NOT MEASUREMENT SENSITIVE

MIL-HDBK-1350-1
Volume 1
July 1994

MILITARY HANDBOOK

VALIDATION OF DATA COMMUNICATIONS PROTOCOL STANDARDS FOR MILITARY APPLICATIONS

VOLUME 1

AMSC N/A AREA DCPS

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

FOREWORD

1. This military handbook (MIL-HDBK) is approved for use by all Department and Agencies of the Department of Defense (DoD).

2. Beneficial comments (recommendations, additions, deletions) and any pertinent data that may be of use in improving this MIL-HDBK should be addressed to:

Joint Interoperability and Engineering
Organization (JIEO)
ATTN: TBBD
Squire Hall, Building 283
Fort Monmouth, New Jersey 07703-5613

by using the Standardization Document Improvement Proposal (DD Form 1426) appearing at the end of this MIL-HDBK or by letter.

TABLE OF CONTENTS

PARAGRAPH PAGE

1. SCOPE 1
1.1 Purpose 1
1.2 Background 1

2. APPLICABLE DOCUMENT 2
2.1 Government documents 2
2.1.1 Specifications, standards, and handbooks 2
2.1.2 Other Government documents, drawings, and publications 3
2.2 Non-Government documents 3
2.3 Order of precedence 4

3. DEFINITIONS 5
3.1 Terms used in this MIL-HDBK 5
3.2 List of acronyms 5

4. GENERAL REQUIREMENTS 7
4.1 General 7
4.1.1 Protocol Design and Status Determination Phase 10
4.1.2 Protocol Formalization Phase 12
4.1.3 Protocol Development Phase 15
4.1.4 Conformance Testing Phase 17
4.1.5 Interoperability Testing Phase 20
4.2. Military Issue Validation Traceability Matrix 22
4.2.1 Military Feature Specification and Protocol Association 22
4.2.2 Requirements Definition 23
4.2.3 Test and Evaluation Milestone Tracing 23

5. SPECIFIC REQUIREMENTS 24
This section is not applicable to this MIL-HDBK. 24

6. NOTES 25
6.1 Intended Use. 25
6.2 Subject Term (Keyword) Listing 25

TABLE OF CONTENTS (Concluded)

APPENDIX PAGE

DEFINED ISSUE AND CRITERIA QUESTIONS 26

Concluding Material 29

FIGURES PAGE

1. Validation methodology 8

2. Validation process 9

3. Protocol design and status determination phase 11

4. Formalization phase 14

5. Development phase 16

6. Conformance test phase 19

7. Interoperability test phase 21

1. SCOPE

1.1 Purpose. The purpose of this volume of MIL-HDBK-1350-1 is to define the methodology, procedures, and supplementary actions required to ensure that proper consideration is given to the incorporation of military features, requirements, and issues into the development of standards and implementation of data communications protocols for use in the Department of Defense (DoD) and the Military Departments. The protocols affected include those conforming to FIPS-146-1 and taken from the US GOSIP Register for DoD use, other adopted protocols, US GOSIP protocols or other adopted protocols extended for use or protocols developed specifically for use by the DoD in accordance with MIL-HDBK-829-2. This MIL-HDBK addresses the development of future protocols and protocol standards which are to include military features, those protocols which are being adapted to accommodate military features, and those protocols believed to already incorporate features required for military use. This MIL-HDBK also delineates those actions necessary to ensure that military features are included in the original design and development of any data communication protocol intended for use in the DoD. This MIL-HDBK is also designed to ensure testability of protocols and profiles in accordance with ISO/IEC 9646/CCITT X.290 at the earliest possible point in their development. It defines the actions required for, and the point in the validation process when, a protocol or extension under development is considered for Data Communications Protocol Standards (DCPS) Technical Management Panel (DTMP) approval. It also defines those points in the validation process when early feedback is provided to the DTMP and protocol developers, in the form of Engineering Change Proposals (ECPs), when protocol errors or inadequacies are uncovered during later validation phases.

1.2 Background. The DTMP was formed in 1990 for the purpose of managing the development of Department of Defense (DoD) data communications standard protocols and to ensure the coordination of the interests of the DoD as they relate to national and international standards organizations. Additionally, the panel was formed to document military features in support of the DoD acquisition process. This role includes the validation of data communications protocol standards and the verification of the implementation of those standards.

2. APPLICABLE DOCUMENTS

2.1 Government documents.

2.1.1 Specifications, standards, and handbooks. The following specifications, standards, and handbooks form a part of this MIL-HDBK to the extent specified herein. Unless otherwise specified, the issues of these documents are those listed in the issue of the Department of Defense Index of Specifications and Standards (DoDISS) and supplements thereto, cited in the solicitation.

STANDARDS

FEDERAL

FIPS 146-1 Federal Information Processing Standard Publication 146-1, *Government Open Systems Interconnection Profile (GOSIP)*, 3 April 1991

HANDBOOKS

MILITARY

MIL-HDBK MIL-HDBK-829-2 *Guidelines for Data Communications Protocol Standards (DCPS) DOD Standardized Profiles (DSPs), Volume 2*, 23 April 1993

MIL-HDBK-1350-2 *Data Communications Protocol Conformance and Interoperability Testing and Registration, Volume 2*, July, 1994

(Copies of FIPS are available to DoD activities from the Commanding Officer, Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, PA, 19120-5099. Others must request copies of FIPS from the National Technical Information Service, 5285 Port Royal Road, Springfield, VA 22161-2171.)

(Unless otherwise indicated, copies of federal and military specifications, standards, and handbooks are available from the Naval Publications and Forms Center, ATTN: NPODS, 5801 Tabor Avenue, Philadelphia, PA 19120-5099.)
(Copies of the MIL-HDBK-829, Volumes 1 and 2, and MIL-HDBK-1350, Volumes 1 and 2, are available from the Defense Information Systems Agency (DISA)/Joint Interoperability and Engineering Organization (JIEO), ATTN: TBBD, Fort Monmouth, NJ 07703-5613.)

2.1.2 Other Government documents, drawings, and publications. The following other Government documents, drawings, and publications form a part of this MIL-HDBK to the extent specified herein. Unless otherwise specified, the issues are those cited in the solicitation.

Department of Commerce

National Institute for Standards and Technology (NIST)

NIST
Technical Report

NCSL/SNA-91/1
NIST Technical Report, *Open Issues in OSI Protocol Development and Conformance Testing, The U.S. GOSIP Testing Program*, January 1991

(Copies of the Department of Commerce, NIST documents are available from NIST, Technical Building, Gaithersburg, Maryland 20899.)

2.2 Non-Government documents. The following non-Government documents form a part of this MIL-HDBK to the extent specified herein. Unless otherwise specified, the issues of the documents that are DoD-adopted are those listed in the issue of the DoDISS cited in this solicitation. Unless otherwise specified, the issues of the documents not listed in the DoDISS are the issues of the documents cited in the solicitation.

International Standards Organization (ISO)/Consultative Committee for International Telegraph and Telephone (CCITT)

ISO/IEC 9646,

CCITT X.290 *OSI Conformance Testing Methodology and Framework for Protocol Recommendations for CCITT Applications*, Melbourne, 1988.

(Application for copies of this document should be addressed to ISO, Van Demonstrate 94, 1013 CN Amsterdam, Netherlands.)

2.3 Order of precedence. In the event of a conflict between the text of this MIL-HDBK and the references cited herein, the text of this MIL-HDBK takes precedence. Nothing in this MIL-HDBK, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

3. DEFINITIONS

3.1 Terms used in this MIL-HDBK. The following terms are defined for specific use in this MIL-HDBK, to the extent indicated.

Validation. Traditionally refers to the testing of software or its specification at the end of the development effort to ensure that it meets its requirements. Validation has also meant the determination that specified requirements are correctly derived from system requirements in accordance with the rules of logic and the needs of the user. In the context of this MIL-HDBK, validation refers to the analysis of the implementations of military features and requirements to ensure that they are correctly and completely specified and that testing correctly addresses these specifications and user requirements.

Verification. Traditionally refers to the evaluation of software during each phase of its life cycle to ensure that it meets the requirements set forth in the previous phase. In this MIL-HDBK, verification is an integral part of the validation process. It is the determination that the validated requirements have actually been appropriately formalized and included in the various test related documentation of the development and testing cycle.

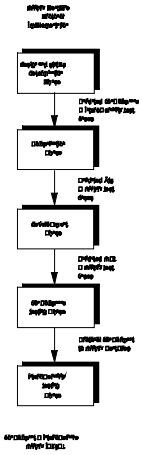
3.2 List of acronyms. The following acronyms are used in this MIL-HDBK.

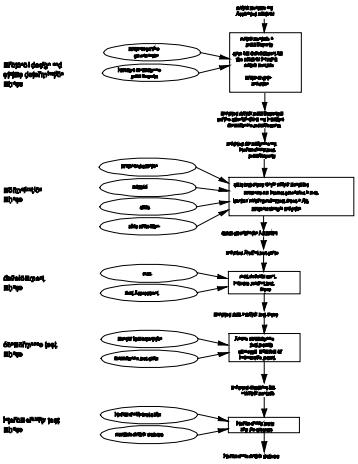
ATS	Abstract Test Suite
CCITT	Consultative Committee for International Telegraph and Telephone
DCPS	Data Communications Protocol Standards
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDISS	Department of Defense Index of Specifications and Standards
DTMP	Data Communications Protocol Standards (DCPS) Technical Management Panel
FDT	Formal Description Techniques
FEC	Forward Error Correction
FIPS	Federal Information Processing Standard
GOSIP	Government Open Systems Interconnect Profile
IUT	Implementation Under Test
JIEO	Joint Interoperability and Engineering Organization
JITC	Joint Interoperability Test Center
MIL-HDBK	Military handbook
MIL-STD	Military standard
MOT	Means of Testing
NCSL	National Computer Systems Laboratory
NIST	National Institute for Standards and Technology
OSI	Open Systems Interconnection
PICS	Protocol Implementation Conformance Statement
PIXIT	Protocol Implementation Extra Information for Testing
SDNS	Secure Data Networking System
SNA	Systems and Networking Architecture (Division - NIST)
SOTS	Service Oriented Test Suite
SUT	System Under Test
TTCN	Tree and Tabular Combined Notation

1

4. GENERAL REQUIREMENTS

4.1 General. The process of validating unique DoD data communications protocols and protocols which have been extended to meet military requirements encompasses five phases which generally conform to the five phases of the Protocol Development and Testing Cycle shown in NIST Technical Report NCSL/SNA-91/1. The phases, or steps in the process, are shown in Figure 1, and the relationships between validation actions are shown in Figure 2. Subsequent portions of this section discuss the individual phases of the validation process and their inherent activities; the actions required and point in the validation process when a protocol or extension under development is considered for DTMP approval; and those points during later validation phases when early feedback is provided to the DTMP and protocol developers, in the form of Engineering Change Proposals (ECPs), because of discovered errors or inadequacies in the protocol. 1



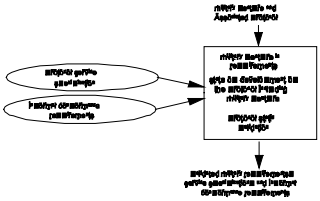


4.1.1 Protocol Design and Status Determination Phase. The initial phase of the validation methodology begins with the validation of the original military requirements and the determination of the state of protocol development. The postulated military requirements and features and the protocol with which they are to be associated are examined for validity. This examination must determine that the features slated for incorporation into a given protocol reflect, exactly, the intended user requirements and desired functionality. Additionally, the features must be examined to determine that their implementation will cause no detrimental effects to the existing functionality of the protocol with which they are to be associated. For example, the implementation of a multi-cast feature must be studied to understand its effects on timers and acknowledgements and how it effects overall protocol performance.

The actions taken during this phase of the validation methodology constitute the static validation of a newly developed candidate protocol or extension. Problems, anomalies or inconsistencies, if any, discovered during the protocol static validation are reported to the DTMP and protocol or extension developers for correction.

Once it has been determined that the requirements and features are indeed valid, an analysis must be conducted to determine the stage of development of the protocol or military extensions. This will enable the validation tester to determine the point in the process where further analysis must commence. For example, if an implementation is already in the market place, the approach must be different than if the implementation is beginning development. If an available means of testing (MOT) does not properly address military features, then entry at an early point in the process may be required. However, the preliminary steps can be avoided if a complete and mature MOT is available, which tests for the required military features. If an MOT is registered on the US GOSIP Register or the DoD Data Communications Protocol Register it can be used as a basis for developing an extension to cover a military extension to the protocol.

After the determination is made that a protocol is at the beginning of this five phased process, several analyses and determinations will begin as shown in Figure 3 (Design and Status Determination Phase). First, the Protocol Service Specification will be examined to ensure that the validated military features, issues, and requirements have been included. The testability of these items will come to light in the comparison of the Informal Conformance Requirements with the Protocol Service Specification. If the military features are correctly included in the Protocol Service Specification they should appear as relatively unambiguous test requirements in the Informal Conformance Requirements. This first phase of the methodology then produces validated and verified Protocol Service Specifications and Informal Conformance Requirements which contain correctly described military features and requirements.ı



4.1.2 Protocol Formalization Phase. The protocol formalization phase of the process should result in the production of one primary product. This product is the collection of Abstract Test Suite (ATS) test cases for the military features and requirements. These test cases result from the following analyses and actions.

Proceeding under the assumption that the Protocol Service Specification and Informal Conformance Requirements (for the military features and requirements) produced by the efforts of the first phase of the process have been individually validated, they will be used for the first step in the formalization phase. This is the description of the military features within the protocol by FDT. The military feature portions of the formal description of the protocol must be compared to the Protocol Service Specification. This comparison is used to verify that the FDT has described the features as they are understood and required by the military user.

The description of the military features by FDT and the follow-on simulation of the protocol or extension performed during this phase of the validation methodology constitute the dynamic validation of a newly developed candidate protocol or extension. Problems, anomalies or inconsistencies, if any, discovered during the protocol dynamic validation are reported to the DTMP and protocol or extension developers for correction.

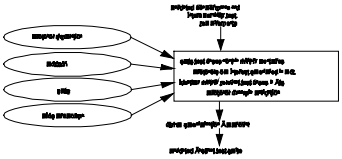
It is at this point in the validation methodology, when both the static and dynamic protocol validation have been accomplished and DTMP required corrections made by the developers, that a protocol or extension under development is considered for DTMP approval.

The next action to be taken is another static analysis. This is the determination that the requirements of the Informal Conformance Requirements have been adequately represented in the test cases of the Service Oriented Test Suite (SOTS). If no test cases for military features exist in the SOTS then they must be developed, and they must be precisely representative of the original user requirements. Also, at this point the presence of proper test cases in the SOTS form the beginning of a Test Traceability Matrix which will be used to chart progress throughout the military feature testing process. This matrix is explained in more detail in Section 4.2.

The SOTS and the formally described protocol are then used to develop the test cases of the ATS. This is made much easier if the formalization of the protocol has been validated against the original user military requirements. The presence of test cases for military features must be verified within the ATS. The test cases must then be validated for their correctness, consistency, completeness, and soundness.

These actions are based on the assumption that the protocol has been properly specified by FDTs. Whether this has been completely and correctly accomplished is not of primary concern. What is important is that the military features have been included in FDT description of the protocol and that their inclusion represents the manner in which they should be tested. The Protocol Implementation Conformance Statement (PICS) Proforma are then examined in a similar manner, as are the Protocol Implementation Extra Information for Testing (PIXIT). Each of the required characteristics of the protocol implementation profiles must be examined for the presence of the desired military features.

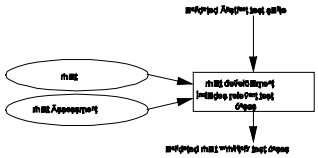
These actions should verify the presence of test cases within the ATS and validate that they completely and adequately test the presence and functionality of military features in an implementation of the protocol. These ATS test cases should be constructed in Tree and Tabular Combined Notation (TTCN). They then become the product of the formalization phase of the process and are noted in the test traceability matrix. All of the actions of this phase are represented in Figure 4.1



4.1.3 Protocol Development Phase. The protocol development phase refers generally to the period during which the protocol implementation is being developed by a particular vendor. It is also the period which should be used for the development of the MOT. All implementations will enter the development phase independent of the development of the MOT which will be used to test them. Two sets of static and dynamic analyses will occur which are intended to ensure that the military features have been included in the protocol implementation and that the test cases of the MOT are sufficiently prepared to test them. The actions which occur during the development phase and the resulting products are shown in Figure 5.

If any protocol errors or inadequacies are uncovered during this validation phase they are reported to the DTMP and protocol developers in the form of Engineering Change Proposals (ECPs).

1


MIL
MIL Applicability
MIL develop MIL
test for one MIL
apply
develop test plan MIL
test plan MIL

Two products will result from the development phase. The first product, which originates at the vendor or developer, is the protocol implementation and its associated PICS and PIXIT. The second product, which is of primary interest in the validation process, is a valid set of test cases from the completed, assessed, and certified MOT. The test cases from the MOT are central to the testing process.

The successful accomplishment of conformance testing of the military features and use of the results will require the successful completion of the earlier phases of the process. If the design, formalization, and the development phases have been accomplished correctly and accurately, the pertinent test cases in the ATS will address the necessary military features. The same follows for the test cases selected from the MOT. However, in this phase the MOT test cases can be compared to the Protocol Service Specification, the Informal Conformance Requirements, and the SOTS. The purpose of these comparisons is to verify that the original test and evaluation requirements for the protocol services are addressed and met in the MOT.

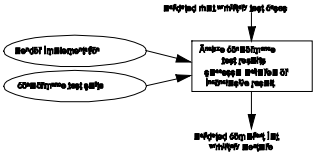
When the applicable MOT becomes available it must be subjected to both static and dynamic analyses to identify those test cases which cover the military features under examination. These actions can be most efficiently accomplished as an adjunct to the formal MOT assessment process. When a protocol is determined to potentially contain military features the test cases which have been identified previously in the SOTS will be compared to test cases in the MOT in order to determine that those in the MOT are adequate for testing the proper implementation of the military features in the protocol. Comparisons of the tests performed in these cases (SOTS and MOT) with the Protocol Service Specification and the Informal Conformance Requirements which have already been examined will add credence and validity to the test cases. The test cases should then be subjected to dynamic analysis as part of the MOT assessment. This analysis will be used to validate the operability and completeness of the military feature test cases, and will be done as part of the overall assessment of the MOT. The assessments of MOTs, which are expected to cover military features, should be accomplished by the DISA(JITC), being the only NIST registered U. S. organization authorized to conduct such assessments.

If it is determined that a MOT which is applicable to military features does not contain the pertinent test cases, the test cases must be developed. The development of military test cases will be accomplished by the DISA(JITC) or another accredited facility. The development of the MOT test cases will be based upon the test cases from the ATS developed earlier.

4.1.4 Conformance Testing Phase. Once the test cases needed to test the presence and functionality of military features in a specific implementation of a protocol have been identified and validated in the MOT, those test cases must then be used in the conformance test of the implementation. This phase of the process comprises the traditional validation of the implementation of the military features. This can be accomplished in one of two ways. The first is to include the military feature test cases in an overall conformance test of the Implementation Under Test (IUT). The other is to conduct a test of only the military features. The danger in an approach of this nature is that an IUT may become certified and placed on the DoD Data Communications Protocol Register without adequate testing of military features. This dictates that stand-alone military feature testing occur either in advance of conformance certification testing or very quickly thereafter.

If any protocol errors or inadequacies are uncovered during this validation phase they are reported to the DTMP and protocol developers in the form of Engineering Change Proposals (ECPs).

These steps are shown in Figure 6. 1

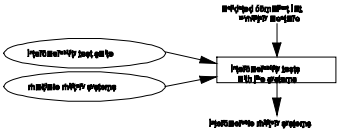

Text Input Data
Text Output Data
Text Input Data
Text Output Data
Text Input Data
Text Output Data

As testing occurs and the MOT test cases are executed against the IUT or System Under Test (SUT), either satisfactory, inconclusive or failure results occur. The results of the conformance tests are then entered into the test traceability matrix. Reporting of the results of military feature conformance testing should be published in accordance with the same procedures used for the publication of standard conformance test results. This will be accomplished as specified in MIL-HDBK-1350-2.

4.1.5 Interoperability Testing Phase. This is the final phase of the methodology. Although conformance to standards is critical for the use of protocols which employ military features, protocols are not usable until interoperation between the IUT and another standards compliant implementation of the protocol has been demonstrated. The example standards compliant implementation of the protocol should contain the desired military features. For the purpose of testing interoperable implementations of military features, only those MOT test cases which have been identified for use in conformance or interoperability testing will be used. Standards compliant implementations (with certified military features) will also be selected which contain those features which are being tested. Implementations with military feature options will be connected to the SUT and the critical services and features invoked. For interoperability to exist, all test cases involving military features must be invoked, tested, and success achieved. All of the results of this testing will be noted in the traceability matrix for each pair of implementations. As the matrix of tested pairs grows, the certainty of interoperability of all implementations grows until all implementations have been tested with all other implementations, achieving complete interoperability.

If any protocol errors or inadequacies are uncovered during this validation phase they are reported to the DTMP and protocol developers in the form of Engineering Change Proposals (ECPs).

The interoperability testing portion of the process is shown in Figure 7. 1


Multimedia test suite
Multimedia test
suite IPs storage
Multimedia test suite
Multimedia test suite
storage

4.2. Military Issue Validation Traceability Matrix. This section traces the accomplishment of testing requirements within the methodology presented in section 4.1 and depicted in Figure 1.

4.2.1 Military Feature Specification and Protocol Association. For complete and comprehensive testing of each military requirement or feature, the feature must be separated into testable issues and criteria against which test cases can be developed and applied. An example of this is the Security feature. Security includes a variety of sub-features, one of which is data integrity. Data integrity can be protected in several ways, one of which is error detection and correction. Error detection and correction is most often implemented in the form of forward error correction (FEC) codes and techniques. Forward error correction techniques can be tested if they are specified by an ability to correct a given quantity of flawed bits in a base amount. As an example, the use of 23,12 Golay code for forward error correction will allow for the correction of 3 bits in a 12 bit data field. Because this is accomplished at the expense of a 100 percent overhead, test cases must inject errors at an appropriate point in the protocol stack and check for the correction of those errors at an appropriate receipt point. These points will depend on the place where the FEC is to be implemented and how the overhead is managed. This results in the definition of a testable issue and an associated criteria:

(1) Issue: Forward Error Correction

(2) Criteria: The protocol must be capable of correcting up to three flawed bits in each twelve bit coded word.

The feature or requirement is then associated with a specific protocol. In the case of the FEC requirement, the association would most likely be with a lower layer protocol which includes the data link layer in a local or wide area network. Thus, the specified security requirement for FEC would be tested in association with the local or wide area network protocol with which it is associated (802.3, 802.4, 802.5, X.25, Mode VII, etc.). The conformance of the military extension becomes the ability of a protocol to transmit data and correct bit errors up to the capabilities of the algorithm which has been employed.

4.2.2 Requirements Definition. The responsibility to ensure that each identified military requirement is prepared for testing is with one of the DTMP working groups. As the requirements and their corresponding issues and criteria are developed within the working groups they will be reported to DTMP Working Group Number 7 for inclusion in the Validation Traceability Matrix. Additionally, Working Group Number 7 will independently

determine issues and criteria. These will be submitted to the other working groups for consideration and adoption. Requirements, issues, and criteria will be included in the matrix and their progress toward and through successful testing annotated once concurrence is achieved.

4.2.3 Test and Evaluation Milestone Tracing. Each issue which results from the process above will be included in the traceability matrix. The traceability matrix will take the form of a list of questions and responses related to each defined issue and criteria. They will be adapted as necessary to the specific issue. Each criteria entry will contain some form of the questions and comments listed in the Appendix.1

5. SPECIFIC REQUIREMENTS

This section is not applicable to this MIL-HDBK.1

6. NOTES

6.1 Intended Use. Documents, products or processes conforming to the requirements of this handbook are intended for use in the development and implementation of Military Data Communications Protocols. The purpose of this handbook is to provide guidance in the validation of Data Communication Protocol Standards and in the testing and registration of products professing compliance with those protocols.

6.2 Subject Term (Keyword) Listing.

Abstract Test Suite (ATS)
Conformance Testing
Data Communication Protocol
Formal Description Technique (FDT)
Implementation Under Test (IUT)
Interoperability
Interoperability Testing
Interoperation
Means Of Testing (MOT)
Open Systems Interconnection (OSI)
Parameterized Executable Test Suite (PETS)
Protocol
Protocol Conformance Test Report (PCTR)
Protocol Formalization
Registration
Requirements Definition
Standards
System Under Test (SUT)
Test Case
Tree and Tabular Combined Notation (TTCN)
US GOSIP
Validationı

APPENDIX

DEFINED ISSUE AND CRITERIA QUESTIONS

10. GENERAL.

10.1 Scope. This Appendix is a mandatory part of this MIL-HDBK. The information contained herein is intended for compliance.

20. APPLICABLE DOCUMENTS. This section is not applicable to this appendix.

30. DEFINED ISSUES AND CRITERIA QUESTIONS. This Appendix is provided to ensure that each def e and criteria resulting from section 4. of this MIL-HDBK can be included in the military feature register of the GC ıformance and Interoperability Register Data Base. Each criteria entry will contain some form of the questions ıments listed below:

(1) Do Protocol Service Specification, Informal Conformance Requirements, and SOTS exist for the protoco

nments:

(2) Does the Protocol Service Specification for the protocol contain requirements to support the speci tary requirement:

nments:

(3) Do the Informal Conformance Requirements for the protocol contain sufficient requirements to deterr the specified military requirement will be conformance tested:

nments:

(4) Specify the test cases from the SOTS which determine the conformance of the protocol implementa er test to the specified military requirement:

nments:

(5) Has the protocol been specified in an accepted FDT:

nments:

(6) Has an ATS been constructed for the protocol which is completely rendered in TTCN and included in GOSIP Register or the DoD Data Communications Protocol Register:

nments:

(7) Have PICs Proforma and PIXIT been prepared for the protocol associated with the specified mili ıirement:

nments:

(8) Does the ATS contain accurately represented test cases from the SOTS, validated to test the ability of :ocol to support the implementation of the specified military feature:

nments:

(9) Does an assessed MOT appear on the NIST register for the protocol:

nments:

(10) Does the MOT contain the appropriate test cases from the ATS, validated to test the ability of the prot upport the implementation of the specified military requirement:

nments:

(11) Has the IUT been conformance tested with the military feature test cases present in the MOT; specify dates, circumstances, laboratory, and those test cases which resulted in success, failure, and inconclusive results:

nments:

(12) What other implementations (containing successful usage of the specified military requirement) exist for :ocol as registered by NIST:

nments:

(13) Has pair wise interoperability testing been conducted between a registered reference implementation implementation under test; specify the test dates, circumstances, laboratory, and those test cases which resulted in succ ıre, and inconclusive results:

nments:

CONCLUDING MATERIAL

todians:

DISA:	DC	Preparing Activity:
Army: SC	Defense Information Systems Agency (DISA) - DC	
Air Force:	90	
Navy:	OM	
DIA:	DI	
NSA:	NS	
USMC:	MC	
DLA:	DH	

iew Activities:

Army: SC	
Air Force:	02, 13, 17, 29, 90
Navy:	EC, OM
DIA:	DI
NSA:	NS
USMC:	MC, CG
DLA:	DH
OASD:	IQ, DO, MA, IR
ODISC4:	AC

STANDARDIZATION DOCUMENT IMPROVEMENT PROPOSAL

INSTRUCTIONS

1. The preparing activity must complete blocks 1,2, 3, and 8. In block 1, both the document number and revision letter should be given.
2. The submitter of this form must complete blocks 4, 5, 6, and 7.
3. The preparing activity must provide a reply within 30 days from receipt of the form.

NOTE: This form may not be used to request copies of documents, nor to request waivers, or clarification of requirements on current contracts. Comments submitted on this form do not constitute or imply authorization to waive any portion of the referenced document(s) or to amend contractual requirements.

	1. DOCUMENT NUMBER	2. DOCUMENT DATE *(YYMMDD)*
3. DOCUMENT TITLE		
4. NATURE OF CHANGE *(Identify paragraph number and include proposed rewrite, if possible. Attach extra sheets as needed.)*		
5. REASON FOR RECOMMENDATION		
6. SUBMITTER		
a. NAME *(Last, First, Middle Initial)*	b. ORGANIZATION	
c. ADDRESS *(Include Zip Code)*	d. TELEPHONE *(Include Area Code)* (1) Commercial (2) AUTOVON	7. DATE SUBMITTED *(YYMMDD)*
8. PREPARING ACTIVITY		
a. NAME	b. TELEPHONE *(Include Area Code)*	
c. ADDRESS *(Include Zip Code)* ATTN: TBBD (DTMP Secretariat) Director, JIEO Ft Monmouth, NJ 07703-5613	**IF YOU DO NOT RECEIVE A REPLY WITHIN 45 DAYS, CONTACT:** Defense Quality and Standardization Office 5203 Leesburg Pike, Suite 1403, Falls Church, VA 22041-3466 Telephone (703) 756-2340 AUTOVON 289-2340	