local or regional post office. MTAs transfer batches of

messages among themselves and ultimately deliver them to the addressed user agents. The MTA Loader (MTAL) provides the capability to emulate up to 50,000 DMS users' message traffic to directly load the network of MTAs. This provides the capability to evaluate the MTA performance while it is under background processing loads approximating various operational conditions. The DMS directory services provide addressing and security certificate information. The Directory Service Agent Loader (DSAL) emulates the directory service access patterns of up to approximately 50,000 users to look up, add, delete and transfer addressing information. This provides evaluation of the local and remote directory services under varying expected operational conditions. The DMS traffic simulation load tools have been used with several DMS releases and continue to support the developmental and operational test and evaluation of DMS releases.

These tools were developed from government-off-the-shelf (GOTS) and commercial-off-the-shelf (COTS) products to minimize the risks associated with new developments and lower the cost of the solutions. The MTAL was developed from a validated X.400 conformance test tool baseline and the DSAL from a validated X.500 conformance test tool. A COTS Remote Terminal Emulator (RTE) was selected and modified to use the DMS user agent interfaces to emulate DMS users and user organizations. The DMS product line can be configured with any of three DMS variants of user agent. These are the Microsoft Exchange, Outlook and Lotus Notes DMS variants. The RTE is adapted to any of these interfaces. All these tools allow message data capture and recording for response time, throughput and other performance analysis. The test scripts are controlled and repeatable so that each different vendor solution can be evaluated with exactly the same input scenario, which cannot be accomplished as well with live operators.

There are limitations to this approach. The tools must be modified with each new release to accommodate even minor changes in the interfaces. Some of the tools are difficult to use and there is some considerable training involved. Vendor support is frequently required. There are portability limitations of the developed tools for use at the operational test sites.

Past test results included finding performance problems with one of the vendor solutions, which otherwise would not have been identified until after DMS was fielded and operating in a stressful environment. The JOSEF DMS testing tools provided information that resulted in improvements and corrections in later version releases. Test results for the MTA determined the MTA was capable of supporting the baseline throughput requirement and determined the throughput breakpoint. The use of DMS DSALs helped result in a redesign of directory services that improved the overall DMS performance. Repeatable test scripts were used to help find problems during Y2K testing. Test results were documented and repeated after date changes for comparison.

The JOSEF emulation of DMS users reduced the need for live users/operators and associated workstations. Significant cost avoidance was possible since employing up to 50,000 or even 500 users and workstations for weeks at a time runs into millions of dollars for each version release. The DMS is a distributed messaging system of unprecedented size, expected to support approximately 2,000,000 users. Providing a representative load environment for test and evaluation is not really possible without using M&S.

JOSEF AND GCCS

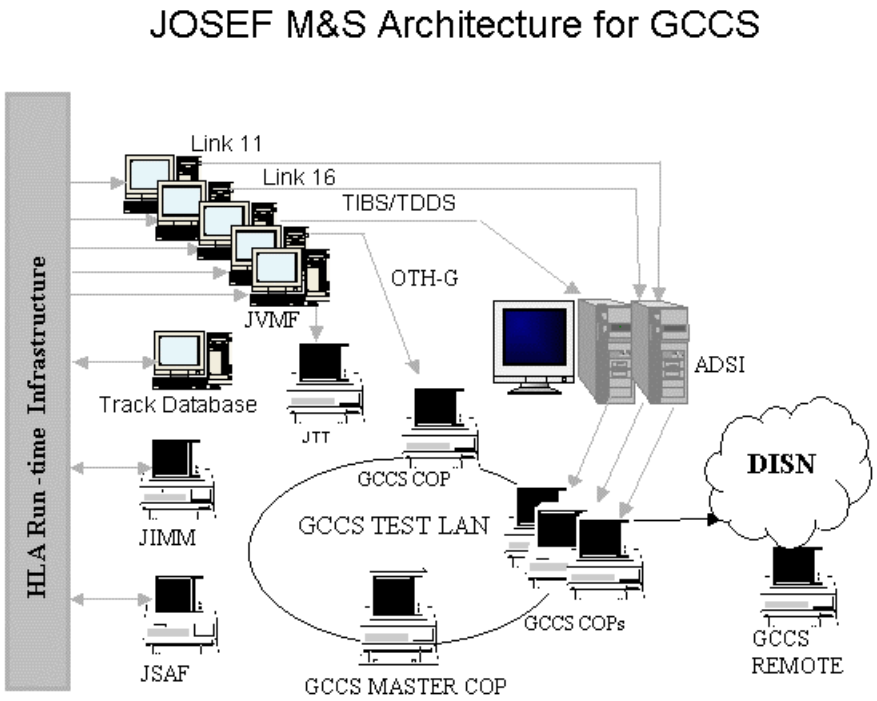

Figure 2

The JOSEF M&S architecture for the GCCS Common Operational Picture (COP) evaluation is displayed in Figure 2. The JOSEF provides tactical and intelligence message traffic to evaluate the GCCS COP's ability to handle and display track information in a scenario approximating actual deployment. The GCCS JOSEF configuration is aligned with the Defense Modeling and Simulation Office (DMSO) High Level Architecture (HLA) Run Time Interface (RTI) Next Generation (NG) standards. Two copies of the Joint Semi-Automated Forces (JSAF) model are integrated into the JOSEF federation with a Joint Integrated Mission Model (JIMM). These provide a virtual battlespace picture. One JSAF provides background loading while the other JSAF and the JIMM run specified battle scripts to be observed. More JSAF or supporting components can be integrated when higher loading is desired. The virtual battlespace environment entity state

information is used to populate the data fields of the tactical and intelligence messages passed to the GCCS COP through network-specific interfaces. Optionally, the tactical data link messages can be routed through an Air Defense System Integrator (ADSI), which is the designated real-time interface for the GCCS.

JOSEF creates a number of tactical and intelligence message feeds from the same environment (truth source). It does not attempt to simulate the limitations of particular sensors or NSS/ITS. Different GCCS COPs are configured to display different message inputs and messages are merged into a master COP to evaluate the GCCS COP correlation capabilities. The GCCS laboratory test configuration can interact with the live GCCS network through the classified portions of the Defense Information Systems Network (DISN). Network analysis and modeling tools capture network performance information and can develop models of network performance. The simulated warfare environment for GCCS provides “ground truth” for the evaluation of GCCS COP on demand without necessity to reserve live weapons platforms or satellite assets. It provides known repeatable conditions that were used to evaluate GCCS COP operation in both the current century and in boundary conditions of year 2000.

This capability is adequate for many types of performance and suitability analysis. The GCCS COP is primarily a passive system that recognizes only a subset of messages. The primary limitation to this capability in other contexts is that the amount of information necessary to fully populate the complete tactical and intelligence messages emulated exceeds the capacity of the data models of the current standard Distributed Interactive Simulation (DIS) interfaces and the replacement HLA real-time platform reference (RPR) Federated Object Model (FOM) interfaces. The JOSEF interface expanded on the RPR FOM but the development of a full high-fidelity interface FOM was considered outside the initial scope for the GCCS. A collection of message emulation tools that could be driven by creating user scripts was acquired for JOSEF to be used in testing that required more complete message emulation, but when a realistic battlespace simulation may not be required. These additional tools can also be provided with actual live or other recorded data and played back, or the message traffic can be scripted with data entered interactively by the user. They can also be used to record outputs of a scenario and subsequently played back without the need for the complete JOSEF hardware environment. The script-driven tools are used to evaluate completeness of GCCS interfaces, including the messages and message fields that are implemented.

These tools allowed Y2K problems identified in the laboratory to be fixed before fielding, GCCS tactical message interface problems to be identified and resolved, ADSI real-time interface problems to be identified and reported, and scalability test scenarios approximating actual combat traffic conditions to identify limitations in the message queuing in early versions of the COP. Significant cost avoidance was possible since the principal alternative for similar testing would be a large,

live event. Live exercises on the order of a ROVING SANDS or an ASCIET can cost 10-20 million dollars and can be impacted by real-world events. JOSEF provided a more relevant operational test environment for the evaluation of GCCS COP than available with limited live assets.

M&S IN TACTICAL DATA NETWORKS

The DMS and the GCCS are examples of NSS/ITS residing on the Joint Planning Network (JPN). The Joint Data Network (JDN) is a network of systems that operate and exchange tactical and intelligence messages in near-real time. GCCS COP operation requires interoperability between the JDN and JPN. Sensor warnings and situation information (tracks) are sent to a command and control node, such as a GCCS, by systems on the JDN, such as an AEGIS or AWACS. Information is disseminated from GCCS via DISN to other C2 nodes and systems on the JPN.

The JOSEF does not attempt to simulate the limitations of actual JDN systems. When high-fidelity JDN system representations are needed, such as for interoperability certification testing, JITC uses hardware-in-the-loop (HWIL) representations with actual operational software. Some JDN systems are available using JITC's Joint Tactical Data Link Laboratory (JTDLL).

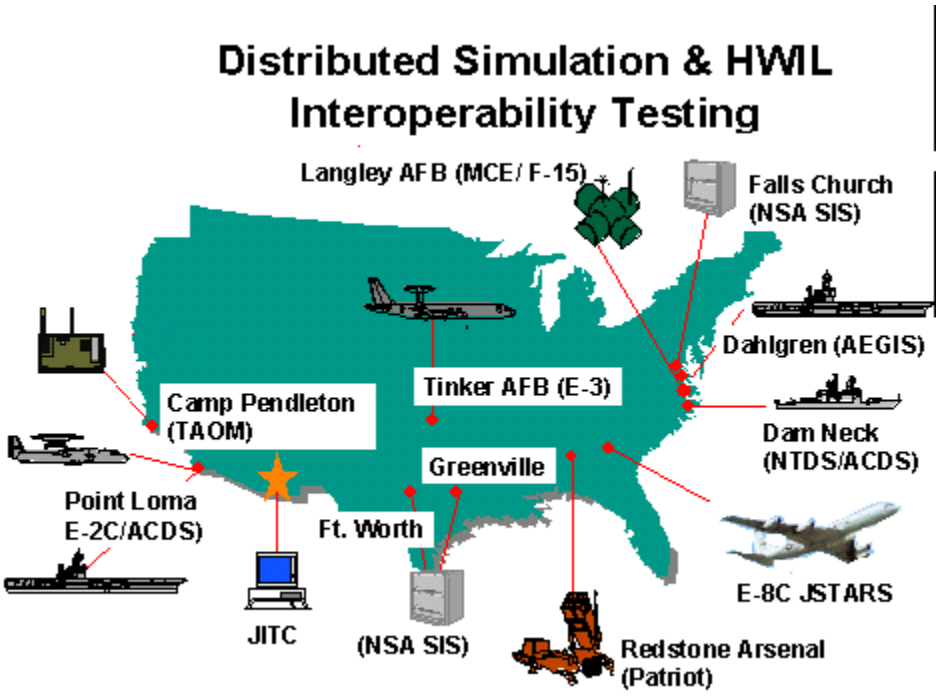

Figure 3

The JTDLL is a distributed simulation and NSS/ITS HWIL network that became operational in 1993. It is used for evaluating the joint interoperability of systems

of the JDN. Figure 3 illustrates some locations and NSS/ITS of the JTDLL distributed network. Link 11 and Link 16 information is transmitted on simulated JDN network interface gateway emulators. The JTDLL includes an integral motion simulation or can be driven by an external battlespace simulation such as the JSAF. The motion simulators are located at the JTDLL Central Test Facility (CTF) at Fort Huachuca, Arizona. The CTF currently sends DIS protocol data units (PDUs) representing ground truth to the remote test facilities (RTF) where the laboratory tactical systems are located. The DIS PDUs representing battlespace objects are detected by sensor simulations at the RTF and used to emulate the sensor signals sent to the tactical data processing components. The sensor stimulus and/or human operator inputs result in the flow of tactical messages on the simulated JDN.

The messages on the JDN are monitored, recorded and analyzed by CTF instrumentation such as the Joint Interoperability Modular Evaluation System (JIMES). JIMES is a modernization of the original FORTRAN and VAX-based instrumentation and evaluation tools. The JIMES receives tactical messages, converts those messages into human-readable format, and displays them to the user. It also parses the track information and displays positions on a graphic display along with the truth data from the battlespace simulation. JIMES allows the user to highlight specific tracks and request more detailed data. JITC has transportable versions of the JIMES and regularly attends operational exercises to collect data on NSS/ITS and to provide technical assistance to the warfighter.

Tests using JTDLL have found numerous interoperability problems, such as tactical unit reporting responsibility issues, data link problems, individual NSS/ITS deficiencies, and position/location anomalies. Since NSS/ITS interoperability is not a static property, the JTDLL is used on a continuing basis as new software releases and new system capabilities are added to the distributed network systems. Other similar DOD distributed simulation networks and tools for interoperability evaluation, such as the Ballistic Missile Defense Office (BMDO) Theater Missile Defense System Exerciser (TMDSE) and Navy Distributed Engineering Plant (DEP), have been developed independently. They are currently not linked and interoperable with the JTDLL, but JITC works closely with these organizations to collect and analyze data for interoperability evaluations. The Interoperability Test and Evaluation Capability (InterTEC) is a new Services and JITC partnership initiative. InterTEC provides the formal framework to link such networks along with open-air test ranges, other M&S capabilities and other instrumentation through standard interfaces. The Joint Distributed Engineering Plant (JDEP) is a joint extension of the DEP and is an ongoing project to establish initial and long-term interoperability of these Service and Agency networks. In the meantime, JITC is transitioning the JTDLL DIS sensor simulation to an HLA-compliant sensor simulation capability. The CTF and RTF are currently being upgraded to an extended HLA RPR FOM interface in a transition to higher fidelity simulations and better compatibility with the JOSEF.

OTHER M&S APPLICATIONS

Another example of JITC M&S-augmented test environments is the electronic commerce test environment, e-test. E-test provides varieties of simulated electronic commerce/electronic data interchange formats between simulated government sources on DISN and simulated commercial vendor sources on the commercial value added networks (VANs). The principal purpose is to provide representative electronic commerce traffic to evaluate the throughput, accountability, accuracy and speed of service of the Electronic Commerce Processing Node (ECPN). Live users produce scripts for evaluation of specific functional performance criteria. Automated or synthetic users exercise the system by generating thousands of transaction sets per day and collecting data for the evaluation of the performance measures. Transactions include requests for bid, bids, purchase orders and payments. The e-test established early performance values that have resulted in significant improvements in the performance and reliability of the ECPN. Not only does the e-test avoid the costs of employing thousands of users to generate transaction sets, but it has helped to minimize the liability of the DOD for lost or delayed vendor responses.

Yet another M&S test tool is the Traffic Loading Device (TLD) and circuit switch traffic simulation (CSTS) which simulate tactical circuit switch users initiating and holding tactical phone calls. Each TLD can emulate up to 256 users and end instruments. The CSTS has been used to generate TLD instructions and to rehearse the call traffic scenarios in software before committing live people and tactical equipment to the tests. Live operators are used during tests to place calls over the simulated background. The original TLD was developed in the 1970's and has been used at least yearly to evaluate upgrades and modifications to the joint tactical switches. It has been used to evaluate the performance of subscriber equipment, tactical switch line units, trunks and tactical-to-strategic switch interfaces and interoperability. It also helps evaluate military-unique features, such as precedence, priority and security in the face of operationally representative tactical call traffic. It is currently being upgraded to use latest technology components. The new design is more modular and expandable to represent greater numbers of users and end instruments. The TLD has helped to improve the quality of the tactical switches and enabled better interoperability between the tactical and strategic communications environments.

CONCLUSION

In summary, it is difficult to do adequate testing of NSS/ITS without the use of M&S. Generally, it is impractical to try to assemble all of the live components and operators that could be involved in a relevant operational scenario of networks of NSS/ITS. JITC has found that supplementing the surrounding context of threats and systems with simulated entities and simulated user inputs can be an effective strategy for testing with limited resources.