ATNP/WG3

WP/7-18

17/06/1996

AERONAUTICAL TELECOMMUNICATIONS NETWORK PANEL(ATNP)

WORKING GROUP 3 - APPLICATIONS AND UPPER LAYERS

Munich, 24-28 June 1996 (seventh meeting)

Agenda Item 7.3 : Validation documentation for ATNP/2

WP/7-18 : MHS SARPs Validation Objectives

Presented by Jean-Marc Vacher (France)

Summary

This paper proposes the approach to be taken for validating the Draft SARPs for ATS Message Handling Services over the ATN (ATS Message Service) for the CNS/ATM-1 Package.

WG3 is invited to endorse the recommendations in this paper.

Table of Contents

References

[1] Draft SARPs for ATS Message Handling Services over the ATN, version 1.1

1. Background

1.1. Objective of the WP

At the sixth meeting of the ATNP/WG3 in Brussels, 15-26 April 1996, SG1 was tasked with the production of Validation Objectives for the MHS SARPs, along the structure used in WP5-17 for the definition of the ULA Validation Objectives.

This working paper is the response with respect to the validation of Sub-Volume 3, Part 1, Chapter 2 (3.1.2 of the overall SARPs material), concerning the ATS Message Service.

1.2. Validation concept

A draft SARPs may be considered as Validated when it has been demonstrated to specify the stated functions (no more, no less) as a series of requirements, and each requirement has itself been Validated. A requirement (expressed in SARPs as a "shall" clause, or a series of related "shall" clauses) is considered to be Validated when it has been inspected, analyzed, simulated and/or tested to determine that it is a true and accurate specification, unambiguous and not in conflict with any other requirement and provides the intended operational capability.

1.3. General objectives of validation

The objectives of SARPs validation are to ensure that the draft SARPs are:

a) complete and self-consistent;

b) unambiguous;

c) mutually consistent (within the CNS/ATM-1 Package); and

d) they achieve the declared user requirement.

2. Discussion of Validation Objectives

2.1. The objectives of the validation of the MHS SARPs (ATS Message Service) are to ensure that:

a) the draft MHS SARPs (ATS Message Service) are complete, consistent, and unambiguous;

b) implementations conforming to the draft MHS SARPs (ATS Message Service) are capable of interworking at the syntactic and semantic level; and

c) the draft SARPs satisfy the user requirements for the exchange of messages between each pair of systems providing an ATS Message Service, namely:

   1) between an ATS Message User Agent and an ATS Message Server;

2) between two ATS Message Servers;

3) between an ATS Message Server and an AFTN/AMHS Gateway;

4) between two AFTN/AMHS Gateways.

2.2 The user requirements are reflected in the Validation Objectives (VOs) for the MHS SARPs (ATS Message Service), which are structured into a hierarchy of high-level requirements as shown in Table 2-1.

Table 2-1 MHS SARPs (ATS Message Service) Validation Objectives

VO	Short Name	Description
1	ISO compliance	Validate that the protocols specified in the MHS SARPs comply with ISO standards to the stated extent
1.1	MHS compliance	Validate the compliance with the ISO MHS standards
1.1.1	ISP compliance	Validate the compliance with the ISO MHS ISPs
1.2	Interworking	Validate the degree of interworking with other MHS/X.400 implementations
1.3	Migration	Validate that requirements for forward compatibility (extended service, optional functional groups, other content types) are satisfied
2	AMHS SLRs	Validate that the SARPs provisions meet the system level requirements relevant to the AMHS internally
2.1	AMHS naming and addressing	Validate the specified AMHS naming and addressing provisions
2.1.1	O/R names	Validate the specified construction of O/R names
2.2	AMHS management domains	Validate that the AMHS may be organized in domains for States and organisations
2.3	AMHS routing	Validate that the AMHS enables the routing along authorized paths for the store-and-forward conveyance of information
2.4	AMHS long-term logging	Validate that the AMHS maintains records of all originated traffic for a period of at least 30 days

3	AFTN interworking	Validate that the AMHS provide an AFTN interworking capability
3.1	AFTN level of service	Validate that the AMHS level of service and functionalities are at least equivalent to that of the AFTN
3.1.1	Message transfer	Validate that the AMHS provides for store-and-forward message transfer
3.1.2	Multiple recipients	Validate that the AMHS accepts and conveys messages with multiple recipients
3.1.3	Distribution lists	Validate that the AMHS accepts and conveys messages addressed to pre-determined lists of multiple recipients
3.1.4	Message priorities	Validate that the AMHS conveys messages with at least three different priority levels
3.1.5	Message identification	Validate that the AMHS allows each message to be uniquely identified
3.1.6	Message continuity	Validate that the AMHS avoids loss of messages
3.1.7	Message integrity	Validate that the AMHS avoids corruption of messages during conveyance
3.1.8	Long-term logging	Validate that the AMHS provides for 30-days administrative logging
3.2	AFTN parameters	Validate that the AMHS conveys information elements semantically equivalent to each AFTN parameter
3.2.1	Priority indicator	Validate that the AMHS conveys an element equivalent to a five-value priority indicator
3.2.2	Filing time	Validate that the AMHS conveys an element equivalent to a message filing time
3.2.3	Originator indicator	Validate that the AMHS conveys an element equivalent to the message originator indicator
3.2.4	Addressee indicator(s)	Validate that the AMHS conveys an element equivalent to the message addressee indicator(s)
3.2.5	Optional heading information	Validate that the AMHS conveys an element equivalent to the optional heading information
3.2.6	Message text	Validate that the AMHS conveys an element equivalent to the optional heading information

3.3	Transparency	Validate that an AFTN user may interwork with the AMHS without knowledge of the AMHS environment
3.4	Reversibility	Validate that an AFTN message entering the AMHS at an AFTN/AMHS Gateway exits the AMHS unchanged at another AFTN/AMHS Gateway as far as elements with end-to-end semantic value are concerned
4	ATS Message Server	Validate the specified ATS Message Server provisions
4.1	AMH22 compliance	Validate the compliance with the AMH22 Profile as specified in ISO MHS ISPs
4.2	Use of transport service	Validate the specific use of the Transport Service
4.2.1	QoS (RER)	Validate the use of the Residual Error Rate parameter
4.2.2	Transport Priority	Validate the use of the Transport Connection Priority parameter
4.2.3	Traffic Type	Validate the use of the Traffic Type parameter
4.3	Traffic logging	Validate that the ATS Message Server records sufficient information for message tracking over a thirty days period
5	ATS Message User Agent	Validate the specified ATS Message User Agent provisions
5.1	AMH21 compliance	Validate the compliance with the AMH21 Profile as specified in ISO MHS ISPs
5.2	ATS Message format	Validate that the specific ATS Message Header can be generated at an originating user's UA, and displayed at a receiving user's UA

6	AFTN/AMHS Gateway	Validate the specified AFTN/AMHS Gateway provisions
6.1	AFTN Component	Validate that the AFTN Component of the AFTN/AMHS Gateway as specified in the MHS SARPs comply with the basic AFTN functional capability to the stated extent
6.1.1	AFTN interface	Validate the interworking of the AFTN Component with the associated AFTN centre provides for the exchange of all AFTN messages between the AFTN Component and the AFTN.
6.1.2	AFTN control	Validate that the implemented communication protocols between the gateway and the AFTN centre will suspend message exchange when the gateway is unable to receive additional messages and automatically resume operation when the gateway is capable of receiving messages again.
6.1.3	Short retention	Validate that the AFTN Component provides short term retention of messages to accomplish recovery of transmission errors, and short term interruptions to service
6.1.4	AFTN logging	Validate that the AFTN Component properly logs the required message history data for all messages sent and received from the AFTN.
6.1.5	AFTN isolation	Validate that the AFTN Component isolates the MTCU Component from all procedures associated with the AFTN
6.2	ATN Component	Validate that the ATN Component of the AFTN/AMHS Gateway as specified in the MHS SARPs comply with the AMHS functional capability to the stated extent
6.2.1	AMHS interface	Validate that the ATN Component interface to the AMHS enables peer-to-peer communication with an ATS Message Server or with another AFTN/AMHS Gateway
6.2.2	AMHS functionality	Validate that the ATN Component incorporates the functionality of an ATS Message Server
6.2.3	AMHS logging	Validate that the ATN Component properly logs the required history data for all reports and messages sent and received from the AMHS
6.3	MTCU	Validate the specified MTCU Component provisions
6.3.1	ATN Component interface	Validate that the MTCU Component functions correctly with the abstract-operations implemented with the ATN Component

6.3.2	AFTN Component interface	Validate that the MTCU Component functions correctly with the procedures implemented with the AFTN Component
6.3.3	MTCU conversion provisions	Validate the specified provisions for the bi-directional mapping of information objects
6.3.3.1	Address mapping	Validate that the MTCU provides a method of mapping any received AFTN address to an ATN address
6.3.3.2	Incoming AMHS message	Validate that an incoming AMHS message is properly converted into an AFTN message, if it bears information which may be conveyed in the AFTN, or that it is rejected using standard AMHS mechanisms
6.3.3.2.1	Incoming AMHS IPM	Validate that an incoming AMHS IPM is properly converted into an AFTN message
6.3.3.2.2	Incoming AMHS IPN	Validate that an incoming AMHS IPN is properly converted into an AFTN service message
6.3.3.3	incoming AMHS report	Validate that an incoming AMHS report is properly converted into an AFTN service message or discarded depending on its category and on the non-delivery rason and diagnostic it conveys, if any
6.3.3.4	incoming AMHS probe	Validate that an incoming AMHS message is properly handled to determine the convertibility of an equivalent message
6.3.3.5	incoming AFTN message	Validate that an incoming AFTN message is properly converted into an AMHS message, if it is not an AFTN service message
6.3.3.6	incoming AFTN acknowledgement service message	Validate that an incoming AFTN acknowledgement service message is converted into an AMHS IPN to the stated extent
6.3.3.7	incoming AFTN unknown address service message	Validate that an incoming AFTN unknown address service message is converted into an AMHS NDR to the stated extent
6.3.4	MTCU logging	Validate that the MTCU records sufficient information for tracking of received and converted information objects over a thirty days period
6.4	Control position	Validate that the control position is informed of any outstanding event at the AFTN/AMHS Gateway for further action

3. Validation Methods

3.1 The following validation methods have been identified:

IA Inspection and Analysis. The SARPs requirement can be judged to be valid or invalid based on a paper analysis. This includes verification that the requirement is consistent with other requirements, and that it is unambiguous.

S Simulation. The SARPs requirement can be validated by a simulation of some aspect(s) of the target environment.

FM Formal modeling. The SARPs requirement can be validated by use of a formal model. The model must ensure that the modeled entity is free from deadlocks, loops, invalid state transitions, ambiguous behavior, etc.

PI Prototype implementation. The SARPs requirement can be validated by specifying and implementing a concrete realization.

IW The SARPs requirement can be validated by demonstrating full interoperability between two independent implementations. Interoperability testing between independent implementations will help ensure there are no ambiguities or omissions in the draft SARPs.

TE Target environment testing. The requirement can only be validated by testing in the real target environment.

EJ Engineering judgment. The requirement can be validated based on experience with similar requirements.

OP Operational experience. The requirement can be validated based on proven operational experience in an operational system where the function is the same as, or exceeds, the draft SARPs requirement.

3.2 The Validation Objectives are proposed to be validated by the means stated in Table 3-1.

Table 3-1 Methods for Draft MHS SARPs (ATS Message Service) Validation

VO	Short Name	Validation Means	Comments
1	ISO compliance	IA	
1.1	MHS compliance	IA	
1.1.1	ISP compliance	IA	
1.2	Interworking	IW	
1.3	Migration	IA	

2	AMHS SLRs		
2.1	AMHS naming and addressing	IA	
2.1.1	O/R names	IA, PI	
2.2	AMHS management domains	IA	
2.3	AMHS routing	IA, TE	
2.4	AMHS long-term logging	IA	
3	AFTN interworking		
3.1	AFTN level of service	IA	
3.1.1	Message transfer	IA	
3.1.2	Multiple recipients	IA	
3.1.3	Distribution lists	IA	
3.1.4	Message priorities	IA	
3.1.5	Message identification	IA	
3.1.6	Message continuity	IA	
3.1.7	Message integrity	IA	
3.1.8	Long-term logging	IA	
3.2	AFTN parameters	IA	
3.2.1	Priority indicator	IA	
3.2.2	Filing time	IA	
3.2.3	Originator indicator	IA	
3.2.4	Addressee indicator(s)	IA	
3.2.5	Optional heading information	IA	

3.2.6	Message text	IA	
3.3	Transparency	IW	
3.4	Reversibility	IW	
4	ATS Message Server		
4.1	AMH22 compliance	IA	Credit may be taken for existing standards and implementations
4.2	Use of transport service	IA, PI	
4.2.1	QoS (RER)	IA, PI	
4.2.2	Transport Priority	IA, PI	
4.2.3	Traffic Type	IA, PI	
4.3	Traffic logging	IA, PI	
5	ATS Message User Agent		
5.1	AMH21 compliance	IA	Credit may be taken for existing standards and implementations
5.2	ATS Message format	PI, IW	
6	AFTN/AMHS Gateway	PI	
6.1	AFTN Component	IA	
6.1.1	AFTN interface	IA	
6.1.2	AFTN control	IA	
6.1.3	Short retention	IA	
6.1.4	AFTN logging	IA	
6.1.5	AFTN isolation	IA	
6.2	ATN Component	IA	
6.2.1	AMHS interface	IA, IW	
6.2.2	AMHS functionality	IA	

6.2.3	AMHS logging	IA	
6.3	MTCU	PI	
6.3.1	ATN Component interface	PI	
6.3.2	AFTN Component interface	PI	
6.3.3	MTCU conversion provisions	PI	
6.3.3.1	Address mapping	PI, TE	
6.3.3.2	Incoming AMHS message	PI	
6.3.3.2.1	Incoming AMHS IPM	PI	
6.3.3.2.2	Incoming AMHS IPN	PI	
6.3.3.3	incoming AMHS report	PI	
6.3.3.4	incoming AMHS probe	PI	
6.3.3.5	incoming AFTN message	PI	
6.3.3.6	incoming AFTN acknowledgement service message	PI	
6.3.3.7	incoming AFTN unknown address service message	PI	
6.3.4	MTCU logging	PI	
6.4	Control position	PI	

4. Dependencies on External Standards

The MHS SARPs (ATS Message Service) incorporate by reference ISO standards and ISPs. A potential advantage of using ISO standards and ISPs is that they are pre-validated, i.e. studied and approved by national standards bodies, implemented and interoperability demonstrated between independent implementations. To benefit from such pre-validation, the validation status of each referenced standard needs to be verified. For each referenced external standard, the following points must be answered:

- What is the status of the standard (committee draft, draft or fully ratified)
- Do implementations exist?
- Has interoperability been demonstrated?
- Are there any outstanding defect reports?
- Are the references in the SARPs sufficiently precise (version no, amendments and defect reports included)?

4.1. ISO/IEC 10021

ISO/IEC 10021 has been a multi-part standard since 1990. A number of compliant implementations exist, and have demonstrated interoperability. A number of technical corrigenda has been published for each part of the standard, leading to a very mature and stable set of standards.

The reference in the SARPs to ISO/IEC 10021 are general in nature. Compliance in the SARPs is expressed by reference to the ISO/IEC MHS ISPs (see 4.2) which themselves make clear and accurate references to the different parts of ISO/IEC 10021, taking the aforementioned technical corrigenda into account.

4.2. ISO/IEC ISP 10611

ISO/IEC ISP 10611 has been an international standardized profile since 1994. Since interoperability is ensured by the standard there is no need to ensure it at this level.

The accurate level of implementations with respect to this ISP need to be determined, in particular concerning the support of optional functional groups, such as the Distribution List Functional Group which is a mandatory requirement in the MHS SARPs.

The SARPs constantly refer to the ISP, and more precisely the AFTN/AMHS Gateway PRLs are derived from the ISPICS appended to the ISP to ensure clear and unambiguous referencing.

4.3. ISO/IEC ISP 12062

ISO/IEC ISP 12062 has been an international standardized profile since 1994.

The accurate level of implementations with respect to this ISP need to be determined, in particular concerning the support of IPM body parts in relation with the MHS SARPs requirements.

The SARPs constantly refer to the ISP, and more precisely the AFTN/AMHS Gateway PRLs are derived from the ISPICS appended to the ISP to ensure clear and unambiguous referencing.

4.4. Upper Layer architecture (RTSE, ACSE, Presentation and Session)

The Upper Layer architecture used in the MHS SARPs (ATS Message Service) is dictated by the reference to the aforementioned standards and ISPs.

The ISO MHS standards rely upon a "traditional" upper layer architecture, using in particular "full-functionality" presentation and session layers. This architecture does not make use of the recent efficiency enhancements used in Sub-Volume 4. However one benefit of this architecture is that it has been demonstrated, mature and stable for long, and it has been widely implemented.

The ISPs refer themselves to other ISPs concerning the Upper Layer profiles, which are based on these mature standards.

5. Recommendations

It is recommended that the validation approach proposed in this paper should be adopted by ATNP/WG3 and followed by the States who are performing validation.