EUR AMHS Manual

EUR AMHS Manual	
Document Reference:	EUR AMHS Manual, Main Part
Author:	Planning Group
Revision Number:	Version 20.0
Date:	22/04/2026
Filename:	EUR_AMHS_Manual_v20_0.doc

Document Control Log

Edition	Date	Comments	section/pages affected
0.1	29/11/2001	Creation of the document.	all
0.2	13/03/2002	Incorporation of comments of FPG Meetings in Geneva and Berlin	all
0.3	19/03/2002	Incorporation of comments from Switzerland	Annex D
0.4	28/03/2002	Incorporation of comments to paragraph 1.1.4; presentation to AFSG/5 (April 2002)	1.1.4
0.5	28/02/2003	Incorporation of comments of AFSG/5; updates and new sections and new chapter, presentation to AFSG/6 (April 2003)	3.1, 3.2, 4.3, 5., 9.1
0.6	09/08/2005	Revision of the document structure, updates of chapters, new sections	all
0.7	03/02/2006	Inclusion of new and updates of sections and chapters, update of statistic paragraphs, deletion of CIDIN/AMHS Gateway requirements	1, 2.2.3.2, 7, 8.1, 5.9, 6.4.5.2, early 9.1.2.6
0.8	09/03/2006	Editorials, reformatting of the notes, updates of chapters, new sections	all 3.5, 6.1.5, 6.5, 8.5.1
0.9	19/03/2006	Editorial refinements of chapters and sections	1, 2.2.1, 3.5, 6.4.1, 6.5
1.0	27/04/2006	Adopted version (AFSG/9)	
1.1	13/03/2007	Editorial updates, incorporation of CP06-002, CP06-003 and CP06-004, Update of Appendices A - F (CP06-001, CP07-001)	all 7.3.2.2, 7.3.2.3, 8.2
2.0	26/04/2007	Adopted version (AFSG/10)	
2.1	19/03/2008	Incorporation of CP-AMHSM-08-004	5.9
3.0	24/04/2008	Adopted version (AFSG/11)	
3.1	17/11/2008	Change of references from ICAO Doc 9705 to ICAO Doc 9880 (CP-AMHSM-08-006), editorial improvements	all
3.2	12/12/2008	Incorporation of comments of PG M34 meeting, inclusion of ACP WG M Amendment Procedure	 Attachment B

3.3	08/02/2009	Incorporation of CP-AMHSM-08-005, CP-AMHSM-08-007, CP-AMHSM-08-008,	3.5, 3.6 and 5.2, 2.2, 3.2, 4.3, 9.1
3.4	11/02/2009	Incorporation of CP-AMHSM-09-002	3.3 and 3.4
3.5	11/03/2009	Update of the referenced documents	References
4.0	02/04/2009	Adopted version (AFSG/12)	
4.1	12/03/2010	Incorporation of CP-AMHSM-09-004 and CP-AMHSM-09-005	References, 2.1.3.3, 2.2.3.1, 3.6.1
5.0	17/06/2010	Adopted version (AFSG/14)	
5.1	24/09/2010	Incorporation of CP-AMHSM-10-001, minor editorial updates	References
5.2	30/11/2010	Removal of CAMAL from the reference list	References
6.0	14/04/2011	Adopted version (AFSG/15)	
6.1	19/03/2012	Incorporation of CP-AMHSM-11-001 and CP-AMHSM-12-001, CP-AMHS-12-002	3.2.5.4, 9.1.3, 9.2, 3.7, 4.4
7.0	26/04/2012	Adopted version (AFSG/16)	
7.1	25/03/2013	Incorporation of CP-AMHSM-12-003, CP-AMHSM-12-005 CP-AMHSM-12-007, CP-AMHSM-12-010	6.5.3, 1.5, 3.7.1, 8.3, 8.4,
8.0	25/04/2013	Adopted version (AFSG/17)	
8.1	12/03/2014	Incorporation of CP-AMHSM-12-014, CP-AMHSM-13-007, CP-AMHSM-14-002 CP-AMHSM-13-005	3.1.3.2, 3.5.4, 5.2.2, 8.4, 3.2.4.2.1.2, 3.2.7.2.4, 5.2.6, 5.2.10, 5.6.3, 5.7.1, 5.8.1, 5.9.6, 6.4.1.3
9.0	10/04/2014	Adopted version (AFSG/18)	
9.1	19/03/2015	Incorporation of CP-AMHSM-14-004	all
9.2	22/03/2015	Incorporation of CP-AMHSM-14-010	8.4, 8.5
9.3	23/03/2015	Incorporation of CP-AMHSM-15-001, Incorporation of CP-AMHSM-15-003, Incorporation of CP-AMHSM-15-005	All 3.2.8.1.2, 1.5, 7.1.3
10.0	23/04/2015	Adopted version (AFSG/19)	

10.1	04/04/2016	Incorporation of CP-AMHSM-15-004	3.2
11.0	26/04/2016	Adopted version (AFSG/20)	
11.1	31/03/2017	Incorporation of CP-AMHSM-15-011, Incorporation of CP-AMHSM-16-007 Incorporation of CP-AMHSM-16-008 Incorporation of CP-AMHSM-16-010 Incorporation of CP-AMHSM-16-012	8.6, References, 1.5, 7.3.2.2, 4.5
12.0	28/04/2017	Adopted version (AFSG/21)	
12.1	23/04/2018	Incorporation of CP-AMHSM-17-005, Incorporation of CP-AMHSM-17-004, Incorporation of CP-AMHSM-16-009	8.2.3 References, 2.1.3.4, 8.4, 8.6, 9.1.2.5
13.0	27/04/2018	Adopted version (AFSG/22)	
13.1	15/02/2019	Incorporation of DR-AMHSM-18-001, CP-AMHSM-18-003	8.6.3.1.2
14.0	05/03/2019	Adopted version (AFSG/23)	
14.1	26/11/2019	Incorporation of CP-AMHS-19-002 Adaption: According to COG/74&RCOG/11 Decision /4, Approval of AFS to SWIM Transition Task Force (AST TF) Terms of Reference (ToR) and coherent Work Programme, the Author of EUR Doc 020 changed from “AFSG PG” to “AST PG”.	all
15.0	12/11/2020	Adopted version (AST TF/01)	
16.0	20/10/2021	Adopted version (AST TF/02)	
16.1	30/05/2023	Incorporation of CP-AMHSM-23-001	8.5
17.0	16/05/2023	Adopted version (AST TF/04)	
17.1	31/05/2024	Incorporation of CP-AMHSM-24-001	Section 2.2.4
18.0	18/06/2024	Adopted version (AST TF/05)	
18.1	11/04/2025	Incorporation of CP-AMHSM-25-001, CP-AMHSM-24-003	2.1.1, 5.10 (new), 8.4, 9.1.2
19.0	05/05/2025	Adopted version (AST TF/06)	
19.1	01/04/2026	Incorporation of CP-AMHSM-25-003	5.10.7
20.0	22/04/2026	Adopted version (AST TF/07)	

Scope of the Document

This document has been developed by the ICAO EUR Aeronautical Fixed Service Group (AFSG), which was replaced in 2019 by ICAO EUR AFS to SWIM Transition Task Force (AST TF) according to COG/74&RCOG/11 Decision /4, in order to present a comprehensive collection of information pertaining to the implementation of ATSMHS in the ICAO EUR Region.

It is intended that the document will evolve into an EUR ICAO Document containing guidance material on EUR AMHS implementation.

Table of contents

LIST OF APPENDICES OF THE EUR AMHS MANUAL

References

ICAO Documentation

[1] ICAO Annex 10 – Aeronautical Telecommunications, Volume II and Volume III

[2] ICAO Annex 11 – Air Traffic Services

[3] ICAO Doc 9880-AN/466: Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI Standards and Protocols, Part II – Ground-Ground Applications - Air Traffic Services Message Handling Services (ATSMHS), Second Edition – 2016

[4] ICAO Doc 9880-AN/466: Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI Standards and Protocols, Part III – Upper Layer Communications Service (ULCS) and Internet Communications Service (ICS) , Second Edition – 2016

[5] ICAO Doc 9880-AN/466: Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI Standards and Protocols, Part IV – Directory Services, Security and Identifier Registration, Second Edition – 2016

[6] ICAO Doc 9896: Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocols, Second Edition – 2015

[7] ICAO Doc 7910, Location Indicators,

[8] ICAO Doc 8585, Designators for Aircraft Operating Agencies, Aeronautical Authorities and Services

[9] ICAO Doc 8259-AN/936: Manual on the Planning and Engineering of the Aeronautical Fixed Telecommunication Network, Fifth Edition – 1991

[10] ICAO Doc 7754, European (EUR) Air Navigation Plan, Volume I

[11] ICAO Doc 7754, European (EUR) Air Navigation Plan, Volume II, Working Copy

[12] EUR Doc 021, ATS Messaging Management Manual

SPACE Documentation

[13] WP201 – Location of AMHS message servers and AFTN/AMHS gateways, SPACE/NATS/201/WPR/034, Version 2.0, 30/06/2002

[14] WP202 – Specification of European AMHS performance objectives, SPACE/EURO/202/WPR/045, Version 2.0, 30/06/2002

[15] WP211 – Topology between servers and gateways, SPACE/DFS/211/WPR/059, 2.0, 08/11/2002

[16] WP223 – Study of routing strategy in SPSOs, SPACE/STNA/223/WPR/120, Version 2.0, 11/11/2002

[17] WP232 – AMHS security issues in SPACE participating States/ Organisations, SPACE/Eurocontrol/232/WPR/047, Version 1.0, 13/09/2001

[18] WP233 – AMHS institutional and financial issues in SPACE participating States/ Organisations, SPACE/STNA/233/WPR/192, Version 1.0, 11/09/2002

[19] WP234 – Analyse requirements for System Management at AMHS level, SPACE/NATS/234/WPR/051, Version 2.0, 30/06/2002

[20] WP411 – SPACE Final Report, SPACE/STNA/411/WPR/224, Version 1.0, 02/12/2002

General technical literature

[21] ISO/IEC 10021-2: Information Technology – Message Handling Systems (MHS): Overall architecture

[22] ISO/IEC 10021-10 International Standard, Information technology – Message Handling Systems (MHS): MHS routing (1998)

Table of Figures

Index of Tables

1 Structure of the EUR AMHS Manual

1.1 The EUR AMHS Manual consists of the “Main Part” and the Appendices.

1.2 In the main part, the following Chapters have been introduced, with the view to provide general guidance and detailed information on requirements concerning AMHS implementation in the EUR Region.

1. Introduction
2. EUR AMHS Requirements
3. European ATS Messaging Service Profile
4. System implementation - Guidelines for system requirements
5. AMHS management
6. Tests and validation of systems
7. Operational procedures and Recommendations
8. Miscellaneous

1.3 Then, for easy reference, the Change Control Mechanism of the EUR AMHS Manual has been included as Attachment A.

1.4 Finally, for better presentation and management, detailed documents, which have been produced on particular subjects initially addressed in the main body of the Manual, have been included as Appendices to the Manual.

1.5 The following Appendices to the EUR AMHS Manual have been produced:

- Appendix A: Abbreviations, Glossary and Definitions
- Appendix B: European ATS Messaging Service Profile
- Appendix C: AMHS Testing Requirements
- Appendix D: AMHS Conformance Tests and
  Appendix D-UA: AMHS UA Conformance Tests
- Appendix E: AMHS Interoperability Tests
- Appendix F: AMHS Pre-operational Tests
- Appendix G: European Directory Service (EDS), Appendix G-A: EDS User Interface Control Document, Appendix G-B: EDS Data Description and Appendix G-C: EDS Testing Guidelines
- Appendix H: Application/Service oriented AMHS Profiles

1.6 *Note.– The EUR AMHS Manual is a "living" document. The Planning Group of the AST TF, as the editor, has collected necessary and relevant information to be used for the Regional deployment of AMHS. All interested partners are invited to contribute. Do not hesitate to contact the Planning Group; each comment, remark or correction is welcome.*

2 Introduction

2.1 Background Information

2.1.1 AFS

2.1.1.1 The Aeronautical Fixed Service provides, among other things, for the exchange of messages pertaining to the safety of air navigation and the regular, efficient and economical operation of air services.

2.1.1.2 The following categories of message are handled by the AFS:

- distress and urgency messages
- flight safety messages
- meteorological messages
- flight regularity messages
- aeronautical information services messages
- administrative messages
- AFTN service messages

2.1.1.3 The principal users of messages in the above categories are ATS and the AIS, ATFM, MET and SAR Services which support and complement the ATS.

2.1.2 AFTN/CIDIN

2.1.2.1 Initially, the operational requirements for such an information exchange were met by the development of the Aeronautical Fixed Telecommunications Network.
The AFTN provides a store-and-forward messaging service for the conveyance of text messages in ITA-2 or IA-5 format, using character-oriented procedures.
Although AFTN served its purpose well for many years, AFTN technology has become outdated due to the fact that is remains bound to its telex/telegraphic origins.

2.1.2.2 One major step towards overcoming the limitations of the AFTN was taken with the introduction of the Common ICAO Data Interchange Network, which is based on packet switching techniques.
The CIDIN provides a common transport service for the conveyance of binary or text application messages in an expeditious and reliable manner.
In the EUR Region, the CIDIN provides the enhanced backbone data communications infrastructure for the AFTN and a general data communications service to non-AFTN applications such as OPMET.

2.1.3 AMHS

2.1.3.1 The most recent development with regard to messaging in the ATS environment is the AMHS. The AMHS is a natural evolution from AFTN/CIDIN, replacing the telegraphic style of working with a modern Message Handling System based on international Standards.

2.1.3.2 It is presumed that the ATSMHS, being an ATN application, utilises the infrastructure of the ATN internetwork. However this is not a prerequisite for the initial deployment of the ATSMHS.

2.1.3.3 There are several advantages of AMHS over AFTN/CIDIN including:

- increased speed, capacity and throughput
- enhanced reliability
- extended functionality
- interoperability with other global messaging services
- security capabilities
- use of COTS equipment and services

Furthermore, AMHS offers services meeting non-AFTN communication requirements.

2.1.3.4 The provisions pertaining to ATSMHS, such as SARPs, technical specifications and general guidance material, are contained in the following ICAO documents, which constitute the main references for this Manual.

- Annex 10, Volume II, Chapter 4 [1]
- Annex 10, Volume III, Part I, Chapter 3 [1]
- Doc 9880 Part II [3]
- ICAO EUR ANP, Volume I [10]
- ICAO EUR ANP, Volume II [11]

2.1.4 ACCESS and SPACE

2.1.4.1 ACCESS Project

2.1.4.1.1 The "ATN Compliant Communications - European Strategy Study" (ACCESS) project was undertaken between January 1997 and March 1999 by National Air Traffic Services Ltd (NATS), the Service Technique de la Navigation Aérienne (STNA) and the Deutsche Flugsicherung (DFS) and part-funded from the European Commission's programme for financial aid in the field of Trans-European Networks - Transport (TEN-T).

2.1.4.1.2 As TEN-T ATM Project 1996-GB-94-S, "Aeronautical Telecommunications Network -Implementation Feasibility Studies", the main objectives of the study were:

a) Development of an ATN Architecture;

b) Development of an Implementation Plan in the European core area in conjunction with EUROCONTROL;

c) Interoperability and validation trials between States using ATN-compliant ATS Message Handling Services.

2.1.4.1.3 The geographical area considered in the ACCESS study comprised the following countries: Belgium, France, Germany, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain and the United Kingdom. These States were chosen for the following reasons:

a) They had a direct connection to the European Central Flow Management Unit and/or were involved in the control of North Atlantic traffic;

b) The study was representative of both Oceanic and Continental ATC.

However, the architectural principles proposed in this Study are also applicable to the whole European area.

2.1.4.1.4 Similarly, whilst the ATN is designed to accommodate all aeronautical communications, the ACCESS Study concentrated on those directly related to the provision of Air Traffic Services (ATS). The other users of the ATN were not ignored, but the resulting network architecture does not consider those user requirements. However, this does not invalidate the design of the ATN in this study.

2.1.4.2 SPACE Project

2.1.4.2.1 The SPACE (Study and Planning of AMHS Communications in Europe) Project is a European Commission Project co-funded by the Commission of the European Union in the framework of the TEN-T ATM Programme. This project is run by a consortium of the following European States and Organisations: France (DGAC/STNA), Germany (DFS GmbH), Spain (Aena), United Kingdom (NATS Ltd) and the EUROCONTROL Agency.

2.1.4.2.2 The overall objective of SPACE is to develop plans to upgrade the current European-wide AFTN messaging system and to replace it using X.400 compliant systems based on the AMHS technical specifications developed by the ICAO ATN Panel and contained in Doc 9880, Part II (old Sub-Volume 3 of ICAO Doc 9705).

2.1.4.2.3 The SPACE Project comprises the following main phases:

- Phase 1: Definition of a European AMHS addressing plan;
- Phase 2: Technical design for the European AMHS; and
- Phase 3: Overall implementation plan.

2.1.4.2.4 The deliverables of the project complement the SARPs and technical specifications by addressing technical issues that are generally of an implementation nature such as:

- the location of servers and gateways;
- the definition of performance objectives;
- the definition of address conversion and routing strategy;
- etc.

2.1.4.2.5 One of the major deliverables of the SPACE Project is the definition of a common unique world-wide addressing scheme. This scheme - the Common AMHS Addressing Scheme (CAAS) - has subsequently been endorsed by the AFSG and the ATN Panel working groups and included in old Edition 3 of ICAO Doc 9705 which was replaced by Doc 9880, Part II.

2.1.4.2.6 The overall implementation plan is developed primarily for the benefit of the partners of the SPACE Consortium but is complemented by a set of extensibility principles in order to help other States and Organisations in planning the deployment of their own AMHS system.

2.2 ATSMHS Overview

2.2.1 General

2.2.1.1 The ATN technical specifications for the Air Traffic Services Message-Handling Service (ATSMHS) define the ICAO store and forward messaging service used to exchange ATS messages between users over the ATN internet.

2.2.1.2 The set of computing and communication resources implemented by Air Navigation Service Providers (ANSP) to provide the ATS Message Handling Service is commonly referred to as AMHS (ATS Message Handling System).
The ATS Message Handling System technical specifications are compliant with mature message handling systems standards such as ISO/IEC 10021 [22] and ITU-T X.400.

2.2.2 Functional Components

In terms of functionality, the ATSMHS comprises the following components:

(a) the Message Transfer Agent (MTA) which performs the function of the message switch,
(b) the User Agent (UA) which performs the user access to the MTA and provides an appropriate user interface,
(c) the Message Store (MS) which provides the intermediary storage between MTA and UA and is usually co-located with the MTA, and
(d) the Access Unit (AU) which provides for intercommunication with other Messaging Systems.

2.2.3 End systems

2.2.3.1 Three categories of ATN end systems are defined for the support of the ATS Message Handling Service:

- the ATS message server
- the ATS message user agent
- the AFTN/AMHS Gateway

2.2.3.2 Together, these systems provide connectivity between users at ATN end systems and users at AFTN Stations in three different end-to-end configurations:

a) from an AFTN/CIDIN Station to another AFTN Station over the ATN;
b) from an AFTN/CIDIN Station to an ATN End System, and vice versa;
c) from an ATN End System to another ATN End System.

2.2.4 Levels of service

2.2.4.1 Two levels of service are defined within the ATS Message Handling Service:

1. The Basic ATS Message Handling Service;
2. The Extended ATS Message Handling Service.

2.2.4.2 The Basic ATS Message Handling Service meets the basic requirements of the MHS Profiles published by ISO as International Standardized Profiles (ISPs), and it incorporates additional features to support the service offered by the AFTN.

2.2.4.3 Compared to the service of the AFTN, the Basic ATS Message Handling Service offers some significant improvements such as:

- practically unlimited message length;
- virtually no limit on the number of addressees of a message;
- provision of non-delivery reports;
- indication of the subject of a message.

2.2.4.4 The Extended ATS Message Handling Service provides functionality in addition to those of the Basic ATS Message Handling Service such as the introduction of directory services and security mechanisms. With the directory services it is possible to obtain information about ATN, address mapping and other application and services participating in the ATN. In the extended ATSMHS, it is possible to provide the security services of message origin authentication and content integrity.

2.2.4.5 Furthermore, in addition to text messages, the extended service allows for the transfer of binary coded data, files etc. File-transfer body parts shall be used for the conveyance of binary data. When conveying binary data, it is possible to avoid the generation of a textual body part in order to carry the ATS message parameters of the ATS-message-Header, namely the ATS-message-Priority, ATS-message-Filing-Time and the ATS-message-Optional-Heading-Info. The respective IPM heading fields extensions and recipients-extensions supported by the extended ATSMHS supports can be used for that purpose.

2.2.4.6 The Extended ATS Message Handling Service is backwards compatible with the Basic ATS Message Handling Service.

2.2.5 Inter-operability

2.2.5.1 During the transition phase from the AFTN or the CIDIN to the AMHS the interoperability between systems is achieved by the use of the AFTN/AMHS Gateway.

2.2.5.2 The technical specifications for the AFTN/AMHS Gateway have been defined by ICAO.

3 EUR AMHS Requirements

3.1 Quality of Service Requirements

3.1.1 Scope

3.1.1.1 The purpose of this section is to define quality of service (QoS) requirements and set target performance objectives for the European AMHS. To this end, the properties of the AMHS are considered from the outside of the network, i.e. at its boundary, without taking into account the way in which the service, as defined on its boundary, is provided from within the network.

3.1.1.2 The performance requirements dealt with in this section are the common understanding on what the applications will get in terms of performance and what level of performance the network has to provide. The performance parameters are therefore necessary for designing applications as well as the network itself.

3.1.1.3 This section is organised as follows:

3.1.1.3.1 First, a collection of terms and concepts is set up for discussing quantitative properties of the service delivered by the AMHS.

3.1.1.3.2 Second, numerical values for performance parameters are defined using the following input:

- anticipated location of message servers and gateways;
- analysis of existing and projected message flows in the EUR area based on presently available information;
- general design principles;
- user expertise.

3.1.1.4 As in most cases, in order to arrive at concrete values for the performance parameters, a number of assumptions and restrictions are made:

- QoS is not dependent on traffic volumes;
- QoS is measured between originator-recipient pairs;
- QoS is not geographically dependent;
- QoS is not dependent on time;
- QoS represents worst case performance;
- the underlying network should be sized to accommodate QoS;
- degree of corruption is not relevant to the Corruption QoS parameter;
- corruption is not dependent on message size;
- non reachability due to network causes is typically of the order of a few minutes (60 per year);
- the bit error rate of an HDLC link is of the order 10^{-11}.

3.1.2 Quantitative approach

3.1.2.1 The formal analysis and formulation of network performance requirements is a difficult task and the pragmatic solution often adopted is to over-dimension the network, resulting in sufficient capacity and service assurance but also significantly higher costs. At a time when ANSPs are becoming increasingly cost conscious, this solution is not acceptable.

This sub-section gives an overview of the problems of quantitative analysis of message handling with special reference to the AMHS.

Existing networks are studied and existing literature and study results (EATCHIP, ACCESS, SPACE) are used.

3.1.2.1.1 Comparison with the development of CIDIN

The introduction of CIDIN in Europe was done with new technology over a period of 15 years, with no overall CIDIN capacity planning. The CIDIN development is characterised by continual upgrading.

In the case of the AMHS, the technology is not new, but is well tried. For this reason it makes sense to establish quantitative performance requirements for it from the beginning. Unfortunately, there is very little experience available and techniques for the specification of performance requirements for message handling systems do not exist.

3.1.2.1.2 The process of continual upgrading

Since the task of specifying numerical requirements is so difficult, most networks experience a process of continual upgrading in order to correct errors in the initial numerical requirements estimates but also to cope with increasing demands on performance. A typical approach of network operators is to keep utilisation of individual network components below a certain level, e.g. 50%. As soon as this level is reached in a component, it is upgraded. This is based on the experience that when components reach high utilisation levels, highly non-linear effects occur and the performance of the network as a whole is no longer predictable.

3.1.2.1.3 EATCHIP – Application requirements for data communications services

In the framework of EATCHIP[1] a study of requirements which ATC applications place on data communications services was conducted. The results of this study, collated in a report titled "Application Requirements for Data Communication Services" have been used as an initial source of information. It must be pointed out that this study was performed with little regard to the actual networks which provide or should provide data communications services.

3.1.2.1.4 ACCESS - ATN Compliant Communications European Strategy Study[2]

This study investigated the ways in which user requirements placed on data transmission through the ATN Internet could be modelled. Although there are significant differences between the behaviour of packets in a connectionless network infrastructure and the behaviour of messages, the modelling approach defined in this study provides valuable insight into the problem of determining QoS parameters.

3.1.2.1.5 SPACE – Study and Planning of AMHS Communications in Europe[3]

---

1 EATCHIP : European ATC Harmonisation and Implementation Programme

2 Project run under the Trans-European Networks for Transport (TEN-T), ATM Task 1996-GB-94-S

3 Project run under the Trans-European Networks for Transport (TEN-T), ATM Task FR/98/228

As part of the SPACE project, a specific work package defined performance parameters and set corresponding numerical values in order to capture all performance aspects that are relevant to the European AMHS. Results of this work package are extensively used in this section.

3.1.2.2 Quantitative aspects of the AMHS

3.1.2.2.1 Messages as the basis of the analysis

In dimensioning the AMHS only complete messages should be considered for the following reasons:

- the message is the basic unit of data at the user interface;
- whole messages are stored and forwarded by MTAs in the network;
- in formulating performance requirements, transport or sub-network performance is not taken into account.

Of course, in dimensioning the network, it will be necessary to consider performance aspects of lower level infrastructure as well, but as a result of the user requirements formulated in this document and their impact on MTA performance.

Further, it is important to note that the specification of performance requirements is based on individual messages, independently of all other messages.

When considering message size, only the volume of user information is relevant since the user has no control (or only very limited control) over the data overhead involved in message handling.

Formulating performance requirements of a given user, taking into account the simultaneous use of the network by other users, does not appear to be feasible. However, it has to be recognised that, in a real world situation, the performance of the network for a given message certainly does depend on the presence of other messages currently being processed. The performance requirements specified here represent minimum or worst-case performance under the load conditions (Traffic Volume Requirements) identified in the framework of the SPACE project.

3.1.2.2.2 Types of performance parameters

There are two distinct groups of performance parameters to be considered in connection with the AMHS.

Parameters not dependent on message volumes: These parameters describe the quality of service (QoS), which is available to each individual message considered by itself, e.g. transit time. They can be measured, i.e. they are the quantitative results of the way in which messages are handled by the network.

Message volumes: These parameters describe the volumes of messages, message sizes and their distribution geographically, as they could be generated by users of the network. The parameters could be measured in the user end systems but it is not realistic to measure them in the network.

3.1.2.2.3 QoS per individual message

QoS requirements have to be satisfied under worst possible/allowable traffic volumes and most unfavourable originator/recipient pairs within a specific network configuration. Consequently, QoS is formulated for each individual message, independently of other messages being handled by the network.

This choice has been made for the following reasons:

- it is difficult to imagine that users would accept a QoS which is dependent on the demands which other users place on the network at the same time;
- the network has to be dimensioned to handle the maximum message volumes, while performing sufficiently well;
- the QoS requirements represent "worst case" performance when maximum degradation through interaction with other traffic occurs.

It must be pointed out, that AMHS provides the facilities to send messages many orders of magnitude greater than AFTN, with attachments measured in Mb. Clearly transfer times for such messages will be considerably longer than for the short text messages exchanged in AFTN. It is, thus, necessary to qualify the statement that QoS is independent of message size by adding ‘for messages containing similar information to that carried over the AFTN’. If a quantitative limit is required, this will be between 4Kb and 6Kb, being the equivalent size of an AFTN message including the AMHS header.

3.1.2.2.4 Independence of QoS on location and time

QoS for an originator/recipient pair is most likely dependent on the relative locations of the two end systems, i.e. whether messages are transmitted with more or less hops through MHS systems (MTAs etc.). However, for simplicity reasons and since QoS requirements are “worst case” requirements, they are stated independently of the location of a message server.

Furthermore, QoS requirements remain constant at all times and are not dependent on date and time of day.

The AMHS performance requirements for the AFTN/AMHS Gateways, could, by agreement, be deemed to apply to interfaces between AMHS functions and AFTN functions in Gateways, e.g. a boundary point consisting of an interface between an internal Message Store and an AFTN handler within a Gateway.

3.1.2.2.5 Dependence of QoS on the AMHS service used

It may be necessary to specify different QoS levels for the AMHS corresponding to different sets of services used, i.e. there may be different classes of messages with respect to QoS. The number of QoS levels should be kept small for simplicity and the way in which service parameters map a message to a QoS level must be simple.

The values of QoS provided by the AMHS are useful to the application designer in deciding which services to use and how they are used. For example, the degree of certainty that a message will reach its destination will determine whether AMHS acknowledgement services are used and in what way. Furthermore, the values of QoS are useful in designing higher-level protocols.

3.1.3 Specification of performance requirements

3.1.3.1 The specification and meaningful application of performance requirements is not a simple task. This sub-section outlines some of the difficulties involved and principles to be adopted.

3.1.3.1.1 Statistical significance

The way in which performance parameters are formulated is necessarily statistical in nature. This is due to the large number of factors, which affect the performance of the network, such as:

- the current network configuration;
- the current overall load of the network, i.e. the behaviour of all users considered as a whole; and
- the dynamic properties of network nodes and transmission systems.

3.1.3.1.2 The need for measurement

For the specification and application of performance requirements to be meaningful, there has to be a framework for measuring performance with respect to the performance parameters. Aspects of a measurement framework which have to be considered are:

- because of the non-deterministic nature of network performance, measurements need to involve large samples of messages, as described in the previous section;
- measurements must be made at different locations simultaneously;
- consistent decisions have to be made as to where measurements are performed, e.g. at service interfaces in MTAs, UAs etc.

3.1.3.1.3 Network aspects relevant to performance

The following list contains factors which can affect message handling performance:

- processing speed, limits the capacity due to the store and forward nature of message handling;
- the finite transmission capacity (line speed) of links between nodes, limits the network throughput;
- the transmission times across links, affects the message transit time since complete messages are stored and forwarded a number of times between originator and recipient;
- the efficiency of message queues;
- transmission line failures and errors are obvious sources of degraded performance;
- table configuration errors can have major negative effects on network performance;
- software failures, which are difficult to treat quantitatively.

In designing the network, the performance requirements (amongst other things) have to be translated into properties of individual network components such that overall requirements are satisfied. Of course other considerations such as policy, expandability, ease of maintenance etc. enter into the network design as well.

3.1.3.2 AMHS Quality of Service Requirements

3.1.3.2.1 For reasons of completeness, simplicity and relevance, a minimal set of parameters was selected out of the large range of possibilities for expressing performance properties, to form a suitable "frame of reference" for discussing the dynamic properties of the European AMHS:

These parameters defined and described in the following sub-sections in more detail, are:

- **Destination Non-Reachability;**
- **Maximum Transit Time;**
- **Message Corruption.**

The selection of these three parameters has been made for the sake of:

- Completeness: all relevant performance aspects of AMHS are covered;
- Simplicity: the formulation of requirements is intentionally kept simple; and
- Relevance: no aspects are included which are not considered to be relevant.

If the performance of the AMHS is such that these parameters are exceeded, then the service is deemed to be of poor quality.

3.1.3.2.2 Destination Non-Reachability

Destination Non-Reachability is expressed with respect to pairs of addresses (originator / recipient). It is the probability that a message sent by the originator will not reach the recipient within the Maximum Transit Delay (as defined below).

The above definition shows that the parameters Destination Non-Reachability and Maximum Transit Time (see below) are not independent of each other: their definitions are coupled. This is intentional. The philosophy behind this definition is that the value of a message to a person or an application receiving it is dependent on its timely receipt. It is assumed, for a given flow type, that all messages belonging to it have the same value of this parameter.

The definition of Destination Non-Reachability is independent of whether the long (or infinite) transit time for a message is reported to its originator or not. It is also independent of whether acknowledgement procedures within the AMHS or on an application level detect the long (or infinite) transit time or not.

Destination Non-Reachability includes the cases in which messages are “lost”, i.e. do not reach their destination in finite time. The probability of message loss must be negligible and this probability is included in the total probability of Destination Non-Reachability. However, there remains a need (for procurement purposes) to place a separate figure on this probability. In keeping with the above rationale, it is required that the probability of message loss is, at most, one tenth of the probability of Destination Non-Reachability.

3.1.3.2.3 Maximum Transit Delay

The Maximum Transit Delay is the time within which a single message has to be transmitted through the network end-to-end so that its transmission is of value to the applications (users). Time critical services, such as CCAMS, impose very stringent requirements for the timely delivery of messages to end users.

If this time is exceeded, the receipt of the message is, in principle, of no value to the application. If the non-receipt within this time is known to the application, then, presumably, error procedures, such as message retransmission, will be initiated.

The transit delay is the time taken by the network to make the message available to the Message Store associated with the message recipient (UA). Therefore the boundary points of the network may, in this context, be considered to be the MTAs connected to the UAs serving the originators/recipients. The boundary points can also be the MTA functionality within AFTN/AMHS Gateways.

It must be borne in mind, that the parameters Maximum Transit Delay and Destination Non-Reachability only have significance when they are taken together.

3.1.3.2.4 Message Corruption

The third Quality of Service Parameter concerns message integrity and is called "Message Corruption". It is the probability that each 1,000 octet content block of a message which arrives at its destination, has been corrupted in any way. The definition of Message Corruption applies only to messages which reach their recipients within the Maximum Transit Delay.

"Corruption" means a deviation, end-to-end, of the content of the received message from the content of the original message. The "content" is also deemed to include parameters, such as originator address, which are delivered together with the message. Corruption can also result from unauthorised changes to a message.

Since the volume unit for defining Message Corruption is large (1,000 octets), the requirement is almost independent of the size of (current) messages. This simplification is based on the assumption that corruption is due to unforeseen system malfunctioning, e.g. faulty software. The corruption of messages due to such causes is not likely to be dependent on the size of messages. (This may need to be reconsidered with the potential forthcoming applications that interchange messages with binary body parts).

The probability of corruption due to other parameters such as system load, queue sizes, transmission errors etc. is almost negligible.

It is estimated, that the volume dependent non-detected bit error probability for a 1000 octet message traversing the AMHS and involving 5 links and 5 different systems (MTAs, UAs, MSs) is of the order of one bit in 10^5 or less. This justifies the (almost) volume-independent character of the Message Corruption parameter.

3.1.3.3 QoS Flow Type Classes

3.1.3.3.1 Different types of information exchange, called Flow Types here, place different QoS requirements on the AMHS.

In principle, each Flow Type might need to be associated with its own specific values of the three QoS parameters. However, taking into account the large number of possible Flow Types, this would result in a very complex analysis. A suitable approach to reducing this complexity is the introduction of “QoS Flow Type Classes” as follows:

Define a number of "QoS Flow Type Classes" and associate a set of fixed values of the three QoS parameters with each class. Depending on the properties and needs of applications using specific Flow Types, assign these to the QoS Flow Type Classes.

When engineering the network, message traffic volumes of each class need to be taken into account rather than individual Message Flow Types.

3.1.3.3.2 Three QoS Flow Type Classes

The approach outlined above is simple and practical provided the number of classes is small. In addition, there is a requirement that the QoS Flow Type Class, to which a message belongs, can be coded in some way in the message itself. This requirement comes from the fact that all AMHS components, e.g. MTAs, must be able, at least in principle, to adapt their processing to the QoS Flow Type Class. The means for this coding must come from standard MHS protocol elements, since development specific to AMHS has to be avoided and the possibility of using third-party-service must be kept open. This rules out, for example, the representation of QoS Flow Type Classes by specific User Parts.

The use of the MHS message priority parameter with three values, "urgent", "normal" and "non urgent", belonging to the P1 protocol handled by MTAs, is currently also not suitable for this purpose. The association of values to messages originating from and destined for the AFTN is fixed by technical specifications, since such messages traverse an AFTN/AMHS Gateway. This means that values of the MHS priority parameter cannot be freely assigned to message types which are currently handled by the AFTN.

There is no short-term solution to this problem. However, in the long-term, when the majority of messages handled by the AMHS are originated by and destined for native users, the priority parameter may become available for this purpose, keeping in mind, nevertheless, that various practical issues may need to be resolved.

3.1.3.3.3 In keeping with the three possible values of the MHS message priority parameter, three corresponding QoS Flow Type Classes are defined:

a) The "High QoS" Flow Type Class

Properties of this QoS Flow Type Class are:

- message transmissions are part of procedures, i.e. the sending and receipt of messages necessarily lead to actions or processing. Without receipt of the message, these actions or processing would not take place, or
- any corrupt information in messages could have serious consequences. This possibility has to be negligible.

b) The "Medium QoS" Flow Type Class

This class has similar properties to the High QoS Flow Type Class; however the Maximum Transit Time requirement can be somewhat less stringent. This distinction is important, because it can be expected that the Maximum Transit Time requirement will have a sensitive effect on network dimensioning.

Properties of this QoS Flow Type Class are:

- message transmissions tend to be of the nature of "information distribution" or "broadcast", possibly based on distribution lists rather than being parts of operational procedures. They are normally not acknowledged. Transit time and reachability constraints are not critical. In the case of non-delivery of messages, this may be noticed by users, in which case backup activities could be initiated, or
- message corruption could have serious consequences and needs to be as low as for the previous class.

c) The "Low QoS" Flow Type Class

This class has similar properties to the Medium QoS Flow Type Class; however the Destination Non-Reachability and Message Corruption requirements can be somewhat less stringent. This is due to a certain amount of redundancy in the message contents and/or the regular updating and transmission of messages with similar content.

3.1.4 Numerical requirements

3.1.4.1 QoS values

3.1.4.1.1 Resulting from the SPACE project, numerical values are assigned to the Performance Parameters defined for the European AMHS. These values, contained in Table 1, are based on the quantitative analysis of the Communications Service Attributes defined in the framework of

EATCHIP as well as performance parameters of typical message switching equipment (see - Guidelines for system requirements).

	High QoS Flow Type Class	Medium QoS Flow Type Class	Low QoS Flow Type Class
Destination Non-Reachability (probability)	$< 10^{-4}$	$< 10^{-4}$	$< 10^{-3}$
Maximum Transit Delay	< 10 seconds	< 5 minutes	< 5 minutes
Message Corruption (probability)	$< 10^{-6}$	$< 10^{-6}$	$< 10^{-5}$

Table 1: Numerical values of SPACE QoS performance requirements

3.1.4.2 It must be noted that the above numerical values:

- have been defined as initial requirements for the AMHS network of the States having participated in the SPACE project;
- could be adopted as possible quantitative and qualitative characteristics for setting up the EUR AMHS network;
- will be reviewed on the basis of compiled AMHS operational experience.

3.1.5 Application of performance requirements

3.1.5.1 The QoS parameters are obviously of importance to the network operators, users and application designers.

3.1.5.2 The QoS requirements along with the volume requirements for each of the Flow Type Classes at the boundary of the network (servers and gateways) are used, in conjunction with a set of well defined design principles (see 3.3 AMHS topology), in order to:

- determine the local performance of servers and gateways, thus dimensioning their configuration,
- determine the throughput of MTAs and capacity of links,
- draft possible network configurations and select the “optimum” network design, and measure actual network performance.

3.1.6 Measurement

3.1.6.1 The specification of numerical values for Performance Requirements is meaningless unless provision is foreseen for measurement of network performance. Such measurement is needed:

- when implementing and enforcing Service Level Agreements between AMHS service providers and users;
- for acceptance testing of network components;
- to determine network capacity;

- to gain experience in network operation (e.g. testing of various routing strategies, etc.).
- to manage the network efficiently.

3.1.6.2 Technically, network performance measurement involves, among other things:

- generation of large message/data volumes;
- automation of measurement;
- time-stamping of messages;
- use of statistical analysis.

Note.– The content of this section is basing on material developed in the framework of the SPACE project. Input reference: [14] WP202 – Specification of European AMHS performance objectives, SPACE/EURO/202/WPR/045, Version 2.0, 30/06/2002

3.2 AMHS Addressing

3.2.1 Introduction

3.2.1.1 This section aims at the production of the AMHS Addressing Plan for all the potential AMHS users in the EUR Region. This Plan should define the AMHS users addressing in an intuitive way and it should be comprehensible and meaningful to the human user and independent of the use (or not) of any type of Directory service such as X.500.

3.2.1.2 The Addressing Plan should also provide the rules to extend the addressing defined to other ANSPs (or not yet identified users).

3.2.2 Requirements

3.2.2.1 The AMHS addressing scheme should meet all of the following requirements:

- The addressing scheme should be as uniform as possible across all AMHS implementations in different Regions (as it is currently the case for AFTN addresses);
- The same addressing scheme should be maintained when indirect AMHS users (i.e. AFTN users or CIDIN users) migrate to AMHS. This implies that the AMHS addressing scheme is pre-defined and published before actual operation of the newly implemented AMHS;
- The addressing scheme should be independent of any constraints that may be imposed by Management Domains (MDs) in the Global MHS (i.e. the non-AMHS services operating globally as commercial services) or by national regulations that may vary from Region to Region; and
- The addressing scheme should allow for the interchange messages with MDs in the Global MHS.

3.2.3 MHS Addressing structure

Each MHS address consists of a set of MHS standard components referred to as address attributes.

3.2.3.1 High level MHS address attributes

3.2.3.1.1 The high level MHS attributes identify an MHS Management Domain as specified in ISO/IEC 10021-2, Section 18.3 [21]. They are determined by the structuring of Management Domains of the MHS Region/organisation to which the address belongs. Each attribute must be registered with an appropriate registration authority to ensure that all addresses remain unambiguous. They are as follows:

- **country-name (C):** this is mandatory, and the possible range of values of the attribute is drawn from the ISO 3166 register of country names. The register contains a special value 'XX', allocated for the purposes of international organisations (i.e. those that are established by international treaty) which do not ‘reside’ within any particular country;

- **administration-domain-name (A):** administration-domain-name (ADMD-name)is mandatory, and its value is the name of an MHS Service provider in the context of a particular country. ADMD-name s must be registered by a national registration authority. ADMDs registered under the 'XX' country must obtain that registration from the Telecommunication Standardisation Sector of the International Telecommunication Union (ITU-T);

- **private-domain-name (P):** private-domain-name (PRMD-name) is optional, and its value is the name of an MHS service usually operated by a private organisation. PRMD-names must be registered either with their respective ADMDs, or with a national register of PRMDs.

3.2.3.1.2 For example, the high level address of a PRMD in the United Kingdom might be:

C = GB; A = BT; P = British Gas;

3.2.3.2 Low level MHS address attributes

3.2.3.2.1 They are as follows:

- **organization-name (O):** the organization-name is the most significant naming attribute of the O/R address. Many organisations will operate as sub-naming authorities, allocating name space below their organization-name attribute. The function of the domain names, both Administrative and Private, is to provide a relaying mechanism for delivery of the message to the intended destination. Relaying to the intended destination is made easier by the combination of a unique organization-name within a unique PRMD-name, thus ensuring that all MHS organisations are uniquely identified.

- **organizational-unit-name (OU):** the organizational-unit-names are used within the context of a hierarchical addressing structure as identified by the organization-name attribute, and should be used to identify meaningful subdivisions of that namespace. The X.400 O/R address allows for up to 4 occurrences of the OU attribute to be specified, each up to 32 characters in length, in descending order of significance within the organisational hierarchy.

  The other *OU* (*OU2-4*) attributes can be used to further subdivide the namespace represented by the *OU1* attribute if necessary. Subordinate OU attributes should <u>only</u> be used if all superior OU attributes are in use.

- **common-name (CN):** The common-name attribute is the preferred way of identifying distribution lists and computer applications, avoiding the (mis)use of the personal-name attribute. The common-name attribute can be up to 64 characters in length.

3.2.3.2.2 A complete list of attributes with different information concerning on the maximum length and type of allowed characters for each attribute type is provided in the following Table:

MNEMONIC FORM ADDRESS ATTRIBUTE	CHARACTERISTICS
country-name	2 alpha or 3 numeric
ADMD-name	16 PrintableString
PRMD-name	16 PrintableString
organization-name	64 PrintableString
organizational-unit-names	32 PrintableString
common-name	64 PrintableString

Table 2: Mnemonic O/R address attributes maximum length and types

3.2.4 AMHS Addressing Schemes

3.2.4.1 XF-Addressing Scheme

3.2.4.1.1 The AMHS technical specifications describe a potential AMHS addressing scheme, the XF-Address (translated), composed of the following:

a) an AMHS Management Domain identifier;

b) an organization-name attribute:

   1) as specified in ISO/IEC 10021-2, Section 18.3,

   2) taking the 4-character value "AFTN", and

   3) encoded as a Printable String; and

c) an organizational-unit-names attribute:

   1) as specified in ISO/IEC 10021-2, Section 18.3,

   2) comprising a sequence of one single element, which takes the 8-character alphabetical value of the AF-Address (AFTN-form address) of the user, and

   3) encoded as a Printable String.

Note 1.– An XF-Address is a particular MF-Address whose attributes identifying the user within an AMHS Management Domain (i.e. those attributes other than country-name, administration-domain-name and private-domain-name) may be converted by an algorithmic method to and from an AF-Address. The algorithmic method requires the additional use of look-up tables which are limited, i.e. which include only a list of AMHS Management Domains rather than a list of individual users, to determine the full MF-Address of the user.

Note 2.– An MF-Address (MHS-form address) is the address of an AMHS user.

3.2.4.1.2 A summary of XF-Addressing Scheme can be found in the following table:

Attribute	Attribute value	Remark
country-name (C)	C = “XX”, as already obtained by ICAO from ITU-T	
ADMD-name (A)	A = “ICAO”, as already registered by ICAO at ITU-T	
PRMD-name (P)	P = a name to be defined by a State, ANSP or body responsible for an AMHS Management Domain and registered with ICAO.	In the absence of such a name being registered with ICAO, a default value will be used to ensure that the attribute value is always defined. This default value is the ICAO two letter State/territory identifier, as may be found in Doc 7910.
organization-name (O)	O = “AFTN”, taking the 4-character value “AFTN” encoded as a Printable String.	
organizational-unit-names (OU1)	OU1 = the 8-letter AF-address (or AFTN indicator) of the considered user.	

Table 3: XF-Addressing Scheme

Note 3.- PRMD Names may be assigned to bodies such as ANSPs, groups of ANSPs, organizations hosting Regional services and applications or third parties connected to the AFS. Relevant requests need to be validated prior to registration, in line with Regional procedures.

Note 4.- The combination of address attributes defined in Table 3 may also be used by bodies managing an AMHS management domain but which are not registered as a State/territory in ICAO Doc 7910. Such a body can be, for example, an aeronautical communication service provider. However, an AMHS address obeying to that scheme cannot be converted by an algorithmic method to and from an AF-address, and it consequently cannot be considered as an XF-address. In such cases the address is considered as an ‘XF-like form’ address.

Example: XF AMHS Address for the Southampton Tower
/C=XX/A=ICAO/P=EG/O=AFTN/OU1=EGHIZTZX/

Example: ‘XF-like form’ AMHS Address for SITA user
/C=XX/A=ICAO/P=SITA/O=AFTN/OU1=LSTTSITA

3.2.4.2 CAAS Addressing Scheme

The Common AMHS Addressing Scheme (CAAS) adopted by ATNP and collected in old Doc 9705 (3rd Edition) (replaced by Doc 9880, Part II) is aligned with the addressing scheme developed in Europe by the SPACE Project Team and endorsed by the third meeting of the Aeronautical Fixed Services Group (AFSG) of the European Air Navigation Planning group (EANPG).

3.2.4.2.1 High-level attributes

3.2.4.2.1.1 The following preferred high-level MD and address structure that meets all of the requirements outlined in paragraph 3.2.1 above:

- country-name = 'XX';
- ADMD-name = 'ICAO';
- PRMD-name = preferred operating name assigned by the State, ANSP or other body concerned.

In this way, ICAO creates an international ADMD without addressing constraints imposed from outside ICAO and its members.

3.2.4.2.1.2 This scheme has placed two requirements on ICAO:

- To obtain from the ITU-T the registration of the name 'ICAO' (or some other suitable acronym agreed between ICAO/ANC and ITU-T); and
- To establish and maintain a register of PRMDs established by States, ANSPs and bodies managing an AMHS Management Domain that operate using the 'XX' + 'ICAO' address structure, in a way similar to Doc 7910 [7]and Doc 8585 [8].

*Note.– This scheme does **not** require ICAO itself to operate the ADMD systems since this is normally delegated to the participating ANSPs and other bodies concerned.*

3.2.4.2.1.3 This registration will enable the establishment of regional AMHS services and their later interconnection, and it will provide States, ANSPs and other bodies concerned with a good deal of stability within which they can develop their AMHS plans.

3.2.4.2.2 Low level attributes

3.2.4.2.2.1 The CAAS addressing scheme includes the following attributes:

- organization-name (O) = Region,
- organizational-unit-names (OU1) = Location,
- common-name (CN) = User

3.2.4.2.2.2 Consequences:

- Each State, ANSP or other body concerned will define the values for the organization-name attribute (O) in its Management Domain. The character set to be used for this attribute will be the set of characters allowed by the ASN.1 type "PrintableString".
- organizational-unit-names (OU1) will be the 4-character ICAO Location Indicator (as specified in ICAO Doc 7910 [7]) of the user.
- common-name (CN) will include the 8-character AFTN address for AFTN users.

3.2.5 EUR AMHS Addressing Plan

3.2.5.1 EUR AMHS Addressing Scheme

3.2.5.1.1 EUR AMHS Addressing Scheme was endorsed by the third meeting of the Aeronautical Fixed Services Group (AFSG) of the European Air Navigation Planning group (EANPG) and is fully compliant with the CAAS Addressing Scheme described above.

3.2.5.1.2 This scheme has been adopted for potential EUR AMHS users, both already identified and users not currently defined.

3.2.5.1.3 It is recognised that the Addressing Plan to be used by EUR States, ANSPs and bodies implementing AMHS will be a combination of AMHS addresses following the Addressing Plan described in this section, for some AMHS EUR Management Domains, and of AMHS addresses following the XF Addressing Scheme, for other EUR AMHS Management Domains.

3.2.5.1.4 Major concepts of this EUR AMHS Addressing Plan are shown as follows:

Attribute	Attribute value	Remark
country-name (C)	C = "XX", as already obtained by ICAO from ITU-T	
ADMD-name (A)	A = "ICAO", as already registered by ICAO at ITU-T	
PRMD-name (P)	P = a name to be defined by a State, ANSP or body responsible for an AMHS Management Domain and registered with ICAO. Such a name will identify a State, an Organisation, or an organisation within a State.	In the absence of such a name being registered with ICAO, a default value will be used to ensure that the attribute value is always defined. This default value is the ICAO two letter State/territory identifier, as may be found in Doc 7910.
organization-name (O)	O = a value corresponding to local/national geographical information, e.g. a region or a geographical area within a State where the user is located.	The syntax and value are to be defined by the considered State, ANSP or body concerned. The table associating such an organization-name to each ICAO Location Indicator (4 characters) needs to be registered and published by ICAO.
organizational-unit-names (OU1)	OU1 = the ICAO Location Indicator (4 characters) of the considered user;	
common-name (CN)	CN = the 8-letter AF-address (or AFTN indicator) of the considered user, irrespective of whether it is a direct or indirect user.	

Table 4: EUR AMHS Addressing Plan

Note 1.- PRMD Names may be assigned to bodies such as ANSPs, groups of ANSPs, organizations hosting Regional services and applications or third parties connected to the AFS. Relevant requests need to be validated prior to registration, in line with Regional procedures.

Note 2.- The combination of address attributes defined in Table 4 may also be used by bodies managing an AMHS management domain but which are not registered as a State/territory in ICAO Doc 7910. Such a body can be, for example, an aeronautical communication service provider. However, an AMHS address obeying to that scheme cannot be converted to and from an AF-address using the rules usually applied to CAAS-addresses. Such addresses need to be fully specified and registered with ICAO for use in the User Address Look-up Table defined in Doc 9880, Part II, section 4.3.2.4. They consequently cannot be considered as CAAS-addresses. In such cases the address is considered as a 'CAAS-like form' address.

Example: MF AMHS Address of Lanzarote's ARO:
/C=XX/A=ICAO/P= SPAIN /O= LEEE /OU1= GCRR /CN= GCRRZPZX

3.2.5.2 Distribution lists.

3.2.5.2.1 The scheme to be used for the identification of AMHS Distribution Lists is the same as for potential AMHS users.

3.2.5.2.2 The O and OU attributes would then represent the expansion point of the distribution list.

3.2.5.3 Indirect AMHS users

3.2.5.3.1 <u>EUR AMHS Addressing Scheme shall be applicable to both direct and indirect users in the EUR Region as soon as the scheme is published</u>. This scheme should be published through ICAO and other appropriate bodies (e.g. the ECAC community or EUROCONTROL Member States). EUR users should use the XF-address of users outside the EUR Region until another addressing scheme (CAAS) is published by the organisations responsible for those users.

3.2.5.4 European Services and Applications

3.2.5.4.1 A special case of the EUR AMHS Addressing Plan is the allocation of a discrete PRMD-name (P=EUROPE) dedicated for use by European Services and Applications for which Location Indicators have been allocated in ICAO Doc 7910, Section: EU – Europe (ICAORD).

3.2.5.4.2 The respective organization-name (O) consists of a value corresponding to the specific European Service or Application.

3.2.5.4.3 When assigning a new value to the organization-name attribute, the following rules should be considered:

1. It should be as short as possible;
2. It should only comprise standard characters, i.e. no accented letters or letters only used in specific geographical areas;
3. The use of figures is not advisable.

3.2.5.4.4 The assignment of the value to the organization-name attribute should be coordinated with the ATS Messaging Management Centre (AMC) Operator to ensure unique naming under the PRMD-name P=EUROPE (detailed information on the AMC is provided in section 6.5).

3.2.5.4.5 With the assignment and publication of the organization-name attribute the ATS Messaging Management Centre (AMC) Operator ensures convertibility (update of the respective CAAS Table) and routing of the complete address of the new European Service or Application via the AFTN/CIDIN/AMHS within EUR, by following the defined procedure.

3.2.5.4.6 This particular PRMD is a virtual PRMD, defined for ICAO Europe in a way similar to the "ICAO" ADMD at a global level. It is formed by the organisations in charge of the centralised European Services and Applications. Two cases may occur for such organisations being part of PRMD "EUROPE":

1. Organisations hosting European Services and Applications, which have already implemented AMHS, and which manage their respective MTAs. Some specific requirements apply to them. They are listed in sections 9.1.3 and 9.2;

2. Organisations hosting European Services and Applications, which are still using AFTN to connect their applications, by means of connections to AFTN/AMHS Gateways of other PRMDs. The present section 3.2.5.4 is defined to also cover this special case for addressing, without any additional requirements.

3.2.5.4.7 Within this PRMD, clauses of ICAO Doc 9880 which refer to a "matter local to an AMHS Management Domain" or to a "matter of policy local to an AMHS Management Domain" therefore may be interpreted as referring to a "matter local to each organisation managing a European Service or Application part of the "EUROPE" AMHS Management Domain".

3.2.6 Guidelines on PRMD-name assignment

3.2.6.1 Purpose

3.2.6.1.1 A PRMD-name attribute shall be formulated and assigned by each State, ANSP or other body concerned in order to uniquely identify the AMHS Management Domain of which they are in charge. Practically, the PRMD-name attribute identifies that part of the AMHS for which an ANSP or other body concerned is responsible.

3.2.6.2 Assignment rules

3.2.6.2.1 When assigning a value to the PRMD-name attribute the following rules should be considered:

1. It should be representative of the whole AMHS Management Domain for which the State, ANSP or other body concerned is responsible;

2. It should be as short as possible, an acronym would be sufficient;

Note.– The use of the two-letter ISO 3166 country codes (e.g. FR for France, AU for Australia, US for the United States, etc.) is not advisable, as these codes are used as values of the country-name attribute and not the PRMD-name attribute. This may confuse the operators.

3. It should be stable and not subject to changes unless there are duly justified technical and/or operational reasons;

4. It should be unique and unambiguous;

Note.– Care should be taken not to use a name or an acronym such as "civil aviation", "ANSP", "DGAC".

5. A default value has been reserved in order to ensure that this attribute value is always defined. This default value is the ICAO two letter State/territory identifier, as may be found in Doc 7910 [7].

6. It should only comprise standard characters, e.g. no accented letters or letters only used in specific geographical areas;

7. The use of figures is not advisable.

3.2.6.3 Registration

3.2.6.3.1 Once assigned by the concerned State, ANSP or other body, the PRMD-name value(s) shall be registered and published by ICAO after checking its uniqueness, as described in paragraph 3.2.6.2.

Note.– ICAO being the naming authority for AMHS addresses, there is no requirement to register the PRMD-name value(s) with a national authority.

3.2.7 Guidelines on organization-name assignment

3.2.7.1 Purpose

3.2.7.1.1 The purpose of the organization-name attribute is to allow each State, ANSP or other body concerned to split, if needed, the AMHS Management Domain (MD) for which it is responsible in distinct geographical areas.

3.2.7.1.2 Within a given AMHS Management Domain (identified by the "C", "A" and "P" attributes) two potential AMHS network architectures are possible:

1. centralised architecture, with one single ATS message server; and
2. geographically distributed architecture, with several regional ATS message servers.

3.2.7.1.3 It is to be noted that architectural aspects and addressing aspects are not completely linked together, in effect the agreed addressing scheme does not place any constraints on the AMHS network deployment plan.

Both types of architecture have advantages and drawbacks, as summarised in the following Table 5.

	Centralised architecture	**Distributed architecture**
Applicability	Relatively small MD; Relatively small number of users.	Large MD; Large number of users.
Advantages	Easy management (one server).	A high quality of service can be offered to the users; Each server is dimensioned to match the requirements of the users attached to it; Allows a better load sharing on the network.
Drawbacks	Require a high grade of service from the network (e.g. in terms of availability, end-to-end throughput, etc.)	A highly distributed architecture may increase the complexity of the management of addresses by operational staff.

Table 5: Centralised AMHS architecture versus distributed AMHS architecture

3.2.7.2 Assignment rules

3.2.7.2.1 Before assigning a value to the organization-name attribute, each State, ANSP or other body concerned should follow the following 3-step process:

1. Develop the general architecture of the AMHS to be implemented;

2. Define the location and the number of sites at which ATS Message Server could be installed within a foreseeable time frame (e.g. 5, 10 or 15 years); and

3. Chose and assign a name to each one of these sites.

3.2.7.2.2 A specific case is the situation where a single ATS Message Server is implemented in an AMHS MD, providing services to AMHS users that are all directly attached to this server (centralised architecture). For simplification, it is suggested that a single organization-name (O) value be allocated to all Location Indicators in the AMHS MD.

3.2.7.2.3 Potential criteria for the selection of sites include:

- Geographic divisions, such as: North, South, East, West, etc.;
- Administrative divisions of the concerned ANSP, such as ATS, Meteorological, etc.;
- Operational divisions centred around the ACCs (if more than one ACCs exist);
- Operational divisions centred around the main airports;
- Mapping of the AMHS architecture on the existing AFTN/CIDIN architecture;
- A mixture of the above criteria; and
- Other.

Note.– Care should be taken not to define too many geographical areas within a given AMHS MD as this may lead to less efficient message routing.

3.2.7.2.4 When assigning a value to the organization-name attribute, the following rules should be considered:

1. It should be as short as possible;

2. It should only comprise standard characters, i.e. no accented letters or letters only used in specific geographical areas;

3. The use of figures is not advisable.

Note.– Typically, a State, ANSP or other body concerned defines different values for the organization-name attribute only if it plans to implement a distributed AMHS architecture in the short, medium or long term future. States, ANSPs or bodies not planning to implement a distributed AMHS architecture allocate a single value for this attribute.

3.2.7.3 Registration

3.2.7.3.1 Once assigned by the concerned State, ANSP or other body, the organization-name values shall be registered and published by ICAO, as described in paragraph 3.2.8.3.

Note.– ICAO being the registration authority for AMHS addresses, there is no requirement to register the organization-name value(s) with a national authority.

3.2.8 Address conversion

3.2.8.1 Addressing Plans requirements

3.2.8.1.1 The selected address conversion strategy must take into account the following principles:

- The selected address conversion solution shall be able to support any X.400 addressing plan making use of any address form.
- The AFTN address of an AFTN or AMHS user is unambiguous, internationally recognised and shall not be replaced by another value.

3.2.8.1.2 The addresses to be considered are: AFTN, XF, CAAS and MF. It can be concluded that:

- All EUR AFTN/AMHS Gateways shall implement the conversion AFTN<=>XF;
- All EUR AFTN/AMHS Gateways shall implement the conversion AFTN<=>CAAS;
- All EUR AFTN/AMHS Gateways shall implement the conversion AFTN<=>MF for individual user addresses which are officially published for integration in the User Address Look-up Table. This is particularly required for AMHS communication with non-ICAO entities using AFTN addresses;

  Note.– The ability to convert these three types of AMHS addresses is required for compliance with Doc 9880.

- To deal with the risk of arrival of spurious XF addresses at EUR ANSPs MDs from the global AMHS, and avoid rejection of messages directed to such erroneous addresses, an ANSP having selected CAAS may implement the X.400 redirection of XF-addresses to CAAS-addresses for its own MD, on a local basis;

3.2.8.2 Address Conversion Scenarios and Criteria

3.2.8.2.1 Several address conversion scenarios may be envisaged (single conversion, AMHS transit conversion, AFTN transit conversion and multiple transit conversion) and were assessed, at the time when an address conversion strategy for Europe was established.

3.2.8.2.2 Once the scenarios were established, the need was identified to take into account the following considerations for address conversion:

- The result of the address conversion performed in an AFTN/AMHS Gateway shall depend only on the pre-defined pair of unambiguously associated AFTN and AMHS addresses, and not on the gateway itself, according to the form published by ICAO and defined by the delivering MD.
- It is required that each gateway performing address conversion has access to the minimal necessary information to perform mappings between AFTN addresses and AMHS addresses and vice-versa. The complete mappings between AFTN addresses and their AMHS equivalents should be published (in electronic form) and made available to all gateways that support address translations.
- The conversion process shall be easy to use and manage, and efficient.

3.2.8.2.3 As a conclusion, a compromise solution combining the use of algorithmic tables and X.500 directory is preferred for the address conversion.

3.2.8.3 General model for address distribution and gateway address conversion

3.2.8.3.1 A model of address distribution and gateway address conversion is depicted in Figure 1 below. The figure represents information exchanges between ICAO and three ANSPs implementing AMHS Gateways, concerning address conversion. ANSP1 and ANSP2 implement a distributed address publishing service (APS), e.g. by means of ATN X.500 Directory Services. This allows electronic distribution. ANSP3 provides this information to ICAO for manual collation and distribution (e.g. on paper, electronic database), and does not support a directory.

The dotted arrows represent exchanges that are performed in an off-line way, e.g. through "paper" or off-line management procedural exchanges. The full arrows represent exchanges that are performed electronically using appropriate communication protocols.

3.2.8.3.2 The model identifies a number of components that are necessary for address conversion:

1) Collection and distribution of the basic addressing information that establishes equivalence between the different addresses identifying each AMHS and AFTN/CIDIN user; the content of this information **must** be standardised and made available to all AFTN/AMHS Gateways;

2) Access to, and/or import of the basic addressing information into AFTN/AMHS Gateways. This depends on the particular gateway implementation;

3) Re-structuring the basic addressing information into a format suitable for use by each gateway's internal address conversion procedures (AMI). This is again gateway implementation specific;

4) The internal procedures and data structures of the gateway (AMP and AMT) that make use of the re-structured addressing information. This is gateway implementation specific.

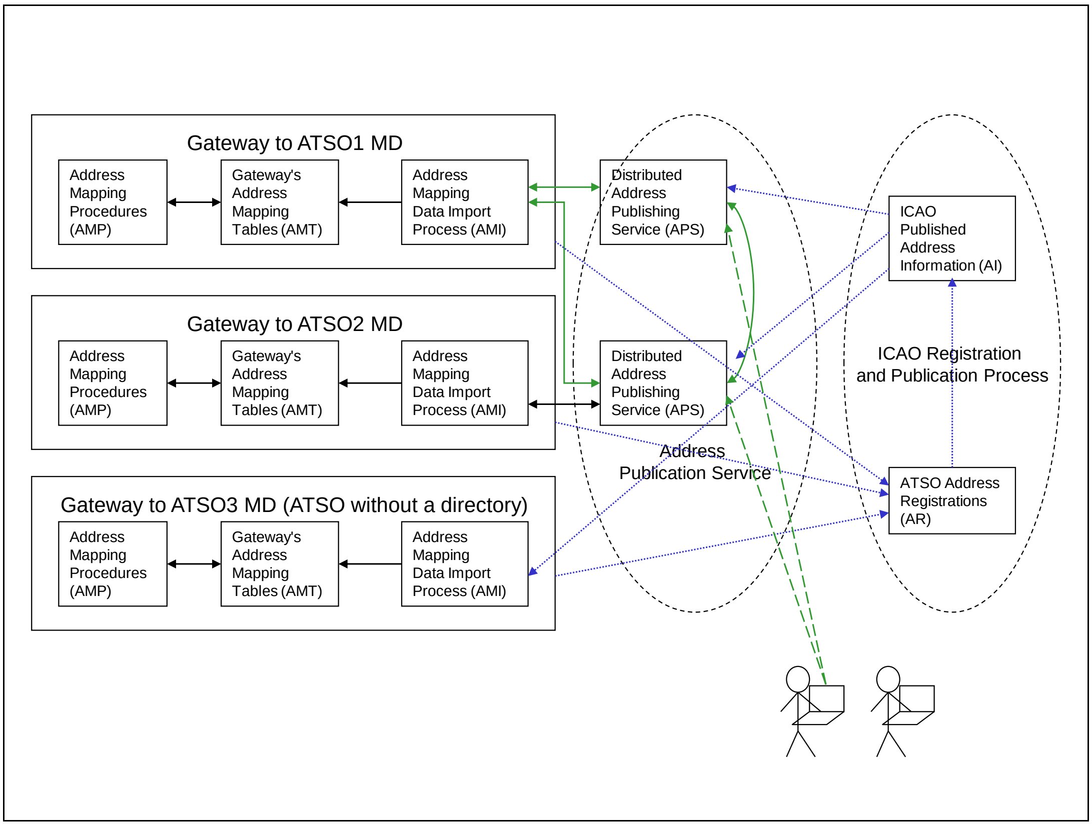

Figure 1: General model for gateway address conversion

3.2.8.3.3 The address mapping information content held in AMT and distributed through APS is identical in nature.

3.2.8.3.4 The structure of APS must be compatible with many different systems (e.g. different ANSP's Gateways), and must therefore be standardised. There are a number of possibilities for structuring APS:

- As an X.500 Directory Information Tree, thereby enabling implementation of a Distributed APS;
- By some other electronic means (e.g. CSV files);
- On paper.

3.2.8.4 The impact of different paths through the AFTN and AMHS

3.2.8.4.1 There is also a potential need for messages to undergo multiple address conversions. In order to minimise message rejection and to regulate the responsibilities for conversions, the following rules should apply:

- Originating MDs (for originator's addresses) shall generate addresses according to the form published by ICAO and defined by the delivering MD (for recipient addresses);
- Delivering MDs are authorised to reject messages received with recipient addresses which do not comply with the address form published by ICAO and defined by the delivering MD;
- Delivering MDs should have the capability of redirecting potential internal XF addresses to the corresponding MF(S) form addresses for use within their delivering MD, for a transition period of at least 6 months after publication of the appropriate ICAO documentation;

- Transit domains should not attempt to perform any AMHS <-> AMHS mapping unless a specific bilateral agreement has been established with the delivering MD (for recipient's addresses) or the originating MD (for originator addresses). Transit MD should only use the attributes C, A, P (which are invariant and predetermined for all AMHS address forms in the ATS) in selecting a message route.

3.2.8.5 Recommended AMHS Address Conversion Strategy

3.2.8.5.1 The recommended AMHS address conversion strategy is the means by which the general model represented in Figure 2 should be realised by States in the EUR Region. It is also applicable on a worldwide basis and has been presented and adopted by the ICAO ATNP as the general AMHS address conversion strategy. This strategy is made of the following elements:

1) the establishment, by an appropriate ICAO body or entity, of an ICAO Registration and Publication process as a set of procedures for collecting and publishing AMHS address conversion information on a periodic basis (e.g. twice yearly). This will include:

   a) the MD information included in the ICAO Registry of AMHS Management Domains, i.e. the MD identifier and the corresponding ICAO two letter State/territory identifier, together with the specification of the type of implemented addressing scheme (XF or CAAS);

   b) for those MDs having implemented the CAAS, the mapping information providing the organization-name address attribute for each ICAO Location Indicator;

   c) for MDs which have selected addressing schemes which are neither XF nor CAAS (this may be 'XF-like' or 'CAAS-like' addresses, for example), the full list of individual AMHS user addresses managed by these MDs, together with the equivalent AFTN addressee indicator.

   Note: this element is currently implemented by means of the ATS Messaging Management Centre (AMC), which collects and publishes AMHS address information on an AIRAC-cycle periodic basis.

2) a Distributed Address Publishing Service (APS), based on ATN Directory Services, that allows publication of real-time AMHS address conversion information. This is to be implemented at the earliest opportunity upon ANSPs initiative, with the following principles:

   a) use of the directory scheme;

   b) initial population of the Directory Information Base with the information distributed through the ICAO Registration and Publication process;

   c) implementation of a single Directory System Agent (DSA) per ANSP to hold the MD Registry sub-tree, the world-wide ANSP information distributed through the ICAO Registration and Publication process, and the local AMHS MD address conversion information sub-tree; and

   Note: this element is being implemented with the support of the European Directory Service (EDS) as a Central information repository enabling synchronisation with national DSAs implemented by ANSPs.

3) in co-existence with the use of Address Mapping Tables (AMT) directly derived from the information published through the ICAO Registration and Publication process, for ANSPs that choose to defer the implementation of ATN Directory Services.

3.2.8.5.2 As a local implementation matter, ANSPs that envisage implementation of Directory Services for the purpose of the Distributed address publication service (APS) at the same time as they implement AMHS, should also consider the use of directory solutions as a technical option for the gateway's address mapping tables (AMT).

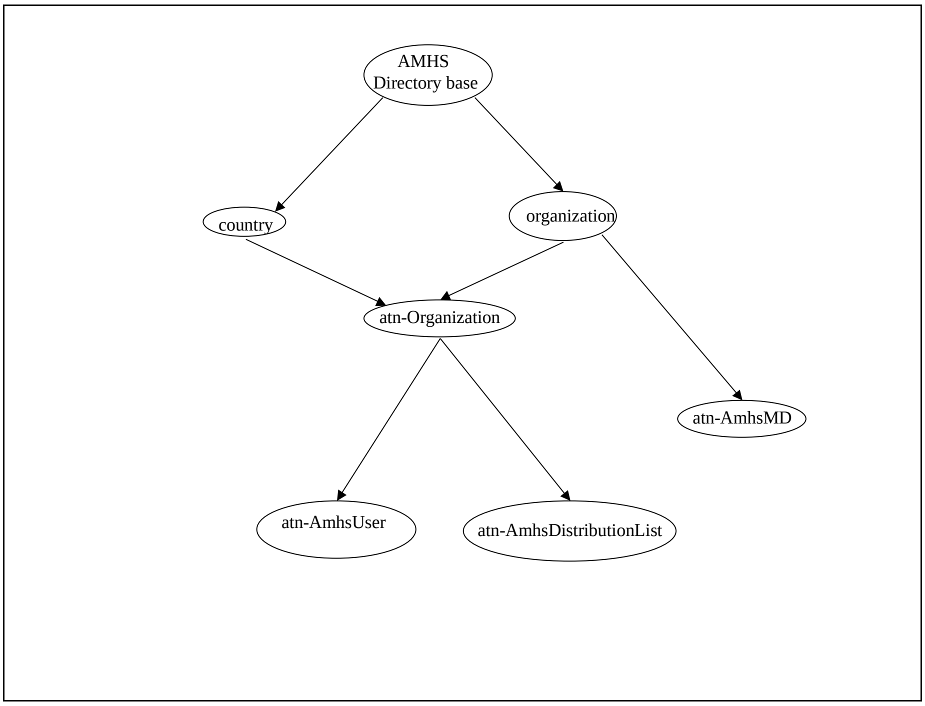

Figure 2: DIT structure for AMHS address conversion

3.2.8.6 Regional provisions

3.2.8.6.1 The strategy above is complemented by the following transitional provisions which may apply regionally.

3.2.8.6.2 In case the first element in the above strategy is not implemented by ICAO in a timeframe compatible with early AMHS implementations, an equivalent process may be set up on an ad-hoc basis among ANSPs forming an AMHS island. This is particularly applicable to any European ANSPs being early AMHS implementers.

3.2.8.6.3 In case of ANSPs implementing the second element in the above strategy that initially prefer to group together for the implementation of a single ICAO Regional DSA, the following should apply:

- the MD Registry sub-tree;
- a local AMHS MD ANSPs information sub-tree for each of the ANSPs in the group;
- and the world-wide ANSPs information distributed through the ICAO Registration and Publication process.

3.2.8.6.4 The Regional DSA thereby becomes an aggregation of the local DSAs envisaged in the principle strategy.

3.2.8.6.5 In the EUR Region, the creation of an Offline Management Centre is recommended to consolidate, co-ordinate and distribute AMHS user address changes across the Region. This Offline Management Centre should implement such a Regional DSA in support of its address management activities.

3.3 AMHS topology

3.3.1 General potential AMHS topologies

3.3.1.1 As for any other network topology, an AMHS topology describes the connectivity among the nodes - which are in this case AMHS COM Centres – and links – which are AMHS logical connections at the ISO/OSI application layer.

3.3.1.2 From a theoretical viewpoint, there are many possible solutions for a network topology. Each of the chosen designs has distinct properties in terms of cost, transit time (number of hops to be passed), routing complexity, reliability (survivability). Furthermore, from a more practical perspective, a network topology is also often related to the organisation and relationships between its users, and possibly network managers. In a situation where traffic flows are not equally distributed between nodes (from a statistical perspective), the traffic patterns have also a great influence on designed topologies.

3.3.1.3 General network topologies include:

- Tree-shaped topologies, including
- Star,
- String,
- Partially meshed topologies, including
- Double star (two interconnected stars centred on two distinct “hubs”),
- Ring,
- Hyper-ring (two rings with several links interconnecting them),
- Hybrid topologies, e.g. using a partial mesh backbone between some nodes and star from the backbone nodes to other nodes,
- Full meshed topology.

3.3.1.4 A general analysis of such topologies, based on the properties listed above, is provided in the following.

3.3.1.5 Reliability, transit time, cost and operational complexity are all factors affected by the topology of a network. Table 6 summarises the characteristics of the topological structures addressed above in order to indicate the advantages of certain topologies over others.

3.3.1.6 In Table 6 measures are used to evaluate the technical merit of a topological structure: Number of links, maximum number of hops, complexity and reliability. Each of these measures is described below.

3.3.1.7 A low *number of links* per node for a design will often be associated with low cost. Vice versa, a higher link-per-node ratio indicates a more expensive network topology. The tree shaped topologies (star, string) have the lowest number of links per node. Ring and hyper-ring architectures have a small number of links per node. At the opposite end from the tree structures, the full mesh network marks the upper limit of the link-per-node ratio.

3.3.1.8 Clearly, a smaller number of *hops* from a source node to a destination node will result in shorter transit times. Here, a full meshed topology is the most desirable. The star topologies, with their very small number of hops, are also very desirable. On the other hand, string and simple ring architectures can have a significantly greater numbers of hops. – A large number of hops is associated with a large number of intermediate nodes and links which have to be dimensioned for conveyance of transit traffic. The related capacity enhancements also constitute a cost factor.

3.3.1.9 *Complexity* provides here a measure for the effort to be spent on network design, establishment of appropriate (re-)routing mechanisms and network operations. The number of potential paths between nodes, as well as the need to sum up multi-hop traffic (in order to get capacity figures for nodes and links), increase the complexity of the network design task. The complexity for re-routing of traffic increases also with the number of candidate links providing alternative paths between each pair of nodes. Finally, the effort for network management and maintenance grows with the number of links providing connectivity between a given set of nodes. Centralised (star) topologies are easier to maintain than those that are highly distributed (as meshed structures).

3.3.1.10 The *reliability* of a network increases with the number of established links allowing alternative paths in case of link failures (provision of adaptive routing assumed). More precisely, if *n* represents the minimum number of nodes to which any node is connected (*n*-connectivity) then we can expect that the probability that a given node has access to at least one of its neighbours increases with the quantity of *n*. A partial mesh topology has 2-connectivity or greater, a full mesh offers as upper limit a (N-1) connectivity (where N represents the number of nodes).

Topology	Number of Links	Relative Number of Links	Max Hop Count	Complexity	Reliability
Star (tree)	N-1	Lowest	2	Lowest	Lowest
Double Star	2 (N-2)+1	Low	2	Low	High at core, low at remote locations
String (tree)	N-1	Lowest	N-2		
Ring	N	Low	(N-1)/2	Low	Moderate
Hyper-Ring	2 N	Low	2	Low	Moderate
Partial mesh	Moderate	Moderate		High	Good
Full mesh	[N*(N-1)]/2	Highest	1	High	Highest

Table 6: Comparison of alternative network topologies

3.3.2 Design elements for the European AMHS

3.3.2.1 In application of the principles above, the following elements have been taken into account for the definition of the European AMHS topology:

1. Quality of service (Transit delays),
2. Quality of service (Availability / Reliability),
3. Cost effectiveness,
4. Complexity of operation,
5. Responsibility for transit traffic.

3.3.2.2 Most of these criteria were already defined as the main considerations for AFTN topology design (ref. ICAO Doc 8259-AN/936/1991 [9]).

3.3.3 Possible approaches for the European AMHS topology

3.3.3.1 SPACE recommendation for a fully-meshed topology

3.3.3.1.1 The objective of ensuring transit delays compatible with the QoS performance requirements specified in section 3.1.4 led to the SPACE recommendation of a **fully-meshed topology for the AMHS network deployed in the EUR Region**, thereby minimising the number of hops between any pair of International MTAs / ATS Message Servers in this area (ref. [15] and SPACE WP321 Report “AMHS Extensibility Principles”).

3.3.3.1.2 The end-to-end transit delay in networks is mainly caused by the processing time in the nodes passed by a message and the transmission times on the links between these nodes. With given processing times, link speed, average message length and protocol overhead a first estimation of the number of allowable hops for a given maximum end-to-end transit delay is possible. – For a link speed of 256 kbps five hops are allowed in the international network to meet the maximum end-to-end transit delay for the high QoS class. With 64 kbps only two hops are allowed (ref. [15] and [20]).

3.3.3.1.3 To be realistic, such a recommendation implies that an underlying network forming a common lower layer infrastructure would be available across the considered geographical area. The requirements placed upon such an underlying network are described in section 3.5.

3.3.3.1.4 This approach favours criteria 1 (QoS – transit delays) and 2 (QoS – availability) among those listed in section 3.3.2. No other topology could rate better than a fully-meshed network regarding these objectives.

3.3.3.1.5 As far as criteria 3 (cost effectiveness) and 4 (complexity of operation), it may be considered that the need to establish and maintain AMHS connections with any other International ATS Message Server in the EUR network represents a non-optimised cost (in network capacity and required staff). However, although parallel operations have to be performed with all communication partners in such a network topology, the similarity between these operations reduces complexity and increases efficiency, thereby reducing the negative impact on costs.

3.3.3.1.6 Complexity of operation, although obviously higher that in a tree-shaped network, is probably lower than in some partially-meshed topologies where network behaviour, required tasks and diagnostics vary depending on the existence or not of a direct link between both MTAs.

3.3.3.1.7 The factor of responsibility of transit traffic (criterion 5) should also be considered. In the fully meshed topology each MTA is managing its own traffic with no transit traffic coming from other international MTAs (except re-routing), representing a clear advantage in comparison with other topologies.

3.3.3.1.8 It must be noted that an AMHS fully-meshed topology could lead to approximately 50 AMHS connections to/from each COM centre, when AMHS is fully deployed in the EUR Region, based on the current number of international COM Centres. This is significantly different from the current AFTN/CIDIN topology in Europe, which is a partially-meshed network with a maximum of 12 connections (AFTN and/or CIDIN) from a COM Centre to its adjacent Centres. Appendix A to the ATS Messaging Management Manual [12] specifies how transition may take place from the current CIDIN connectivity and topology to a fully meshed AMHS network.

3.3.3.2 EUROCONTROL/NM approach for a hybrid topology

3.3.3.2.1 The EUROCONTROL/NM (former CFMU) is in a specific situation as a European Facility, which is an end-user of communication flows, rather than a COM Centre like other parties in the international AFTN/ CIDIN/ AMHS network. The organisation of the EUROCONTROL/NM in two Centres also creates specific requirements.

3.3.3.2.2 Because of the significant change between the current CIDIN topology and a fully-meshed network, and due to specific operational requirements related to EUROCONTROL/NM contingency (see AFSG/PG31 WP08, “Considerations in the integration of EUROCONTROL/NM in the AMHS network”, Roma, March 2008), EUROCONTROL/NM favours for AMHS a hybrid topology similar to the current CIDIN connectivity:

- A double-star to six adjacent COM Centres, through which EUROCONTROL/NM traffic is relayed to other communication partners;
- The existing AFTN/CIDIN topology between these six COM Centres and other COM Centres in Europe when the traffic flow is originated/directed to a State “beyond” those of the six COM Centres.

3.3.3.2.3 Such a topology could be revisited when more experience is gained in AMHS operation, and depending upon the availability of some automatic re-routing capabilities. Based on such conditions a more complete level of meshing could be envisaged. Such an approach clearly favours criteria 2 (availability) and 4, in order to reduce complexity of operation.

3.3.3.3 Approach favouring cost effectiveness

3.3.3.3.1 Based on the estimation that cost reductions could be obtained if only a partially-meshed topology is implemented, some States have expressed their intention to limit the establishment of direct links from their international MTA to the international MTAs in other States with which they have a given volume of traffic, or specific connectivity requirements.

3.3.3.3.2 In this approach favouring criterion 3 (cost effectiveness), the goal is to reduce the workload and cost of operation, including configuration, testing and in service support.

- Initial system configuration,
- Interoperability testing,
- Transition activity,
- In service support, including fault management,
- Re-testing when MTAs are changed and/or upgraded.

3.3.3.3.3 Whilst the intent to minimise operation costs is obviously a valid objective, this should not be detrimental to the overall quality of service and to the (partly contradictory) objective to minimise the number of hops in the network. Furthermore it may also be considered that when a certain number of AMHS connections is established from a COM Centre, and a high AMHS operational experience is available in that COM Centre, then the establishment of an additional connection to another COM Centre increases only marginally the cost of operation.

3.3.3.4 Influence of the current AFTN/CIDIN topology

3.3.3.4.1 This subject has been partly and/or indirectly addressed in the sections above.

3.3.3.4.2 With the assumption that approximately 50 States are part of the EUR Region, a fully-meshed AMHS network when AMHS is available is all of these States will also represent approximately 50 direct AMHS connections (international MTA to MTA associations) to/from each COM Centre. This number is to be compared to the current number of (intra-Europe) international connections to/from an international COM centre, which is between three and twelve links before migration to AMHS.

3.3.3.4.3 If transition was to take place quickly (e.g. between a few months and one or two years) from the pre-AMHS situation to such a fully-meshed topology, the effort would indeed be considerable and the target would be difficult to achieve. However, it is recognised that the transition to AMHS at the European scale will be progressive and may take a number of years.

3.3.4 Recommended European AMHS topology

3.3.4.1 The objective of this section is to specify a European AMHS topology which meets the various objectives expressed in section 3.3.3, taking into account the fact that they are sometimes contradictory.

3.3.4.2 The general principle adopted is that the expected quality of service, in terms of transit times and availability (criteria 1 and 2) should be maintained to define the target topology.

3.3.4.3 This leads to confirm that **the AMHS topology in Europe should be fully-meshed, as a long-term objective**. However, it should also be recognised that:

- there is a pre-requisite to the implementation of such a topology, which is the availability of a seamless underlying network across the considered geographical area;
- during the transition to this target topology, a partially-meshed network following the constraints of the various ANSPs and participants to the EUR AMHS network.

3.3.4.4 Principles need to be established for the transition phase, so that a clear direction is provided to ANSPs implementing AMHS in their COM Centres.

3.3.4.5 These principles are the following:

1. until a common underlying network at a European scale is available, the implemented AMHS topology should:

    a. **at least replicate the former AFTN/CIDIN topology**;

    b. in areas where a common underlying network is already available but for a smaller area than Europe (e.g. multi-States, or “sub-Regional”), **implement a fully-meshed AMHS island, with at least two entry points** into the island;

2. when a common underlying network at a European scale is available, and while transition to the fully-meshed target is in progress, the topology should be such that:

    a. **no more than two hops are needed for communication between any two International MTAs** in the considered area;

    b. **Two distinct paths are available at AMHS level** for communication between any two International MTAs.

3.3.4.6 The transitional partially-meshed topology specified in item 2 above can be achieved, for example, by the establishment of several partly overlapping fully-meshed AMHS islands:

- each pair of AMHS islands must have a non-empty intersection, with at least two "multi-island" AMHS COM Centres;
- the central facilities (e.g. EUROCONTROL/NM (former CFMU), EAD, etc.) must form a fully meshed island with the "multi-island" AMHS COM Centres.

3.3.4.7 This example is depicted in Figure 3.

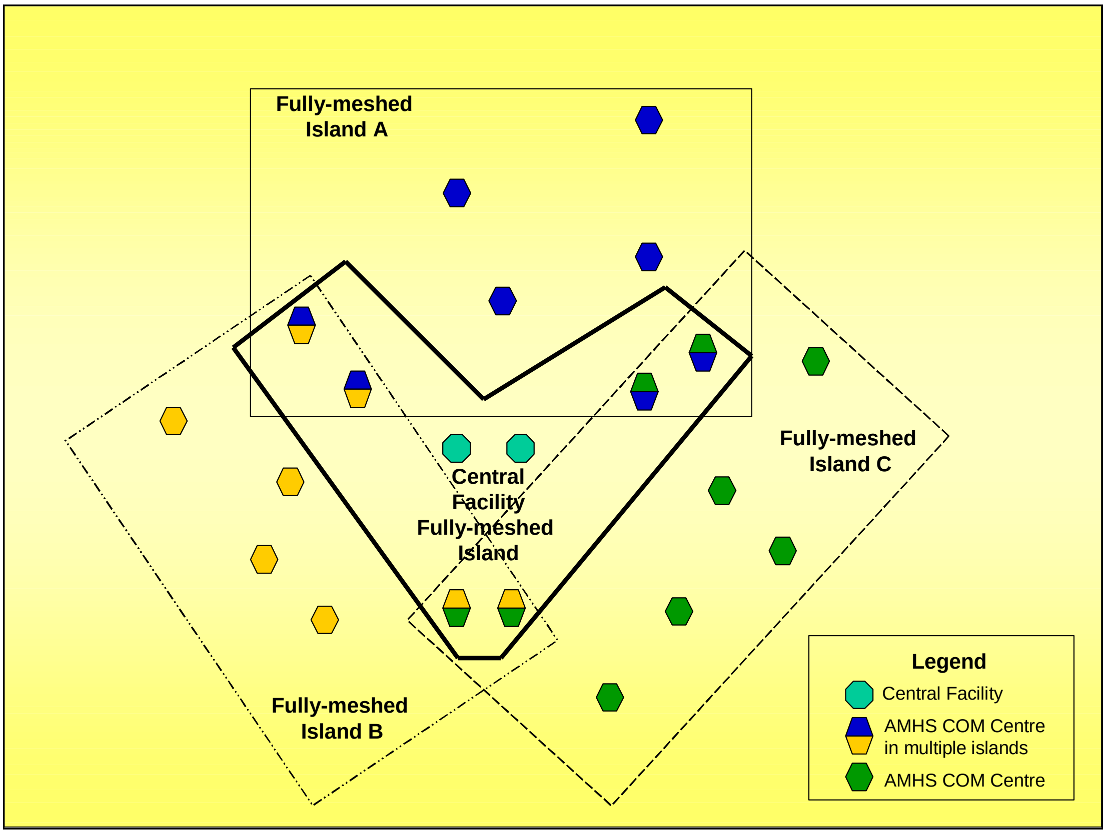

Figure 3: Example of partially-meshed AMHS topology before transition to fully-meshed

3.3.4.8 In line with the numerical requirements for QoS adopted in section 3.1.4, the strategy for AMHS topology may be reviewed on the basis of compiled AMHS operational experience, when a common underlying network at a European scale is available and a significant number of AMHS COM Centres are in operation.

3.4 Routing mechanisms

3.4.1 Available routing mechanisms

3.4.1.1 AMHS uses the routing mechanisms of its X.400 base standards. X.400 routing is static by nature, it uses the address attributes forming O/R addresses to determine the next hop towards which the message must be routed:

- local delivery,
- AFTN/AMHS Gateway (MTCU), or
- adjacent MTA inside the AMHS Management Domain of the current MTA,
- adjacent MTA in a different AMHS Management Domain.

3.4.1.2 Conceptually, X.400 routing tables are made of records associating a potential combination of address attribute values to a next hop. For each message, the route record with the best match for each AMHS recipient's address attributes is looked for in the routing table, to determine where the message is to be routed. In case of a message with multiple recipients and different routes, the message is "expanded" or "split" into several messages, according to the various destinations.

3.4.1.3 This section focuses on international AMHS routing, i.e. inter-domain routing.

3.4.1.4 Unlike in AFTN, where any substring from 1 to 7 characters may be used to determine a route, X.400 address attribute values are generally considered "as a whole" when looking for a best match. Some X.400 implementations may implement substring matching but this is not a standard feature.

3.4.1.5 Inter-domain routing, from an international MTA in an AMHS MD to an international MTA in another AMHS MD, should therefore use only entire address attribute values. The attributes country-name, ADMD-name, PRMD-name and potentially organization-name, usually represented by their initials C, A, P and O are sufficient for Inter-domain routing. The attribute organization-name must be used only in specific cases, when destinations are located in AMHS MDs with multiple International MTAs, and having implemented the CAAS Addressing Scheme.

3.4.1.6 It may be noted that ISO/IEC 10021-10 (2003) [22], which is aligned on ITU-T Recommendation X.412 (1999), "INFORMATION TECHNOLOGY – MESSAGE HANDLING SYSTEMS (MHS) – MHS ROUTING" describes an X.400/MHS Routing functionality based on Directory Services. There is no requirement to implement this feature in AMHS, including when the Extended ATS Message Handling Service is deployed.

3.4.2 X.400 re-routing mechanisms

3.4.2.1 Based on the general routing principles described above, re-routing consists in the definition of an alternative route to the intended destination, if for any reason there is a transfer-failure or delivery-failure to the initially determined next hop.

3.4.2.2 Re-routing may be either manual or automatic. In the first case, the MTA operator, in view of the transfer-failures, modifies temporarily (or definitively) the routing tables to specify an alternative next hop. The main requirements placed on the software by manual re-routing are related to:

- the ease of reconfiguration;

- the immediate applicability of the modification: it is preferable that the routing be modifiable on line, or require only a fast restart or parameter load.

3.4.2.3 Regarding automatic re-routing, although not prevented by the X.400 base standards, nor by the way they are designed, this feature was initially not a standard practice in X.400 products. The main reasons were the following:

1. MHS/X.400 was initially designed for messaging traffic with relatively low transfer time requirements, clearly non-real time, where it was possible to “wait” for the availability of a connection to the intended MTA, in case such a connection was not immediately available;

2. In this context, the usual practice in the store-and-forward MHS/X.400 is to store a message, and, in case of transfer failure to the next MTA, to perform a pre-defined number of “retry” towards this same MTA (based on timers), before a non-delivery-report is sent back to the message-originator (or to the originating-MTA).

3.4.2.4 However, due to the adoption of X.400 by communities with more stringent transfer time and availability requirements (Defence, Air Traffic Services), it should be possible to obtain from X.400 software manufacturers automatic re-routing mechanisms.

3.4.2.5 The principle of such re-routing would be that, after the number of retries to the main route to the next MTA, an alternative route already specified in the routing table would be used. It is important that those responsible for system operation be aware that this re-routing facility is activated.

3.4.2.6 Care should be taken about a possible interaction with X.400 timers when such a mechanism is used. For example, if no alternative route is specified, a MTA will retry to transfer until the expiry the MTA and MTS timers, before a NDR is generated. If an alternative route is defined, then a time allocation should be kept to use the alternative route before the timers expire. This should be considered in conjunction with the re-routing mechanisms at the underlying network level: timers and re-routing mechanisms at the underlying network level have to be shorter than timers and re-routing mechanisms at the AMHS level. The reason for this is that most of the time the unavailability of a P1 association is going to be caused by a transitional problem in the underlying network.

3.4.3 Routing in the recommended EUR AMHS topology

3.4.3.1 In the fully-meshed target topology, routing is trivial as there is a direct route from any International MTA to any other International MTA in the EUR AMHS network.

3.4.3.2 Transfer failures could be caused by unavailability of underlying network (that have their own resources to recover the failure, out of AMHS procedures) or by the failure of the destination MTA itself. In such a situation re-routing does not improve quality of service, but simply overloads the AMHS network by moving the problem from place to place. Depending on the underlying network and on the operator capability (e.g. depending upon the management tools and information available to him/her) to determine the reason of a failure, manual re-routing may however have benefit in some cases.

3.4.3.3 Automatic or manual re-routing is required, however, for efficient handling of AMHS traffic to other ICAO Regions (see next section).

3.4.3.4 In the temporary partially-meshed topology, the next hop for each destination MTA is either of the following:

1. the destination MTA itself, if a direct connection/route exists, or

2. an intermediate MTA which has a direct connection to the destination MTA.

3.4.3.5 The first case is identical to the situation of a fully-meshed AMHS network, where automatic re-routing is not really useful but manual re-routing may have some value, if an accurate fault diagnosis can be established.

3.4.3.6 In the second case, the availability of two distinct paths established as a design principle enables to use manual or automatic re-routing at AMHS level. Use of re-routing is essential in this situation, and automatic re-routing should be preferred whenever as it is available. This allows to make sure that the failure of an international MTA (e.g. in one of the multi-island AMHS COM Centres, in the depicted example) does not cause loss of communication between two islands.

3.4.3.7 Therefore, in the partially meshed network, it is recommended that:

1. one single route be specified in the AMHS routing tables if a direct connection exists,

2. a main route and an alternate route be specified in the AMHS routing tables if no direct connection exists and a two hops path is required between the considered MTA and the destination MTA.

3.4.4 Routing to/from other ICAO Regions

3.4.4.1 For message flows incoming to or outgoing from the EUR Region, the routing strategy is to route messages from/to one of the Regional boundary ATS Message Servers to/from the international MTA of the destination/source EUR AMHS MD, using either a single direct route if existing, or one of the main/alternate routes in case a two hops path is available between these MTAs.

3.4.4.2 The assumption is that, in the target environment, these Regional boundary ATS Message Servers would be implemented by States or ANSPs that already provide Regional boundary AFTN/CIDIN COM centres towards other ICAO Regions.

3.4.4.3 For resilience purposes, a minimal number of two inter-Regional boundary MTAs needs to be implemented to connect to each other ICAO Region. To gain full benefit of this duplication, automatic or manual re-routing is required, so that alternate routing via the "alternative" MTA can be activated in case of loss of connectivity with the "main" boundary MTA to be used.

3.4.4.4 The "alternative" MTA can be connected with the same MTA in the other ICAO Region, as the "main" MTA, or preferably it can also be connected with an alternative MTA in the other ICAO Region.

3.5 Underlying network

3.5.1 Background

3.5.1.1 In terms of the ISO/OSI seven layer model, AMHS resides in the application layer. The design of such an application is dictated by both the end users, who best know their particular needs, and by the state of the art technological environment, which determines the way in which these needs are transformed to concrete technical specifications. The current situation, the way of migrating from this situation to the targeted future, the process flow, the safety requirements, the security requirements, the quality of service requirements and the expected results are all translated into the application specification. These requirements not only affect the design of the application but their influence permeates to the lower layers.

3.5.1.2 Therefore, the creation of an appropriate underlying network is seen as essential for the smooth deployment of AMHS.

3.5.2 General principles

3.5.2.1 In current communications practices, the independency between application and network levels is highly desirable.

3.5.2.2 The separation of application and network brings several benefits:

- the provision, development and management of the network and AMHS can proceed largely independently (provided sufficient capacity is available within the network), leaving each discipline free to concentrate on its particular sphere of competence,
- there are economies of scale to be gained by the sharing of the network between multiple applications, resulting in better utilisation of resources,
- the increased size of the network (over a purely AMHS network) should deliver a better quality of service and in particular a more robust infrastructure,
- routing, at the AMHS level, is independent of the lower level network and in particular any European International ATS Message Server is directly accessible by any other.

3.5.2.3 The logical connection (links) of the AMHS topology implemented by means of a transport service could make use of the physical connectivity provided by a layer-3 network infrastructure.

3.5.2.4 The following Figure 4 illustrates the relationship between logical and physical connectivity for the international AMHS. Each international COM centre will accesses the underlying network over the local network node through a network access line.

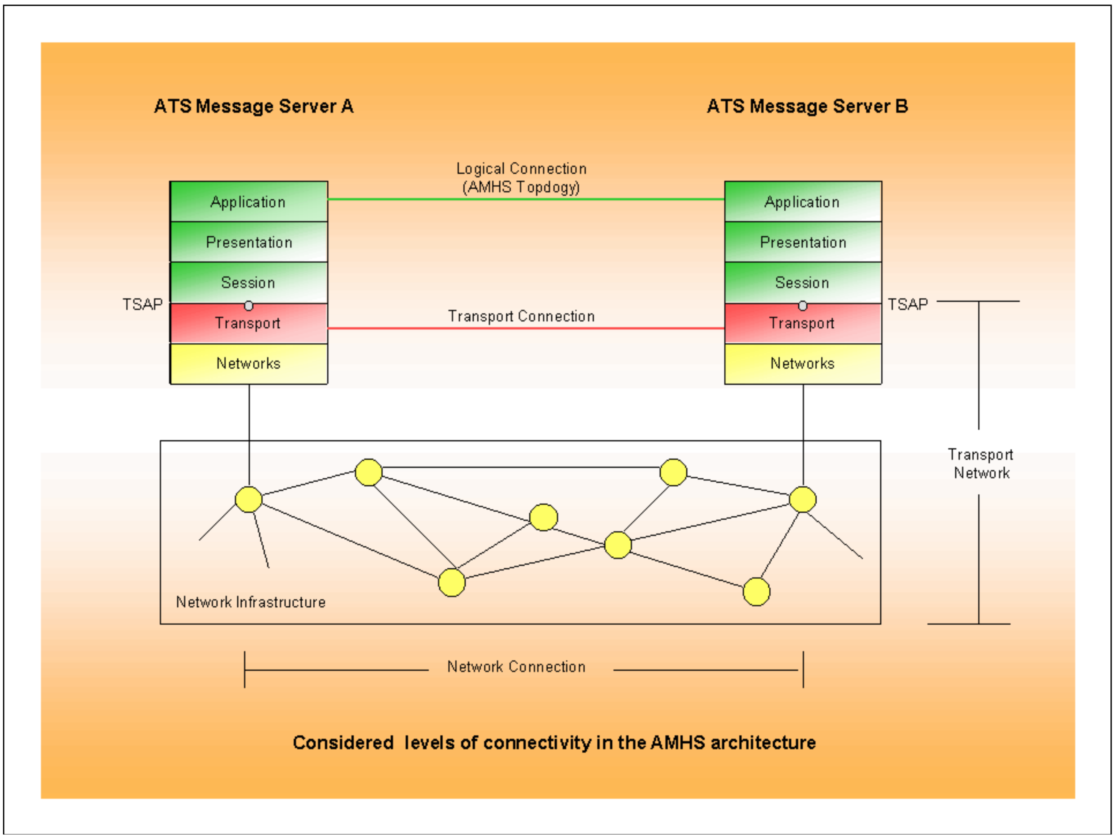

Figure 4: Logical and physical AMHS connectivity

3.5.3 Considerations

3.5.3.1 In the European area, a European wide TCP/IP based communications service dedicated to Air Traffic Management Communications is envisaged for supporting current and forthcoming applications.

3.5.3.2 This approach is supported by ANSPs' large experience in defining general principles (addressing, routing, …) and providing TCP/IP services for supporting ATC operational applications.

3.5.3.3 Furthermore, concerning international communications, ANSPs are acquiring expert knowledge about underlying network interoperability.

3.5.3.4 The European AMHS will be implemented on top of a TCP/IP stack, as stipulated by EANPG Conclusion 44/45:

> "That, States in the EUR Region use the TCP/IP communication protocol for the initial implementation of ATS Message Handling Systems, as a transition mechanism to enable AMHS operations to commence ahead of eventual full SARPs compliant data transmission systems."

3.5.3.5 At the time of the EANPG conclusion, the reasons for using TCP/IP communication in support of AMHS operation were:

1. There was no European ATN/OSI internet communication service available, nor were there any real plans for implementation of such a service for other ATN applications in a timeframe compatible with the short-term implementation planned for AMHS. In the longer term, i.e. for the target profile, there was no sufficient reason identified that could

justify the substitution of the initial TCP/IP underlying network with a fully ATN-compliant infrastructure.

2. Following successful testing results, there was a straightforward activity supported by EUROCONTROL and Member States, aiming at the establishment of an international TCP/IP infrastructure for aeronautical purposes in the ECAC area.

3. There were already national AMHS implementations in place based on the TCP/IP protocol suite. In addition, ANSPs have the necessary TCP/IP expertise on hand from various national applications.

4. The broad market of TCP/IP products would facilitate rapid implementation with reasonable costs.

3.5.3.6 Through Amendment 83 to ICAO Annex 10 (November 2008), the possibility to implement ATN/IPS was introduced into the SARPs, thus rendering the deployment of AMHS over TCP/IP fully SARPs compliant.

3.5.3.7 The de-coupling that exists in an AMHS system between upper layers and lower layers (transport and network services) allows implementing AMHS systems with multiple lower layer protocol stacks (ATN/OSI, TCP/IP, TP0/X.25).

3.5.3.8 The ability to implement AMHS over multiple lower layer stacks may be used to ensure global AMHS interoperability. In particular, as other Regions may deploy AMHS based on ATN/OSI, there could be a need for a limited number of Regional boundary ATS Message Servers (inter-Regional entry-exit points) to implement dual stacks. However, as most AMHS products support TCP/IP, the relevance of such a requirement can only be determined when inter-Regional communication discussions are initiated between peer inter-Regional entry-exit points.

3.5.4 Conclusion

3.5.4.1 An underlying network infrastructure that can provide physical connectivity between AMHS systems needs to be implemented as a Common Facility, in a timeframe compatible with the short-term AMHS deployment plan. It is foreseen that the Pan-European IP network resulting from the ongoing PENS programme, launched under the aegis of EUROCONTROL, will form an appropriate basis for this network infrastructure.

3.5.4.2 Bilateral or multilateral connectivity arrangements should be made to accommodate initial AMHS operations, until such a common facility becomes available.

3.5.4.3 In any case, the AMHS Quality of Service requirements, as they are prescribed for the various flow class types, should be supported by any type of underlying network infrastructure used. In this direction, the recommended availability is in the order of 99.99% with a mean time to restore outages in the order of 5 minutes.

3.6 Interregional communication aspects

3.6.1 Guidance provided by ATNP on "AMHS over TCP/IP"

3.6.1.1 As a consequence of EANPG Conclusion 44/45, the ATNP provided guidance for implementation of “AMHS over TCP/IP” in 2002. Following the introduction of ATN/IPS SARPs through Amendment 83 to Annex 10 in 2008, these guidelines have been superseded by events, but they are **presented** hereunder **for historical purposes**.

”1. It has been observed that some States or even Regions are implementing or planning to implement AMHS systems making use of lower communication layers that are not conformant to the ATN Internet Communication Services (ICS). Such AMHS systems conform to Doc 9705, Sub-Volume III, Chapter 1 (replaced with Amendment 83 by Doc 9880, Part II), with the exception of the clauses related to interfacing with ATN ICS. The most frequent occurrence of such non-compliant systems is related to AMHS systems making use of TCP/IP lower layers through a RFC1006 interface ("AMHS over TCP/IP").

2. Due to the store-and-forward nature of the AMHS, this can be done without compromising the end-to-end interoperability at the AMHS application layer with SARPs-compliant AMHS implementations, but at the cost of some dual-stack systems[4] for lower layers. Strict conformance to Doc 9705, Sub-Volume III, Chapter 1 is required, with the only exception of clause 3.1.2.2.2.1.2 ("Use of Transport Service"), to ensure such end-to-end interoperability.

3. The reasons invoked by States adopting such local policies include the following:

- The need for an immediate or short-term transition from existing ground networks, and in particular from X.25 networks that are reaching obsolescence;

- The use of a common ground network infrastructure shared with other ground applications, such as radar data distribution or inter-centre communications (such as OLDI in Europe), such infrastructure being sometimes already in operation.

4. It should be noted that in all known cases, the IP network used or planned to be used is a network infrastructure in which switching equipment and links are dedicated to ATS communications, building a so-called "private" IP network.

5. It is recognized that other transition strategies can also be developed, that make use of the proposed IP SNDCF to enable IP sub-networks to be used as ATN sub-networks, in a fully SARPs-compliant ATN ICS architecture. However such an architecture is not discussed in the present document.

6. Despite the fact that the implementation of "AMHS over TCP/IP" can meet, as described above, the specific objectives of a State on a local or regional basis, the attention of implementers should be drawn to the fact that the implementation of two different architectures has the following drawbacks:

- It limits "any-to-any" communication between AMHS systems on a global basis that could be needed in specific cases, e.g. for performance requirements;

- it requires the implementation by some States of "dual-stack" AMHS systems, to gateway between AMHS systems using the ATN ICS and AMHS systems using TCP/IP. This may reduce performance and availability;

- The cost of such gateway facilities is expected to be borne by States implementing non SARPs-compliant AMHS systems.

7. In view of the elements above, the following guidance is offered by the ATN Panel on the use of "AMHS over TCP/IP":

a) "AMHS over TCP/IP" implementations should not be presented as fully SARPs-compliant ATN implementations.

---

[4] Such dual-stack systems are beyond the baseline ATN architecture which is specified by ICAO.

b) Non-SARPs-compliant "AMHS over TCP/IP" implementations are seen as a “local solution” within a State or Region. Inter-State or inter-Regional connections between such systems using TCP/IP should be subject to bilateral/regional agreements.

c) States or Regions that implement "AMHS over TCP/IP" systems within their domains are responsible for taking those necessary measures to ensure interoperability with SARPs-compliant implementations in other States or Regions.

d) Appropriate security measures should be taken when using an IP network, irrespective of whether AMHS uses TCP/IP directly or via the IP SNDCF.

8. The ATNP will continue to monitor related developments and will provide further guidance as appropriate.”

3.6.1.2 With introduction of the Internet Communications Service (see Doc 9880 – Part III [4]) the “European” solution “AMHS over TCP/IP” is now fully SARPs compliant.

3.7 European Directory Service

3.7.1 This section provides general information on the European Directory Service (EDS) Operational Concept. Appendix G of the EUR AMHS Manual provides the details of the concept.

3.7.2 Directory services are seen as a global function. However they are expected to be implemented at a regional and international level rather than on a global basis. The EDS is specified as a common European facility but is also open to support, to coordinate with and to integrate with States and Organisations outside Europe. The EDS Operational Concept considers distribution and use of information at the national level a local implementation matter.

3.7.3 The EDS Operational Concept adopted and refined the approach of the ATN Directory as specified by ICAO Doc 9880 Part IV. The EDS is specified in support of ATN applications such as the AFTN/AMHS Gateway. In addition the EDS supports human users interfacing the EDS through their Directory User Agent (DUA).

3.7.4 The architecture of the EDS allows for centralised management of information, versioning of information as well as periodic and automated distribution of information using X.500 Directory protocols. In parallel the EDS Operational Concept reduces the individual effort of States and Organisations for management and coordination.

3.7.5 The EDS Operational Concept takes into account the existing infrastructure for management and distribution of AMHS address information by the ATS Messaging Management Centre (AMC) and deploys the EDS in three steps. In the first, initial step, the information is maintained and managed by AMC and distributed by AMC and EDS. In the second, intermediate step, the information is maintained by EDS and managed and distributed by AMC and EDS. In the third, final step, the information is maintained, managed and distributed by EDS. The stepwise introduction of EDS for AMHS address information ensures a smooth introduction of European directory services and seamless operation of the AMHS.

3.7.6 In support of the AMHS, the EDS provides and distributes in the initial step information to support the messaging functions name resolution, user capabilities and AFTN/AMHS address conversion. The EDS is prepared to support further ATN applications and functions such as AMHS security.

4 European ATS Messaging Service Profile

4.1 Introduction

4.1.1 The detailed specifications for ATSMHS are currently spread over a number of different documents such as the ISO/IEC ISPs, ICAO SARPs and technical specifications (Annex 10 and Doc 9880) and the SPACE Final Report.

4.1.2 The EUR-ATSMHS Profile is intended to provide one single document that brings together these specifications by referencing the basic documents and by providing any additional specifications necessary for ATSMHS implementation in the EUR Region.

4.1.3 The scope of the Profile is limited to the specification of those aspects of systems that are involved in exchange ATS messages between international COM Centres. Other aspects, that involve gateways e.g. to the AFTN and CIDIN or communications that remain entirely within a State, are not dealt with in this Profile.

4.1.4 The first version of the EUR-ATSMHS profile was developed by EUROCONTROL. Following a thorough review procedure which was supported by various stakeholders (suppliers, SPACE, COMT, AFSG), the Profile has been approved for use in the specification and procurement of AMHS systems in the EUR Region and it has been included as Appendix B to the EUR AMHS Manual.

4.2 EUR ATSMHS Profile Objectives

4.2.1 The purpose of the Profile is to provide a single, relatively short specification containing interoperability requirements between international Message Transfer Agents (MTA).

4.2.2 Furthermore, the Profile contains the following requirements applicable within the EUR Region:

- Use of TCP/IP for the underlying Data Communications Service;
- Message Legal Recording;
- Distribution Lists;
- Use of IPM File Transfer Body Parts for the transfer of binary data (e.g. to support WMO BUFR coded messages);
- Specifications of message maximum and minimum lengths (e.g. to support ADEXP messages).

4.3 Scope of Profile

4.3.1 The EUR-ATSMHS Profile specifies a number of AMHS protocols and systems capabilities for the exchange of ATS messages between direct and indirect AMHS users through international MTAs. In other words, the Profile is intended to ensure end-to-end message transfer between International COM Centres over AMHS.

4.3.2 The Profile is applicable to the following aspects of message interchange:

- Transfer of messages between the AMHS systems at International COM Centres operated by different ANSPs;

- Submission, Delivery and Retrieval of messages that are to be transferred between AMHS systems operated by different ANSPs;
- The content of Message Envelopes, IPM Headings, Body Part Types and AMHS Addressing used for the protocols identified above.

4.3.3 The Profile does not specify any of the purely local requirements within an ANSPs individual systems – e.g. MTS Access, MS Access, and interconnections between MTAs within an ANSP's Private Management Domain, other than to ensure adequate interchange of ATS messages internationally. Nor does it specify aspects of interconnections between Regional AFTN/AMHS Gateways where additional requirements may apply, such as support of an ATN lower layer protocol stack as specified in ICAO Document 9880, Part III [4].

4.3.4 Access to the Directory Information used to support Directory Name Resolution and address mapping between AFTN and AMHS address forms is indicated for information only.

4.3.5 The following diagram illustrates the scope of the protocols and system types specified in the EUR-ATSMHS Profile:

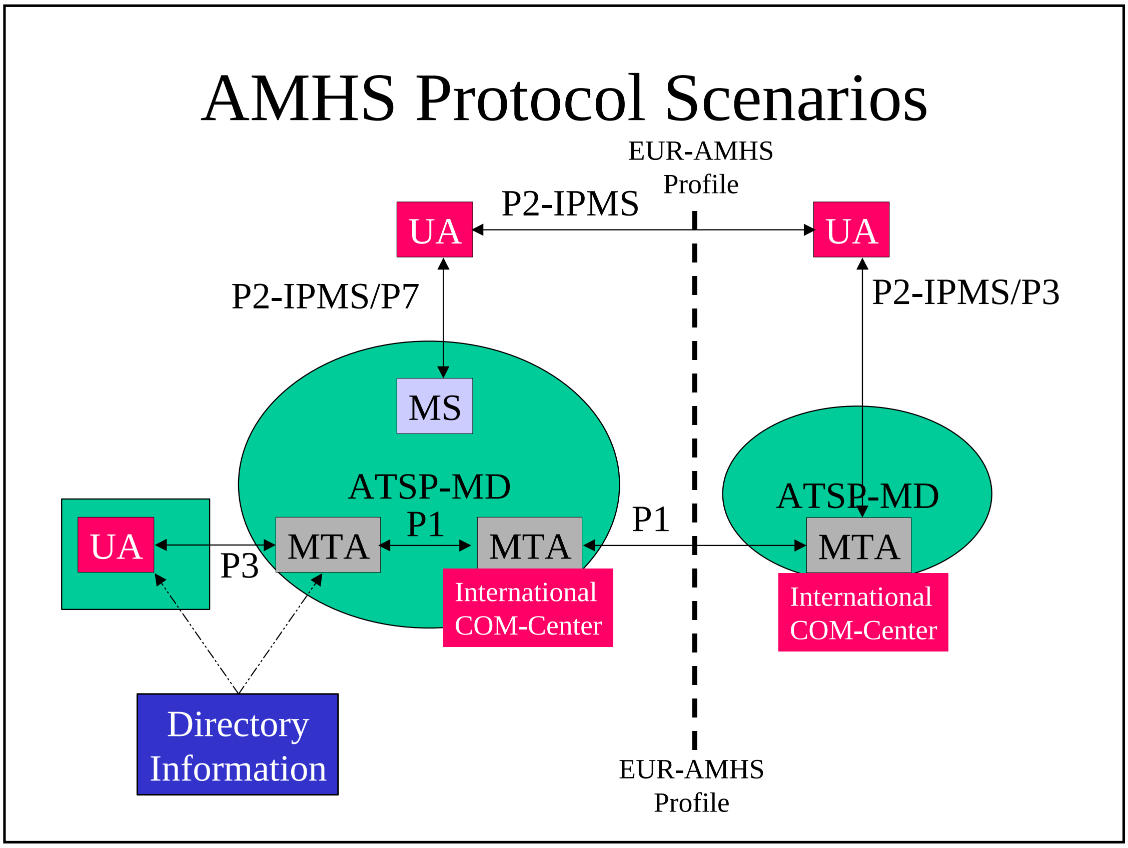

Figure 5: AMHS Systems and interconnecting Protocols

4.3.6 The Profile applies to the following AMHS system components:

- User Agents UA
- Message Transfer Agents MTA
- Message Stores MS

4.3.7 The Profile applies to the following AMHS protocols:

- IPM Content P2

- Message Transfer P1
- Message Submission/Delivery P3
- Message Retrieval P7

4.3.8 The Profile specifies a Profile of ATS Message Handling Service conformance called the EUR-AMHS Profile. It is based on the requirements of following:

- The Basic ATS Message Handling Service (Bas), introduced in the Doc 9880, Part II, para. 1.1.3-1.1.8;
- A number of further Functional Groups and options selected from the Extended ATS Message Handling Service (Ext), introduced in the Doc 9880, Part II, para. 1.1.3-1.1.8;
- Further requirements specified by the SPACE Final Report for use in Europe.

4.3.9 The resulting scope is sufficient to ensure inter-State message interchange using AMHS according to the Basic AMHS requirements stated in Doc 9880, which covers Basic Message Transfer Capabilities, Distribution Lists, appropriate message size capability and Legal Recording.

4.3.10 In addition, the following requirements are included:

- Use of TCP/IP as the underlying Data Communications Service;

It must be pointed out that specification of an AMHS based on TCP/IP necessarily references a wide range of standards from different sources. This is complicated by the fact that procurement of a complete AMHS/TCP solution involves the specification of three different system component types (Message Transfer Agents, Message Stores and User Agents), each of which has a number of implementation options. The Profile therefore also provides guidance on the correct use of the referenced ISO/IEC ISPs, ICAO Documents and Internet RFCs for each type of system.

- Provision for the transfer of binary data using the File Transfer Body Part

It must be pointed out that the originally planned mechanism for this requirement was to use the Bilaterally Defined Body Part. However, this was found to be deficient in two ways:

a) its use is now discouraged by the base standards;

b) it provides no way for recipients to determine the nature of the binary encoding actually contained in a received Bilaterally Defined Body Part.

For these reasons, the use of the Bilaterally Defined Body Part was removed from old Doc 9705 during 2003 now Doc 9880, Part II, and was replaced by the File Transfer Body Part, which is known to overcome the previously mentioned drawbacks.

4.3.11 Security requirements are not a mandatory part of the EUR-ATSMHS Profile. However, the Profile mandates IP address validation and the protocol includes system identification following transport connection establishment. It must be pointed out that certain Messaging Application Security functions are also mandated in the MHS S0 optional Functional Group for the Extended ATS Message Handling Service but these are not mandated by this Profile.

4.4 Use of the Directory

Under development

4.5 Application/Service oriented AMHS Profiles

4.5.1 The EUR ATS Messaging Profile, as described in Appendix B to the EUR AMHS Manual, defines the specifications necessary for ATSMHS implementation in the EUR Region. Nevertheless, the support of the complete set of features defined by the EUR ATS Messaging Service Profile from user agent implementations developed for given applications/services, acting in limited environments, may not be necessary.

4.5.2 In order to facilitate the adoption of the ATS Message Handling Service by end users dedicated for specific applications/services, the support of a subset of requirements can be accepted. The requirements that need to be supported should be specified per case depending on the specific application/service. Appendix H to the EUR AMHS Manual defines such ‘Application/Service oriented AMHS Profiles’.

5 System implementation - Guidelines for system requirements

5.1 Introduction

5.1.1 This section is intended to deal with technical and operational requirements for a COM system replacing the AFTN/CIDIN system by an AMHS or adding the ATSMHS capability. As indicated by its title, this section covers guidelines for requirements not specified in the AMHS technical specifications, but considered by the Group important enough for being included in a Call for Tender for the procurement of an AMHS system.

5.1.2 The main input of this section was a subset of the specifications of an actual Call For Tender issued by one of the Group members, adapted and modified in order to have a 'template' able to be used by any ANSP who intends to procure an AMHS system.

5.1.3 The section covers technical and operational requirements like:

- General facilities
- Addressing - mapping table facilities
- Queue management facilities
- Message repetition facilities
- Tracing facilities
- Sizing
- Availability and reliability
- Malware protection

5.1.4 For such a COM system in the following paragraphs the term "**AMHS System**" will be used.

5.1.5 Due to the character of this section (as guidelines for system requirements) the term "**should**" is used. In a specific Call for Tender this term can be replaced by shall.

5.2 General requirements

5.2.1 The AMHS System should implement the ATSMHS and AFTN/AMHS Gateway facilities in accordance to the specifications defined in the latest approved ATN technical specifications for Basic Services, but supporting AFTN messages with a message length up to 64 Kbytes.

Note.– This requirement is not covered by the technical specifications, which mandate support of standard AFTN message length only.

5.2.2 The AMHS System should support the monologue dialogue-mode and one or several incoming and outgoing P1 associations with an MTA partner simultaneously.

Note.– An MTA may establish permanent or dynamic (i.e. on-demand) P1 associations. The type and specific number of associations to be set up for operations depends on different factors and has to be agreed between the MTA partners, after consideration of their traffic exchange requirements.

5.2.3 The AMHS System should support simultaneous associations with several MTA partners (one or several associations with each MTA partner) with the same or different “transport” protocols (e.g. TCP/IP to be used within EUR, ATN/OSI).

5.2.4 The AMHS System should support the total number of simultaneous associations (sum of all associations) without any restrictions caused by inherent limitations of the system (memory, interfaces, etc).

5.2.5 The AMHS System should allow control of establishment of associations with MTA partners via on-line operator commands; i.e., it should be able to:

- Prevent/allow the establishment of associations with a given MTA partner by AMHS System (local MTA), by MTA partner only or by both partners.
- Prevent/allow the establishment of associations with all configured MTA partners by AMHS System (local MTA), by all MTA partners only or by all partners.
- Force the termination of associations already established with a given MTA partner.
- Force the termination of associations already established with all configured MTA partners.

Note.– The number of actual simultaneous associations to be supported will depend on:

- o *the target 'logical' AMHS network topology: for example each centre establishes direct associations with all the other centres or each centre establishes associations with adjacent centres only (as in AFTN);*
- o *whether permanent or dynamic connections will be established. Such distinction is only applicable in case there is no requirement for continuous traffic exchange.*

5.2.6 The AMHS System should implement MTA queues. These queues will keep the AMHS messages that:

a) either are pending to be sent;

b) or have been transmitted but for which a delivery report is expected.

Note 1.– The queue referred to in a) is typically implemented in the MTA.

Note 2.– The queue of messages for which a DR is expected is normally implemented in the User Agents and MTCUs of the AFTN/AMHS Gateways.
The reaction of an AMHS System in case of loss of a DR is fixed (implementation matter): E.g., would it have to resend the message after timeout? How many attempts to resend the message should be made? A DR or NDR is addressed to the originator of the message; therefore it should be left to the originator to react upon non-arrival of a DR as it is his task to react upon reception of a NDR. If the originator is an indirect (AFTN) user, the AFTN/AMHS Gateway has to perform this task on his behalf. Furthermore, a report may take another route than the message it refers to, that means it does not necessarily pass through the same MTAs as the original message.

5.2.7 There should be a logical MTA queue per configured MTA partner. Management of these queues is specified in section 5.4).

5.2.8 The configuration of an MTA partner (via on-line commands) should provide flexibility for each of its parameters. For example:

a) It should be possible to configure the “transport” protocol (e.g. ATN, TCP/IP, TP0/X.25) to be used per each MTA partner.

b) In case of selection of TP0/X.25, it should be allowed to configure at least two local X.25 attachments to be used for the connections, several calling – called addresses to be used for initiating a call or acceptance of an incoming call, etc.

c) It should be possible to configure the maximum number of simultaneous associations with each MTA partner.

d) It should be possible to configure whether the associations have to be left permanently established or whether they have to be established and closed depending on traffic.

5.2.9 The AMHS System should allow configuration of all profile items if possible.

5.2.10 The AMHS System should allow configuration of the following profile items, at least:

a) Mapping between AFTN priorities and AMHS Message Transfer Envelope priorities.

b) Values of “rn” and “rnr” in the notification-requests element in the recipient fields in the IPM heading. These values should depend on the value of the AFTN priority.

Note 1.– Both functions are implemented in the UAs and MTCUs of the AFTN/AMHS Gateway as the MTA does not deal with the ATS Message Priority (or AFTN priority) which is contained in the ATS Message Header as part of the IPM body.

Note 2.– The technical specifications specify the values of these profile items. It is good practice that the implementation allows the possibility to change them just by configuration in case operational experience recommended other settings. The processing is an implementation matter.

5.3 Addressing – mapping tables requirements

5.3.1 The AMHS System should support the CAAS (see section 3.2).

5.3.2 The AMHS System should process and manage AMHS messages received with the O/R name in the XF Addressing Scheme also, even if the ANSP has chosen the CAAS for its internal users.

5.3.3 The AMHS System should provide mechanisms to import mapping tables needed in the AFTN/AMHS Gateway. The tables to be imported will be downloadable from the AMC system.

5.3.4 The implemented facilities in the AFTN/AMHS Gateway which map an AFTN address to an O/R name should be flexible enough to accommodate different O/R structures (Addressing Schemes) and use the minimum number of configuration / lookup tables with the minimum number of entries. As an example for the implementation of the mapping of an AFTN address to an O/R name, the following information should be entered in configuration tables:

a) Attributes and associated values that are fixed for each State. E.g. in the case of States using the address scheme described in section 3.2 the attributes and associated values to be entered should be country-name, ADMD-name and PRMD-name. Each entry will be indexed by the ICAO routing area or State/territory identifying letters (first characters of the AFTN address).

b) Attributes whose values can be determined directly from the AFTN address. E.g., in the case of States using the CAAS described in section 3.2, the organizational-unit-names attribute (first to fourth characters in the AFTN address) and the common-name (all characters in the AFTN address) should be declared here for them.

c) Attributes whose values depend on a mapping table. For each such attribute for each State, the following should be specified: the name of the mapping table and the subset of the AFTN address (e.g. one to four first characters, the complete AFTN address, wild characters could be used to define the subset ...) that gives the index to the mapping table. The mapping table itself should also be provided. E.g., in the case of countries using the CAAS address scheme described in section 3.2, the value for the organization-name attribute should be defined this way.

5.3.5 The possibility to use a directory should also be contemplated, even if this is not part of the Basic Services.

5.4 Queue management requirements

5.4.1 The AMHS System should provide, in addition to a pure diversion facility of outgoing queues, a reprocessing of messages in X.400 (outgoing) queues in case of longer outages of adjacent MTAs (non-reachability).

Note.– Such reprocessing facilities will be very important during the time period when both AMHS and AFTN/CIDIN centres coexist in the EUR Region.

5.4.2 Two types of reprocessing should be envisaged:

- at the pure X.400 level;
- at the AFTN level (in the case of AFTN/AMHS Gateways).

Reprocessing at the pure X.400 level

5.4.3 The reprocessing at pure X.400 level should allow:

- to extract messages waiting in an X.400 queue from this queue;
- to process these messages again by the X.400 routing software; and
- to route according to possible new or temporarily modified X.400 routing tables.

Such a mechanism would allow to extract the messages from the queue associated to a non-reachable MTA. The messages could be routed through another centre (MTA) and forwarded through the alternate route only for those recipient addresses for which alternate routes have been activated. For all other recipients addresses the messages remain in the queue. This kind of reprocessing prevents a general forwarding of messages to other centres (MTAs) containing recipient addresses for which rerouting is not intended.

5.4.4 The reprocessing at the pure X.400 level should be present in the ATS Message Servers, in AFTN/AMHS Gateways.

Reprocessing at the AFTN level

5.4.5 The reprocessing at AFTN level should allow:

- to extract messages waiting in an X.400 queue;
- to re-process them by the AFTN layer; and
- to route them according to the current AFTN, CIDIN and X.400 routing tables respecting the updated route availability information (predefined alternate routing).

This reprocessing would solve the problem of non-reachability due to outages, in a heterogeneous AFTN/CIDIN/AMHS environment.

5.4.6 An X.400 queue can contain messages, reports and probes. The AFTN reprocessing function should only concern the messages.
These messages can be of different 'types': messages from AFTN/AMHS Gateways, 'pure' UA to UA exchanges, etc. All these messages will be IPM messages, so there is no way to distinguish them at the X.400 (envelope) protocol level.

5.4.7 The reprocessing should be restricted to messages generated by an AFTN/AMHS Gateway.

5.5 Message repetition requirements

5.5.1 The AMHS System should provide powerful message repetition facilities in the AFTN, CIDIN and AMHS subsystems implementation.

5.5.2 The repetition facilities should be able to repeat messages as they were originally transmitted i.e. sent to all recipients following the same transmission paths.

5.5.3 Additionally, the repetition facilities should be able to specify (with the use of wildcards) 'detailed' or 'generic' destinations. Such destinations can be an AFTN address, an O/R name, all AFTN addresses mapped to a given Ax, all O/R names of a given PRMD, etc.

5.5.4 The AMHS System should find all the messages that were transmitted to such specified 'generic' destinations within a specified time interval and retransmit them only to pending destinations and following the current routing. To avoid a transmission to other destinations originally contained in the message the addresses not matched by the 'generic' destination should be suppressed (address stripping).

5.6 Tracing facilities requirements

5.6.1 The AMHS System should provide a facility to allow generation of X.400 probes.

5.6.2 The user interface of the facility should allow entering of the priority, the O/R name of the originator / destinations and the message length.

5.6.3 The AMHS System should send the reports regarding the probes (delivery, non-delivery) to a configurable instance (e.g. the rejection queue).

Note.– This requirement relates to a user interface requirement. The user needs some notification when the delivery report related to the probe has been received. It is an implementation matter to decide whether this is performed just by allocating a fixed originator O/R name to one of the queues of the system or by another way.

The contents of such reports should be decoded and presented in a 'human' readable and understandable format.

5.6.4 The AMHS System should provide association-tracing facilities to monitor in real time the establishment, interruption and finalisation of associations related to adjacent MTAs.

5.7 Sizing requirements

5.7.1 The sizing of the AMHS System operational platform should support the traffic in peak hour situations with:

a) Average peak hour total CPU usage at 30% maximum.

b) Communication adapters loaded at a maximum 30% of their real bandwidth capacity (not the theoretical one) and excluding the redundancy needs.

Note.– The previous values have to be reconsidered by each ANSP depending on the expected lifetime of the AMHS System. As e.g., if the lifetime is expected to be 10 years and the traffic estimates for the peak hour relate to the end of the lifetime, the usage requirements for the CPU and the communication adapters are typically greater than 30% (if not, the purchased system will be oversized during quite a number of years).

c) Processing time of a message (High QoS flow type class, see section 3.1) at least less than 1.5 seconds. The processing time is defined as the difference between the moment the latest character of the message enters into the AMHS System and the moment the first character of the message is sent out. This applies for all implemented in / out protocol combinations. For messages of other flow types, the processing time should be less than 3 seconds.

Note.– This value, especially for AMHS, has significant implications in the platform sizing and total network transit time (this also depends on the network topology, see section 3.3 AMHS topology). If the value is too low, a very powerful platform is required; If the value is too high, it could introduce a significant delay in the overall message transmission (especially if the other centres also have high values).

d) Response time to configuration / management on-line commands less than 3 seconds. This response time is related to requests from a management position for actions which do not require a query / browsing of a log (e.g. close a PVC, create an Ax, etc).

e) At least 50% of the disk space remaining available after:

i) all the standard and specific developed software versions (including the possibility of more than one software versions and two configurations per version) are present on disk,

ii) all logs and archive folders corresponding to the number of days to be kept on-line in the system are present on disk.

Note.– The precise number of days depend on the particular policy of each ANSP to comply with the ICAO Legal Requirements (see section 9.1 Legal Recording in AMHS).
If its policy indicates that all the data has to be kept on the AMHS System, the system is dimensioned to support at least 30 days. If the policy indicates that the data are saved for such purpose somewhere else (e.g. in another system, in an external media like CD-ROM, DAT, cartridge, etc.), data concerning fewer days need to be kept on-line (e.g. three days, one week...).

Note.– As for the CPU and communication adapter usage, the value for disk space is reconsidered by each ANSP depending on the expected lifetime of the AMHS System and the traffic estimates related to this lifetime.

5.8 Availability and reliability requirements

5.8.1 The AMHS System should operate 24 hours per day and 365 days per year.

Note.– The values provided below represent 'minimum' requirements. Each ANSP may reconsider them according to its own policy and internal SLAs with its internal users.

5.8.2 Interruptions for system maintenance and installation should be limited to the strict minimum and should be less than 60 minutes.

5.8.3 After power is switched on, the AMHS System should be fully operational after a maximum of 15 minutes.

5.8.4 The AMHS System should auto monitor:

- the state of its application processes;
- the state of its system processes;
- the state of its system components (hardware).

5.8.5 The AMHS System should generate an SNMP MIB of the states monitored (see above).

5.8.6 The AMHS System should automatically try to recover from failure conditions in its application processes. If it is not possible to recover without impacting the service, the AMHS System should terminate all its application processes in an orderly manner and restart them afterwards automatically.

5.8.7 The AMHS System should allow an operator to:

a) Stop the AMHS application gracefully (with automatic restart).
b) Stop the AMHS application gracefully (with no automatic restart).
c) Force the AMHS application to stop (with no automatic restart).
d) Start the AMHS application with message recovery (messages that were in queue when the system was stopped are processed and forwarded).
e) Start the AMHS application without message recovery (messages that were in queue when the system was stopped are discarded).

5.8.8 The AMHS System should lose no message that has been acknowledged by it (according to the respective messaging protocol), unless an operator explicitly requests to drop the messages.

5.8.9 The AMHS System should lose no message because of its load.

5.8.10 In case of a switchover (cluster, master/standby) configuration the following requirements apply:

a) After detection of failure of the primary system unit or after an operator command, the switchover process should last less than five minutes. The duration of the switchover is counted as the time from the failure detection (or operator command) until the time the AMHS restarts forwarding messages again (assuming there are messages in queue or there are new incoming messages).
b) The time needed for the standby unit to detect failure of the primary one should be less than three minutes.
c) The switchover process should be completely automatically without requiring any plugging/unplugging of any type of cables (communications, disks ...). A matrix switch action (if a matrix switch is proposed) is not considered as a cable plug / unplug.

5.8.11 Any period of time longer than one minute, during which the AMHS System does not perform message switching (in a total or partial manner) due to software or hardware problems, should be considered as an interruption of service.

5.8.12 An interruption of service of an AMHS System should be less than 10 minutes when the recovery is automatic. The duration of an interruption is calculated as the time from the moment the last received message was forwarded until the moment the AMHS System starts forwarding messages again (assuming there are messages in queue or there are new incoming messages).

5.8.13 There should be no more than one interruption of service without automatic recovery in a sliding window of six months.

5.8.14 There should be no more than one interruption of service with automatic recovery per day.

5.8.15 There should be no more than two interruptions of service with automatic recovery per month.

5.8.16 There should be no more than three interruptions of service with automatic recovery in a sliding window of three months.

5.8.17 The MTBF of the AMHS System hardware should be higher than 52 weeks.

5.9 Requirements for statistics

5.9.1 The AMHS System should monitor and produce statistics per direct MTA partner as follows, where the term "data message" includes all X.400 P1 information objects, i.e. messages, probes and reports:

a) Number of data messages transmitted
b) Average size of the data messages transmitted
c) Maximum size of the data messages transmitted
d) Average number of destination addresses per message transmitted
e) Number of data messages received
f) Average size of the data messages received
g) Maximum size of the data messages received
h) Average transfer time
i) Number of delivery reports transmitted (a subset of item a)
j) Number of non-delivery reports transmitted (a subset of item a)
k) Number of delivery reports received (a subset of item e)
l) Number of non-delivery reports received (a subset of item e)
m) Minimum size of data messages received
n) Minimum size of data messages transmitted
o) Maximum, mean and minimum response time
p) Number of recipients processed
q) Number of messages deferred (the criterion for a deferred message should be specified by a configurable system parameter)
r) Number of messages redirected
s) Number of messages rejected
t) Number of loops detected

5.9.2 The AMHS System and its management tools should enable to monitor and produce statistics per direct MTA partner, related to traffic volume and quality of service at an overall system level, as follows:

a) Overall traffic volume at the level of IP packets;

b) Maximum outage duration of association between MTAs (if any);

c) Cumulated outage duration of association between MTAs (if any).

Note.– The use of IP network measurement tools distinct from the message switch, and/or manual intervention may be required to produce these elements.

5.9.3 Additionally the AMHS System should produce the information specified in 5.9.1 and 5.9.2 for all partner MTAs as a total.

5.9.4 The AMHS System should be able to generate the above statistics in at least the following intervals: 1 day interval, 1 hour interval, 30 minutes interval or better.

5.9.5 The AMHS System should be flexible in configuring other intervals for application statistics generation.

5.9.6 The AMHS System should be flexible in generating statistics at a more detailed level, as e.g., MTA route entries, particular O/R attributes, individual O/R names (to be discussed).

Note.– Each ANSP may consider what requirements on statistics are put on the AMHS System in accordance with its requirements (national and international) and its policy for statistics production. E.g., there can be ANSPs which transfer the traffic logs to another system which will produce all required statistics; in such a case, the AMHS System may be relieved of too many statistics requirements. If an ANSP does not have such other system, it is the responsibility of the AMHS System itself to produce all statistics needed.

5.9.7 The AMHS System should be able to export specific statistic files on a monthly basis. Such a statistic file should contain daily as well as peak hour statistical data in a standard format, covering certain items in 5.9.1 and all items in 5.9.2, because of their specific international relevance. Detailed specifications of the file formats and statistical indicators are provided in the ATS Messaging Management Manual.

5.10 Malware Protection

Note.– This section provides informal explanations and further considerations in addition to guidelines for requirements. Where a statement expresses a potential requirement or recommendation, the term "should" is used in accordance with paragraph 5.1.5. The term "may" is used to indicate options.

5.10.1 Introduction

5.10.1.1 The development of information technology has been followed by the increase of security threats, making systems more vulnerable targets of harmful attacks. The European Parliament and the Council have adopted relevant EU Directives, at the time of writing 2016/148 and 2022/2555, establishing measures for a high common level of security of network and information systems across the Union.

5.10.1.2 ATSMHS has expanded in a world-wide scale and the evolving communication requirements of the applications served by ATSMHS have led to the conveyance of binary data with the use of file-transfer body parts.

5.10.1.3 The dissemination of binary data, in correlation with the increasing cyber threats and the development of EU legislative acts in the field of cybersecurity have led to the awareness of ANSPs in matters related to the protection of systems. In addition, the existence of relevant national legislation and/or ANSP specific policies (safety assessment/security risk assessment processes) may enforce additional measures in the AMHS systems.

5.10.1.4 The following sections are dedicated to guidelines and potential technical options for consideration in the event of developing malware protection in AMHS. It is highlighted that the security provisions of ICAO Doc 9880, Part II and the malware protection mechanism provide different levels of protection.

Note.– The X.400 base standards and ICAO Doc 9880 Part II, to which reference could be made, do not take protection against malware into account.

5.10.2 Deployment

5.10.2.1 The AMHS System of a COM Centre as per paragraph 5.1.4 is composed of a set of end systems identified as the ATS Message Server (MTA and optional MS), the ATS Message User Agent (UA), and the AFTN/AMHS Gateway.

Note.– The Directory User Agent (DUA) incorporated into end systems is out of scope for considerations on malware protection.

5.10.2.2 End systems of a COM Centre should provide malware protection if directly connected over the AMHS to end systems of other COM Centres or third parties.

5.10.2.3 End systems of a COM Centre may provide malware protection if connected to other end systems of the same COM Centre, or to end systems of other COM Centres but not over the AMHS.

5.10.2.4 Malware protection can be integrated into the end system, implemented by an add-on to the end system, or provided by infrastructure such as the operating system or a proxy server depending on local requirements and the design of the end system.

5.10.2.5 A local policy for malware protection should be developed by the operator of the AMHS System identifying the end systems implementing malware protection.

5.10.3 Message Characteristics

5.10.3.1 AMHS messages are encoded using the Basic Encoding Rules (BER) for conveyance by the X.400 MTS Transfer Protocol (P1), the MTS Access Protocol (P3), or the MS Access Protocol (P7).

5.10.3.2 The potential risk of an AMHS message depends on the type and characteristics of the AMHS message. By nature, Interpersonal Messages (IPM) constitute a higher risk than Interpersonal Notifications (IPN), Probes, and Reports.

5.10.3.3 The content of an Interpersonal Message is encoded using the Basic Encoding Rules for conveyance by the Interpersonal Messaging Protocol (P2).

5.10.3.4 The element body of an Interpersonal Message consists of zero, one or more body parts.

5.10.3.5 Body part types suitable for conveyance of binary contents, such as the bilaterally-defined body part or the file-transfer-body-part types, are by nature of higher risk than text-based body part types. Nevertheless, text-based body part types can convey scripts and macros constituting malware.

5.10.3.6 Body parts conveying binary contents can contain compressed data.

5.10.3.7 The local policy for malware protection should consider the potential risk of Interpersonal Messages and Notifications, Probes, and Reports, of individual body part types, and of compressed data.

Note.– Malware protection is assumed on the basis of individual AMHS messages being conveyed by an end system.

5.10.4 Time of Scanning

5.10.4.1 Scanning for malware can be triggered by event or by time.

5.10.4.2 Event-driven or online malware scanning is usually initiated during or immediately after the creation or reception of an AMHS message by the end system. It enables malware detection prior to further processing or conveyance of the AMHS message to other end or third-party systems, thus stopping distribution of malware at the earliest opportunity.

5.10.4.3 Time-driven or offline malware scanning occurs periodically on stored AMHS messages. Malware detection can occur after the AMHS message have already been processed or conveyed to other end or third-party systems.

5.10.4.4 The local policy for malware protection should identify the time of scanning considering the characteristics of event- and time-driven scanning methods.

5.10.5 Preparations

5.10.5.1 The end system should decode the BER data stream of an AMHS message on conveyance prior to scanning for malware in order to have access to the individual elements of the AMHS message as a result of paragraph 5.10.3.1.

5.10.5.2 The end system should decode the content of an Interpersonal Message prior to scanning for malware in order to have access to individual body parts and for identification of related body part types as a result of paragraphs 5.10.3.3 and 5.10.3.5.

Note.– Usually, an ATS Message Server (MTA) is not required to decode the content of an Interpersonal Message except for particular operations such as conversion of content.

5.10.5.3 The end system may uncompress compressed data prior to scanning for malware in order to detect malware in compressed format as a result of paragraph 5.10.3.6.

5.10.6 Actions

5.10.6.1 The end system should scan for malware depending on the local policy for malware protection and considering the characteristics of AMHS messages.

5.10.6.2 The end system should perform a primary action on infected AMHS messages, only one of which is applicable per AMHS message, such as,

- Continue
  Process or convey infected AMHS message without any modification resulting from malware detection. This action does not stop the distribution of malware and is therefore discouraged.
- Delete body parts
  Remove infected body parts from the AMHS message. Proceed with processing and conveyance of the modified AMHS message. This action modifies the AMHS

message without further notice and is therefore discouraged. Automated end systems can fail in processing the modified AMHS message.

- Replace body parts
  Substitute infected body parts with body parts reporting on the removal of infected body parts. Proceed with processing and conveyance of the modified AMHS message. This action modifies the AMHS message but provides a cause for the modification along with the AMHS message. Automated end systems can fail in processing the modified AMHS message.

- Discard
  Stop processing the infected AMHS message and remove the AMHS message from the message queue without further operations on the infected AMHS message. This action prevents the AMHS message from being delivered to the intended recipients.

- Quarantine
  Move the infected AMHS message to quarantine for further investigation and measures by the operator. This action delays the processing of the infected AMHS message and requires the attention of the operator. Measures taken by the operator can result in further implications.

- Non-deliver
  Perform the non-delivery operation on the infected AMHS message and generate a non-delivery report, as requested. This action applies to MTA implementations only. This action prevents from delivery of the AMHS message to the intended recipients but through the non-delivery report informs the originator of the non-delivery and the cause therefor.

5.10.6.3 The local policy for malware protection should determine the primary action applied to infected AMHS messages.

5.10.6.4 A non-delivery report resulting from malware detection should make use of one of the following pairs of the attributes non-delivery-reason-code (NDRC) and non-delivery-diagnostic-code (NDDC):

a) NDRC: transfer-failure-for-security-reason (8)
   NDDC: unable-to-complete-transfer (48)
   This combination of NDRC and NDDC constitutes the preferred pair.

b) NDRC: unable-to-transfer (1)
   NDDC: unable-to-complete-transfer (48)

c) NDRC: restricted-delivery (5)
   NDDC: content-syntax-error (12)

5.10.6.5 A non-delivery report resulting from detection of malware should provide the attribute supplementary-information providing further information.

5.10.6.6 A non-delivery report resulting from malware detection should not include the infected subject message in the element returned-content.

5.10.6.7 The local policy for malware protection should determine the NDRC and NDDC used for non-delivery reports generated as a result of malware detection, if applicable.

5.10.6.8 The end system should perform secondary actions as a result of detection of malware which occur in parallel, such as,

- Logging
  Record the detection of malware on a permanent storage for information, analysis, and further investigation by the operator.
- Alarming
  Inform the operator of the end system of the detection of malware by means of acoustic or visual alarms to enable the operator to take immediate action as necessary.
- Notification
  Pass the event of malware detection on to a 2nd level or monitoring facility such as a security operations centre (SOC) if reporting of malware detection is requested by the local security architecture.

5.10.6.9 Operators of end system should assess malware notifications using logged information, quarantined AMHS messages, if any, and particularly considering false positives.

5.10.6.10 Operators of end systems may inform the originator of an infected AMHS message on the detection of malware, independent of the generation of a non-delivery report.

5.10.7 Management

5.10.7.1 The scanning engine should be maintained and kept up to date.

5.10.7.2 For situations where an update of the scanning engine malfunctions, the update process should anticipate measures known from software deployment such as staging, i.e. testing prior to deployment, or rollback of update.

5.10.7.3 The virus patterns used by the scanning engine should be updated on a regular basis.

5.10.7.4 The local policy for malware protection should identify the frequency of pattern updates.

5.10.7.5 The update of virus patterns can occur automatically or manually. The update of the virus patterns can require additional measures in order to prevent from unintended exposure of the end system and to protect the end system from interferences. Such measures can include additional infrastructure such as firewalls, proxy servers, demilitarised zones (DMZ), and virtual private networks (VPN) as well as procedures.

5.10.7.6 Malware detection is subject to unpredictable factors. Malware protection might not detect malware (false negative) or might identify malware erroneously (false positive). For false positives please see also paragraph 5.10.6.9.

5.10.7.7 For situations where new malware or a virus pattern update results in service degradation, such as poor detection rate or too many false positives, the local policy for malware protection should identify suitable measures such as staging, rollback, high frequency of updates or out-of-band updates in order to prevent such situations or to recover from the service degradation as soon as possible. Measures appropriate for a given situation have to be determined on a case-by-case basis, depending on the degree of degradation, severity of issue, support by the virus pattern provider, capabilities of the system and potential further factors.

5.10.7.8 The end system should integrate with a 2nd level or monitoring facility to provide notifications of malware detection events in accordance with 3rd bullet of paragraph 5.10.6.8 if reporting of such events is requested by the local security architecture.

5.10.8 Performance

5.10.8.1 The design of the end system should consider the increase in the overall processing time for individual AMHS messages by the end system caused by malware protection which can have an impact on latency and maximum transit time.

5.10.8.2 The design of the end system should consider the system resources required by malware protection such as processing time, memory, and storage capacity.

5.10.8.3 The design of the end system should consider the decrease in the maximum throughput of AMHS messages caused by additional system load through malware protection.

Note.– Further considerations on performance can be found in section 3.1.3 and on sizing in section 5.7.

6 AMHS management

6.1 Introduction

6.1.1 In general, network management is essential for reliable and efficient operation of a network like the EUR AMHS Network.

6.1.2 This chapter contains a general introduction on the management aspects for an EUR AMHS network. It contains a list of required functions that are to be fulfilled by a management system.

6.1.3 The breakdown of the management areas is according to the ISO FCAPS scheme.

6.1.4 At the end in section 6.5 the European approach of AMHS Network management by implementing the ATS Messaging Management Centre is described.

6.2 Requirements for AMHS Management

6.2.1 The following AMHS Management activities can be distinguished:

Timeframe **Activity**	**Online 24 hr*7 day**	**Off line - short term**	**Offline – long term**
Fault Management	Helpdesk, fault reporting. 1st line support. Service availability monitoring	Fault resolution, fault management	High level changes to increase reliability, reduce user queries
Configuration Management	These are not a regular feature of online systems management. System and user changes recorded online but usually applied to offline system.	Activation/turn-up of changes. Regular published changes	High level planning, for international connectivity and national service upgrades
Accounting management	N/A	Production of regular statistics	Policy and planning activities relating to budgeting, charging, capacity planning
Performance management	Monitoring utilisation, processors, queues, connections, discs etc.	Performance tuning activities	Long term and international planning for capacity management

Timeframe Activity	Online 24 hr*7 day	Off line - short term	Offline – long term
Security	Monitoring for attacks, taking countermeasures	Regular health checks, reviewing warnings from industry and other ANSPs, security training	Security policy, significant architecture/topology changes to increase security

Table 7: Breakdown of activities by timeframe

6.3 System Management data flows

6.3.1 How system management will be implemented and operated at local level can be freely chosen by a State. The ATN technical specifications define requirements to make information available to other States through XMIBs, with as a primary goal the support of boundary management.

6.3.2 The ATN technical specifications define the XMIB sets, and the information is used to serve the following purposes:

- Enable other participating organisations to query the current operational status of the ATN system (ES or IS);
- The cross domain MIB should support the capability to allow a SM Manager to be warned by notification as soon as an error occurs in an adjacent domain.

6.3.3 This “public” management information is to be made freely available by the State to the international community.

6.3.4 Alarms raised in one management domain that affect the provision of AMHS service should be made available to other management domains.

Note.– The exact standard distribution of reports and alarms is for further study.

6.4 Realisation options

6.4.1 Information database

6.4.1.1 For the exchange of information with the management database the ISO XMIB solution is foreseen in the technical specifications. In this context, States have been requested to implement XMIBs from the onset of AMHS for international co-ordination. Eventually a conversion mechanism should be implemented.

6.4.1.2 Such an implementation should cover both the AMHS application (entry and exit MTAs, Gateways, MTCUs and routes through a State carrying traffic) and the underlying ATN network XMIBs.

6.4.1.3 A capability to broadcast alarms to other States should be foreseen.

Note.– The use of XMIB is under discussion. Especially in the light of TCP/IP in the EUR Region other options (MIB) may be studied.

6.4.2 Fault management

6.4.2.1 Fault management can be subdivided in 3 distinct areas:

- Fault rectification – the process of providing a long term solution to a fault. This is highly implementation dependent and thus very much a national issue.
- Fault management – the process of ensuring that faults are correctly recorded, assigned for rectification and the entire process managed Also this is a national function.
- Fault reporting – covers the area of helpdesks and first line support and spans both local and international systems.

6.4.2.2 Helpdesks can be organised either nationally or internationally. In the international model a centralised regional or global helpdesk operates on behalf of member States which maintain the operational responsibility for their own domains.

6.4.2.3 The international approach has a better overview of the network as a whole, offers economies of scale and relieves national operations centres. The national approach deals more efficiently with local users in the local situation.

6.4.2.4 Weighing advantages and disadvantages a regional helpdesk has been chosen for the EUR AMHS.

Note.– The Terms of Reference of the Helpdesk are to be defined. For the time being the helpdesk is of passive nature and is intended to operate off-line.

6.4.3 Configuration Management

6.4.3.1 Although Configuration Management is a local responsibility there is a significant requirement for co-ordination of addressing and routing information.

6.4.3.2 An AMHS Offline Management Centre is created to consolidate, co-ordinate and distribute AMHS address and routing information across the EUR Region. The configuration changes follow the 4-week AIRAC cycle.

6.4.3.3 The following information will be co-ordinated and maintained:

- Declaration and changes to PRMD;
- Declaration and changes to mapping of “4 character Location Indicator” to “Geographical Unit”, i.e. relationship between OU1 and O attributes;
- Declaration and changes to mappings of “8 character AFTN address” and Geographical unit i.e. CN to OU1;
- Declaration and changes of network addresses for primary and backup boundary MTAs and AFTN/AMHS Gateways;
- General awareness of deployment and transition activities;
- Routing and alternate routing.

6.4.3.4 ICAO will hold a registry of PRMDs.

6.4.4 Accounting management

6.4.4.1 In the initial phase of AMHS operation accounting will not be performed.

6.4.4.2 Cost assignment will eventually be locally introduced.

Note.– The requirements for eventual later implementation of the facility are under study.

6.4.5 Performance management

6.4.5.1 Performance

6.4.5.1.1 Online performance monitoring includes monitoring of metrics like queue size, transit times utilisation factors and status, where manual and/or automatic procedures are being invoked when thresholds are passed.

6.4.5.1.2 Offline performance management is aimed at the ability of the service to meet future needs. This requires accurate statistics on traffic patterns and system performance.

6.4.5.1.3 Both management aspects are local to an ANSP and no matter for international harmonisation.

6.4.5.2 Statistics

6.4.5.2.1 It is recommended that statistics should be collected using the internationally agreed objects (MTA). (For detailed requirements for statistics see 5.9)

6.4.5.2.2 Implementers should use a flexible design and should be able to obtain the information down to the level of individual operators or recipients with a granularity of 30 minutes or better.

6.4.5.2.3 A minimum set of monthly statistic should be exportable. Such a file should contain daily as well as peak hour statistical data in a standard format. Detailed specifications are provided in the ATS Messaging Management Manual.

6.4.5.3 Reporting of statistics

6.4.5.3.1 The statistic file containing daily as well as peak hour statistical data should be provided to the ATS Messaging Management Centre monthly.

6.4.5.3.2 There are no specific recommendations for statistics that are to be reported for national use.

6.4.6 Security Management

6.4.6.1 The management of security within a State is considered to be a local issue. However, when a breach of security or a threat is detected, it is recommended that the helpdesk is informed, and that the helpdesk subsequently passes on security warnings to other States and Regions and co-ordinates exchanges.

6.5 Implementation of AMHS Management in the EUR Region

6.5.1 Introduction

6.5.1.1 This section is intended to give the reader information necessary for an understanding of AMHS Management as currently planned, and has been written for those implementing, operating, using and planning the procurement of management systems.

6.5.1.2 Section 6.5.3 defines a group of functions known as "off-line" management functions. To a certain extent, these functions represent updated CIDIN Management Functions already being carried out. They are not highly demanding in an implementation and operational sense and they are typically introduced first.

6.5.1.3 The other functions in the context of AMHS Management are termed "on-line" functions. They are defined in section 6.5.4.

6.5.2 On-line and off-line management

6.5.2.1 The Terms "Off-line" and "On-line"

6.5.2.1.1 A basic principle underlying the structure of AMHS management is the distinction between the two groups of functions designated as "off-line" and "on-line" management functions.

6.5.2.1.2 **Off-line** functions do not need to be executed in a short time period. These relate to medium and long-term requirements and include, e.g., collection and processing of information from COM Centres (inventory, planning, addressing, statistics, etc.) and preparation of configuration proposals (routing, addressing). Provision of technical support (help desk, consultancy, etc.) is also included in off-line management, even though these functions do not belong to one of the OSI Functional Areas.

6.5.2.1.3 **On-line** management refers to functions that need to be executed in a short time period in order to maintain the level of service required from AMHS. This necessitates the rapid exchange of management information between the COM centres and possibly between the COM centres and AMHS Management Unit (on-line Regional Help Desk).

6.5.2.2 The Distinction

6.5.2.2.1 The terms "off-line" and "on-line" are used to classify two separate groups of functions. The following table summarises the distinction with respect to a number of characteristics.

Characteristic	off-line	on-line
on-line connections between the systems?	not essential	essential
human intervention in the "management loop"	yes	in transition phase and in exceptional circumstances
new application software to be implemented in AMHS centres?	not essential	essential

Characteristic	off-line	on-line
operational time constraint	a few time-critical functions	more time-critical functions
degree of technical sophistication	relatively simple	more complex
period of operation	office hours	7 days / 24 hours
order of implementation	it is being implemented	to be studied

Table 8: Characteristics of "off-line" and "on-line" functions

6.5.2.3 Implementation Aspects

6.5.2.3.1 The off-line group of functions is less demanding than the on-line functions to implement. They can be introduced within a relatively short timescale.

6.5.2.3.2 The on-line functions are more ambitious and not yet defined as the off-line functions. The timescale for their implementation is longer and network management experience in the AMHS context needs to be built up before they can be introduced. The introduction of an on-line mode of operation supplementing the off-line mode is expected to be a major design issue.

6.5.3 AMHS off-line Management

6.5.3.1 AMHS off-line Management is described in the ATS Messaging Management Manual. ATS Messaging refers to the integrated, heterogeneous messaging environment comprising AFTN, CIDIN and AMHS.

6.5.3.2 The ATS Messaging Management Manual provides the information necessary for understanding and operating within the environment of the integrated AFTN/CIDIN/AMHS off-line Management.

6.5.3.3 The ATS Messaging Management Manual describes the framework in which the services of the ATS Messaging Management Centre (AMC) are provided to States/ANSPs in the EUR/NAT Regions, and, in a more limited manner, to States/ANSPs in other Regions.

6.5.3.4 Two categories of AMHS off-line Management Functions are defined, i.e.: Implementation Support Functions primarily for States in the process of implementing AMHS, and Operational Functions in support of States with AMHS in operational service:

6.5.3.5 Implementation Support Functions:

- Download support information
- AMHS PDR monitoring
- Inter-working test support
- View operational data
- Implementation planning
- Helpdesk function

6.5.3.6 Operational Functions:

- Network inventory

- Network planning
- Routing management
- Address management
- AMHS user capabilities management
- Security management (for future development)
- Statistics
- Support

6.5.3.7 The AMC procedures associated with the performance of the AMHS off-line management functions by Co-operating COM Centres (CCCs) are described in detail in the ATS Messaging Management Manual.

6.5.3.8 The goal of the AMC is twofold:

- the AMC facilitates the transition from AFTN/CIDIN to AMHS, particularly with routing management and address management functions;
- the AMC provides new tools in support of AMHS operations.

6.5.3.9 When States in the EUR/NAT Regions implement AMHS, the transition is complex to manage. Considering that ill-coordinated actions may create risks for the overall ATS Messaging quality of service, it is therefore recommended that every State implementing AMHS in the EUR/NAT Regions participates in AMC activities.

6.5.3.10 Detailed information on the AMC organisation, features, functions, procedures and implementation issues can be obtained from the AMC.
(https://www.eurocontrol.int/amc/).

6.5.4 AMHS on-line Management

- to be studied if needed -

7 Tests and validation of AMHS systems

7.1 Objective

7.1.1 Experience has shown that, although it is claimed that systems have been implemented according to the one set of protocol specifications, they are often not capable of inter-working. This is due to errors in implementation or to different interpretations of the specifications (SARPs and Doc 9880). Testing and validation of systems according to the same set of principles aims at the detection of such errors and the prevention of incompatibility instances.

7.1.2 The primary objective of this chapter is to formulate recommendations for testing the ability of a given AMHS implementation to function as required at the level of an International Communication Centre within the AFTN/CIDIN/AMHS network environment.

7.1.3 This chapter provides general information on the AMHS testing concept. The actual testing methodologies, configurations and procedures are defined in Appendix C, Appendix D and D-UA, Appendix E and Appendix F. In these Appendices, tests are described in sufficient detail to give an appreciation of the variety of functions that are covered, the facilities required and the expected results.

7.2 General Principles

7.2.1 The creation of standards for testing is subject to consideration by a number of standardization bodies concerned with open systems (e.g. ISO, ITU-T).

7.2.2 In these standards, *conformance testing* is prescribed for testing a protocol implementation (IUT) with respect to its specification.

7.2.3 If conformance testing could be done in a complete and correct manner then two different implementations that passed the conformance test would be interoperable. In practice, conformance testing does not necessarily reach the intended point of completeness and correctness. Consequently, conformance testing may be followed by *interoperability testing* to determine whether two or more implementations will produce the expected behaviour under actual operating conditions.

7.2.4 In a more detailed analysis of the objectives of conformance and interoperability testing the following distinctions can be made:

- The primary objective of interoperability testing is to confirm the end-to-end interoperability of two systems, which have both been developed to a common specification. Performance and load testing are possible, at least in principle.

- Conformance testing can be defined as the exhaustive testing of an IUT against the functions and procedures defined in an agreed standard. Performance and load testing are not usually part of conformance testing which is restricted to the "logic" of the protocol implementation.

7.2.5 Furthermore, two essential practical differences between conformance and interoperability testing should be pointed out:

- Incorrect protocol behaviour. – Conformance testing allows "provoking" of the IUT, through incorrect protocol behaviour, in order to study its stability. Interoperability testing provides only limited possibilities due to (normally) correct protocol implementations in real systems.

- Distribution of test locations. – Conformance testing can be performed locally between IUT and a conformance testing equipment. Interoperability testing is normally distributed over at least two remote locations, therefore requiring more co-ordination effort.

7.2.6 Figure 6 depicts the principal differences in test arrangements for interoperability and conformance testing.

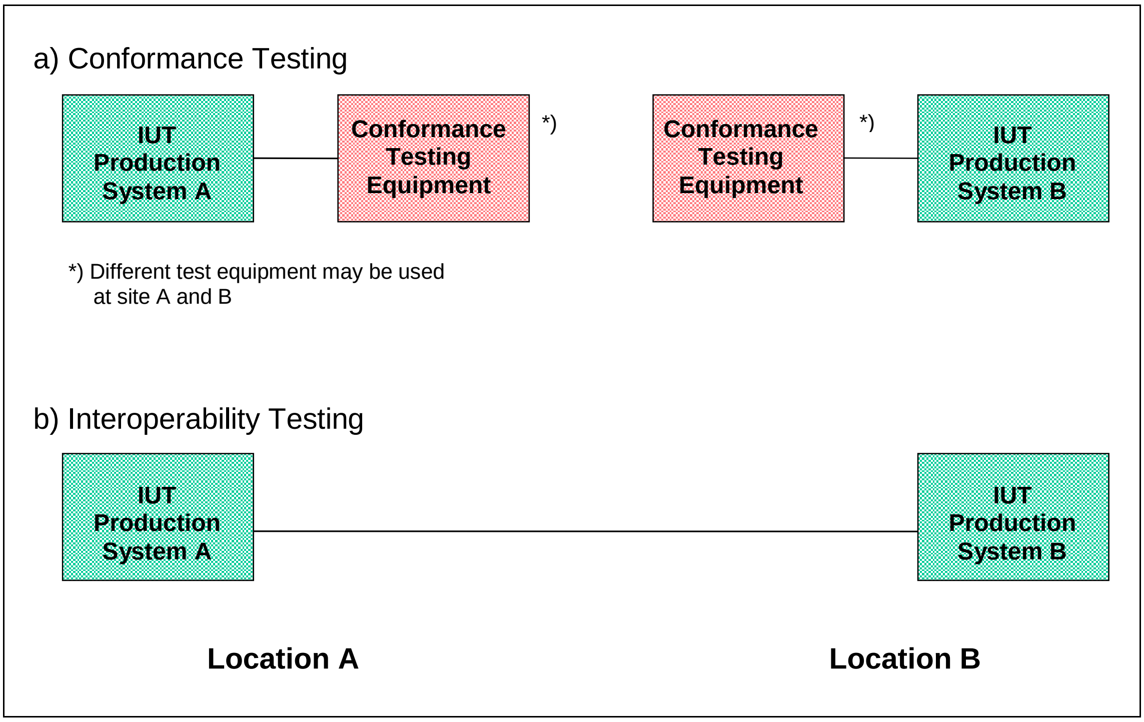

Figure 6: Principal test arrangements for conformance and interoperability testing

7.3 AMHS testing concept

7.3.1 Testing strategy

7.3.1.1 AMHS system implementations consist of protocol layers according to the principles of the Reference Model for Open Systems Interconnection. The AMHS functions to be tested reside in the application layer of the ISO/OSI reference model. The underlying layers provide supporting communication services, however they are not primarily subject to testing.

7.3.1.2 Figure 7 provides a generic functional presentation of an AMHS implementation under test.

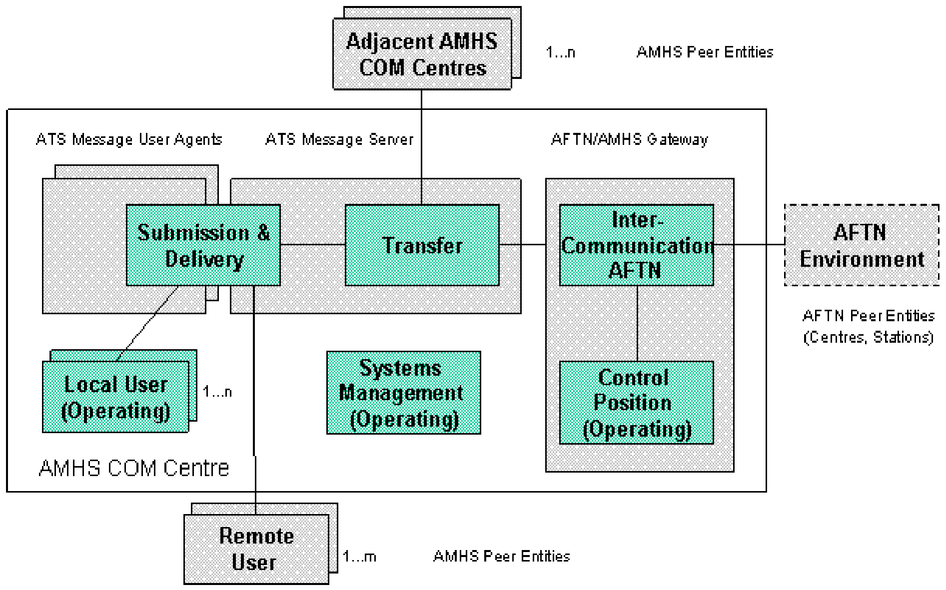

Figure 7: Functional view of an AMHS IUT

7.3.2 AMHS testing phases

7.3.2.1 AMHS Conformance testing

7.3.2.1.1 For the purposes of AMHS, *conformance testing* is considered mandatory and shall be performed in parallel with or after the acceptance testing of a new system.

7.3.2.1.2 The new system is tested as a *black box*, meaning that that required features are verified by observation of the external *behaviour* of the IUT upon stimulation with well-defined input events.

7.3.2.1.3 A *conformance testing equipment*, called the *AMHS test tool*, is used typically for the production of such input events and the monitoring of the resulting outputs from the IUT. In case such an AMHS test tool or reference implementation is *not* available, a test environment could be configured by using functional components of the IUT itself. Testing in such an environment may be seen as consistency testing rather than conformance testing.

7.3.2.1.4 The main AMHS functional areas covered by conformance testing are:

- Transfer of messages probes and reports;
- Submission of messages and probes / delivery of messages and reports;
- Intercommunication with AFTN;
- Naming and addressing;

- Parameters;
- System management functions.

7.3.2.2 AMHS Interoperability testing

7.3.2.2.1 After successful completion of conformance testing, *interoperability testing* is recommended, particularly in the following cases:

- one of the involved parties is establishing a first AMHS connection;
- one of the involved parties is joining an AMHS island;
- the connection is being established between AMHS implementations of manufacturers which have not performed IOT before;
- one of the involved parties requests to perform interoperability tests.

7.3.2.2.2 With due consideration given to paragraph 7.3.2.2.1, and by mutual agreement, interoperability testing may be omitted between two Com Centres that are in the same AMHS island and already have operational AMHS connections.

7.3.2.2.3 As a first step to interoperability testing the interconnection between pairs of systems should be established and checked.

7.3.2.2.4 Then, at the bilateral level, the following functional areas should be covered:

- Submission, Transfer and Delivery operations (AMHS to AMHS)
- Gateway operations (AFTN to AMHS)
- Gateway operations (AMHS to AFTN)
- Gateway operations (AFTN to AMHS to AFTN)
- Gateway operations– special case scenarios
- Stress traffic situations
- Submission/Transfer/Delivery and Relay operations
- Test of special situations

7.3.2.2.5 At the multilateral level, interoperability testing involves more than two organizations, interchanging normal messages and generating specific reactions of their systems.

7.3.2.3 AMHS Pre-operational testing

7.3.2.3.1 Before going into operation, *pre-operational testing* should be carried out between the AMHS systems concerned, within the operational network environment and using duplicated operational traffic.

7.3.2.3.2 The configuration details and the actual sub-sets of traffic to be used, have to be co-ordinated between the test partners. In any case, the operational traffic selected for this purpose should be traffic under the responsibility of the Communication Centres under test.

7.3.2.3.3 The AMHS relation between the two systems is considered operational, if the exchange of the total of operational traffic between them (or a subset of that), is performed by means of AMHS only. For this operational traffic no other transmission means (AFTN or CIDIN) is used.

7.4 Integration to the operational network

7.4.1 A common stepwise transition plan for migrating a successfully tested system into the operational AFTN/CIDIN/AMHS network should be applied.

8 Operational procedures and Recommendations

8.1 Introduction of a new AMHS COM Centre in the AMHS network

8.1.1 Scope of the procedure

8.1.1.1 This procedure specifies the actions necessary to perform the introduction of a new AMHS COM Centre in the International AMHS network. The term "new AMHS COM Centre" may refer to three distinct cases:

- the COM Centre already exists. It provides CIDIN and possibly conventional AFTN connectivity, and it supports the AFTN application of the CIDIN for national users. AMHS is introduced as an additional functionality and service in the existing COM Centre. This case corresponds to the majority of COM Centres in the EUR/NAT Regions;

- the COM Centre already exists. It provides conventional AFTN connectivity. AMHS is introduced as an additional functionality and service in the existing COM Centre. This case corresponds to a smaller number of COM Centres in the EUR/NAT Regions;

- the COM Centre does not exist yet and it will start operational service directly with AMHS. Although theoretically possible, there is no such case foreseen in practice in the EUR/NAT Regions. This case will consequently not be further discussed in the present version of the procedure[5].

8.1.1.2 From the above, it results that, strictly speaking, the procedure is related to the introduction of the AMHS operational service in a COM Centre of the international AFTN/CIDIN/AMHS network.

8.1.2 Target AMHS network

8.1.2.1 The target AMHS network which this procedure aims at reaching, when applied to all COM Centres in the EUR/NAT Region, has the following characteristics:

- it is an integrated AMHS network, composed of one single AMHS island in which all COM Centres are interconnected;

- it is a fully-meshed network, which means that there is an any-to-any connectivity at the level of AMHS connections (associations between MTAs) between COM Centres.

8.1.3 Assumptions

8.1.3.1 The principles of [1] are used for the definition of procedure.

8.1.3.2 The procedure relies heavily upon the use of the ATS Messaging Management Centre, implementing off-line management of AFTN, CIDIN and AMHS.

8.1.4 Qualitative objectives

8.1.4.1 The proposed approach aims at three main goals:

---

[5] It might be subject for further study if a future major reorganisation of European COM Centres were envisaged in the future.

1. to migrate all the flows conveyed over the CIDIN link to the AMHS connection. CIDIN connectivity is not maintained at the end of the transition;

2. to migrate operational flows progressively to the AMHS connection, so as to:

   - facilitate operational validation (reduce the number/extent of changes at each step, to facilitate the analysis of behaviour/results),

   - enable easy rollback, in case it would be absolutely needed;

3. to limit impact on COM Centres other than those to which the procedure is applied, to reduce as much as possible inter-Regional co-ordination tasks during transition. Co-ordination will still be needed anyway, making use of the AMC.

8.1.5 General procedure

8.1.5.1 The introduction of a new AMHS COM Centre to the operational AFTN/CIDIN/AMHS network shall be performed in a stepwise manner. Initially, the activation of an operational AMHS connection takes place, after appropriate lower layer connectivity has been implemented and bilateral interoperability testing has been successfully completed. Then progressive migration of AMHS, AFTN and CIDIN traffic to the new connection is performed.

8.1.5.2 The detailed description of this procedure is provided in the ATS Messaging Management Manual (see [12]).

8.2 Recommended default values for international MTA names and passwords

8.2.1 Introduction

8.2.1.1 AMHS implementation requires the setting of the MTA names and passwords for each communication partner (MTA) connected. In a future fully meshed AMHS Network, unique identification of the MTAs would be required. Additionally, the naming should respect the knowledge and experiences of the operator staff, in order to avoid any unnecessary complications in the transition to AMHS.

8.2.1.2 One way to achieve this is to use a scheme, in which MTA names and passwords contain keywords which uniquely identify the MTA and facilitate recognition.

8.2.2 Default values for international MTA names

8.2.2.1 The recommended scheme of MTA names consists of:

- the term “MTA”;

- the Location Indicator of the MTA location; and

- a number (for future extensions if required).

8.2.2.2 All items are separated by a hyphen (hexadecimal 2D). The result is a printable string which can be exchanged in a message without difficulties.

Example: In accordance with this scheme the name of the MTA in Frankfurt, Germany should be: MTA-EDDD-1.

8.2.2.3 This scheme could be used for the national MTA naming as well.

8.2.3 Default values for international MTA passwords

8.2.3.1 Password complications arise because manufacturers deviate in the interpretation of an “empty” password. Some implementations await “nothing”, some hexadecimal 00, others a single “space” character. To avoid misinterpretations during establishment of association(s) all tests could be performed with a common (known) password or with default passwords that follow the scheme recommended in the next section. Individual secure passwords should be established for operational systems, in order to ensure the necessary security of operational AMHS facilities.

8.2.3.2 The recommended scheme of the default password consists of:

- the term “ICAO”;
- the Location Indicator of the MTA location; and
- the specific number of the MTA.

8.2.3.3 All items are separated by a hyphen (hexadecimal 2D). The result is a printable string which can be exchanged in a message without difficulties.

Example: In accordance with this scheme the default password of the MTA in Frankfurt, Germany should be: ICAO-EDDD-1.

8.2.3.4 By following this scheme, the default passwords of future MTAs can be determined at any time and the integration of new MTAs in a fully meshed AMHS Network topology could be simplified. Nevertheless in order to increase the level of systems protection, the use of secure passwords by operational MTAs is highly recommended. The creation of quality passwords and their proficient management in general would improve security.

8.3 Recommended setting of timers

8.3.1 Message related timers

8.3.1.1 MTS Timer related to Message lifetime

8.3.1.1.1 If the MTS (Message Transfer System) cannot deliver a message within a determined period of time, a NDR will be returned to the originator.

8.3.1.1.2 If this MTS timer is different per message priority and potentially different at each MTA, an AMHS user will receive NDRs depending on the different settings, which could create confusion and result in inaccurate NDR handling.

8.3.1.1.3 In order to ensure that the behaviour of the MTS is predictable it is recommended that every MTA in the AMHS network should use the same timer values related to message lifetime and that these values should be the same for messages of any priority.

8.3.1.1.4 Furthermore, the recommended value for the MTS timer related to message lifetime should ensure that:

- temporary communication failure / maintenance actions do not cause timer expiry;

- Direct Users do not receive unnecessary NDRs (if values are too low);
- message lifetime does not conflict with 'latest delivery' (optional Element of Service);

8.3.1.1.5 Based on the above analysis, the following values of the message lifetime MTS timer are recommended:

Message priority	Message lifetime
Urgent	168 hours (7 days)
Normal	168 hours (7 days)
Non-urgent	168 hours (7 days)
Report	168 hours (7 days)

Table 9: Recommended Message Lifetime per priority

8.3.1.1.6 This recommended timer setting ensures that in normal situations no NDR is generated with diagnostic code 'maximum-time-expired'. AMHS COM Centre operators can act in accordance with established procedures, when a message queue is detected.

8.3.1.2 Usage of the Latest Delivery Time

8.3.1.2.1 As outlined in Doc 9880 the Element of Service "latest delivery time" should never be set in an MTCU.

8.3.1.2.2 Furthermore, it is recommended not to set this parameter in an UA by default.

8.3.2 Network related timers

Tbd.

8.4 Processing of AFTN service messages in the Gateway

8.4.1 Introduction

8.4.1.1 This section is retained for reasons of reference. In previous versions of this document this paragraph contained recommendations deviating from ICAO Doc 9880 – 1st Edition requirements for specific processing of AFTN service messages in the MTCU. The rationale of the deviating recommendation is preserved in the following paragraph. ICAO Doc 9880 – 2nd Edition, published in 2016, is in line with the EUR AMHS Manual recommendations. Therefore, this section has been reworked.

8.4.1.2 The AMHS COM Centre implementations in the EUR Region as well as in other Regions are expected to be adapted to the EUR AMHS Manual or the ICAO Doc 9880 – 2nd Edition at different speeds. As a result, in the operational environment some COM Centres may still conform to now obsolete SARPs. Hence, the observed processing of AFTN service messages in an MTCU might correspond to the scenario described in the following section. This section is kept with the intention to explain potential issues related to AFTN service messages.

8.4.1.3 It is recommended to implement the processing of AFTN service messages in MTCU according to ICAO Doc 9880 – latest edition.

8.4.2 Rationale of the previously deviating recommendation

8.4.2.1 AFTN service message "ADS … UNKNOWN …"

8.4.2.1.1 In a specific operational scenario in a mixed AFTN/AMHS environment it was observed that the original originator information of AFTN service messages "ADS … UNKNOWN …" was lost due to double conversion from AFTN (AFTN service message) to AMHS (NDR) and back to AFTN (AFTN service message).

8.4.2.1.2 Such a scenario was relevant during the migration to AMHS when traffic was relayed by AMHS "bridging" two AFTN areas by an AMHS connection as shown in Figure 8.

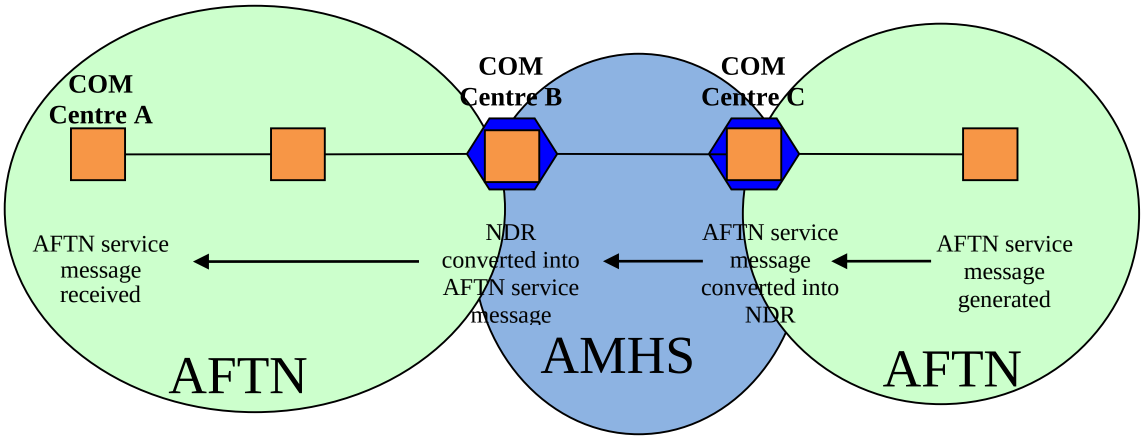

Figure 8: Mixed AFTN/AMHS environment

8.4.2.1.3 If COM Centre A sends an AFTN message to COM Centre D containing an unknown address, then COM Centre D generates an AFTN service message "ADS … UNKNOWN …", addressed to the originator of the AFTN message.

8.4.2.1.4 Due to the fact that between A and D an AMHS network existed, the AFTN service message originated from COM Centre D was converted into an NDR in COM Centre C, if the subject AMHS message had passed through COM Centre C.

8.4.2.1.5 The NDR generated in COM Centre C was converted back to an AFTN service message "ADS … UNKNOWN …" in COM Centre B, but with the originator of COM Centre B.

8.4.2.1.6 Consequently, COM Centre A received an AFTN service message "ADS … UNKNOWN …" with the originator of COM Centre B. The originator of the original AFTN service message ("ADS … UNKNOWN …" generated by COM Centre D) was lost, as a report has no originator.

8.4.2.2 Other AFTN service messages

8.4.2.2.1 Due to the strict implementation of the AFTN service message processing according to obsolete ICAO Doc 9880, Part II – Edition 1, paragraph 4.2.1.4, it might not have been possible in some cases to convert and/or forward AFTN service messages through the AFTN/AMHS Gateway. In particular, an AFTN service message could have been prevented from passing through an AMHS link interconnecting two AFTN islands. Such behaviour did not meet the operational expectations. In order to avoid the potential loss of any AFTN service message paragraphs 4.2.1.4 and 4.2.1.12 have been modified in ICAO Doc 9880, Part II – Edition 2.

8.4.2.2.2 Any AFTN service message "QTA RPT" requesting from an originator repetition of an incorrectly received message should be processed according to Annex 10 Vol. II, 4.4.11.1 and 4.4.16.2.2. If the message(s) requested for repetition cannot be repeated for any reason, ICAO Doc 9880, Part II – Edition 2, 4.2.1.12 requests the AFTN component to forward the AFTN service message to the MTCU for further processing, i.e. conversion into an IPM conveying the AFTN service message towards its destination.

8.4.2.2.3 ICAO Doc 9880, Part II – Edition 2, 4.2.1.4 e) requests the AFTN component to forward any other AFTN service message which is not addressed to the AFTN/AMHS Gateway to the MTCU for further processing in the same manner.

8.4.2.2.4 Any AFTN service message message addressed to the AFTN/AMHS Gateway should be processed as specified in Annex 10, Vol. II. Depending on the position where the AFTN service message is to be displayed (control position, local AFTN terminal or local AMHS User Agent) the AFTN service message may or may not pass through the MTCU; this is considered a local implementation matter.

8.4.3 Recommended processing related to AFTN Acknowledgment messages

8.4.3.1 Guidance concerning this special case may be found in the section that follows.

8.5 Recommended practices for processing of AFTN acknowledgement messages (SS ACK) / Receipt notification (RN)

8.5.1 Introduction

8.5.1.1 In ICAO Annex 10, Vol. II, it is foreseen that AFTN distress messages (SS priority) are acknowledged directly by their actual recipients, to ensure that they are aware of the distress situation and have undertaken appropriate actions.

8.5.1.2 In the same spirit, it has been foreseen in ENRD, Section 6.9, that a User Agent (UA) shall be able to generate a Receipt notification (RN) only after manual user/operator interaction as a reaction to the reception of an AMHS message with priority "urgent" (distress message).

8.5.1.3 In ICAO Doc 9880, Part II, section 4.5.3, it is foreseen that an AFTN/AMHS Gateway converts an incoming RN to an AFTN acknowledgement message, assuming that the subject AFTN distress message has traversed this Gateway. If it has not, an NDR is generated, an error report is provided to the Gateway control position and manual investigation is required.

8.5.1.4 As a consequence of the above, in a mixed AFTN/AMHS environment there is a potential risk that an AFTN acknowledgement message will not reach its intended recipient in a timely manner, if the corresponding RN is addressed to an AMHS Indirect User and it has to follow a different route than the original AFTN distress message (asymmetric routing). In such cases, the concerned MTCU is not able to convert the RN into the corresponding AFTN acknowledgement message due to the absence of the related subject message.

8.5.2 Recommended practices

In order to minimise such operational situations during the transition phase towards AMHS the following practices are recommended:

8.5.2.1 Manual processing of the acknowledgement by a UA

8.5.2.1.1 The AMHS user at the UA should have the choice to acknowledge an ATS message with priority SS in the ATS-message-header either by an RN or by an ATS message in the format of the Acknowledgement message.

8.5.2.1.2 The decision is taken by the AMHS user at the UA knowing that the originator of this AFTN distress message is an AMHS Direct User (generate an RN) or an AMHS Indirect User (send an ATS message in the format of the Acknowledgement message).

8.5.2.1.3 In the current AFTN/AMHS transition phase the default assumption is “AMHS Indirect User”.

8.5.2.2 Automated processing of the acknowledgement by a UA

8.5.2.2.1 If an AMHS user at the UA intends to acknowledge an ATS message with priority SS in the ATS-message-header, he initiates a function of the UA which generates either an RN or an ATS message in the format of the Acknowledgement message.

8.5.2.2.2 The decision which kind of message (RN or ATS message) needs to be generated should be taken by the UA based on the user capability information made available via the Directory Service (EDS).

8.5.2.2.3 If the originator of the distress message is an AMHS Direct User, an RN is generated, otherwise (originator is an AMHS Indirect User) an ATS message in the format of the Acknowledgement message is generated.

8.5.2.2.4 If the originator of the distress message cannot be identified by directory means, the default value is “AMHS Indirect User”.

8.5.2.3 Processing of AFTN Acknowledgement by an AFTN/AMHS Gateway

8.5.2.3.1 The occurrences of unconvertible RNs can be further reduced by the application of temporary conversion alternatives at the level of the AFTN/AMHS Gateway.

8.5.2.3.2 Specifically, the possibility for the AFTN/AMHS Gateway to convey incoming AFTN Acknowledgement messages into IPMs, instead of converting them to RNs, should be made available, preferably as a configuration parameter, and used during the transition phase.

8.6 Recommended processing of characters not authorized by ICAO Annex 10, Volume II

8.6.1 Introduction

8.6.1.1 This section presents recommended processing of characters or character sequences not authorized by ICAO Annex 10, Volume II and contained in the text part of a message or the optional heading information (OHI). Guidance for implementation is provided for the AFTN component and the MTCU of an AFTN/AMHS Gateway, as well as for User Agents.

8.6.2 Recommended processing by an AFTN component

8.6.2.1 ICAO Doc 9880, Part II, section 4.2.1.7 requires the AFTN component to pass to the MTCU only messages which are constructed in strict accordance with the provisions of ICAO Annex 10, Volume II, 4.4.15.1 through 4.4.15.3.12 and 4.4.15.6. This requirement includes that the message text may only contain characters allowed by ICAO Annex 10, Vol. II, 4.1.2.

8.6.2.2 How this requirement is achieved, should be considered as a local implementation matter. It is the objective of section 8.6.2.3 to provide guidance for appropriate implementation in the AFTN component of the AFTN/AMHS gateway.

8.6.2.3 *Guidance for implementation*

8.6.2.3.1 Each of the two implementations described in the following paragraphs 8.6.2.3.2 and 8.6.2.3.3 ensures that the AFTN component of an AFTN/AMHS gateway passes to the MTCU only messages of which the text and the OHI only contain characters and character sequences as authorized by ICAO Annex 10, Vol. II, 4.1.2.

8.6.2.3.2 The AFTN component of an AFTN/AMHS gateway can check the text and the OHI, if any, of each message received from the AFTN for characters and character sequences not authorized by ICAO Annex 10, Vol. II, 4.1.2. If such characters or character sequences are identified, the message can be forwarded to the Control Position for manual correction and retransmission by an operator. When no error is detected, the AFTN component passes the message to the MTCU for further processing.

8.6.2.3.3 Alternatively, the AFTN component of an AFTN/AMHS gateway can apply local conversion to the text and the OHI, if any, of each message received from the AFTN. Any character or character sequence not authorized by ICAO Annex 10, Vol. II, 4.1.2 is replaced by an allowed character or character sequence. Principles for local conversion are proposed below.

8.6.2.3.3.1 *Local conversion*

Local conversion may be based on the following rules:

- conversion of each IA5IRV alphabetical character in the text or in the OHI, if it is in lower case, into the equivalent upper case character;
- replacement by a question-mark (“?”, 0x3F) of each character in the text or the OHI, of which the use is not authorized by Annex 10, Volume II, 4.1.2;
- replacement by a question mark (“?”, 0x3F) of each character within a character sequence in the text or the OHI of which the use is not authorized in Annex 10, Volume II, 4.1.2.

8.6.2.3.3.2 *Event at the Control Position*

The Control Position of the AFTN/AMHS gateway should display an event for each message which was subject to character conversion. The operator should identify the originating station of the message and take action in order to avoid further submission of non-standard messages.

8.6.3 Recommended processing by an MTCU

8.6.3.1 *Initial processing of AMHS messages*

8.6.3.1.1 ICAO Doc 9880, Part II, section 4.5.2.1 defines initial processing of AMHS messages upon reception by the MTCU. More specifically, section 4.5.2.1.6 specifies how the MTCU shall process IPMs depending on the abstract-value of the *conversion-with-loss-prohibited* element. The conditions listed in sub-clauses 4.5.2.1.6 c) and d) do not cover all possible cases of characters or character sequences in the text that are not authorized by Annex 10. Furthermore, sub-clauses 4.5.2.1.6 c) and d) do not foresee any reaction by the MTCU in case the abstract-value of the element *conversion-with-loss-prohibited* is ‘prohibited’ and at least one character or character sequence in the optional-heading-information or the originators-reference is not authorized by Annex 10.

8.6.3.1.2 *Guidance for implementation*

8.6.3.1.2.1 The MTCU shall process an IPM according to ICAO Doc 9880, Part II, section 4.5.2.1. Especially for the processes described in 4.5.2.1.6 c) and d) it is recommended to consider all possible cases of not authorized characters or character sequences in the text or the optional-heading-information or the originators-reference in compliance with the procedure described below.

8.6.3.1.2.2 Referring to ICAO Doc 9880, Part II, section 4.5.2.1.6 c), in case the MTCU receives an IPM, at which the abstract-value of the element *conversion-with-loss-prohibited* is “prohibited” and at least one punctuation symbol in the text or the optional-heading-information or the originators-reference is not authorized in Annex 10, Volume II, 4.1.2, then:

1) the message should be rejected for all the message recipients; and

2) a non-delivery report should be generated as specified in ICAO Doc 9880, Part II, section 4.5.6 with the following elements taking the following abstract-values in all the *per-recipient-fields* of the report:

i) “conversion-not-performed” for the *non-delivery-reason-code*; and

ii) “punctuation-symbol-loss” for the *non-delivery-diagnostic-code*.

8.6.3.1.2.3 Referring to ICAO Doc 9880, Part II, section 4.5.2.1.6 d), in case the MTCU receives an IPM, at which the abstract-value of the element *conversion-with-loss-prohibited* is “prohibited” and at least one alphabetical character in the text or the optional-heading-information or the originators-reference is not authorized by Annex 10, Volume II, 4.1.2, then:

1) the message should be rejected for all the message recipients; and

2) a non-delivery report should be generated as specified in ICAO Doc 9880, Part II, 4.5.6 with the following elements taking the following abstract-values in all the *per-recipient-fields* of the report:

i) “conversion-not-performed” for the *non-delivery-reason-code*; and

ii) “alphabetic-character-loss” for the *non-delivery-diagnostic-code.*

8.6.3.1.2.4 In case the MTCU receives an IPM, at which the abstract-value of the element *conversion-with-loss-prohibited* is “prohibited” and the text or the optional-heading-information or the originators-reference contains at least one IA5IRV character sequence not authorized by Annex 10, Volume II, 4.1.2, taking into account sequences of lower case characters, upper case characters and combinations thereof then:

1) the message should be rejected for all the message recipients; and

2) a non-delivery report should be generated as specified in ICAO Doc 9880, Part II 4.5.6 with the following elements taking the following abstract-values in all the *per-recipient-fields* of the report:

i) “conversion-not-performed” for the *non-delivery-reason-code*; and

ii) “conversion-with-loss-prohibited” for the *non-delivery-diagnostic-code*;

8.6.3.1.2.5 In case the MTCU receives an IPM, at which the abstract-value of the element *conversion-with-loss-prohibited* is “prohibited” and the text or the optional-heading-information or the originators-reference contains at least one character which is not in the IA5IRV character repertoire (non-IA5IRV), then:

1) the message should be rejected for all the message recipients; and

2) a non-delivery report should be generated as specified in ICAO Doc 9880, Part II 4.5.6 with the following elements taking the following abstract-values in all the *per-recipient-fields* of the report:

i) “conversion-not-performed” for the *non-delivery-reason-code*; and

ii) “conversion-with-loss-prohibited” for the *non-delivery-diagnostic-code*.

Note.— Occurrence of non-IA5IRV characters is limited to the body part type “general-text-body-part” with repertoire identifiers {1, 6, 100} (Basic-1).

8.6.3.1.2.6 In case the MTCU receives an IPM, at which the abstract-value of the element *conversion-with-loss-prohibited* is “prohibited” and the text or the optional-heading-information or the originators-reference contains at least one control character other than <CR> or <LF> and not part of an escape sequence indicating which character set following characters belong to, then:

1) the message should be rejected for all the message recipients; and

2) a non-delivery report should be generated as specified in ICAO Doc 9880, Part II 4.5.6 with the following elements taking the following abstract-values in all the *per-recipient-fields* of the report:

i) “conversion-not-performed” for the *non-delivery-reason-code*; and

ii) “conversion-with-loss-prohibited” for the *non-delivery-diagnostic-code*.

8.6.3.1.2.7 In case the MTCU receives an IPM, at which the abstract value of the element *conversion-with-loss-prohibited* is “prohibited” and

- the text contains at least one line which is longer than 69 characters (ICAO Doc 9880, 2nd Edition, Part II, 4.5.2.1.6 b)) and the text or the optional-heading-information or the originators-reference meet any condition as described in 8.6.3.1.2.2 – 8.6.3.1.2.6, or

- the text or the optional-heading-information or the originators-reference meet at least two of the conditions as described in 8.6.3.1.2.2 – 8.6.3.1.2.6, including the case that one of these conditions is met by the text and another one is met by the optional-heading-information or the originators-reference, then:

1) the message should be rejected for all the message recipients; and2) a non-delivery-report should be generated as specified in ICAO Doc 9880, Part II, 4.5.6 with the following elements taking the following abstract-values in all the *per-recipient-fields* of the report:

i) “conversion-not-performed” for the *non-delivery-reason-code*; and

ii) “multiple-information-loss” for the *non-delivery-diagnostic-code*.

This recommendation is in line with ICAO Doc 9880, 2nd Edition, Part II, 4.5.2.1.6 e) considering text with several types of information loss (“line-too-long”, “punctuation-symbol-loss” and “alphabetic-character-loss”).

8.6.3.2 *IPM conversion*

8.6.3.2.1 ICAO Doc 9880, Part II, section 4.5.2.2 defines the generation of an AFTN message by the MTCU, depending on the results of the initial processing of a received IPM. ICAO Doc 9880, Part II, section 4.5.2.2.11 specifies rules for the conversion of the IPM text of an AMHS message with a valid body part type into the text part of an AFTN message.

8.6.3.2.2 ICAO Doc 9880, Part II, section 4.5.2.2.10 specifies how the OHI of an AFTN message derived from an IPM received by the MTCU, is generated. Nevertheless, ICAO Doc 9880, Part II does not specify any conversion rules for the OHI similar to those mentioned for the IPM text in 8.6.3.2.1 above. In order to ensure that the OHI of an AFTN message, derived from an IPM, does not contain any characters or character sequences not authorized by Annex 10, Vol. II, 4.1.2, the optional-heading-information or the originators-reference of the subject IPM should be converted as recommended in the following paragraph.

8.6.3.2.3 *Guidance for implementation*

8.6.3.2.3.1 For the conversion of an IPM message by the MTCU, the content of the OHI of an AFTN message derived from an IPM is according to ICAO Doc 9880, Part II, section 4.5.2.2.10, in compliance with the following procedure:

- conversion of each character which is not in the IA5IRV character repertoire into an IA5IRV character according to the locally defined conversion rules;
- conversion of each IA5IRV character, if it is in lower case, into the equivalent upper case character;
- replacement by a question-mark (“?”, 0x3F) of each character of which the use is not authorized in Annex 10, Vol. II, 4.1.2;
- replacement by a question-mark (“?”, 0x3F) of each character within a character sequence of which the use is not authorized in Annex 10, Vol. II, 4.1.2.

Note.— If the capability of the AFTN connected to the AFTN/AMHS Gateway is extended in terms of character set then the procedures described above may be adapted in accordance with the extended AFTN capabilities.

8.6.4 Recommended processing by a UA

8.6.4.1 ICAO Doc 9880, Part II, does not explicitly define the characters allowed in the optional-heading-information element (section 3.3.3.7.5 and 3.3.4.4) in contradiction to section 3.3.3.8 that specifies that ‘the ATS-message-text element shall be composed of IA-5 characters with no further restriction’.

8.6.4.2 *Guidance for implementation*

8.6.4.2.1 Upon generation of an IPM by an originator supporting the basic ATSMHS service the optional-heading-information element of the ATS-message-header is composed of IA-5 characters with a maximum length of either:

a) 53 characters if the message priority differs from “SS”; or

b) 48 characters if the message priority is “SS”.

8.6.4.2.2 When an IPM is generated by an originating extended ATSMHS user and all intended recipients of the message support the extended ATSMHS service, the optional heading information is contained in the originators-reference IPM heading field. The value of the optional heading information is composed of IA-5 characters with a maximum length of either:

a) 53 characters if the message priority differs from “SS”; or

b) 48 characters if the message priority is “SS”.

9 Miscellaneous

9.1 Legal Recording in AMHS

9.1.1 Annexes to the Convention on Civil Aviation

9.1.1.1 In an AMHS environment the rules for recording of communication are valid as expressed in Annexes 10 [1] and 11 [2] to the Convention on Civil Aviation, in sections 3.5 and 6 respectively. For easy reference, the pertinent paragraphs are quoted below.

9.1.1.2. A telecommunication log, written or automatic, shall be maintained in each station of the Aeronautical telecommunication service except that in an aircraft station, when using radiotelephony in direct communication with an aeronautical station, need not maintain a telecommunication log. [Annex 10, 3.5.1.1]

9.1.1.3 Telecommunication log, written or automatic, shall be retained for a period of at least thirty days. When logs are pertinent to inquiries or investigations they shall be retained for longer periods until it is evident that they will be no longer required. [Annex 10, 3.5.1.5]

9.1.1.4 Recommendation.— In all cases where automatic transfer of data to and/or from air traffic services computers is required, suitable facilities for automatic recording should be provided. [Annex 11, 6.2.2.3.3]

9.1.1.5 All facilities for direct-speech or data link communications between air traffic services units and between air traffic services units and appropriate military units shall be provided with automatic recording. [Annex 11, 6.2.2.3.7]

9.1.1.6 Recommendation.— All facilities for direct speech or data link communications required under 6.2.2.2.1 [Annex 11] and 6.2.2.2.2 [Annex 11] and not otherwise covered by 6.2.2.3.7 [Annex 11] should be provided with automatic recording. [Annex 11, 6.2.2.3.8]

9.1.1.7 Recommendation.— In all cases where automatic exchange of data between air traffic services computers is required, suitable facilities for automatic recording should be provided. [Annex 11, 6.2.3.5]

9.1.2 Manual on detailed technical specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI standards and protocols

9.1.2.1 In the Manual on detailed technical specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI standards and protocols [Doc 9880] the logging provisions for the Basic and Extended ATS Message Handling Service are defined. The AMHS management shall include logging provisions which are defined for the ATS Message

User Agent, for the ATS Message Server and for the AFTN/AMHS Gateway. Pertinent extracts from this Manual are presented below for easier reference.

9.1.2.2 AMHS Traffic logging upon origination [Doc 9880 , Part II, 2.7]

9.1.2.2.1 An AMHS Management Domain shall be responsible for long-term logging of all messages in their entirety, which are originated by its direct AMHS users, for a period of at least thirty days.

9.1.2.3 Traffic logging requirements at an ATS Message User Agent [Doc 9880, Part II, 3.1.3]

9.1.2.3.1 *Note.– The requirement expressed in 9.1.2.2.1 may be implemented in the ATS Message User Agent.*

9.1.2.4 Traffic logging requirements at an ATS Message Server [Doc 9880, Part II, 3.2.3]

9.1.2.4.1 The ATS Message Server shall perform a long-term logging, for a period of at least thirty days, of the actions taken with respect to every message received at the ATS Message Server, whether from an ATS Message User Agent or from another ATS Message Server, and to every report received or generated at the ATS Message Server.

9.1.2.4.2 For the long-term logging of information related to a message submitted to or received by an ATS Message Server, the following parameters related to the message shall be logged:

a) *message-identifier*;
b) *priority*;
c) *content-type*;
d) *originator-name*;
e) *recipient-name* elements on responsibility list;
f) message-content-size;
g) last element of the *trace-information* (if any);
h) arrival-time or submission-time;
i) transfer destination (if any);
j) transfer time (if any);
k) *this-recipient-name* (if message delivery is performed by the ATS Message Server);
l) *delivery-time* (if any);
m) delivery and/or non-delivery reports generated (if any); and
n) event date/time.

Note.– The responsibility list identifies recipients whose perRecipientIndicator responsibility bit has the abstract-value "responsible".

9.1.2.4.3 For the long-term logging of information related to a report generated or received by an ATS Message Server, the following parameters related to the report shall be logged:

a) *report-identifier*;
b) *subject-identifier*;
c) *actual-recipient-name* elements;
d) *report-type* elements;
e) *report-destination-name*;
f) last element of the *trace-information* (if any);
g) *arrival-time* in the ATS Message Server or generation time;
h) transfer destination (if any);
i) transfer time (if any);

j) *OR-name* of the report recipient (if report delivery is performed by the ATS Message Server);
k) *delivery-time* (if any); and
l) event date/time.

9.1.2.5 Traffic logging requirements at an AFTN/AMHS Gateway [Doc 9880, Part II, 4.3.1]

9.1.2.5.1 The Message Transfer and Control Unit shall perform long-term logging, as specified in 9.1.2.5.2 to 9.1.2.5.5, for a period of at least thirty days, of information related to the following exchanges of information objects with the ATN Component and with the AFTN Component:

a) AMHS message transfer out (to the ATN Component);
b) AMHS report transfer out (to the ATN Component);
c) AMHS message transfer in (from the ATN Component);
d) AMHS report transfer in (from the ATN Component);
e) AFTN message conveyance out (to the AFTN Component);
f) AFTN message conveyance in (from the AFTN Component);
g) AFTN service message indicating an unknown addressee indicator conveyance in (from the AFTN Component); and
h) AFTN service message indicating an unknown addressee indicator conveyance out (to the AFTN Component).

9.1.2.5.2 For the long-term logging of information related to an AMHS Message Transfer In and AFTN message conveyance out, the following parameters, relating to the messages, shall be logged by the Message Transfer and Control Unit:

a) input *message-identifier*;
b) *IPM-identifier*, if any;
c) *common-fields* and either *receipt-fields* or *non-receipt-fields* of IPN (Inter-Personal Notification), if any;
d) action taken thereon (reject with *non-delivery-reason-code* and *non-delivery-diagnostic-code*, convert as AFTN message, convert as AFTN acknowledgement message, splitting due to number of recipients or message length, delivery report generation);
e) event date/time;
f) Origin line of converted AFTN message or AFTN service message, if any; and
g) transmission identification of AFTN message(s) or AFTN service message(s), if returned by the AFTN Component.

9.1.2.5.3 For the long-term logging of information related to AFTN message conveyance in and AMHS Message Transfer Out, the following parameters, relating to the messages, shall be logged by the Message Transfer and Control Unit:

a) Origin line of AFTN message (or AFTN acknowledgement message);
b) transmission identification of AFTN message or AFTN service message, if any;
c) action taken thereon (reject with rejection cause, convert as IPM, convert as RN, AFTN service message indicating an unknown addressee indicator generation);
d) event date/time;
e) *MTS-identifier*, if any; and
f) *IPM-identifier*, if any.

9.1.2.5.4 For the long-term logging of information related to an AMHS Message Report In and/or AFTN service Message indicating an unknown addressee indicator conveyance out, the following parameters, relating to the report and/or AFTN service message, shall be logged by the Message Transfer and Control Unit:

a) *report-identifier* (if report in);
b) *subject-identifier* (if report in);
c) action taken thereon if report in (discard, convert into AFTN service message);
d) event date/time;
e) Origin line of converted AFTN service message (if AFTN service message out);
f) Origin line of subject AFTN message (if AFTN service message out and no report in); and
g) transmission identification of AFTN message or AFTN service message, if any.

9.1.2.5.5 For the long-term logging of information related to an AFTN service message indicating an unknown addressee indicator conveyance in and/or to an AMHS Message Report Out, the following parameters, relating to the AFTN service message and/or report, shall be logged by the Message Transfer and Control Unit:

a) Origin line of converted AFTN service message (if AFTN service message in);
b) Origin line of subject AFTN message (if AFTN service message in);
c) transmission identification of AFTN message or AFTN service message, if any;
d) action taken thereon if AFTN service message in (discard, convert into AMHS report);
e) *report-identifier* (if report out);
f) *subject-identifier* (if report out);
g) MTS-identifier of resulting message, if the AFTN service message was converted into an IPM; and
h) event date/time

9.1.2.5.6 If, for any reason, the processing of the AMHS component cannot be properly achieved, the procedure shall unsuccessfully terminate and:

1) logging of the error situation and reporting to a control position, and

2) storage of the concerned message for appropriate action at the control position,

shall be performed.

Note.– ICAO Doc 9880, Part II [3] specifies all cases for the AFTN/AMHS Gateway in more detail.

9.1.3 Additional logging requirements for PRMD “EUROPE” and AMHS MDs adjacent to this MD

9.1.3.1 AMHS Traffic logging upon origination

9.1.3.1.1 In addition to 9.1.2.2.1 above, in the specific case of PRMD “EUROPE”, the referred Doc 9880 requirement applies to each European Service or Application part of the “EUROPE” AMHS Management Domain.

9.1.3.2 Traffic logging requirements at an ATS Message Server

9.1.3.2.1 In addition to 9.1.2.4.2 above, in the specific case of PRMD “EUROPE” and of PRMDs adjacent to PRMD “EUROPE”, for the long-term logging of information related to a message submitted to or received by an ATS Message Server, the following parameters related to the message shall also be logged:

a) the last element of the *internal-trace-information* (if any).

9.1.3.2.2 In addition to 9.1.2.4.3 above, in the specific case of PRMD “EUROPE” and of PRMDs adjacent to PRMD “EUROPE”, for the long-term logging of information related to a report generated or received by an ATS Message Server, the following parameters related to the report shall also be logged:

a) the last element of the *internal-trace-information* (if any).

9.2 Specific requirements applying to PRMD “EUROPE”

9.2.1 Local identifier values in MTS-Identifiers

9.2.1.1 There is no base standard requirement ensuring that MTS-Identifiers generated by different MTAs managed by different organisations within PRMD “EUROPE” would be different. From a theoretical viewpoint, there is a possible risk of duplicate use of MTS-Id. An additional requirement applying only to MTAs belonging to PRMD “EUROPE” is therefore needed to remove this risk. The requirement is specified in the clause which follows.

9.2.1.2 Organisations coordinating under the aegis of ICAO-Europe to form PRMD “EUROPE” shall agree upon, and implement a technical means ensuring uniqueness of the *local-identifier* sub-part values of the *MTS-identifier* and *report-identifier* elements generated by MTAs belonging to PRMD “EUROPE”.

9.2.1.3 It may be noted that one such technical means could be the insertion of the *MTA-name* as a prefix to *the local-identifier* element.

9.2.2 Trace-information and internal-trace-information

9.2.2.1 *Trace-information* is used in MHS/X.400 systems to provide information about the path followed by a message, probe or report. However*, trace-information* includes only MD-related records. In the context of PRMD “EUROPE” where MTAs are managed by independent organisations, *trace-information* is more difficult to use and may be seen as ambiguous. Additional requirements applying only to MTAs belonging to PRMD “EUROPE” are therefore needed to enable accurate identification of the source MTA and related organisation. These requirements are specified in the clause which follows. They are based on the use of *internal-trace-information* which, conversely to *trace-information*, includes the *MTA-name* and thus provides an accurate reference. The base X.400 standards allow a MTA to remove internal-trace-information before sending a message, probe or report to an adjacent MD. This has to be avoided for MTAs belonging to PRMD “EUROPE”, to make sure that:

a) the accurate tracing information is maintained when exiting PRMD “EUROPE”, and

b) loop detection algorithms counting the number of trace-information-elements and internal-trace-information-elements will be effective for messages exchanged within PRMD “EUROPE”.

9.2.2.2 MTAs belonging to PRMD “EUROPE” shall insert *internal-trace-information*, if not yet present, in the messages, probes and reports which they transfer. If internal trace is present, these MTAs shall append an *InternalTraceInformationElement to internal-trace-information*. MTAs belonging to PRMD “EUROPE” shall be prevented from removing *internal-trace-information* from messages, probes and reports transferred to MTAs outside PRMD “EUROPE”.

9.2.2.3 Due to the use of *internal-trace-information* for tracing purposes when exiting PRMD “EUROPE”, it becomes necessary that this information become subject to long-term logging for all MTAs adjacent to PRMD “EUROPE”, and by extension, for all ATS Message Servers.

9.2.3 Use of PerDomainBilateralInformation

9.2.3.1 *PerDomainBilateralInformation* is an optional element which may be used in MHS/X.400 systems to exchange (at P1 level) information related to a message, probe or report and intended for a given MD. There is no known example of ANSPs using this information element in the European AMHS, however, this is not precluded by any of the applicable standards and documents. A *PerDomainBilateralInformation* information element includes the Global Domain Identifier (GDI) of the MD for which the information is intended. In the context of PRMD "EUROPE" where MTAs are managed by independent organisations, bilateral information, if used, would be between a PRMD other than "EUROPE" and an organisation part of PRMD "EUROPE". In such a case, the GDI for PRMD "EUROPE" may be seen as ambiguous to specify the intended recipient of bilateral information. Additional requirements applying to MTAs belonging to PRMD "EUROPE", and to their partners for this type of exchanges, are therefore needed to enable accurate identification of the destination MTA and related organisation. These requirements are specified in the clause which follows.

9.2.3.2 If *PerDomainBilateralInformation* is used in reception by one of the organisations coordinating under the aegis of ICAO-Europe to form PRMD "EUROPE", the sub-element *bilateral-information* shall be structured in a way such that the relevant organisation and/or its MTA can be identified unambiguously among the organisations forming PRMD "EUROPE" and/or their MTAs.

9.3 Institutional / financial issues

- to be developed -

<u>Attachment A: Change Control Mechanism of the EUR AMHS Manual and its Appendices.</u>

Note.– Changes, problems or defects detected concerning the Standards and Recommended Practices (SAPS) summarised in the ICAO Documentation (Doc 9880 as well as Doc 9537) are not affected by this mechanism. For these documents the change control process set up by ACP and its Working groups, by using PDR (Preliminary Defect Reports) applies.

Proposals to introduce changes to the EUR AMHS Manual and its Appendices may arise from users, implementers or manufacturers. The procedure for submission and processing of a Defect Report (DR) or a Change Proposal (CP) involves the following steps:

A.1 Procedure for DR

a) A problem is detected concerning the operation of the AMHS network, which is reflected in the EUR AMHS Manual and may be attributed to implemented AMHS procedures and/or inconsistencies in the documentation.

b) The problem is reported to the Rapporteur of the Planning Group of the AST TF, by submission a defect report (DR). A standard reporting format is used (see attached template).

c) The Rapporteur assigns a number and priority to the defect report and introduces it to the agenda of an upcoming meeting of the PG.

d) The PG evaluates the report and either adopts it as a working item or rejects it. The party, which submitted the defect report, is notified accordingly.

e) Experts of the PG are assigned to the problem and milestone dates are set.
Outside expertise may be invited to participate, as appropriate.

f) The PG develops proposals for resolving the problem and submits them to the AST TF for approval.

g) The AST TF approves or rejects the presented proposals. In case of the latter, the subject is referred back to the PG (step e) or discarded.

h) The PG drafts appropriate text for amendment of the EUR AMHS Manual and submits it to the AST TF for approval.

i) The AST TF approves or rejects the proposed material. In case of the latter, the subject is referred back to the PG (step h).

j) The proposed amendments to the EUR AMHS Manual are presented to the EASPG for approval.

k) Solutions are implemented.

Steps (f) and (h) may run in parallel.

A.2 Procedure for CP

The same structured procedure, with the exception of steps (f) and (g) applies in case of proposed enhancements to the EUR AMHS Manual or inconsistencies in existing EUR AMHS documentation.

In this case, a change proposal (CP) should be submitted to the PG. The format of the CP is similar to that of the DR.

(If Doc 9880 documentation is concerned the change control process set up by ACP and its Working groups has to be followed (see Attachment B).)

A.3 Template for Defect Reports / Change Proposals

TEMPLATE FOR DEFECT REPORTS / CHANGE PROPOSALS

DR_____ **CP_____**

Title:	Short, indicative textual name
Reference:	Number assigned by the PG Rapporteur
Originator reference:	Provided by the originator
Submission date:	
Submitting State/Organization:	
Author:	
Contact Information:	e-mail, fax, telephone and postal address
Experts involved:	
Status:	Assigned by the PG Rapporteur
Priority:	Assigned by the PG Rapporteur
Document reference:	Affected section(s) of the EUR AMHS Manual or its Appendices
Description of defect:	Nature of the problem in detail Reason(s) for requesting changes
Assigned expert(s):	
Task history:	Working Papers and Information Papers Produced on the subject
Proposed solution:	Including amendments to the text, if feasible

DR/CP STATUS control sheet				
Event	**Date**	**Status**		**Remark**
DR or CP received submission date		Set to submitted		
discussion at PG/ ...		Set to accepted	Set to rejected	
Date for development of proposals/ solutions				Responsible:
discussion at PG/ ...		Set to resolved		
presentation to AST TF/ ...		Set to adopted	Set to rejected	
Date for development of amendment to the Manual				Responsible:
discussion at PG/		Set to approved		
presentation to AST TF/ ...		Set to approved for application		
Additional DATES and comments				

Attachment B: Amendment Procedure for the detailed Technical Specifications for Air/Ground and Ground/Ground Data Links

(updated 2008-06-12)

Published in the Report of the twelfth meeting of the Aeronautical Communications Panel (ACP), Working Group M (WG M) -(Reconstituted), Montreal, 16-19 June 2008

B.1 Introduction

B.1.1 Detailed technical specifications for air/ground and ground/ground data link systems are contained in the following ICAO documents:

ATN/OSI	Doc 9880, Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI Standards and Protocols
ATN/OSI	Doc 9705, Manual on technical provisions of the aeronautical telecommunication network (to be withdrawn)
ATN/OSI	Doc 9739, Comprehensive Aeronautical Telecommunication Network (ATN) Manual (to be withdrawn)
AMS(R)S	Doc AMSRS, Manual for Aeronautical Mobile Satellite (Route)_Service
VDL Mode 2	Doc 9776, Manual on VHF Digital Link (VDL) Mode 2
VDL Mode 3	Doc 9805, Manual on VHF Digital Link (VDL) Mode 3 (currently not being maintained)
VDL Mode 4	Doc 9816, Manual on VHF Digital Link (VDL) Mode 4
HF data link	Doc 9741, Manual on HF Data Link

B.2 Amendment Procedure

B.2.1 ACP Working Group M (WG M) will continue to maintain the material identified in section B.1.1 as indicated in the terms of reference agreed in ACP. In this task, the working group will consider proposals for amending this material as a result of ongoing validation of the detailed technical specifications and experience gained during the implementation of these systems. Amendments are necessary when a statement of information in the manuals or their supporting material, if not corrected, will prevent the system from meeting its stated operational requirements.

B.2.2 Amendment Proposals will be submitted to ACP Working Group M, preferably in the format of Table B-2. ACP Working Group M will review each amendment proposal and agree on the changes, to be made to the relevant detailed technical specifications. The amendment proposals will be distributed to the members of WG M by the secretariat through placing the information on the ACP website. This would also enable all panel members to also consider the proposals.

B.2.3 Amendment Proposals may be required when:

i. implementation hardships occur, resulting from schedule and/or costs;

ii the detailed technical specifications over-specify the actual requirements for achieving interoperability or may unnecessarily constrain implementation or further development;

iii the detailed technical specifications inadequately specify the actual requirements for achieving the intended operational capabilities;

iv ambiguities in the detailed technical specifications result in different implementations that are not interoperable;

v interoperability discrepancies are discovered.

Note.– Should a State [or a relevant international organization] identify a safety critical problem, which might e.g. necessitate grounding of aircraft, an ICAO fast track procedure should be established. Such a procedure would enable an amendment of the SARPs at very short notice (e.g. 1 - 2 months). A fast track procedure is not expected to be required for detailed technical specifications.

B.3 Maintenance procedures

B.3.1 The following maintenance procedures apply:

i interested parties submit an amendment proposal, preferably using the form in Table B-2. The proposal will address aspects relating to the backwards compatibility of the amendment proposal. The proposal will also indicate a category from Table B-1 and identify a coordinator.

ii the amendment proposals will be placed on the ACP website as soon as practicable;

iii WG M will consider amendment proposals will be submitted not later than four weeks prior to a WG M meeting;

iv the amendment proposal will be reviewed during meetings of WG M. If necessary, a special group will be formed to study detailed aspects of the proposal. If the working group cannot complete its re view, the amendment proposal will be added to the list of action items.

v the Working Group M will recommend to ICAO on the amendments necessary;

vi ICAO will publish regularly the necessary amendments to the manuals on detailed technical specifications and implementation aspects.

Table B-1 Category of an Amendment Proposal (AP)

Category	**Description**
Critical	The AP addresses a serious flaw in the manuals text which either: a) if implemented in an operational system could jeopardize safety in the air, and/or b) would result in non-interoperability between operational systems which have implemented the amendment proposal and those which have not.
Bug	The AP addresses bugs in the manuals, which affect SARPs, and/or operational implementations to be fully compliant with the technical provisions in the manuals.
Clarification	The AP clarifies an ambiguity or omission in the manuals. APs in this category are useful but not essential to ensure interoperability and proper functioning of the system.
Minor	The AP clarifies or improves the internal consistency of the manuals, but has no effect on implementations.
Editorial	The AP corrects one or more editorial or typographical errors in the manuals, or adds detail, which has no effect on implementations.
Registration	The AP proposes placeholders for activities other than those identified in the manuals.

Table B-2 Format of an Amendment Proposal (AP)

Title:	
AP working paper number and date:	
Document(s) affected:	Doc 9880, Manual on detailed technical specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI standards and protocols Doc AMSRS, Manual for Aeronautical Mobile Satellite (Route) Service Doc 9776, Manual on VHF Digital Link (VDL) Mode 2, Doc 9816, Manual on VHF Digital Link (VDL) Mode 4 Doc 9741, Manual on HF Data Link
Sections of Documents affected:	
Coordinator:	
Coordinators address:	
Coordinators Phone:	
Coordinators Fax:	
Coordinators e-mail address:	
Category:	CRITICAL | BUG | CLARIFICATION | MINOR | EDITORIAL | REGISTRATION
Problem description:	
Background:	
Backwards compatibility:	
Amendment Proposal:	
WG-M status:	PROPOSED | APPROVED | PENDING | REJECTED

-END-