Improved Distributed I&T Efficiency Through Automated Testing

Michael Aldinger, Brad Bridges
Northrop Grumman Corporation
Orlando, Florida
Mike.Aldinger@ngc.com, Brad.Bridges@ngc.com

Robert Ingalls
USAF ACC/A8AT
Langley AFB, VA
Robert.Ingalls.ctr@langley.af.mil

ABSTRACT

Programs spend extensive time and money for system wide Integration & Test (I&T) when networking dissimilar live, virtual, and constructive training and simulation systems into a common training environment. Simply implementing DIS, TENA or HLA gateways is not enough to bridge the gaps between dissimilar systems. A mature standards set provides system requirements to guide the development of incoming training systems. This information further benefits the training program through well defined requirements and training objectives.

The Combat Air Force (CAF) Distributed Mission Operations (DMO) program implements detailed interoperability standards/requirements which span interfaces, protocols, procedures and processes, and performance. An early assumption was that once systems implemented the interoperability standards, integration would be relatively straightforward. Integration efforts over the past eight years have shed light on the many complexities associated with the integration of disparate, high fidelity, Mission Training Centers. These training centers are comprised of high fidelity virtual cockpits, manned threat stations, Environment Generators, Instructor Operator Station, and Brief/Debrief suites.

One effective means for achieving improved I&T efficiency is through an automated tool which determines whether participating systems meet the agreed upon training system standards/conventions. The CAF DMO program is currently implementing a distributed, standards based validation tool which supports I&T of CAF DMO training systems. This tool, using a variety of modes (e.g. passive, interactive) evaluates real-time simulation traffic for compliance with the CAF DMO standards and recommends corrective actions for non-compliance issues. This paper will discuss the technical and procedural I&T issues which prompted the development of this tool, provide Metrics that illustrate the benefits of this type of tool in both distributed I&T efforts and event troubleshooting, and proposes how such a tool can be leveraged to mitigate inter-service integration challenges (e.g. connectivity, security) that can impede joint training desires.

ABOUT THE AUTHORS

Mike Aldinger is the Manager for Advanced Programs and Technologies at Northrop Grumman Information Systems on the Combat Air Force (CAF) Distributed Mission Operations (DMO) program. He holds a B.S. in Industrial and Systems Engineering from the University of Florida and an M.S. in Simulation Modeling and Analysis from the University of Central Florida. His current roles include DMO Standards Development Lead, DMO-Space Chief Architect, and PACAF L-V-C Program Manager/Tech Lead.

Brad Bridges is the Manager of the Systems Integration and Test Team at Northrop Grumman Information Systems supporting the CAF DMO program. He has over 20 years of experience in the automated test, communication, and simulation industry both as an Integration Test Lead and a Software Development Director. He holds a B.S. in Computer Science from the University of Central Florida. His current roles include CAF DMO Federation Testing Manager, CAF DMO DMON Portal Integration Lead, and Navy FST Program Manager.

Rob Ingalls, Lt Colonel, USAF (retired), is a Senior Program Analyst with Santa Barbara Applied Research, Inc., in support of HQ Air Combat Command (ACC) Distributed Mission Operations (DMO) Requirements, managing the DMO network and system interoperability/integration requirements for the CAF. He has over twenty years flight and simulator experience, and seven-plus years testing aircraft, simulators, and computer systems. He holds an M.S.

in Operations Management and a B.S. in Computer Science. He is also a Certified Modeling and Simulation Professional (CMSP).

Improved Distributed I&T Efficiency Through Automated Testing

Michael Aldinger, Brad Bridges
Northrop Grumman Corporation
Orlando, Florida
Mike.Aldinger@ngc.com, Brad.Bridges@ngc.com

Robert Ingalls
USAF ACC/A8AT
Langley AFB, VA
Robert.Ingalls.ctr@langley.af.mil

M&S I&T CHALLENGE

Standards based simulation architectures are becoming prevalent in the simulation training community as a means to both mitigate the increasing cost, duration, and complexity of distributed systems integration. The virtues of a standards based training solution includes collaboratively developed and agreed upon system requirements, a “controlled” test environment, and simplified troubleshooting which facilitates better planning and minimized system integration timelines.

Through the implementation of a standards-based architecture, the Combat Air Force Distributed Mission Operations (CAF DMO) program has reaped these benefits and made great strides towards achieving a persistent, on-demand training environment. With this improved integration methodology comes greater expectations for both program wide and inter-service growth. This is reflected in Air Combat Command’s (ACC) CAF DMO outyear projections which show continued expansion of the CAF DMO program in the form of new training platform types and/or sites. This growth presents new mission package training opportunities (e.g. Combat Search and Rescue, Close Air Support) and thus additional requirements necessitating standards solutions. Standards requirements (e.g. visual models, Infrared, emissions, weather) to support these new training requirements compounded by additional platforms dictated that a new, more efficient integration solution was needed which would address both escalating time and staffing requirements necessary to support integration of the CAF DMO training federation. There was also a need to mitigate testing delays due to site connectivity constraints attributed to security approval issues. The solution discussed in this paper meets ACC’s challenge for a more efficient I&T methodology in CAF DMO. This solution is applicable to other programs that implement SISO 1278.1a based system requirements.

CAF DMO OVERVIEW

DMO is critical to Air Force readiness and is the cornerstone of United States Air Force (USAF) training transformation in accordance with OSD-directed Joint National Training Capability Initiatives. CAF DMO is the foundation for revolutionizing training for the USAF. The CAF DMO program, formerly know as Distributed Mission Training (DMT), provides a training architecture that supports both inter-team and intra-team composite force training for warfighters located in geographically separate locations. The training focus is on the tactical training of the warfighter.

CAF DMO Mission Training Centers (MTCs), also identified as Federate Systems in this paper, provide a capability for a platform (e.g. F-15C, E-3, F-16CJ, JSTARS, A-10C, and B-1B) to participate in a distributed training event. These MTCs provide high fidelity man-in-the-loop virtual cockpits for pilots, weapon system officers, and C2ISR crew stations. The MTCs also provide training aids which include manned threat stations, instructor-operator stations, environment generators, and Brief/De-brief solutions. These MTCs are connected via our DMO Network (DMON), a Wide Area Network (WAN) that facilitates global connectivity between the MTCs as well as the means for continuous monitoring and control of the CAF DMO System. The CAF DMO system executes in excess of 900 distributed training events per year. Some key discriminators of the CAF DMO system include:

- Training availability is 24/7.
- State-of-the-art, high fidelity man-in-the-loop virtual cockpits for pilots, and C2ISR crew stations.
- All training systems adhere to rigid set of interoperability standards.
- Manned threat stations that provide man-in-the-loop friendly/adversary forces.
- Integrated scheduling system in support of coordinated multi-site Aerospace Expeditionary Force (AEF) training and rehearsal.
- Supports multiple/simultaneous training events.
- Provides interface to allow participation in theatre scale training.
- Rapid mission execution in support of user training. Lead-time is 1 hour for archived scenarios.
- MTCs are located at home bases of aircrews.

The primary elements of the CAF DMO architecture include the DMO Network, Interoperability Standards, DMON Portal, and Mission Training Centers. To provide the automated standards compliance assessment capability requested by ACC we leverage our knowledge of the CAF DMO architecture/systems to develop an efficient, cost effective solution. Components of the CAF DMO architecture are described below.[1]

DMO Network (DMON)

The DMON is a persistent network that provides an on-demand daily training capability for CAF DMO systems. The deployment status for MTCs onto the DMON is illustrated in Figure 1. The DMON is a robust, scalable, secure, highly reliable network service for use by CAF DMO systems. High bandwidth, low latency, and the high availability of commercial data services are enablers for achieving our network availability goals.

The DMON implements a Virtual Private Network (VPN) that provides connectivity between the sites as well as the means for continuous monitoring and control of the DMON from the Network Operations Center (NOC). The NOC and DMT Operations Center (DOC) are located in Orlando, FL.

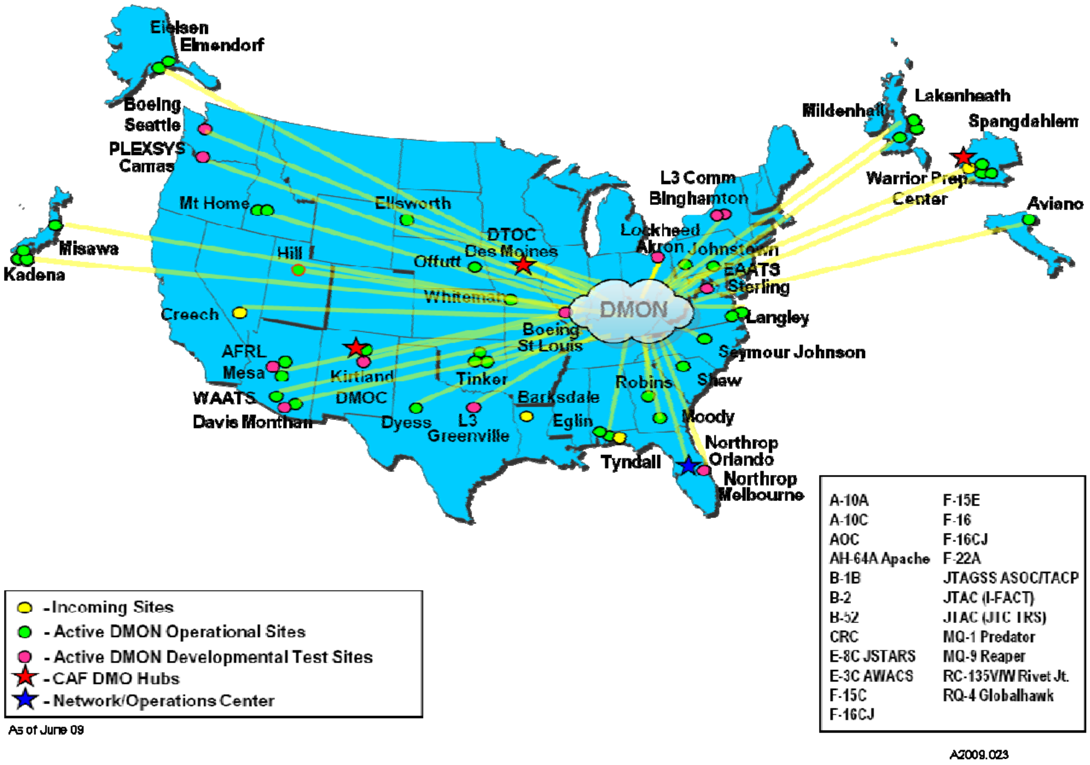


Figure 1. CAF DMO Training System

Over the past 12 months, the DMON has provided the connectivity required to facilitate in excess of 10,000 training hours.

An additional benefit of the DMON environment is that MTC developer contractor locations are also connected. This provides contractors a secure connection to their operational sites to perform system updates and testing without the expense of travel or special shipping of classified media. This also allows them to test with other MTC developers without taking the operational training site offline. This allows developers to test system changes with other development sites before these changes are deployed to operational sites as production builds. [1]

CAF DMO Standards

The objective of standards development is to facilitate a routine, daily training capability, through the development of an overarching inter-site interoperability solution in the form of standards. These interoperability standards apply to all Federate Systems/MTCs participating in CAF DMO events being executed on the DMON. Currently, standards are developed to address the inter-team training requirements of 22 different platforms fielded at over 75 locations worldwide.

Standards requirements are derived though a top-down process which is initiated via the identification of new training platforms and/or training requirements as defined by ACC. These operational requirements are defined in a Mission Package Plan to scope the yearly standards development effort.

The collaborative development process utilized in the development of these standards is governed by the Standards Maintenance Process (SMP) as illustrated in Figure 2. The CAF DMO Standards Development process is executed by two working groups, the Standards Development Working Group (SDWG) and Standards Implementation Working Group (SIWG). The primary purpose of the SDWG is to assess the merits of proposed standards modifications in support of the evolving CAF DMO system. Tiger Teams are tasked by the SDWG chair as necessary to develop and/or validate proposed standards modifications. Tiger Team participation is open to government, industry stakeholders, and interested community members. The SIWG's primary purpose is to evaluate the programmatics associated with a proposed standards revisions.[1]

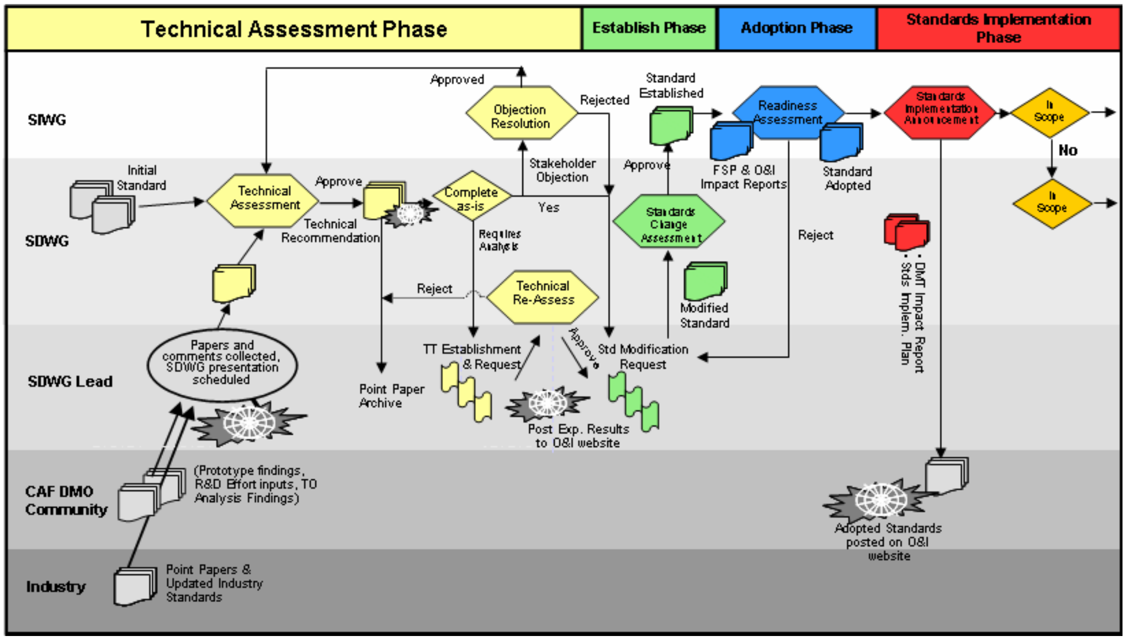


Figure 2. Standards Maintenance Process

CAF DMO DMON Portal

A critical component of the CAF DMO architecture is the DMON Portal which supports the CAF DMO training system by isolating one MTC implementation from another. It also facilitates communication across the DMON among MTCs which implement different simulation protocols (e.g. HLA, DIS) as illustrated in Figure 3. As the DMON Portal evolves, its capabilities and functionality continue to increase as the CAF DMO standards expand to meet the training requirements of the CAF DMO training system. Recently added functionality to the DMON Portal includes a state database, Dead Reckoning (DR), support for NATO EX (NEX) simulation protocol, support for multiple Local Area Network (LAN) endpoints supporting similar or disparate protocols to include DIS, HLA, NATO EX, TENA.

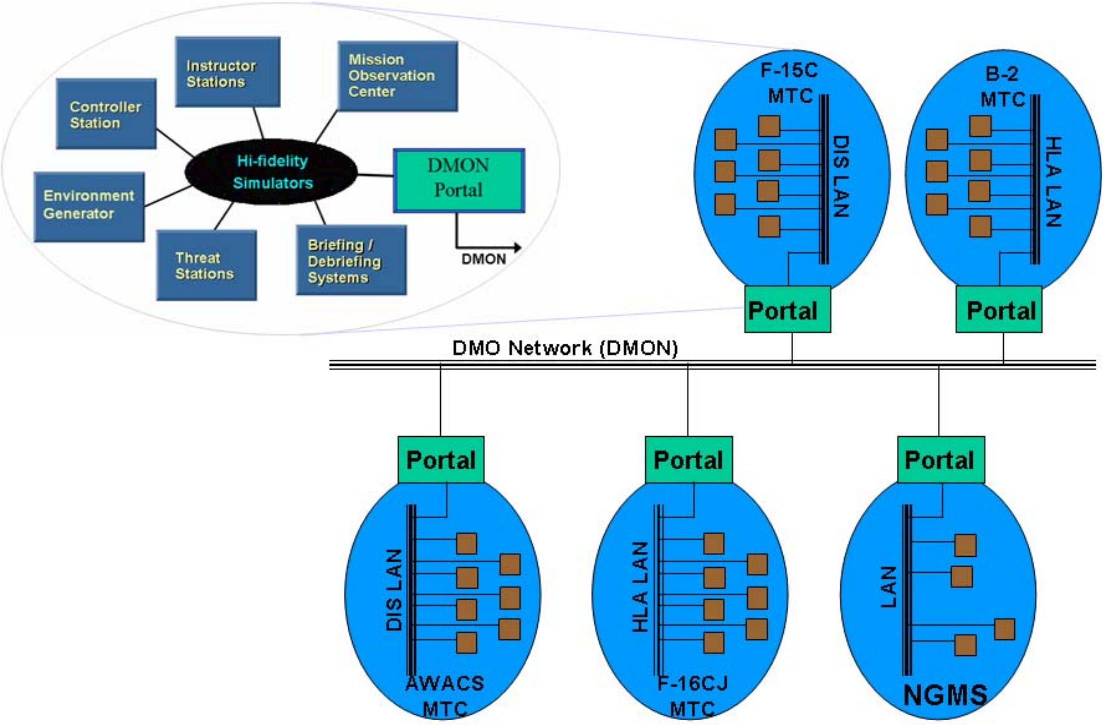


Figure 3. DMON Portal Concept

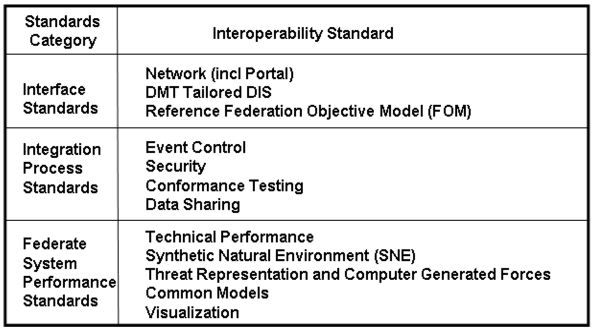
Mission Training Centers

CAF DMO MTCs are comprised of high fidelity man-in-the-loop virtual cockpits for pilots, weapon system officers, and C2ISR crew stations. These systems are complemented with training aids which include manned threat stations, instructor-operator stations, environment generators, and Brief/De-brief solutions. All MTCs interface to the DMON via the CAF DMO Network Standard. The interface, process/procedures, and simulation protocols utilized by these federate system sites for distributed training is in accordance with the CAF DMO standards.[1]

CAF DMO INTEROPERABILITY SOLUTION

Achieving a persistent, on-demand training capability for CAF DMO required the implementation of standards by all program elements. The O&I contractor's approach to achieving interoperability among the disparate Federate Systems connected across the CAF DMO Network (DMON) is through the CAF DMO System Standards (Table 1). Participation in the CAF DMO Standards Maintenance Process provides stakeholders a voice in determining the focus and content in the evolution of standards. Through this participation, future CAF DMO participants are provided with information to assist in the development and/or integration of their Federate Systems into CAF DMO.

Table 1. CAF DMO Standards



Standards Category	Interoperability Standard
Interface Standards	Network (incl Portal) DMT Tailored DIS Reference Federation Objective Model (FOM)
Integration Process Standards	Event Control Security Conformance Testing Data Sharing
Federate System Performance Standards	Technical Performance Synthetic Natural Environment (SNE) Threat Representation and Computer Generated Forces Common Models Visualization

CAF DMO Standards are categorized into three areas: Interface, Process, and System Performance. Interface Standards address the network connectivity, software and hardware interfaces, and protocols necessary for MTCs to exchange information. Process Standards document common processes and procedures that facilitate coordinated operation of Federate Systems as part of the harmonized CAF DMO system. Federate System Performance Standards address consistency, fidelity and performance factors, ensuring a fair fight among training participants.

Stakeholders interested in conducting or participating in CAF DMO training events must use Federate Systems and processes that comply with effective CAF DMO System standards criteria. The 12 standards with criteria effective for the CAF DMO training federation are those necessary to achieve CAF DMO training objectives with the integrated capabilities of the available Federate Systems in a DIS and HLA compliant network.[1]

CAF DMO I&T METHODOLOGY

The CAF DMO training system continues to evolve to include new training platforms, sites, and system capabilities necessary to support inter-team training requirements. Efficient integration of training systems into the CAF DMO training environment dictates verification of platform compliance to CAF DMO standards prior to CAF DMO Network (DMON) integration. This process, while effective, does not scale to meet the integration efficiencies required for this diverse, training solution. To meet the aggressive integration requirements of the CAF DMO program a new integration paradigm was needed.

Conformance Testing Standard

The Conformance Testing Standard defines the process, documentation and personnel required to accomplish each level of the standards conformance testing process and assigns responsibilities to the CAF DMO O&I Contractor, CAF DMO Federate Sponsors and CAF DMO Federation Sponsors. This standard defines the processes to be followed to ensure CAF DMO Federates and Federations comply with the various CAF DMO System Standard criteria and are able to interoperate over the DMON.

Standards Certification

The CAF DMO Certification Process is a rigorous and comprehensive verification of training system capabilities to ensure interoperability of training partners on the DMON. Each CAF DMO platform type must be verified against the applicable CAF DMO standards set before it will be included in the federation test process with other platforms.

This process has evolved since its inception in 1999 to include many guiding artifacts necessary to ensure timely integration of systems. This includes the development of Federate System Test Plans (FSTPs), Reports (FSTRs), and Non-compliance System Problem Reports (SPRs) which document the training systems conformance to standards and associated non-compliance training impacts. Non-compliant systems can still be certified to CAF DMO requirements provided SPRs are documented and training impacts are documented. The guiding documents/templates strive to improve efficiency through common expectations for documentation/ responses of standards compliance. In 2004, the requirements generated from the Mission Package Plan required almost 100 standards criteria to support systems interoperability in CounterAir, CounterLand, and C2 missions. The recently published Mission Package Plan-09 (MP-09) required in excess of 200 standards criteria that platforms must evaluated against.

Federation Integration

Once a training system has verified it’s compliance and has been certified to the CAF DMO standards, the formal integration process of the system with the DMON and other training systems can begin.

Federation integration focuses on verification of the normative training requirements and scenarios that training systems want to achieve in a distributed fashion. The CAF DMO Mission Package Acceptance Plan specifies the criteria to verify as part of the integration phase. This criteria includes training capabilities, scenarios, and primary training federation partners and objectives that are pertinent to distributed federate system training in the CAF DMO training environment.

The objectives and scope of Federation Integration includes:

- To verify that Primary Federation level objectives as specified in the Mission Package Acceptance Plan are met by the Training System.
- To verify Mission Package Objectives are met for the Training System.
- To verify that Training System is compliant to the applicable CAF DMO standards.
- Initially Accept and Approve a Training System for operation on the DMON within their Primary Federation configuration.

Federation integration is accomplished as a formalized, methodical approach that incorporates a variety of Standalone, Integration, Functional and Acceptance testing phases.

Standalone testing occurs at an engineering and functional level to ensure that prior to testing efforts with other distributed systems, each individual simulation system meets the interface and simulation standards requirements of the distributed mission or event. This standalone testing is typically peer to peer with the training system with the DMON network or a single training partner.

Integration Testing is conducted also at the engineering level and is designed to ensure that the individual components of the disparate systems interoperate at the data protocol level as intended across the DMON. Integration testing also includes verification of any network or gateway interface devices that provide interoperability.

Functional Testing assures that the simulation systems, while working in conjunction with each other, provide the individual functional activities (move, shoot, communicate) required for inter-team training, usually through the use of mission vignettes. Verification of the effectiveness of these mini-training missions is accomplished with both engineering personnel and knowledgeable operational site personnel, such as pilot instructors or pilot station operators.

The final phase of the federation integration is the formal Acceptance test which verifies that a complete mission scenario with all simulation systems participating can be achieved and meet training objectives. This testing typically includes engineering support personnel, but also actual end users of the simulation systems to confirm that successful training value and mission objectives were achieved.

The typical timeline and duration of federation integration activities ranges based on the training system, its capabilities, and its training objectives. For a new platform type, with three or four training partners, an average of two to three months is required to complete the process.

Training system integration is a time intensive process that requires substantial efforts to support test plan/procedure development, test planning and coordination, test execution, problem analysis and resolution, retest, and final acceptance. In addition to the operational assessment of training capabilities, analysis and debug of problems at an engineering and protocol level is also required. This engineering level analysis can be quite time consuming and labor intensive. While this distributed I&T solution was effective for ensuring distributed I&T is conducted in a "controlled environment", support levels to meet the incoming swell of platforms identified in ACC's CAF DMO roadmap is becoming untenable using the current process.

In order to improve the efficiency of both data analysis and verification of protocol and standards level criteria, test automation tools can be introduced to identify interoperability or non-compliance issues of the training system. This capability will lead to faster problem resolution, as well as streamline the test execution steps.

Standards CERT Overview

To improve integration efficiency and expedite system verification to training timelines, ACC funded the development of a CAF DMO Standards Certification, Evaluation, and Verification Regression Tool (CERT). This tool provides both the training system providers and system integrator with an automated, objective, and repeatable analysis tool for assessment of CAF DMO standards compliance. CERT also provides a capability for real-time inter-site integration and event analysis to troubleshoot and/or monitor data compliance.

Technical Overview

The CERT tool is an interactive graphical user interface (GUI) application that currently provides real time analysis of DIS protocol data unit (PDU) information. The purpose of the tool is to verify that a training system can both generate and receive DIS/HLA compliant packet data as specified in the CAF DMO standards.

CERT is divided into two logical components (see Figure 3), the first being the network layer that receives and validates the data, and secondly an interface layer that manages the input and interaction with the user. The tool provides two modes of operation, one being a background or "passive" assessment of data that confirms data structures, integrity, and discrete field values. The second is an interactive interface that instructs the user for specific actions to initiate and execute test cases against specific platform requirements (e.g. IFF, comms).

CERT employs a data driven model that controls the evaluation and analysis of the packet data against the CAF DMO standards criteria. Each CAF DMO criteria is verified by the control of a validation test script and test case files (see Figure 4). These files use a simple xml-based format that allows a wide range of verification checks to be performed. The test scripts contain a set of test cases that drive the criteria analysis. The test cases are defined to analyze Protocol

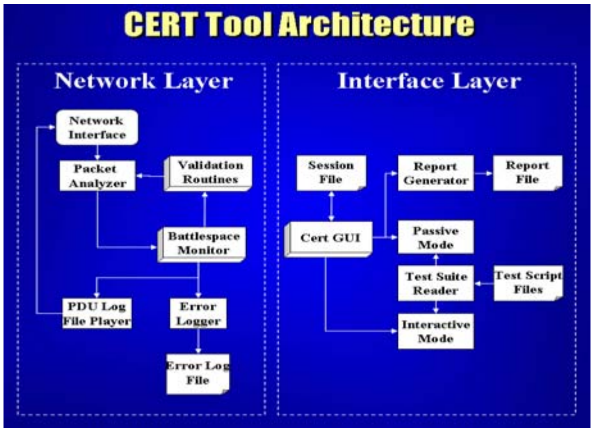
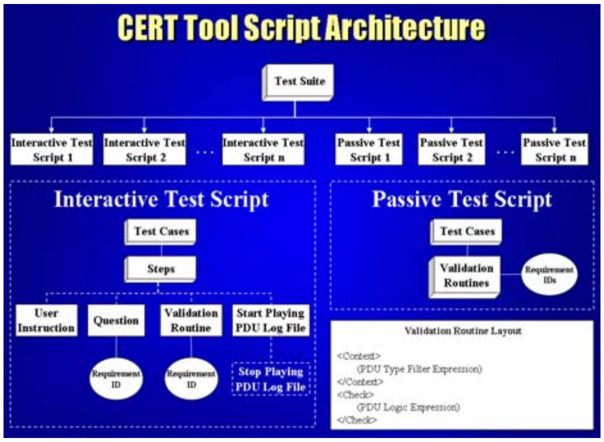


Figure 4. CERT Architecture

Data Unit (PDU) level data based on criteria specified in the standards. The test cases are fully customizable and easy-to-use for test designers, allowing them to configure the system to check any fields within any PDU. Conversely, mechanisms are also provided within a test case to generate data towards the network. A test suite is then created based on a desired test verification set and contains the requisite test scripts. The user is able to modify or create additional automated test scripts and cases to meet any verification needs their system may have beyond the standard Mission Package criteria tests delivered with CERT.



```
<Context>
    (PDU Type Filter Expression)
</Context>
<Check>
    (PDU Logic Expression)
</Check>
```

Figure 5. CERT Script Architecture

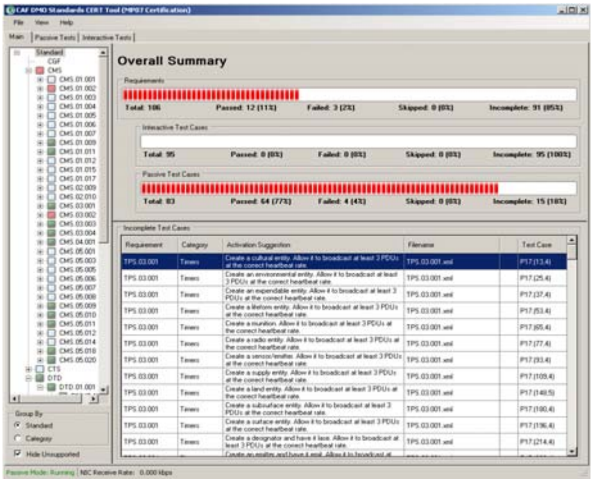
The Test Script architecture is completely separate from the network interface portion of the verification capability, thus providing an efficient and clean migration to supporting future network protocols (i.e. HLA).

Each supported Mission Package requirements set is analyzed and verified by a defined Test Suite which evaluates system compliance against criteria applicable to that platforms training requirements.

User Interfaces

The user interface for CERT is a simple design to provide easy control and display of verification status of the particular standards requirements (see Figure 5).

The initial CERT entry screen provides the means to select a Test Suite for execution, and initiate the passive or interactive mode of operation. Execution of a Test Suite is started based on creating a (or loading an existing) Session. A session is an instantiation of a test run or execution. When creating an initial session, the Test Suite is specified. As described previously, the Test Suite specifies the Requirements and related Test Cases that are available for verification. The session also caches the result data from the execution and evaluation of the test cases. This data is retained in the session file across ensuing invocations of CERT.



Overall Summary

Requirements
Total: 106 Passed: 12 (11%) Failed: 3 (2%) Skipped: 0 (0%) Incomplete: 91 (85%)

Interactive Test Cases
Total: 95 Passed: 0 (0%) Failed: 0 (0%) Skipped: 0 (0%) Incomplete: 95 (100%)

Passive Test Cases
Total: 83 Passed: 64 (77%) Failed: 4 (4%) Skipped: 0 (0%) Incomplete: 15 (18%)

Incomplete Test Cases

Requirement	Category	Activation Suggestion	Filename		Test Case
TPS.03.001	Timers	Create a cultural entity. Allow it to broadcast at least 3 PDUs at the correct heartbeat rate.	TPS.03.001.xml		P17:(13.4)
TPS.03.001	Timers	Create an environmental entity. Allow it to broadcast at least 3 PDUs at the correct heartbeat rate.	TPS.03.001.xml		P17:(25.4)
TPS.03.001	Timers	Create an expendable entity. Allow it to broadcast at least 3 PDUs at the correct heartbeat rate.	TPS.03.001.xml		P17:(37.4)
TPS.03.001	Timers	Create a lifeform entity. Allow it to broadcast at least 3 PDUs at the correct heartbeat rate.	TPS.03.001.xml		P17:(53.4)
TPS.03.001	Timers	Create a munition. Allow it to broadcast at least 3 PDUs at the correct heartbeat rate.	TPS.03.001.xml		P17:(65.4)
TPS.03.001	Timers	Create a radio entity. Allow it to broadcast at least 3 PDUs at the correct heartbeat rate.	TPS.03.001.xml		P17:(77.4)
TPS.03.001	Timers	Create a sensor/emitter. Allow it to broadcast at least 3 PDUs at the correct heartbeat rate.	TPS.03.001.xml		P17:(93.4)
TPS.03.001	Timers	Create a supply entity. Allow it to broadcast at least 3 PDUs at the correct heartbeat rate.	TPS.03.001.xml		P17:(109.4)
TPS.03.001	Timers	Create a land entity. Allow it to broadcast at least 3 PDUs at the correct heartbeat rate.	TPS.03.001.xml		P17:(148.5)
TPS.03.001	Timers	Create a subsurface entity. Allow it to broadcast at least 3 PDUs at the correct heartbeat rate.	TPS.03.001.xml		P17:(180.4)
TPS.03.001	Timers	Create a surface entity. Allow it to broadcast at least 3 PDUs at the correct heartbeat rate.	TPS.03.001.xml		P17:(196.4)
TPS.03.001	Timers	Create a designator and have it lase. Allow it to broadcast at least 3 PDUs at the correct heartbeat rate.	TPS.03.001.xml		P17:(214.4)

Passive Mode: Running | NIC Receive Rate: 0.000 kbps

Figure 6. CERT Operations View

Operating Modes

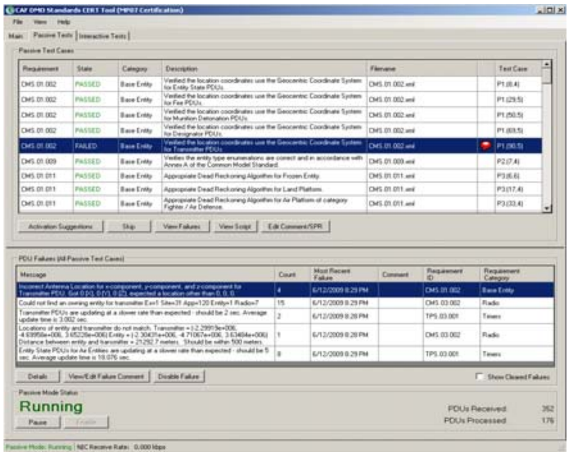
The CERT system uses the Test Suite to provide the user with an overview of all requirements that are covered by that suite, and provide mechanisms to test local systems on the network against those requirements. These mechanisms include a Passive Mode of operation, which requires no user input, and an Interactive Mode which walks users through a series of steps. For either mode, the user configures the network interface (User Datagram Protocol (UDP) Internet Protocol (IP) address, port number, etc) data via Network Configuration selection within CERT.

Both Passive Mode and Interactive Mode run a series of Test Cases defined in the Test Script files.

Interactive and Passive Test Cases use very similar methods of analyzing PDU data. Each Test Case has one or more Validation Routines, which is simply an 'if/elseif/else' block of code with failure messages to be reported when certain conditions are detected. The conditions for reporting failures are expressions that evaluate the content of a PDU. The references to the PDU data are generic in format, and are not explicit to a particular network protocol. This will allow test cases to be reused regardless of the particular network protocol being used.

Passive Mode

When running in Passive Mode (see Figure 6), the system requires no user interaction. It simply observes the traffic on the network and analyzes the contents of the PDUs that it receives. The PDU is passed through the Validation Routines defined and if any failures are encountered, they are sent to the reporting system. The failure messages are stored for later reporting and also presented to the user in real-time.



Requirement	State	Category	Description	Filename		Test Case
CMS.01.002	PASSED	Base Entity	Verified the location coordinates use the Geocentric Coordinate System for Entity State PDUs.	CMS.01.002.xml		P1.(8.4)
CMS.01.002	PASSED	Base Entity	Verified the location coordinates use the Geocentric Coordinate System for Fire PDUs.	CMS.01.002.xml		P1.(29.5)
CMS.01.002	PASSED	Base Entity	Verified the location coordinates use the Geocentric Coordinate System for Munition Detonation PDUs.	CMS.01.002.xml		P1.(50.5)
CMS.01.002	PASSED	Base Entity	Verified the location coordinates use the Geocentric Coordinate System for Designator PDUs.	CMS.01.002.xml		P1.(69.5)
CMS.01.002	FAILED	Base Entity	Verified the location coordinates use the Geocentric Coordinate System for Transmitter PDUs.	CMS.01.002.xml	●	P1.(90.5)
CMS.01.009	PASSED	Base Entity	Verifies the entity type enumerations are correct and in accordance with Annex A of the Common Model Standard.	CMS.01.009.xml		P2.(7.4)
CMS.01.011	PASSED	Base Entity	Appropriate Dead Reckoning Algorithm for Frozen Entity.	CMS.01.011.xml		P3.(6.6)
CMS.01.011	PASSED	Base Entity	Appropriate Dead Reckoning Algorithm for Land Platform.	CMS.01.011.xml		P3.(17.4)
CMS.01.011	PASSED	Base Entity	Appropriate Dead Reckoning Algorithm for Air Platform of category Fighter / Air Defense.	CMS.01.011.xml		P3.(33.4)

Message	Count	Most Recent Failure	Comment	Requirement ID	Requirement Category
Incorrect Antenna Location for x-component, y-component, and z-component for Transmitter PDU. Got 0.0(X), 0.0(Y), 0.0(Z), expected a location other than 0, 0, 0.	4	6/12/2009 8:29 PM		CMS.01.002	Base Entity
Could not find an owning entity for transmitter Ex=1 Site=31 App=120 Entity=1 Radio=7	15	6/12/2009 8:29 PM		CMS.03.002	Radio
Transmitter PDUs are updating at a slower rate than expected - should be 2 sec. Average update time is 3.002 sec.	2	6/12/2009 8:28 PM		TPS.03.001	Timers
Locations of entity and transmitter do not match. Transmitter = (-2.29915e+006, -4.63956e+006, 3.65226e+006) Entity = (-2.30431e+006, -4.71067e+006, 3.63494e+006) Distance between entity and transmitter = 21292.7 meters. Should be within 500 meters.	1	6/12/2009 8:28 PM		CMS.03.002	Radio
Entity State PDUs for Air Entities are updating at a slower rate than expected - should be 5 sec. Average update time is 19.076 sec.	8	6/12/2009 8:29 PM		TPS.03.001	Timers

PDUs Received 352
PDUs Processed 176

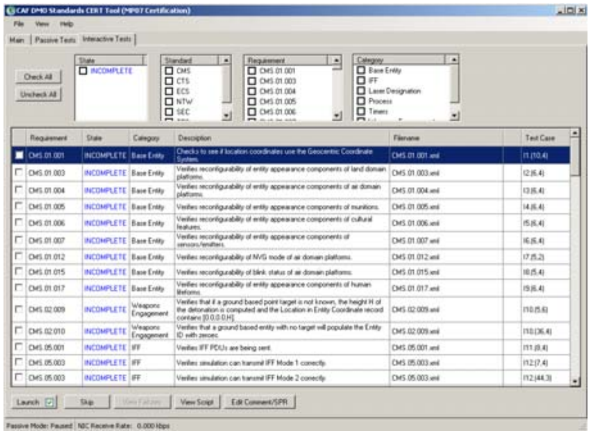
Passive Mode: Running | NIC Receive Rate: 0.000 kbps

Figure 7. CERT: Passive Mode

All PDUs detected on the selected network interface are evaluated against the Test Case criteria while operating in Passive Mode.

Interactive Mode

When running in Interactive Mode (see Figure 7), a Test Script contains a series of interactive test cases. CERT presents each Test Case with summary information including a description and a list of the relevant requirements. It then walks the user through various test steps in a wizard-like fashion. Following execution of the tests steps, a summary display is provided including a list of any validation failures that occurred.



State: □ INCOMPLETE
Standard: □ CMS □ CTS □ ECS □ NTW □ SEC
Requirement: □ CMS.01.001 □ CMS.01.003 □ CMS.01.004 □ CMS.01.005 □ CMS.01.006
Category: □ Base Entity □ IFF □ Laser Designation □ Process □ Timers

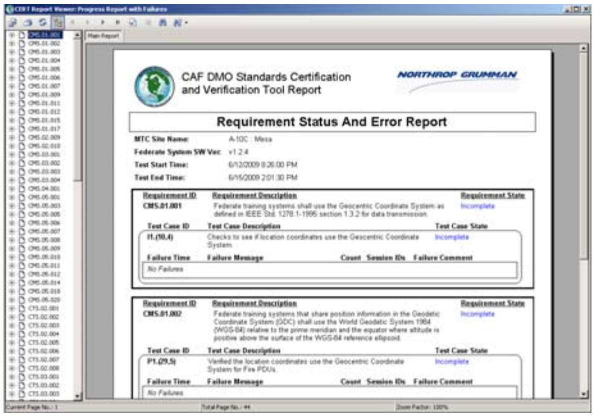
	Requirement	State	Category	Description	Filename		Test Case
■	CMS.01.001	INCOMPLETE	Base Entity	Checks to see if location coordinates use the Geocentric Coordinate System.	CMS.01.001.xml		I1.(10.4)
□	CMS.01.003	INCOMPLETE	Base Entity	Verifies reconfigurability of entity appearance components of land domain platforms.	CMS.01.003.xml		I2.(6.4)
□	CMS.01.004	INCOMPLETE	Base Entity	Verifies reconfigurability of entity appearance components of air domain platforms.	CMS.01.004.xml		I3.(6.4)
□	CMS.01.005	INCOMPLETE	Base Entity	Verifies reconfigurability of entity appearance components of munitions.	CMS.01.005.xml		I4.(6.4)
□	CMS.01.006	INCOMPLETE	Base Entity	Verifies reconfigurability of entity appearance components of cultural features.	CMS.01.006.xml		I5.(6.4)
□	CMS.01.007	INCOMPLETE	Base Entity	Verifies reconfigurability of entity appearance components of sensors/emitters.	CMS.01.007.xml		I6.(6.4)
□	CMS.01.012	INCOMPLETE	Base Entity	Verifies reconfigurability of NVG mode of air domain platforms.	CMS.01.012.xml		I7.(5.2)
□	CMS.01.015	INCOMPLETE	Base Entity	Verifies reconfigurability of blink status of air domain platforms.	CMS.01.015.xml		I8.(5.4)
□	CMS.01.017	INCOMPLETE	Base Entity	Verifies reconfigurability of entity appearance components of human lifeforms.	CMS.01.017.xml		I9.(6.4)
□	CMS.02.009	INCOMPLETE	Weapons Engagement	Verifies that if a ground based point target is not known, the height H of the detonation is computed and the Location in Entity Coordinate record contains [0.0,0.0,H].	CMS.02.009.xml		I10.(5.6)
□	CMS.02.010	INCOMPLETE	Weapons Engagement	Verifies that a ground based entity with no target will populate the Entity ID with zeroes.	CMS.02.009.xml		I10.(36.4)
□	CMS.05.001	INCOMPLETE	IFF	Verifies IFF PDUs are being sent.	CMS.05.001.xml		I11.(8.4)
□	CMS.05.003	INCOMPLETE	IFF	Verifies simulation can transmit IFF Mode 1 correctly.	CMS.05.003.xml		I12.(7.4)
□	CMS.05.003	INCOMPLETE	IFF	Verifies simulation can transmit IFF Mode 2 correctly.	CMS.05.003.xml		I12.(44.3)

Passive Mode: Paused | NIC Receive Rate: 0.000 kbps

Figure 8. CERT: Interactive Mode

Reporting System

The results of running Test Cases in any of the provided testing modes are logged in a built-in reporting system (see Figure 8). At any time, the user may review validation status of any requirement and view any outstanding test failures. The reporting system also provides a means to export all test session information in a final report that can be deliverd to the CAF DMO Standards Certification Authority for approval.



CMS.01.001
CMS.01.002
CMS.01.003
CMS.01.004
CMS.01.005
CMS.01.006
CMS.01.007
CMS.01.009
CMS.01.011
CMS.01.012
CMS.01.015
CMS.01.017
CMS.02.009
CMS.02.010
CMS.03.001
CMS.03.002
CMS.03.003
CMS.03.004
CMS.04.001
CMS.05.001
CMS.05.003
CMS.05.005
CMS.05.006
CMS.05.007
CMS.05.008
CMS.05.009
CMS.05.010
CMS.05.011
CMS.05.012
CMS.05.014
CMS.05.018
CMS.05.020
CTS.02.001
CTS.02.002
CTS.02.003
CTS.02.004
CTS.02.005
CTS.02.006
CTS.02.007
CTS.02.008
CTS.03.001
CTS.03.002
CTS.03.003

CAF DMO Standards Certification
and Verification Tool Report

Requirement Status And Error Report

MTC Site Name: A-10C : Mesa
Federate System SW Ver: v1.2.4
Test Start Time: 6/12/2009 8:26:00 PM
Test End Time: 6/15/2009 2:01:30 PM

Requirement ID	Requirement Description	Requirement State
CMS.01.001	Federate training systems shall use the Geocentric Coordinate System as defined in IEEE Std. 1278.1-1995 section 1.3.2 for data transmission.	Incomplete

Test Case ID	Test Case Description	Test Case State
I1.(10.4)	Checks to see if location coordinates use the Geocentric Coordinate System.	Incomplete

Failure Time	Failure Message	Count	Session IDs	Failure Comment
No Failures				

Requirement ID	Requirement Description	Requirement State
CMS.01.002	Federate training systems that share position information in the Geodetic Coordinate System (GDC) shall use the World Geodetic System 1984 (WGS-84) relative to the prime meridian and the equator where altitude is positive above the surface of the WGS-84 reference ellipsoid.	Incomplete

Test Case ID	Test Case Description	Test Case State
P1.(29.5)	Verified the location coordinates use the Geocentric Coordinate System for Fire PDUs.	Incomplete

Failure Time	Failure Message	Count	Session IDs	Failure Comment
No Failures				

Current Page No.: 1 | Total Page No.: 44 | Zoom Factor: 100%

Figure 9. CERT System Compliance Report

Troubleshooting and Debugging

In both passive and interactive modes, CERT identifies and presents to the user standards non-compliances ("failures") detected. These failures are identified against the specific standards criteria being evaluated. The user is presented with a detailed description of the failure, including expected data and received data. The DIS PDU captured that did not meet the standards criteria is displayed and can be interrogated.

Additionally, all CAF DMO Standards documents are delivered as part of the CERT package and accessible via CERT, so the user can quickly compare the test result data with the explicit criteria description in the standard. This allows efficient analysis of the failure condition reported, and aids in problem resolution for the user.

CERT Benefits

CERT is designed to reduce the time, cost, and effort required for training systems to obtain approval to train on the CAF DMO Network. A summary of the benefits the CERT provides include:

- Provides an objective verification reference for all training systems.
- Reduces integration cost of system-wide upgrades.
- Simplifies process for training system verification.
- Expedites system integration timeline for DMON training.
- Identifies unexpected MTC configuration or interface changes.
- Supports regression testing of current and previous CAF DMO standards criteria.
- Supports evaluation of joint service systems/models.
- Mitigates the need for security accreditation prior to system verification.

CERT Capabilities

CERT replaces a variety of test verification methods that typically would require manual inspection, analysis, and confirmation of data to ensure conformance to the CAF DMO interoperability standards. CERT capabilities are as follows:

- Provides automated analysis of DIS 1278 PDU level data.
- Supports interactive sequencing of complex test/verification scenarios.
- Provides standardized and repeatable test verification across all training systems.
- Supports all CAF DMO requirements.
- Operates with both unclassified and secure systems.
- Supports test execution across multiple sessions and systems/sites.
- Generates detailed reports specifying the exact non-compliant data.
- Facilitates System Problem Report (SPR) tracking and closure.

CERT Tool Applicability

CERT is readily expandable to provide support for a variety of functional areas. The CERT also facilitates the automated assessment of CAF DMO systems requirements against other service solutions (e.g. Army, Navy, NATO) without the cost, security, and political constraints that typically deter this type of evaluation. This ease of assessment may promote a greater willingness to pursue joint and coalition training opportunities. The CERT can seamlessly be integrated into a variety of other training processes to include:

- Pre-training configuration analysis for training mission setup.
- Real time notification of non-compliance during training events.
- Integration of error detection into the CAF DMO System Problem Reporting
- Enhanced analysis and verification of additional IEEE 1278 specified standards data.
- New user protocols and interfaces (e.g. HLA, TENA).

Conclusion

The CERT is currently available for download by all CAF DMO stakeholders in support of CAF DMO training system certification. It is also being utilized to evaluate other service systems (ex AVCATT, JLVC Federates) for compatibility with CAF DMO training platforms. CERT findings provide a clear entry point for collaboratively negotiating inter-service training solutions. To date, use of this standards compliance tool has greatly simplified our intra and inter-service integration efforts and ultimately contributes to providing solutions to the warfighter in a more timely fashion.

REFERENCES

M. Aldinger, S. Keen, NATO Modeling & Simulation Group Symposium (2007). CAF DMO Standards-Based Approach for Achieving M&S Interoperability. Pages 2-7.