DEFENSE INFORMATION SYSTEMS AGENCY

JOINT INTEROPERABILITY TEST COMMAND
FORT HUACHUCA, ARIZONA

COMBINED INTEROPERABILITY TEST PLAN (CITP) FOR TACTICAL DATA LINKS (TDL) AND UNITED STATES MESSAGE TEXT FORMAT (USMTF)

JITC PLAN 3014

April 2007

COMBINED INTEROPERABILITY
TEST PLAN

April 2007

Submitted by: **Byron Baker**
                          Chief
                          Tactical Data Link Branch

                              //signed//

Approved by: _____
                          Timothy Albers, LTC
                          Portfolio Chief
                          Force Application/Force Protection

Prepared by

Joint Interoperability Test Command
Fort Huachuca, Arizona 85613-7051

(This page intentionally left blank.)

EXECUTIVE SUMMARY

United States Pacific Command (USPACOM) requested a standing document to provide guidance for interoperability testing of Pacific Command (PACOM) Area of Responsibility (AOR) partner countries systems. This document is the overarching testing guidance for Joint Interoperability Test Command (JITC) and partner countries with system(s) under test (SUT) for tactical data links (TDL) to include Link 11, Link 11B, Link 16, and Variable Message Format (VMF), as well as United States Message Text Format (USMTF).

The goal of this document is to provide basic guidance for planning, scheduling, testing, and post test requirements. Additionally, it provides information regarding the scope of testing, limitations and methodology of testing.

Once a test is scheduled for a foreign system, JITC will provide in-depth test procedures for the system to be tested in accordance with JITC policies and procedures.

(This page intentionally left blank.)

TABLE OF CONTENTS

APPENDICES

LIST OF ENCLOSURES

LIST OF FIGURES

LIST OF TABLES

(This page intentionally left blank.)

TEST BACKGROUND

Tactical Data Link (TDL) Combined Interoperability Testing (CIT) is required IAW United States Pacific Command's (USPACOM's) Combined Communications Interoperability Program (CCIP) and applicable bilateral Memorandum of Agreements (MOAs) with combined nations. The JITC is the designated interoperability test agency for the Defense Information Systems Agency (DISA) and has been providing the testing for TDL and United States Message Text Formatting (USMTF) systems. TDL consists of Link 11, Link 11B, Link 16, and Variable Message Format (VMF). TDLs and USMTF are further described in appendix E.

TEST PURPOSE

The U.S. joint interoperability programs provide the basis for U.S. initiatives toward achieving combined interoperability with allied and friendly nations. Testing TDL systems and USMTF information exchange in a combined environment provides relevant, statistical information regarding interoperability with the participating nations. Some interoperability testing will be required in an operational environment to validate the level of interoperability with the operators and equipment in place.

REQUIREMENTS

JITC will promulgate available test windows approximately 18 months in advance. Combined partners operating with PACOM in the CCIP who wish to participate in a TDL CIT will nominate a system for test at the appropriate Command and Control Interoperability Board (CCIB) or Interoperability Management Board (IMB). PACOM J61 will establish a test priority and request JITC conduct the test.

Combined partners will only nominate systems that have been evaluated for standards conformance for the appropriate interface. JITC may waive this requirement in the rare instance that it could benefit the test but only with the approval of all test participants.

The country scheduled for testing will provide a system implementation document indicating message implementation down to the field level and a system description document if available, no later than six months prior to the test date. In addition they will provide the software version numbers for each application involved in the test.

JITC will ask each United States (U.S.) Service and Agency (S/A) to provide a tactical data system (TDS) to participate in each TDL CIT. JITC will attempt to have at least one moving TDS present during all TDL CITs in order to test the exchange of positional data.

JITC will staff a yearly Memorandum of Agreement (MOA) between scheduled U.S. Forces, JITC and applicable combatant commanders (COCOMs). This MOA replaces the System Security Verification (SSV) document. It is implied that COCOMs maintain valid Communication Information System Memorandum of Agreements (CISMOAs)/MOAs between the host country and PACOM and those documents define

the requirements to safeguard tactical data exchange between the host country and U.S. Forces.

SCOPE

Link 11/11B/Link 16

For Link 11 and Link 16 testing, the JITC's Joint Tactical Data Link Laboratory (JTDLL) uses the Joint Interoperability Modular Evaluation System (JIMES), Multi-link System Test and Training Tool (MLST3), and the Dual Link System (DLS) or a Battlefield Operations Simulation System (BOSS) to conduct the TDL CIT. The JIMES connects with U.S. S/As' TDSs located at Operational Facilities (OPFACs) throughout the Continental United States (CONUS). Systems not located at one of the OPFACs may be connected through a dial-up phone line. In addition to test tools, JITC has the ability to provide a Joint Air Defense Systems Integrator (JADSI) as an operational system for the test. The JIMES contains the hardware and software necessary to conduct and evaluate test operations. Sensor stimulators are used to generate sensor inputs to S/A systems within CONUS when required.

The distributed sites involved in testing are linked together by secure voice and encrypted digital data links. The SUT will be linked to the secure voice via Secure Telephone Unit (STU)-IIIs or the new generation of Secure Telephone Equipment (STE).

An overview configuration for Link 11/16 testing is shown in appendix D, figure D1.

VMF

JITC uses various test collection and analysis equipment, including but not limited to the Army's VMF Test Tool (VTT), JITC's VMF Link Processor and Bit Oriented Module Editor (JVLP/BOM), the Army's Common Message Processor (CMP), JITC's JIMES, and the Theater Air Missile Defense Interoperability Assessment Capability (TIAC) suite of tools as part of JITC's Net-Centric Enterprise Services (NCES) lab.

For testing specific to VMF capable systems, JITC requires the systems' implementation down to the data item level as specified in the Variable Message Format Master Test Procedure. For interoperability testing of VMF capable systems, JITC requires the system requirements in order to develop in order to develop operationally relevant test scenarios.

USMTF

There are no current requirements to conduct USMTF Combined Interoperability Test (CIT) events. When this type of testing is required, it is imperative that the SUT provide detailed information on their USMTF message implementation. JITC will develop test procedures and test messages based on this information and the USMTF information exchange requirements of the SUT. The information exchange requirements detail

what other systems the SUT exchanges USMTF information with, and how those messages will be exchanged.

JITC will provide test procedures and test messages to the SUT for review and to allow them to conduct their own pre-test activities. JITC will provide test messages on magnetic media or via e-mail. JITC will design the test procedures to test each USMTF message type used by the SUT, and JITC-built messages will consist of a representative sample of the segments, sets, fields, and data items implemented by the SUT. Testing will include the transmission and receipt of pre-built, manually-entered, or system-generated messages (based on system capabilities and requirements). Testers will observe, document, and analyze results of testing through the use of visual displays, graphical user interfaces (GUIs), hard copy printouts, output from system databases, or other available means. Testers will use JITC-certified USMTF test tools or message processors to determine the compliance of all USMTF test messages with Military Standard 6040, US Message Text Formatting Program.

Current USMTF interoperability testing is generally conducted on-site (either at JITC or the SUT's location) and not done via a distributed network. The methodology used for USMTF CIT testing and data collection will be based on the requirements of the SUT and the availability of resources to conduct the event.

JITC can also observe/review the results of USMTF testing activity that occurs in combined exercise events. Due to the varying nature of these events, JITC will determine data collection requirements and methods on a case by case basis.

STANDARDS CONFORMANCE TESTING

JITC can provide standards conformance testing and certification of a combined system. However, this type of event would be done on a reimbursable cost basis outside of a TDL or USMTF CIT event.

LIMITATIONS

The TDL CIT configuration is a controlled laboratory environment. Because of this, the operational realism of sensor input, operator interaction, sensor registration effects and environmental propagation are not available. In addition, emulators are used vice Link 16 terminals; therefore, most of the network management and host/terminal requirements are not evaluated.

METHODOLOGY

After scheduling a combined system for a TDL CIT, JITC will write the test procedures to support the SUT. The test procedures will detail the information and provide guidance required for the test conduct from initiation to completion and are in sufficient detail to provide each test participant with a clear understanding of the planned test activities. Test procedures are prepared by JITC and sent to the SUT test lead via PACOM J61 for their inputs prior to JITC producing the Final Test Procedures. The test

procedures specify test objectives and performance criteria and contain the individual test events that must be executed to ensure test objectives are met. Special instructions are included for clarification when necessary. At a minimum, test procedures will include:

- Identification of required resources and participants.
- Test configuration.
- Test objectives.
- Performance criteria.
- Test events - detailed procedures for test conduct.
- Analysis procedures.
- Special instructions (as required).
- Data collection, recording, and reduction requirements.
- Network designs, as required.
- Trouble Reports (TRs) declared ready for test.

If necessary, and as coordinated with the host country, JITC will conduct a site survey and a Communications Dry Run several weeks prior to the actual test to ensure connectivity and data exchange.

The TDL CIT is usually conducted in a one-week period, 8-10 hours per day, Monday through Friday in the US. This equates to a Tuesday through Saturday daytime event for the combined country. Test start times vary according to test laboratory availability. Participants and SUT will establish TDL connectivity and voice communications one hour prior to test.

The JITC Test Director (TD) controls test conduct in coordination with the test leads of participating systems. The SUT is exercised by exchanging messages based on test events and stimulated sensors to test conformance and confirming interoperability in accordance with the applicable MIL-STDs and system implementation. Neither participating systems nor their connectivity configuration shall be altered during a test without concurrence of JITC and all participating test leads.

During TDL test execution, the participants and JITC will monitor, record, and extract test data IAW the "Multi-TDL Data Extraction & Reduction Guide" (DERG) (Appendix F) to support post-test analysis. This Data Extraction (DX) is reduced and uploaded (for U.S. systems) to the JITC TDL web page on the Secret Internet Protocol Router Network (SIPRNET) on a daily basis during testing. This data is accessible to the U.S. Participants for further analysis. The SUT's DX should be reduced and uploaded via secure telephone or sent to JITC via other means (whichever is more practical) for use by the U.S. participants during post-test analysis.

All the test participants will perform on-line or real-time analysis, enabling an opportunity to determine if test events that produced questionable results should be repeated and provide a good way to document issues as they happen.

Each participant will conduct definitive analysis that addresses all functional areas exercised during testing. This includes identification of problem identification in message implementation and processing as well as problems with the standard. Any problems that occur during testing are documented as PTRs for later analysis.

As required, test participants and JITC will write Preliminary Trouble Reports (PTRs). Refer to appendices H and I for further information. JITC will consolidate the PTRs to be published as an agenda for review by the Analysis Review Panel (ARP).

At any time during test conduct, the test lead of the SUT may determine it appropriate to discontinue testing and declare a NO TEST. Normally this declaration automatically cancels the post-test analysis and the ARP for the SUT. If a NO TEST is declared, the test will continue only if there is another SUT to evaluate.

JITC convenes the ARP to review and finalize the disposition of the PTRs and determine actions to resolve those problems identified as a result of testing. The ARP will provide an interoperability recommendation based on technical and operational evaluation of the SUT's performance in the test. ARPs are generally convened approximately four to six weeks after each TDL CIT, and are normally a one (1) day event.

JITC recommends a representative from the SUT attends the ARP to participate in discussions regarding their system. Attendees should be fully knowledgeable of system functions and be ready to discuss all PTRs written against the system and interface. If a representative is unable to attend JITC, upon request, can act on their behalf if supporting documentation for the PTRs is provided. If possible a secure video or teleconference, at that country's expense, may be used in lieu of the SUT representative attending in person. ARP procedures are further described in appendix J.

JITC publishes and distributes a test report approximately four weeks after the conclusion of the ARP. The test report summarizes ARP actions and includes ARP minutes. Multi-system testing may increase the time required to publish and distribute a test report. The test report will provide an assessment of the interoperability of the combined system with U.S. systems, along with recommended modifications to improve interoperability. JITC will provide an electric copy of the test report via the SIPRNET to the USPACOM JITC Liaison Officer (LNO), who will coordinate distribution to HQ USPACOM

(This page intentionally left blank.)

APPENDIX A

ACRONYMS

ACDS	Advanced Combat Direction System
ACT SYS	Action System
AF	Air Force
AFB	Air Force Base
AMCOM	Air and Missile Command
AOR	Area of Responsibility
ARP	Analysis Review Panel
ATDS	Air Tactical Data System
AWACS	Airborne Warning and Control System
BPS	bits per second
BOSS	Battlefield Operations Simulation System
CIP	Combined Interoperability Plan
CISMOA	Communication Information System Memorandum of Agreement
C/S/A	Combatant Commander/Services/Agencies
C2	Command and Control
CCB	Configuration Control Board
CCIB	C2 Interoperability Board
CECOM	Communications and Electronics Command
CIT	Combined Interoperability Test
CITP	Combined Interoperability Test Plan
CLEW	Conventional Link 11 Waveform
CMP	Common Message Processor
COCOM	Combatant Commander
COM	character-oriented message
CONUS	Continental United States
CTL NO	Control Number
DAA	Designated Approving Authority
DERG	Multi-TDL Data Extraction and Reduction Guide
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DISR	DoD IT Standards Registry
DLS	Dual Link System

DNCS	Data Net Control Station
DoD	Department of Defense
DTS	Data Terminal Sets
DX	Data Extraction

| EDAC | Error Detection and Correction |

| FFIRN/FUDN | Field Format Index Reference Number/Field Use Designator Number |
| FH | Fort Huachuca |

| GMT | Greenwich Mean Time |

| HF | High Frequency |

IAW	in accordance with
ICP	Interface Change Proposal
IDH	Implementation Design Handbook
IMB	Interoperability Management Board
IT	Information Technology
ITP	Interoperability Test

JADSI	Joint Air Defense Systems Integrator
JIEO	Joint Information and Engineering Organization
JIMES	Joint Interoperability Modular Evaluation System
JITC	Joint Interoperability Test Command
JMAL	Joint Message Analysis Laboratory
JTDLL	Joint Tactical Data Link Laboratory
JTIDS	Joint Tactical Information Distribution System
JTRS	Joint Tactical Radio System
JVLP/BOM	JITC's VMF Link Processor and Bit Oriented Module Editor

| LOS | Line Of Sight |

MAS	Message Analysis System
MCEB	Military Communications-Electronics Board
MIDS	Multifunctional Information Distribution System
MIL-STD	Military Standard
MLST3	Multi-link System Test and Training Tool
MOA	Memorandum of Agreement

MSGID	Message Identity
MTF	Message Text Formatting
NCES	Net-Centric Enterprise Services
NCTSI	Navy Center for Tactical Systems Interoperability
N-MLST3	Navy-MLST3
NR-KPP	Net-Ready Key Performance Parameter
NSA	National Security Agency
OPFAC	Operational Facilities
OPR	Office of Primary Responsibility
ORIG NO	Originator Number
PCSAIMP	Personal Computer for Service and Agency Implementation
PTR	Preliminary Trouble Report
PTUC	Primary Test Unit Coordinator
PU	Participating Unit
R2	Reporting Responsibility
S/A	Services and Agencies
SATCOM	satellite communications
SCT	Standards Conformance Test
SIPRNET	Secret Internet Protocol Router Network
SIS(RJ)	Special Information Systems (Rivet Joint)
SLEW	Single-tone Link 11 Waveform
SSV	System Security Verification
STE	Secure Telephone Equipment
STU	Secure Telephone Unit
SUT	System Under Test or Systems Under Test
TD	Test Director
TDL	Tactical Data Link
TDMA	Time Division Multiple Access
TDS	Tactical Data System
TIAC	Theater Air Missile Defense Interoperability Assessment Capability
TR	Trouble Report
TV	Technical View

UHF	Ultra High Frequency
U.S.	United States
USA	United States Army
USAF	United States Air Force
USCOCOM	United States Combatant Commander
USEUCOM	United States European Command
USMC	United States Marine Corps
USMTF	United States Message Text Format
USN	United States Navy
USPACOM	United States Pacific Command
VMF	Variable Message Format
VTT	VMF Test Tool

APPENDIX B

TEST SCHEDULES AND MILESTONES

The test windows for TDL CITs are determined approximately 18 months in advance based on laboratory and systems availability to support testing. JITC schedules 4-5 TDL CITs per year and countries should make recommendations for systems for test at least 12 months prior to the desired test date. A sample timeline of milestones in a TDL test cycle are listed below:

TIMELINE	MILESTONE
PRIOR TO TEST	
24 WEEKS	SUT IMPLEMENTATION DATA RECEIVED AT JITC
14 WEEKS	SUT SITE SURVEY (time may vary)
23-8 WEEKS	DRAFT TEST PROCEDURE DEVELOPED
7-5 WEEKS	SUT REVIEW OF DRAFT TEST PROCEDURE, COMMENTS TO JITC
4 WEEKS	SUT COMMENTS INCORPORATED
2 WEEKS	FINAL TEST PROCEDURES DISTRIBUTED
1 WEEK	PRE-TEST BRIEF CONDUCTED
TEST WEEK	TEST CONDUCT (data extraction (DX) loaded to JITC TDL web site daily by U.S. participants)
POST TEST	
1-6 WEEKS	POST-TEST ANALYSIS (PTRs written by all participants)
7 WEEKS	PTRS PROVIDED TO JITC (All analyze their PTRs. JITC consolidates PTRs into an ARP agenda)
8 WEEKS	ARP CONDUCTED
10 WEEKS	TEST REPORT DEVELOPED
12 WEEKS	TEST REPORT ISSUED

(This page intentionally left blank.)

APPENDIX C

TEST REPORT FORMAT

JITC will develop a test report for each CIT event, providing an overview of the test objectives, test configuration, overall execution of the event, and a summary of any issues found during testing. The CIT Test Report will be provided to PACOM J61, who will review the report and forward a copy to the appropriate combined country representative. Due to the discussion of problems found during testing, the test report is normally classified CONFIDENTIAL.

A TDL CIT Test Report normally includes the following sections:

- Executive Summary
- System Functional Description
- Test Background
- Test Purpose
- Scope and Methodology
- Limitations
- Problem Identification Procedure
- Results and Analysis
- Recommendation

The report will also include the following appendices:

- Acronyms
- Test Criteria and Procedures
- Network Description and Configurations
- Trouble Report Classes and Prefix Designations
- Trouble Report Assessment Definitions
- References
- Assigned Trouble Reports

A sample, unclassified TDL CIT Test Report is available for review upon request.

The TDL CIT Test Report will include a summary of all new and existing TRs for the SUT. Table C-1 is a sample TR Summary table.

Table C-1: Sample TR Summary Table

SYSTEM NAME

IMPLEMENTED FUNCTIONAL AREAS	TDL CIT XX-YY TRs			TOTAL OPEN TRs		
	MINOR	MODERATE	CRITICAL	MINOR	MODERATE	CRITICAL
System Information Exchange						
Air Surveillance	1			2		
Surface Surveillance						1
Subsurface Surveillance						
Control						
Amplification/Threat Warning						
Weapon Coordination and Management						
Information Management	1			1		
Land Surveillance						
Space Surveillance	1			1		
Reference/Emergency Points						
Electronic Warfare Surveillance						
Other *						
Total	**3**			**4**		**1**

*NOTE: Includes implementation documentation and other TRs of a general nature that do not fall into a particular functional area.
LEGEND:
TDL - Tactical Data Link
CIT - Combined Interoperability Test   TR - Trouble Report

The TDL CIT Test Report will also include a table listing the system implemented functional areas and the corresponding test results from the CIT. Table C-2 is a sample functional area status table.

Table C-2: Sample Functional Area Status Table

INFORMATION EXCHANGE METHOD	IMPLEMENTED FUNCTIONAL AREA	STATUS
Link 16 (MIL-STD-6016C)	System Information	Met, PARTIALLY MET, or Not Met
	Air Surveillance	
	Surface Surveillance	
	Subsurface Surveillance	
	Air Control	
	Weapon Control	
	Information Management	
	Electronic Warfare/Intelligence	

LEGEND:
MIL-STD - Military Standard

STATUS DEFINITIONS:
MET - No problems found
PARTIALLY MET - Moderate or minor problems found. Acceptable workarounds exist.
NOT MET - Critical problems founds

Although it is not a part of the TDL CIT Report, JITC uses a TDL Testing Summary Matrix to summarize the testing status for a combined country. Table C-3 is a sample matrix.

Table C-3: Sample TDL Testing Summary Matrix

System Type	# of Platforms	Interface Type	Test Number	Report Date	System Version	Test Result	Next Test Date??
Ship	4	Link 11	CIT 04-04	Jan 99	1.2.3	Complete	None
Airborne C2	4	Link 11/16	CIT 05-05	Jul 01	C3.0	10 Minor 2 Moderate	CIT 07-04
Ground C2	10	Link 11	SCT event		1.X.Y.Z	Complete	TBD
Fighter	24	Link 16	CIT 05-01	Apr 05	4.7.0.3	15 Minor 3 Moderate 2 Critical New and totals	Apr 08
Etc	5	Link 11	Live Exercise	Aug 06	ABCD	15 New Minor 30 Total Minor	Aug 09

APPENDIX D

CONFIGURATION DIAGRAMS

JITC will develop configuration diagrams for each TDL CIT event.

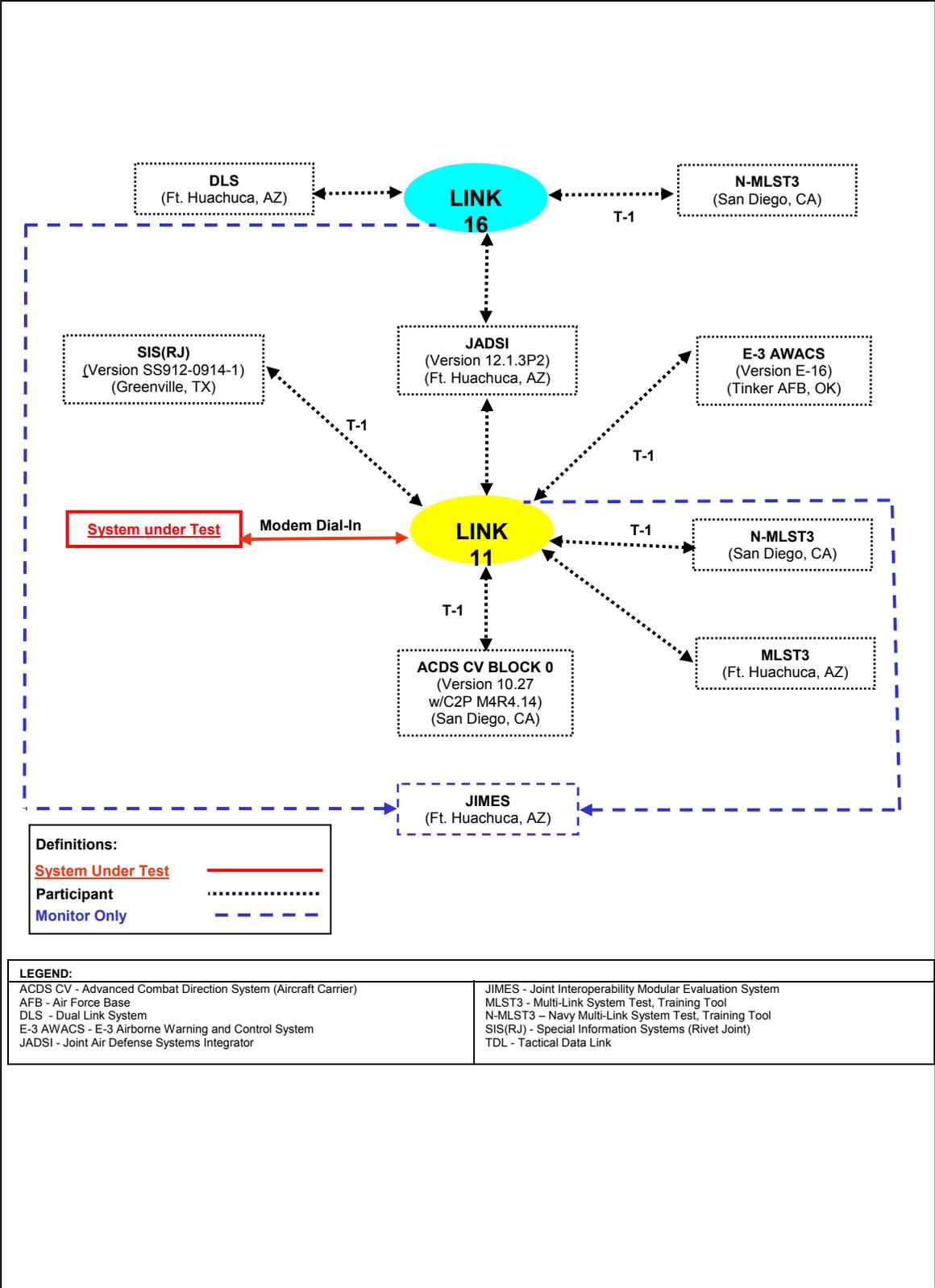Figure D-1 is a sample configuration diagram for a Link 11 and Link 16 TDL CIT event.

Figure D1. Representative Link Configuration For Link 11/Link 16 System Under Test

APPENDIX E

DATA LINK DESCRIPTION

Tactical Data Link (TDL)

A Joint Staff – approved, standardized communication link suitable for transmission of digital information. Tactical digital information links interface two or more C2 or weapons systems via a single or multiple network architecture and multiple communication media for exchange of tactical information

Link 11

Link 11 is a half-duplex, netted link that normally operates by roll call from a Data Net Control Station (DNCS). Link 11 can also operate in the broadcast mode. The roll call mode of operation used in the Link 11 interface requires that each Participating Unit (PU) respond in turn while all other stations are receiving. A DNCS initiates the roll call by addressing and transmitting an interrogation message to a specific PU that then responds by transmitting its data. The DNCS then interrogates the next PU in the prescribed roll call. Link 11 can be transmitted on High Frequency (HF) and/or Ultra High Frequency (UHF) bands. Data speed can be selected from bit rates of 2250 or 1364 bits per second (bps). Dual sideband diversity operation and Doppler shift correction features improve reliability and accuracy of data exchange. Link 11 operates on HF (2-30 MHz) and/or UHF (Line Of Sight (LOS)) (225-400 MHz). Some Data Terminal Sets (DTS) provide the option to select either the Conventional Link 11 Waveform (CLEW) or the Single tone Link 11 Waveform (SLEW). SLEW and CLEW are not compatible waveforms. SLEW, among other enhancements, provides increased propagation and a more powerful Error Detection and Correction (EDAC) algorithm. While the option exists to operate in either CLEW or SLEW, all participants in a given Link 11 net must select the same waveform to achieve connectivity between units. Link 11 is defined in Military Standard (MIL STD) 6011, Tactical Data Link (TDL) A/B Message Standard.

Link 11B

Link 11B is a full duplex, point-to-point link that operates with continuous transmissions. Link 11B can be transmitted over a variety of media, such as cable, satellite communications (SATCOM), and single or multi-channel radio links. Data are transmitted in a serial mode at the basic rate of 1200 bps with optional capabilities of 600, 2400, 4800 and 9600 bps (as available in some systems). Link 11B is defined in MIL-STD-6011, Tactical Data Link (TDL) A/B Message Standard.

Link 16

Link 16 is a secure, high-capacity, jam-resistant, nodeless data link which uses the Joint Tactical Information Distribution System (JTIDS) or Multifunctional Information Distribution System (MIDS) transmission characteristics and the protocols, conventions, and fixed-length message formats. Link 16 provides for the real/near-real-time exchange of air, space, surface, subsurface, land tracks as well as orders and commands among participating units. Link 16 uses the principle of Time Division Multiple Access (TDMA), an architecture that employs time slot interleaving to provide multiple, simultaneous communications nets. Link 16 is defined in MIL-STD-61016, Tactical Data Link (TDL) J Message Standard.

Variable Message Format (VMF)

VMF is the DoD mandated standard for fire support information digital entry device exchange over tactical broadcast communications systems. The use of VMF has been extended to all war fighting functional areas. VMF messages shall be used for information transfer between systems in communications bandwidth constrained environments. VMF is a message format designed to support the exchange of digital data between combat units with diverse needs for volume and detail of information using various communication media. This flexibility is achieved through the information variability of each message and by use of message standards that are independent of the textual format of the message. Individual messages composed of data elements are adjusted in length to suit the information content of that particular message. Although bit-oriented, VMF can also accommodate character-oriented message (COM) encoding. VMF is the primary messaging component of Army and Marine Corps Battlefield Digitization initiatives. VMF is defined in MIL-STD-6017, Interface Standard Variable Message Format.

United States Message Text Format (USMTF)

The USMTF Program is a set of character-oriented message text formats used in support of Command and Control (C2) systems for the exchange of information. The objectives of the USMTF Program are to:

  • Produce messages that are both machine processed and human readable.
  • Reduce the time and effort required drafting, transmitting, analyzing, interpreting, and processing messages.
  • Improve information exchange through vocabulary control.
  • Provide uniform reporting procedures to be used in all defense conditions from peacetime through crises, war, and post-attack.
  • Facilitate exchange of information between the United States (U.S.) and allied commands and reduce or eliminate dual reporting by U.S. units when they operate with allied commands or units or after their change of operational control to allied nations or organizations.

USMTF message processing systems are systems that can:

• Automatically parse information from incoming messages, and with little or no human intervention, update a C2 system database or display.
• Automatically query the C2 system database to generate, with or without human intervention, valid USMTF messages for transmission.
• Validate USMTF messages in accordance with (IAW) the current USMTF standard.

USMTF is defined in MIL-STD-6040, U.S. Message Text Formatting Program.

(This page intentionally left blank.)

APPENDIX F

REFERENCES

Military Standard 6011 (MIL-STD-6011) "Tactical Data Link (TDL) A/B Message Standard," current version

Military Standard 6016 (MIL-STD-6016) "Tactical Data Link (TDL) J Message Standard," current version

Military Standard 6017 (MIL-STD 6017) "Interface Standard Variable Message Format (VMF)" current version

Military Standard 6040 (MIL-STD-6040), "U.S. Message Text Formatting Program," current version

Defense Information Systems Agency, Standards Management Branch (DISA/GE332) "Multi-TDL Data Extraction and Reduction Guide," current version

JIEO Circular 3010, "Procedural Interface Standards Security Classification Guide," current version

U.S. Pacific Command Combined Interoperability Program Plan, 9 June 1995

U.S. Pacific Command Combined Interoperability Program Management Plan, 9 June 1995

U.S. Pacific Command/Combined Country Sample Memorandum of Agreement

(This page intentionally left blank.)

APPENDIX G

PRELIMINARY TROUBLE REPORTS

Preliminary Trouble Reports (PTRs) document problems pertaining to the MIL-STD, system implementation, system hardware, software, test design, doctrine, etc. They are also used to document reference publication errors, test inconsistencies, and unexecuted or improperly executed test events. All problems discovered during and after testing are reported to JITC in the form of PTRs (appendix H for TDL and appendix I for USMTF). PTRs are also used to recommend modification or closure of open TRs.

Any participant and JITC may submit PTRs. Problems should be stated as clearly and as fully as possible, supported by applicable DX and MIL-STD references. The U.S. originator assigns a security classification, based on content, IAW Joint Information and Engineering Organization (JIEO) Circular 3010, "Procedural Interface Standards Security Classification Guide" (appendix F). Foreign countries will assign a security classification IAW national doctrine. Each originator also assigns their own unique four-character originator number to each submitted PTR according to the number assignments specified in appendix H (TDL) and appendix I (USMTF).

All PTRs must be submitted to JITC. TDL PTRs from U.S. participants will be uploaded to the JITC TDL web site on the SIPRNET. USMTF PTRs from U.S. participants may be sent via Internet e-mail to the address provided in the test procedure.

The JITC TD will provide a specific date on which all PTRs must be submitted, normally allowing fifteen working days after test completion to conduct analysis. Test analysts then have approximately one week to review all submitted PTRs prior to the ARP.

Upon receipt, JITC control numbers are assigned to all PTRs. Numbering begins at 001 for each test and continues sequentially. Multiple PTRs documenting the same problem are consolidated by JITC during preparation of the ARP agenda. All PTRs are evaluated at the next scheduled ARP. During the ARP, PTRs can be validated, withdrawn by the originator, or voted invalid. If the problem is valid, an Office of Primary Responsibility (OPR) is assigned and the PTR is given a seven-character TR number as specified below.

The participants determine whether a PTR has documented a system anomaly that exhibits or has the potential for significant adverse impact to the combined network or to a particular system. This can be identified during PTR generation or during PTR discussion at the ARP. An operational impact statement is written to document the specific consequences and is added to the assigned TR by the ARP prior to validation. Any one or a combination of participant subject matter experts may provide the impact statement. If the ARP participants cannot agree on the specific wording for a single impact statement, multiple impact statements may be written for the same TR. If JITC finds a TR that needs an impact statement added after the ARP has concluded, it will be referred back to the participant for coordination, review, and comment.

The ARP will assign a Network Interoperability Impact Category (Critical, Moderate, or Minor) to each TR as a number is assigned. The purpose of assigning categories is to assist decision-makers in gauging the seriousness of the network interoperability impact that results from the discrepancy documented in the TR. Definitions of each category, along with specific examples, are provided below. As these categories are considered guidelines, mitigating circumstances may cause a slightly different category to be assigned to any particular TR.

Category 1 – Critical

An error that prevents accomplishment of an essential function, for which no alternative work-around solution exists. Reloading or restarting the software is not an acceptable workaround solution. Overly complex actions that place an unacceptable burden on the system operator are also not acceptable workaround solutions. Additionally, an error that prevents accomplishment of an essential function jeopardizes personnel safety, or causes unrecoverable equipment or data loss is considered to be Critical.

Examples

•System incorrectly reports critical data upon assuming Reporting Responsibility (R2).
•System fails to forward critical data as received, or does not forward all data to all links.
•System crashes for any reason, e.g., on receipt of erroneous messages.
•System causes a track to go unreported, e.g., fails to assume R2 after receipt of a drop track.
•System incorrectly resolves R2 identity conflicts.
•System does not display a critical identity conflict, e.g., HOSTILE to FRIEND.
•System does not display critical data or incorrectly displays critical data.

Category 2 - Moderate

An error that degrades performance of an essential function, for which there is a reasonable alternative work-around solution.

Examples

•System incorrectly reports or fails to forward non-critical data.
•System transmits less than the required number of messages for critical data, e.g. commands.
•System does not display non-critical data or incorrectly displays non-critical data.
•System transmits extraneous messages that significantly contribute to network loading.

Category 3 - Minor

An error which is an operator inconvenience or annoyance and does not affect a required function. System documentation errors are considered to be minor.
Examples

•System fails to display/report non-mission essential data, e.g. Altitude Source, fails to terminate control prior to dropping track.

•System transmits extraneous messages that contribute slightly to network loading or transmits fewer than the required messages for non-critical data.

•Implementation Specification discrepancies, e.g. system receives Height Source of Aircraft report, but Implementation Specification shows "Does Not Process" or vice versa.

(This page intentionally left blank.)

APPENDIX H

TACTICAL DATA LINK (TDL) PTR INSTRUCTIONS

The following describes the data requirements for each field of the PTR (Enclosure H-1).

OPR/ACT SYS: The Office of Primary Responsibility/Action System is completed by the originator. This block identifies the system the PTR is written against. Only one system is allowed per PTR, (e.g., DDG).

ARP DATE: ARP date is completed by the originator (MM/DD/YYYY)

TEST TYPE: Completed by the originator. This identifies the SUT and test type, (i.e., TDL CIT). (e.g. U.S. DDG TDL CIT)

TEST: Completed by the originator. This identifies the TDL CIT test number in which the trouble was discovered (e.g., TDL CIT-07-1).

ORIG. NO: Originator Number is completed by the originator. This is the sequential number assigned by each S/A prior to submission to JITC, (e.g., J001).

CTL NO: A Control Number is assigned by JITC as a cross-reference of PTRs for the ARP agenda, (e.g., 003).

RELATED MESSAGES: Completed by the originator. This indicates which TDL messages are involved in the PTR, (e.g., M.2/82 or J 12.0).

PAGE: Completed by the originator. This identifies the page in the test procedure where the trouble occurred, (e.g., B-25).

EVENT: Completed by the originator. This identifies the event from the test procedure where the trouble occurred, (e.g., 1.1.a).

TIME: Completed by the originator. This is the 4-digit Greenwich Mean Time (GMT) time (to the whole minute) when the trouble occurred or began, (e.g., 0014).

DAY: Completed by the originator. This identifies the TDL CIT test day (starting with 1 even if testing did not get started) on which the trouble occurred.

MIL-STD/DOCUMENTATION REFERENCE: Completed by the originator. PTRs require a page and paragraph number as well as the identity of the document, (e.g., MIL-STD-6011C, P. 20, Para. 2.a).

PROBLEM STATEMENT: Completed by the originator. Each PTR contains only one problem. This block has two parts.

Part One is a Short Title. This should be a short, unclassified sentence defining the problem.

Part Two is an accurate description with track numbers and circumstances surrounding the trouble and includes the operational impact statements. The originator assigns a security classification after careful consideration of the material IAW JIEO Circular 3010 (appendix F) or national doctrine.

SUPPORTING DATA: Completed by the originator. This section indicates which participants DX was used when the trouble was discovered, along with precise times and DX contents. Several participants' DX may be listed. This section is also classified IAW JIEO Circular 3010 (appendix F) or IAW national doctrine.

RESOLUTION: Completed during the ARP.

TR NO: Completed during the ARP.

S/A IDENTIFIERS. This number consists of one alphabetic character that identifies the initiator's S/A and three numeric characters that identify the PTR. PTR numbers are assigned sequentially using their assigned block of numbers for each test. PTRs should be arranged and numbered in the order of the test procedure, i.e., section, page, event, and time, prior to number assignment. Combatant Commander/Services/Agencies (C/S/A) identifiers and PTR number block assignments are as follows:

USA	A001 - A199 (CECOM)
	P001 - P199 (AMCOM)
USN	N001 - N199 (ACDS)
	N200 - N399 (SUT)
	N400 - N699 (NCTSI)
	N700 - N999 (ATDS)
USAF	F001 - F199 (Langley AFB)
	F200 –F299 (Other AF Systems)
	F300 - F399 (AF PTUC)
	F500 - F699 (Tinker AFB)
USMC	M001 - M199
NSA	S001 - S199
JITC	J001 - J199
Combined	C001 – C199

NOTE: Special PTR identifiers may be assigned as necessary to meet TDL testing requirements.

ENCLOSURE 1

APPENDIX H

TDL PRELIMINARY TROUBLE REPORT

OPR / ACT SYS	ARP DATE	TEST TYPE		TEST	ORIG NO.	CTL NO.
RELATED MESSAGES		**PAGE**	**EVENT**	**TIME**		**DAY**

MIL-STD / DOCUMENTATION REFERENCE

( ) PROBLEM STATEMENT   SHORT TITLE: (U)

( ) SUPPORTING DATA

( ) RESOLUTION

	TR NO.

All portions of this PTR are
UNCLASSIFIED unless marked with
a higher classification

DERIVED FROM: JIEO Circular 3010
                           February 1998
DECLASSIFY ON:

(This page intentionally left blank.)

APPENDIX I

UNITED STATES MESSAGE TEXT FORMAT (USMTF) PTR INSTRUCTIONS

The following describes the data requirements for each field of the PTR (Enclosure I-1). The participants and JITC exchange PTRs on a pre-determined schedule as specified in the test procedure. Test participants may submit PTRs to JITC up to ten working days after the end of the test.

OPR/ACT SYS: Office of Primary Responsibility/Action System is completed by the originator. Only one SUT is allowed per PTR.

ARP DATE: Completed by originator (e.g., 07/28/1999).

TEST TYPE: Completed by the originator. Identifies the test type (e.g. K TDL CIT).

TEST: Completed by the originator. Identifies the TDL CIT test number in which the trouble was discovered, (e.g., 07-1).

ORIG. NO.: Originator Number is completed by the originator. The sequential number assigned by each participant or SUT prior to submission to JITC, (e.g., J001).

CTL NO.: The Control Number is assigned by JITC as a cross-reference of PTRs for the ARP Agenda (e.g., 001).

AUTHOR: Completed by the originator. Identifies the person who wrote the PTR.

MIL-STD/DOCUMENTATION REFERENCE: Completed by the originator PTRs that are generated due to violations of the MIL-STD/Implementation Design Handbook (IDH) require a page and paragraph number. PTRs generated against any other documentation must identify the document, page number, and paragraph.

MESSAGE IDENTIFICATION: Completed by the originator. USMTF message map lines are extracted from JITC, participant, and SUT test messages. Message name (MTF Identifier), originator (test message/file number), set name, field number, and data items using the Field Format Index Reference Number/Field Use Designator Number (FFIRN/FUDN) are extracted from the test message and cross-referenced with MIL-STD-6040.

PROBLEM STATEMENT/SHORT TITLE: Completed by the originator. The originator assigns a security classification after careful consideration of the material. Classification will be IAW JIEO Circular 3010 (appendix F) or national doctrine. The body of the statement can be a maximum of 14 lines. Each PTR will contain only one problem. This block has two parts. Part one is a Short Title defining the problem. The Short Title is a mandatory field of the PTR. Part two is an accurate description with amplifying information and circumstances surrounding the problem. Include sufficient

information so the analysis team or other interested parties can duplicate the problem. Operational impact statements shall be included here.

OPERATIONAL IMPACT: Completed by the originator.

SUPPORTING DATA: Completed by the originator. Indicates additional specific information about the problem. For example, operating system anomalies, unique system implementation of MIL-STD-6040, and data conversion problems during communications link transfers are the kinds of additional conformance and interoperability issues discovered during testing. This section is classified IAW JIEO Circular 3010 (appendix F) or national doctrine.

TR NO.: To be completed during the ARP. The participating voting representatives determine, by consensus, whether a PTR becomes a TR.

C/S/A IDENTIFIERS. This number consists of one alphabetic character which identifies the initiator and three numeric characters which identifies the PTR. PTR numbers are assigned sequentially using their assigned block of numbers for each test. PTRs should be arranged and numbered in the order of the test procedure, i.e., section, page, event, and time, prior to number assignment. Participant identifiers and PTR number block assignments are as follows:

USA	A001 - A199
DIA	D001 - D199
JITC	J001 - J199
USMC	M001 - M199
USN	N001 - N199
NSA	S001 - S199
USAF	F001 - F199
Combined	C001 – C199

NOTE: Special PTR identifiers are assigned as necessary to meet USMTF testing requirements.

ENCLOSURE 1

APPENDIX I

US MESSAGE TEXT FORMATTING (USMTF)

PRELIMINARY TROUBLE REPORT

OPR/ACT SYS	ARP DATE	TEST TYPE	TEST	ORIG NO.	CTL NO.

AUTHOR:
MESSAGE IDENTIFICATION:
MSGID: **TEST MESSAGE:**
    USMTF Identifier

SET NAME: **FIELD NO:**   **FFIRN/FUDN:**   /

MIL-STD-6040 / DOCUMENTATION REFERENCE

**(   )   PROBLEM STATEMENT
        SHORT TITLE (U)**

(   ) OPERATIONAL IMPACT

(   ) SUPPORTING DATA

(U) RESOLUTION   **TR NO**

All portions of this PTR are   DERIVED FROM: JIEO Circular 3010
UNCLASSIFIED unless marked with   February 1998
a higher classification   DECLASSIFY ON:

I-1-1

(This page intentionally left blank.)

APPENDIX J

ANALYSIS REVIEW PANEL (ARP) PROCEDURES

The ARP will consist of a JITC chairman, one voting member from the country with the SUT and each S/A. Additional non-voting personnel may be present to assist as necessary. As previously mentioned, JITC, upon request, can act on behalf of the combined country if they are unable to attend the ARP. All members attending the ARP should have sufficient expertise to adequately address technical evaluations and network/operational impact statements. In addition, personnel from JITC attend to provide technical and administrative support.

The ARP will review and evaluate the analysis of test results documented in PTRs. Each PTR on the agenda will be discussed in order, and its status determined. All PTRs on the agenda must be addressed and given a status by the end of the ARP. If an impasse occurs, the ARP is polled and the majority opinion determines the status for the PTR in question.

Previous TRs can be closed or modified at each ARP. The ARP is the only forum in which the TRs against the SUT can be closed, unless test circumstances warrant administrative closure. USMTF TRs against a SUT for no longer existing data codes, fields, sets, segments, and message types (which are not found in other message types) may be administratively closed.

If the ARP determines that the PTR requires action, a TR number will be assigned in accordance with appendix H or I as applicable. The TR number is composed of two letters (JM for USMTF, JT for TDL A/B, JJ for TDL J, and JK for VMF) and the next available number plus a suffix to indicate the TR class (e.g., JT0001A, JM0002A, etc.) as follows (appropriate letters will be added as necessary):

Class A (Interface Problems). This class identifies problems with the MIL-STD. An example of this class of problem would be an ambiguity in the MIL-STD or the failure of a message format to meet operational requirements. This class of TR requires that the OPR generate an Interface Change Proposal (ICP) that is forwarded to the appropriate Configuration Control Board (CCB) for action. The CCB is considered to be the final authority on standards issues.

Class B (Systems and/or Software Problems). This class identifies program coding errors or system design problems which require corrections in a participating system to effect compliance with the MIL-STD or to meet interoperability requirements. Also included are software errors that impact on the interface, failure of an automated system to interface as specified or Data Extraction errors.
Class C (Test Problems). This class identifies any errors associated with test procedures, interpretation of test procedures, or operator errors that result in incomplete or improperly executed events.

Class D (Simulator, DX, Gateway, and/or other Laboratory Software and Hardware Problems). Identifies problems or limitations with the laboratory hardware and/or software used during testing.

Class H (Hardware Problems). Identifies problems or limitations with a C2 system's hardware, which impact TDL CIT.

Class I (System Implementation Document Problems). Identifies problems with a system's Implementation Document or System Description.

Class J (Combined Doctrine/Procedures). Identifies deficiencies in combined doctrine or procedures that were identified during testing. A letter signed by the Commander, JITC will be forwarded to the Interoperability Test Panel (ITP) of the Military Communications-Electronics Board (MCEB) identifying a problem that is beyond the scope of the ARP to resolve. The ARP chairman reports the ITP decision to the ARP when available.

Prior to the conclusion of the ARP, each test participant will provide an overall assessment of the interoperability of the SUT with U.S. systems based on a technical and operational evaluation. The assessments will not be a "pass/fail" recommendation.

Each test participant will provide a signed position paper with amplifying statements with their evaluation that is included in the test report. The written statements must be provided to the ARP chairman prior to adjournment. The ARP chairman will provide copies of all comments to participants to allow for a reply if desired. Statements should contain, as a minimum:

> •Overall impression of the SUT performance.

> •Functional areas impacted, including a technical and operational evaluation of the TRs effect on the tested system's mandatory operational implementation.

> •Assessment of impact on the combined network or the SUT.

In the event a C2 system/software version is found not to be interoperable, all TRs that were tested shall remain open. In addition, the TRs written against the version that was not interoperable will remain in effect until future versions demonstrate that the problems no longer exist, or they are administratively closed.