

Kommunikationsprotokolle des Aeronautical Traffic Service

SEMINARARBEIT

S 911.039 Seminar aus Informatik

Eingereicht von:

Ing. Gottfried Schobersteiner, BSc, Mat.Nr. 1021429

Ing. Ernst Wolfgang Tillian, Bakk.Techn., Mat.Nr. 0320806

Angefertigt auf:

Universität Salzburg, Fakultät Computerwissenschaften

Betreuung:

Univ.-Prof. Dipl.-Ing. Dr.techn. Wolfgang Pree

Salzburg, 15. Juli 2012

Diese Seminararbeit entstand im Rahmen des

Masterstudiums Angewandte Informatik

an der Universität Salzburg
zum Pflichtfach Seminar
Seminar aus Informatik
in

Sommersemester 2012

Betreuer:

Univ.-Prof. Dipl.-Ing. Dr.techn. Wolfgang Pree

Inhaltsverzeichnis

Kurzfassung	v
Abstract	vi
Kapitel 1 Einführung in das Thema	1
1.1 Einleitung	1
1.1.1 Wissenschaftliche Ausarbeitungen	1
1.1.2 Standardisierungsgremien	1
1.1.3 Motivation	2
1.2 Ziele der Seminararbeit	2
Kapitel 2 Klärung von Begriffen	3
2.1 Aeronautical Telecommunication Network (ATN)	3
2.1.1 Aeronautical Fixed Telecommunication Network (AFTN)	4
2.1.2 Air Traffic Services Message Handling System (AMHS)	4
2.1.3 Übergangsphase	5
2.2 Air Traffic Messages	6
2.2.1 ATS-Meldungen	6
2.2.2 AMHS-Message Handling Service	7
Kapitel 3 Bestehende Implementierungen	9
3.1 AFTN	9
3.1.1 Limitierungen in AFTN	9
3.2 Datenübertragung Protokollfamilie X.25	10
3.2.1 Entstehung	10
3.2.2 Aufbau	11
3.2.3 Kommunikationstelegramme	12
3.2.4 Kommunikationsablauf	14
3.3 Implementierung in AFTN	16
3.3.1 Kanalbezeichnung und Laufnummer einer ATS-Meldung	16
3.3.2 Adressierung einer ATS-Meldung	16
3.3.3 ATS-Flugplan	17
Kapitel 4 Ziel - Systeme und Protokolle	19
4.1 AMHS	19
4.2 Anforderungen an AMHS	20
4.3 AMHS over TCP/IP	20
4.3.1 Meldungszustellung in AMHS	21
4.4 Protokollfamilie X.400	22
4.4.1 Entstehung	22

4.4.2	Aufbau	22
4.4.3	Kommunikationstelegramme	23
4.4.4	Kommunikationsablauf.....	24
4.5	Funktionalitätserweiterung durch AMHS	25
4.5.1	IT-Security	25
Kapitel 5	Schlusswort	26
5.1	Fazit	26
5.2	Empfehlungen und Ausblick	27
Literatur		28
Abbildungsverzeichnis		31

Kurzfassung

Das „*Aeronautical Telecommunication Network*“ (ATN) steht im Rahmen der weltweiten Luftfahrt als Datenkommunikationsnetzwerk zur Verfügung und ist durch die ICAO („*International Civil Aviation Organization*“) standardisiert.

Der Dienst der Flugsicherung bedient sich dabei der Hauptapplikation „*ATS Interfacility Data Communications*“ (AIDC) und davon des Teiles „*Aeronautical Traffic Service*“ (ATS). Diese Applikation setzt eine Datenkommunikation zwischen den Bodenkontrollzentren voraus.

Bisher sind Implementierungen des AFTN („*Aeronautical Fixed Telecommunication Network*“) auf Basis des Übertragungsprotokoll X.25 umgesetzt. Bereits in den 1970er Jahren wurde die Technologie der fixen Knotenverbindungen unter Anwendung von festgelegten Prozeduren und betrieblichen Ablaufregelungen nach dem Grundsatz „Store-and-Forward“ von Meldungen weltweit normiert.

Nunmehr werden die veraltete Technologie und organisationsaufwändigen Abläufe durch bereits etablierte Technologien abgelöst. Als Standard ist AMHS („*Air Traffic Service Message Handling System*“) auf Basis des Übertragungsprotokolls X.400 definiert.

Die Umstellung der Systeme von AFTN auf AMHS kann jedoch weltweit nur sukzessive erfolgen. Daraus entstehen Forderungen diesen Umstieg ohne Betriebsunterbrechungen im Luftverkehr sowie bei gleichzeitiger Aufrechterhaltung der Kompatibilität zwischen beiden Systemen bewerkstelligen zu können. Die Übergangsphase bringt Anforderungen an die technischen, als auch organisatorischen Komponenten mit sich, die zu berücksichtigen sind.

In dieser Arbeit erfolgt eine Betrachtung der Erfordernisse an die Systeme die diese erfüllen müssen. AMHS wird als Zielsystem bezeichnet.

Weiters werden die verwendeten Kommunikationsprotokolle beleuchtet und Grundlagen des Meldungsaustausches und somit der Kompatibilität beider Systeme erarbeitet. Fragestellungen betreffend der Vorteile und möglichen Chancen in Verbindung mit dem Umstieg auf den neuen, sicheren, kostengünstigen und etablierten Kommunikationsstandard werden beantwortet.

Abstract

The Aeronautical Telecommunication Network (ATN) is in the context of the global aviation standardized as a data communications network by the ICAO (International Civil Aviation Organization).

The air traffic control service uses the main application “*ATS Inter-Facility Data Communications*” (AIDC) especially the “*Aeronautical Traffic Services*” (ATS). This application presumes a data communication between the ground control centres.

So far, implementations of the AFTN (Aeronautical Fixed Telecommunication Network) are implemented on base of the X.25 transmission protocol. Already in the 1970s, the technology of the fixed node connections using established procedures and operational discharge control according to the “store-and-forward” messages was standardized worldwide.

Now, the outdated technology and the complex organizational processes are superseded by already well-established and standardized technology. The new Standard AMHS (“*Air Traffic Service Message Handling System*”) based on the X.400 protocol transmission is defined.

The transition from AFTN to AMHS systems may be accomplished worldwide only successively without disruption in air traffic as well, while maintaining compatibility between the two systems is defined. This transition brings the requirements to the technical implementation and to the organizational components with it.

In this work, the consideration of the requirements of the systems must be satisfied, whereby AMHS is called the target system.

Further highlights are the communication protocols and the principles of the message exchange used to propose the compatibility of both systems. Questions regarding the benefits and potential opportunities associated with the transition to the new, safe, inexpensive and well-established communication standard are to be answered.

Kapitel 1

Einführung in das Thema

1.1 Einleitung

In dieser Arbeit erfolgt die Darstellung und die Betrachtung der Anwendung unterschiedlicher Kommunikationsprotokolle, wie sie für den Meldungsaustausch in der weltweiten Luftfahrt vorgesehen sind. Dazu werden die Systeme des *Aeronautical Telecommunication Network* (siehe 2.1 Aeronautical Telecommunication Network (ATN)) betrachtet. Grundlage dazu stellen einerseits wissenschaftliche Ausarbeitungen sowie veröffentlichte Standards von für den Flugverkehr rechtlich zuständige Organisationen dar.

1.1.1 Wissenschaftliche Ausarbeitungen

Basis dieser Arbeit sind wissenschaftliche Texte in Bezug zum Thema. Einerseits werden die Grundlagen im Umfeld ATN, als auch die darin verwendeten Kommunikationsprotokolle beleuchtet. Mündet eine wissenschaftliche Ausarbeitung in einen Implementierungsstandard, so wird versucht ein Bezug zu diesen hergestellt.

1.1.2 Standardisierungsgremien

Die *International Civil Aviation Organisation* (ICAO)¹ erarbeitet und legt verbindliche Regelungen und Standards für die Luftfahrt fest, um einen weltweit sicheren grenzüberschreitenden Luftverkehr zu ermöglichen.

Der Einhaltung dieser Standards unterliegen alle Flugsicherungsdienste der Mitgliedsländer². Die Flugsicherungsdienste haben dabei die Aufgabe den Luftraum zu überwachen und im von ihnen kontrollierten Luftraum und Flugplätzen durch Weisungen an die Piloten für die nötigen Sicherheitsabstände zwischen den Flugzeugen zu sorgen und somit Zusammenstöße zu verhindern.

Diese nationalen Flugsicherungsdienste sind in Europa in der *European Organisation for the Safety of the Air Navigation* (EUROCONTROL)³

¹ Dt.: Internationale Zivilluftfahrtorganisation, <http://www.icao.int>

² 191 Member States, <http://www.icao.int/Pages/icao-in-brief.aspx>, per 6.April 2012

³ <http://www.eurocontrol.int/>

organisiert. Die Übertragung der rechtlichen Grundlagen erfolgte durch die Europäische Kommission im Rahmen der Verordnung EG Nr. 552/2004⁴ über die Interoperabilität des europäischen Flugverkehrsmanagementnetzes.

1.1.3 Motivation

In der Luftfahrt sind auf Grund der weltweiten Zusammenarbeit grundlegende Datenübertragungen in ihren Kommunikationsprotokollen als auch Nachrichtenübermittlungen stark normiert. Die Kommunikationsverbindungen zwischen den meist nationalen Zentren sowie der Luftfahrtgesellschaften als leistungsfähige, sichere sowie redundante Netzwerkverbindungen realisiert.

Netzwerkverbindungen zwischen den Boden-Organisationselementen im Luftverkehr sind dagegen noch meist im seit mehr als 30 Jahren weltweit etablierten Standard „*Aeronautical Fixed Telecommunication Network*“ (AFTN) realisiert.

Nunmehr sollen nach einer Empfehlung der ICAO alle Organisationselemente (meist Flugsicherungsstellen auf kleineren Flugplätzen) auch auf einen neueren aber zugleich sicheren, kostengünstigen und etablierten Kommunikationsstandard als Basis des ATN umgestellt werden.

In dieser Arbeit soll nunmehr der wesentliche Unterschied der dafür in Betracht kommenden Standards erarbeitet werden. Begleitende Beispiele werden erläutert und kennzeichnen die Unterschiede.

Eine Systemumstellung kann weltweit nicht gleichzeitig erfolgen und somit ist großes Augenmerk auf die Aufrechterhaltung der Rückwärtskompatibilität zu legen.

1.2 Ziele der Seminararbeit

Dabei sind folgende Fragestellungen zu betrachten:

- Welche Übertragungsstandards und Datenübermittlungen sind bei AFTN relevant?
- Sind für ATN andere Standards festgelegt?
- Was sind die Erfordernisse um ein ATN-Netzwerk betreiben zu können?
- Sind Standards vorgegeben, die diese „Übergangsphase“ unterstützen bzw. eingehalten werden müssen?
- Liegen Empfehlungen vor, um technische Sicherheitsmaßnahmen hinsichtlich der IT-Sicherheit integrieren zu können?
- Bringt der Umstieg auf einen neuen, sicheren, kostengünstigen und etablierten Kommunikationsstandard noch weitere Chancen und Vorteile mit sich.

⁴ Des europäischen Parlaments und des Rates vom 10.März 2004 im *Amtsblatt Nr. C 323 vom 31/12/2009 S. 0024*

Kapitel 2

Klärung von Begriffen

2.1 Aeronautical Telecommunication Network (ATN)

Oishi [Ois01, 3-1339] stellt fest, dass die Kommunikation des bestehenden aeronautischen Netzwerkes auf Basis des ISO/OSI-7-Schichten-Modells⁵ verwirklicht wurde. Im ATN erfolgt die Kommunikation zwischen den Bodenstationen sowie zwischen Flugzeug und den Bodenstationen, wobei er folgende Hauptapplikationen identifiziert:

- Automatic Dependent Surveillance (ADS)⁶
- Controller Pilot Data Link Communications (CPDLC)⁷
- ATS Interfacility Data Communications (AIDC)⁸
- Data Link Flight Information Service (DFIS)⁹
- ADS Broadcast (ADS-B)¹⁰

In dieser Arbeit erfolgt die Betrachtung der Datenkommunikation zwischen Bodenkontrollzentren (ATC center¹¹) und dies definiert *Oishi* wie folgt:

AIDC mirrors exchanges currently performed between international ATC centers either by telephone or via the Aeronautical Fixed Telecommunication Network (AFTN) which was originally defined as a teletype network. [Ois01, 3.1340]

⁵ OSI – Open Systems Interconnection, ISO – International Standardization Organisation, Standard ISO 7498

⁶ ADS – Automatic position reports from aircraft to controller

⁷ CPDLC – Voice communication between pilot and controlstation

⁸ AIDC – Data communication between control centers

⁹ DFIS – Broadcast as audio on dedicated radio channels

¹⁰ ADS-B – automatic position and identification information broadcast

¹¹ ATC – Air Traffic Control, mit der Organisation ATS-unit

2.1.1 Aeronautical Fixed Telecommunication Network (AFTN)

Das weltweit etablierte (AFTN) [ICA01, 4-3] Netzwerk verbindet fix definierte Zentren über Kanalverbindungen und dient als Basis der Kommunikation zum Austausch von vordefinierten Meldungen.

Auf Basis der Technologie der fixen Knotenverbindungen wurden bereits in den 1950er Jahren Prozeduren nach dem Grundsatz „Store-and-Forward“ von Meldungen erarbeitet.

Aufgrund der Erneuerung von Technologien etablierte sich in den 1980er Jahren ein fortschrittlicheres Netzwerk, das „Common ICAO Data Interchange Network“ (CIDIN) [ICA01, 4-26]. Dabei wurden die Verfahren, Meldungstypen und Inhalte aus den Grundsätzen des AFTN übernommen. Als Datenübertragungsprotokoll zwischen den Netzwerkknoten wurde X.25 (siehe 3.2 Datenübertragung Protokollfamilie X.25) nach ITU-T¹² als Standard definiert.

Der Begriff AFTN subsumiert neben der technischen Infrastruktur mit den notwendigen Netzwerkprotokollen, den formalen Meldungs austausch als auch die prozeduralen Abläufe zur Sicherstellung von Services im Rahmen der Luftfahrt.

2.1.2 Air Traffic Services Message Handling System (AMHS)

Das seit über 30 Jahren laufende AFTN-Basisnetzwerk wurde aufgrund der technischen Marktentwicklungen im Netzwerksektor mittlerweile durch zeitgemäße TCP/IP- Netzwerke¹³ abgelöst.

Nunmehr wird durch die Standardisierungsgremien (siehe 1.1.2 Standardisierungsgremien) im Rahmen der Luftfahrt als neues Kommunikationssystem das „Air Traffic Service Message Handling System“ (AMHS) [ICA01, 4-27] vorgegeben. Dieses System ist im ISO/OSI Schichtenmodell auf dem „Application Layer“ anzusiedeln und basiert auf dem Kommunikationsstandard X.400 (siehe 4.4 Protokollfamilie X.400) nach ITU-T (Message Handling System).

EUROCONTROL gibt für den Übergang zum neuen Protokoll folgende Hintergrundinformation:

The Aeronautical Fixed Telecommunications Network (AFTN), complemented in Europe by the Common ICAO Data Interchange Network (CIDIN), has provided an effective store-and-forward messaging service for the conveyance of text messages, using character-oriented procedures, for many years. However AFTN / CIDIN technology is now becoming obsolescent,

¹² International Telecommunication Union – Telecommunication Standardization Sector

¹³ Transmission Control Protocol / Internet Protocol

and is not sufficiently flexible to support messaging functions found in modern messaging systems (such as transfer of binary information).

It is intended that existing AFTN and CIDIN users and systems will transition to the architecture of the Aeronautical Telecommunication Network (ATN), and this is enabled in part by the ATSMHS application, which has been defined by ICAO to replace the AFTN telegraphic style of working with a modern store and forward Message Handling System based on international Standards.¹⁴

Im europäischen Kontext wird die Kommunikation zwischen den Knotenpunkten auf Basis von AHMS bis zum Jahr 2013 sukzessive umgesetzt. AMHS ermöglicht den durchgängigen Einsatz einer TCP/IP Netzwerkinfrastruktur wie sie im Gesamtkontext des ATN („Aeronautical Telecommunication Network“) vorgesehen ist [Ois01, 3-1340]. Im ATN ist die zusätzliche Übertragung von binären Daten vorgesehen. Weiters lässt ATN auch einen sicherheitsrelevanten, verschlüsselten Datenaustausch wie er beispielsweise für einen Authentifizierungsmechanismus notwendig ist, zu. Restriktionen in der Meldungslänge (AFTN sah eine Begrenzung auf 1800 Charakter vor) obsolet.

2.1.3 Übergangsphase

Als grundwichtiges Kriterium bei der Überführung einzelner Netzwerkknoten von AFTN/CIDIN in das Zielsystem AMHS ist die Aufrechterhaltung des operationellen Betriebes anzuführen. Eine gleichzeitige Umstellung aller Knoten ist nicht notwendig und nicht möglich und wird daher von den Regelungs- und Standardisierungsorganisationen ICAO und EUROCONTROL als „Transistionphase“¹⁵ bezeichnet.

Smith [Smi01, 7.A.6-2] fasst die Anforderungen an diese „Transistionphase“ zusammen:

The ATN is a data communication inter-network that is to provide:

1. A common communications service for all Air Traffic Services Communications (ATSC).
2. Integrates and uses existing communications network and infrastructure wherever possible

¹⁴ <http://www.eurocontrol.int/articles/air-traffic-services-message-handling-system-amhs-specification>, Zugriff vom 6. April 2012.

¹⁵ Dt. Übergangsphase

3. Provides a communication service, which meets the security and safety requirement of all applications
4. Accommodates the different grades of service required by each application.

ATN has been specified to meet the requirements of the Civil Aviation Community and is expected to give the following benefits:

- Use the existing infrastructure
- High availability and Scalability
- Prioritized end-to-end
- Policy Based Routing
- Use of COTS Products and improved Communication

Ishibashi [Ish05, 1.D.1-1] beschreibt die Problemstellung dieser „Transitionphase“:

Necessarily, this technology needs to be exact, secure and safe, meet integrity and availability and follow the rules and standards imposed by ICAO.

Actually, ATN networks have no development platform to help an ATN system designer. This necessarily involves understanding various data link services (applications), numerous data link technologies and essentially a detailed protocol by means of an ad hoc process, that is, there is not a widespread Framework for ATN design.

2.2 Air Traffic Messages

Um den Flugsicherungsservice in der Luftfahrt sicherzustellen werden „Air Traffic Service“-Meldungen¹⁶ zwischen den involvierten „Air Traffic Centres“ (ATC) ausgetauscht. Diese Meldungen werden im „Aeronautical Telecommunication Network“ (ATN) übertragen. Dabei ist die Einhaltung der Kompatibilität gegenüber dem AFTN sicherzustellen.

2.2.1 ATS-Meldungen

Der syntaktische Aufbau [ICA01, 4-1] einer ATS-Meldung ist genau definiert. Festgelegte ATS-Meldungen [ICA07, 11-1] sind in Kategorien eingeteilt und dabei wird auf die „Flight Safety Messages“ im Folgenden näher eingegangen.

¹⁶ Air Traffic Service Messages

Die „Flight Safety Messages“ definieren Flugsicherungsmeldungen wobei ein Teil davon Flugbewegungsmeldungen darstellen, die alle Flugpläne und dazu assoziierte Flugplanänderungsmeldungen, wie Start- und Landemeldungen, definieren [ICA07, 11-1].

Wesentliche Elemente jeder ATS-Meldungen sind im Meldungsbeginn definiert und diese sind für die weitere Behandlung wesentlich:

- Vorrangvermerk, der die priorisierte Abarbeitung und Weiterleitung der Meldung festlegt.
- Adressierung, die den Empfänger der Meldung festlegt und somit für die Weiterleitung relevant ist.

Als Beispiel für einen ATS-Flugplan wird eine Form [ICA07, A2-15] angeführt:

FLIGHT PLAN PLAN DE VOL					
PRIORITY Priorité		ADDRESSEE(S) Destinataire(s)			
FF		EHAA ZQZX EBURZQZX EDDYZQZX LFFFZQZX LFRR ZQZX LFBBZQZX LECMZQZX LPFCZQZX			
FILING TIME Heure de dépôt		ORIGINATOR Expéditeur			
190836		EHAA MZPX			
SPECIFIC IDENTIFICATION OF ADDRESSEE(S) AND/OR ORIGINATOR Identification précise du(des) destinataire(s) et/ou de l'expéditeur					
3 MESSAGE TYPE Type de message		7 AIRCRAFT IDENTIFICATION Identification de l'aéronef		8 FLIGHT RULES Règles de vol	
(FPL)		ACF402		I	
9 NUMBER Nombre		TYPE OF AIRCRAFT Type d'aéronef		10 EQUIPMENT Équipement	
1		EA30		S/C	
13 DEPARTURE AERODROME Aérodrome de départ		TIME Heure		WAKE TURBULENCE CAT Cat. de turbulence de sillage	
EHAA		0940		H	
15 CRUISING SPEED Vitesse croisière		LEVEL Niveau		ROUTE Route	
K0830		F290		LEK2B LEK UA6 XMM/M078 F330 UA6 PON URION CHW UA5 NTS DCT 4611N00412W DCT STG UA5 FTM FATIM1A	
16 DESTINATION AERODROME Aérodrome de destination		TOTAL EET Durée totale estimée		ALTN AERODROME Aérodrome de déviation	
LPPT		0230		LPPR	
18 OTHER INFORMATION Renseignements divers		2ND ALTN AERODROME 2 ^e aérodrome de déviation			
REG/FBVG SEL/EJFL EET/LPPC0158					

Abbildung 1: Flightplan

Mit der Versendung einer ATS-Meldung im AFTN wird diese in ein syntaktisch festgelegtes Meldungsformat¹⁷ gebracht und an den vorgesehenen Empfänger übermittelt.

2.2.2 AMHS-Message Handling Service

Zur Gewährleistung der Kompatibilität kann das oben angeführte Meldungsformat auch mit dem AMHS zwischen den ATC ausgetauscht werden.

¹⁷ Message Format International Alphabet No. 5 (IA-5)

Die Interoperabilität zwischen den Systemen AFTN / CIDIN und AMHS wird durch die im Standard [ICA01, 4-27] festgelegten Komponenten gewährleistet:

- ATS message server
- ATS message user server
- AFTN / CIDIN / AMHS gateway

Mit der Einführung neuer „Inter-Centre Communication“-Applikationen (ICC), prior für AIDC (siehe 2.1 Aeronautical Telecommunication Network (ATN)) werden auch neue Übertragungsformate eingeführt. Als ein neues Meldungsformat wird „ATS Data Exchange Presentation“ (ADEXP) - Format eingeführt. Nach diesem auf XML-basierenden¹⁸ Format werden alle ATS-Meldungen durch EUROCONTROL spezifiziert [Eur07], wobei die semantische Bedeutung der ATS-Meldungen bestehen bleibt.

¹⁸ Extensible Markup Language

Kapitel 3

Bestehende Implementierungen

3.1 AFTN

Im „Aeronautical Fixed Telecommunication System“ (AFTN) wird eine Meldungsübermittlung nach dem Prinzip „store-and-forward“ vorgesehen. Dieser Grundsatz sieht die Verpflichtung der Zwischenspeicherung der Meldungen und eine Weiterleitungsverantwortung der involvierten „Air Traffic Centre“ (ATC) vor. Diese Meldungen werden in den zeichenorientierten Meldungsformaten ITA-2 oder IA-5 [ICA01, 4-1ff] übermittelt, welche aus dem ursprünglichen Fernschreibernetzwerk [Ois01, 3-1340] übernommen wurden.

3.1.1 Limitierungen in AFTN

Folgende Einschränkungen und Limitierungen sind bei AFTN zu berücksichtigen [EUR11, 16]:

- Meldungslänge maximal 1800 Zeichen
- Eingeschränkter Zeichensatz nach ITA-2, bzw. mit Sonderzeichen nach IA-5
- Limitierung der Anzahl der Adressaten durch die max. zulässige Meldungslänge
- Keine Benachrichtigung bei Nichtzustellbarkeit einer Meldung
- Zur Feststellung der Meldungstypen ist der Inhalt der Meldung zu untersuchen
- Syntaktische Aufbereitung von Meldungen nur anhand von ASCII-Zeichen¹⁹ wie Trennzeichen „-“ (Bindestrich) oder Zeichensequenzen (druckbare oder auch Sonderzeichen wie „Carriage Return“ und „Line Feed“ (siehe 3.3 Implementierung in AFTN).

¹⁹ American Standard Code for Communication Interchange

3.2 Datenübertragung Protokollfamilie X.25

3.2.1 Entstehung

Das X.25 Protokoll ist eines der Basis Protokolle in WAN²⁰ Netzwerken und existiert seit nunmehr fast 40 Jahren [Wik122]. Seine primäre Aufgabe ist die Paket- Verteilung in den Netzwerken zu übernehmen. Entwickelt wurde es ursprünglich für die Vermittlung in herkömmlichen Telefonnetzwerken in den '70ern und stammt somit aus einer Zeit vor dem ISO OSI Reference Model. Erst im Zeitraum von 1993-1996 wurde X.25 durch die ITU-T Study Group 7 überarbeitet und am 5. Oktober 1996 mit WTSC²¹ Resolution No. 1 freigegeben [ITU96]. Das ist auch die Erklärung warum sich in diesem Protokoll Funktionalitäten finden, die im eigentlichen ISO OSI Reference Model nicht unterstützt werden.

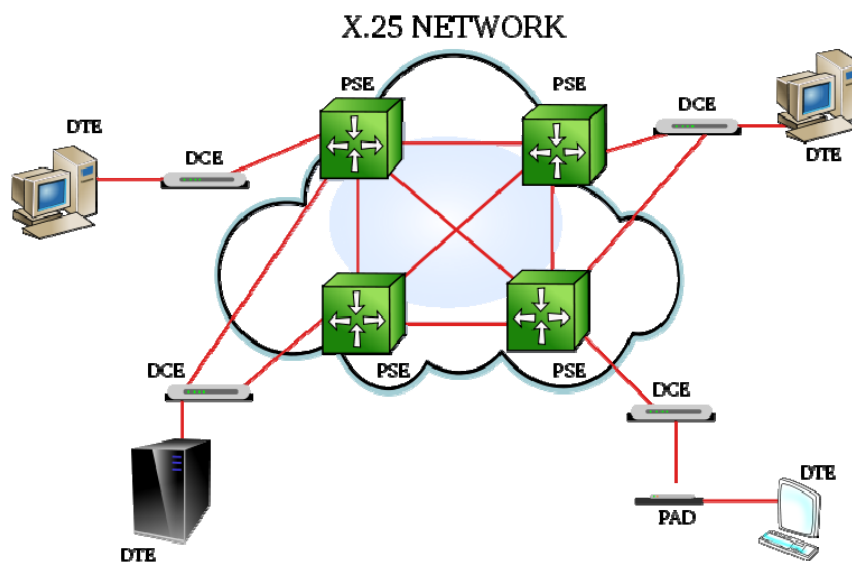


Abbildung 2: X.25 WAN²²

²⁰ Wide Area Network

²¹ The World Telecommunication Standardization Conference

²² <http://en.wikipedia.org/wiki/X.25>

3.2.2 Aufbau

Das X.25 Protokoll ist eigentlich eine Protokollfamilie bestehend aus drei voneinander unabhängigen Schichten [Ryb77][Cis12]. Diese haben wie auch das ISO OSI Reference Model eine Nummerierung. Später wurde diese aber weggelassen um Verwechslungen mit dem OSI Model zu vermeiden.

- Physical Layer (X.21)
- Data Link Layer (LAP and LAPB)
- Network Layer

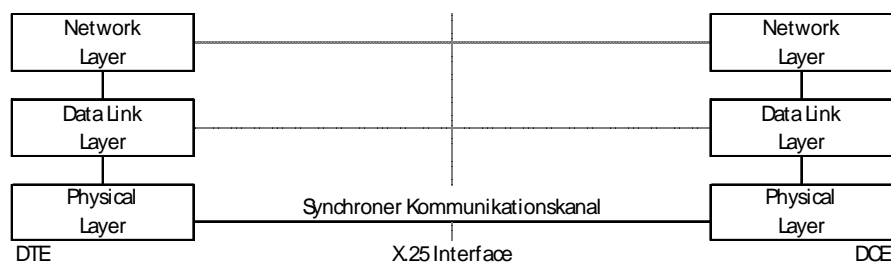


Abbildung 3: X.25 Layer

Der Physical Layer ermöglicht den Aufbau von Duplex Verbindungen zwischen den Nodes (DTE²³) per Point to Point über das Netzwerk (DCE²⁴).

Der Data Link Layer wiederum ermöglicht eine zu HDLC²⁵ kompatible Verbindung zwischen den Teilnehmern. Da die Nodes jeweils sowohl primäre als auch sekundäre Funktionen übernehmen können handelt es sich nicht um eine klassische Master-Slave Kommunikation sondern um eine Full Duplex Verbindung. Beide Teilnehmer können daher je nach Bedarf Verbindungen aufbauen und ein Pollen von Informationen ist nicht notwendig.

Der Network Layer, oft auch als Packet Layer oder Transport Layer bezeichnet, ist dafür zuständig die übermittelten Nachrichten den jeweiligen Verbindungsaufrufen zu zuordnen. Zudem spezifiziert dieser Layer das Format der Pakete für die Nachrichten, den Auf- und Abbau der Verbindung sowie für den Fehlerfall einer Übermittlung.

²³ Data terminal equipment

²⁴ Data communication equipment

²⁵ High-Level Data Link Control

3.2.3 Kommunikationstelegramme

Für das X.25 Protokoll wurden drei mögliche Telegrammarten definiert [Tan81]:

- Call Request Packet
- Control Packet
- Data Packet

3.2.3.1. Call Request packet

Um einen Virtual Circuit mit einem entfernten Terminal aufzubauen sendet der Host (DTE) ein Call Request Telegramm [Cos77].

Format ID	Group No
Logical channel	
Type (=Call Request)	1
Length 1	Length 2
Addresses	
0 0	Facilities Length
Facilities	
User Data	

Abbildung 4 Call Request packet

Die **Format ID** gibt den General Format Identifier an. Dieser definiert ob die Pakete Modulo 8 oder Modulo 128 codiert sind.

Die **Group No** steht für die Logical channel group number die für jedes Packet außer Restart- und Diagnostic- Pakete.

Das Feld **Logical channel** ist eine vom ausgehenden DTE gewählte Nummer die zur Identifikation aller weiteren zugehörigen Pakete dient.

Im Feld Packet **Type** wird wie der Name schon sagt, der Typ des Pakets angegeben und ist zum Beispiel im Falle eines Call Requests als 0000101 definiert.

Die nächsten beiden Felder **Length** geben die Länge der jeweiligen Adressen in Anzahl der Dezimalstellen (ein Überbleibsel aus der Entstehungsgeschichte) an. Dabei steht Length 1 für die Länge der Adresse des Rufenden Teilnehmers und Length 2 für die Länge des Gerufenen Nodes.

Im Bereich **Addresses** befinden sich dann die in BCD²⁶ codierten Adressen wie eben beschrieben. Die verbleibenden Stellen die sich Modulo 8 bzw. 128 ergeben werden mit „0“ aufgefüllt.

Das Feld **Facilities Length** gibt die Länge für das folgende Feld **Facilities** an, mit dessen Hilfe zum Beispiel Call Collect²⁷ initiiert werden können.

Im Feld **User Data** können bis zu einer Länge von 128 Bytes freiwählbare Informationen übertragen werden.

²⁶ Binary coded decimal

²⁷ R- Gespräch

3.2.3.2. Control packet

Format ID	Group No
Logical channel	
Type	1

Um einen Call request zu beantworten, positiv oder negativ, wird ein Control packet gesendet. Dieses baut auf dem Schema des Vorherigen auf, jedoch benötigt ein Kontroll-

Abbildung 5 Control packet

Telegramm nur die ersten drei Bytes.

Über das Feld **Type** wird die Antwort signalisiert. Diese kann wahlweise „accepted“ oder „rejected“ sein.

Um die Verbindung wieder abzubauen, wird ein Kontroll- Telegramm vom Typ „Clear Request“ gesendet. Dieses würde dann mit einem „Clear Confirmation“ Control Packet bestätigt werden.

3.2.3.3. Data packet

Q	D	0	1	Group No
Logical channel				
Next	M	Seq	0	
0 - 128 Bytes of Data				

Das Datenpaket ist wieder analog aufgebaut, abweichend sind hier nur die Felder **Next** und **Sequence**. Diese wiederum sind analog zu den entsprechenden Feldern in HDLC

Das Feld **Q**²⁸ ist vorgesehen damit der Transport Layer zwischen Daten und

Abbildung 6 Data packet

Kontroll- Telegrammen unterscheiden kann.

Das Feld **D**²⁹ gibt an ob eine Empfangsbestätigung gesendet werden soll.

Mit dem Feld **M**³⁰ wird dem Empfänger angezeigt, dass weitere Pakete folgen.

Mit Hilfe dieser Telegrammart werden natürlich noch weitere Informationen bzw. Befehle gesendet wie zum Beispiel „Restart“, „Reset“, „Diagnostic“ und die entsprechenden Antworten, „Receiver ready“, „Receiver not ready“ oder auch „Interrupt“ und andere mehr.

²⁸ Qualifier bit

²⁹ Delivery bit

³⁰ More data bit

3.2.4 Kommunikationsablauf

Widmen wir uns nun dem Ablauf der Kommunikation anhand von einigen Beispielen. Im Allgemeinen sieht das Szenario so aus, dass die Terminals (DTE) über die Anbindung zum Netzwerk (DCE) die Schnittstelle des X.25 basierenden Netzwerks nutzen [Ryb77].

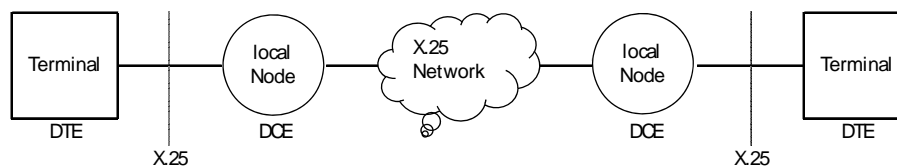


Abbildung 7: Schema der Netzstruktur

Um nun beispielsweise eine Verbindung aufzubauen ist folgender Ablauf notwendig.

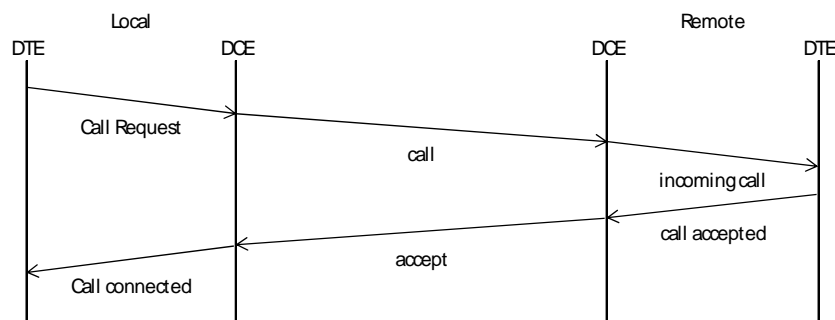


Abbildung 8: Call Request

Um die Verbindung wieder zu trennen, wird ein ähnlicher Prozess durchgeführt

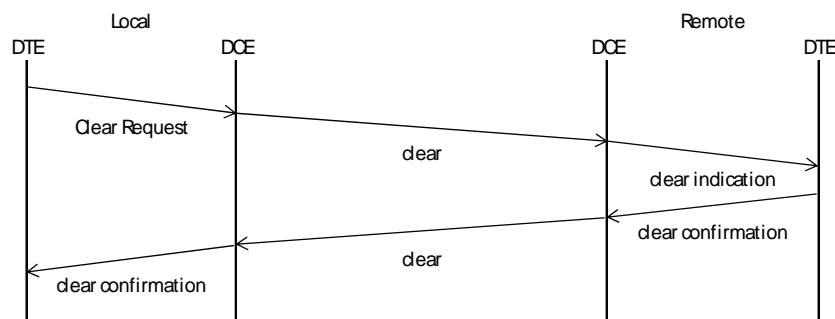


Abbildung 9: Clear Request

Abschließend sei unter den vielen verbleibenden Prozessen nur noch der Ablauf für die Datenübertragung erwähnt.

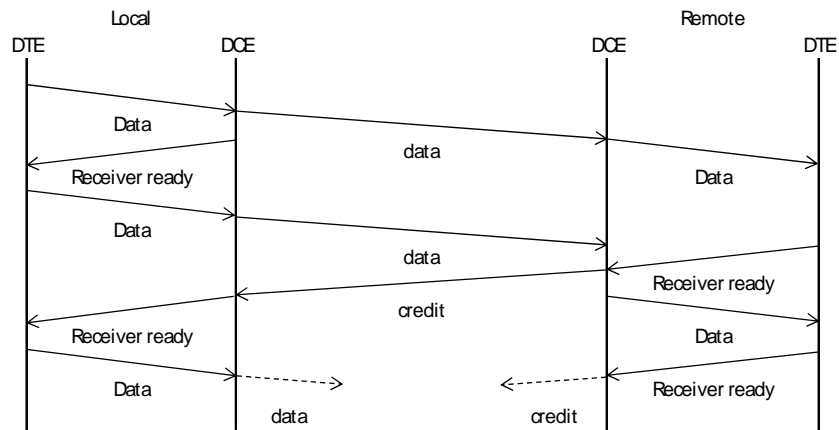


Abbildung 10: Data Transfer

Was sich aber hieraus leicht ersehen lässt, ist das dieses Protokoll nicht flexibel ist. Die einzelnen Telegramme sind bit-weise spezifiziert genauso wie auch der Ablauf der Kommunikation genau definiert ist. Abweichungen davon wären nicht bzw. nur in isolierten Anwendungen möglich.

3.3 Implementierung in AFTN

Der Standard [ICA01, 4-1ff] schreibt eine Übertragung der Daten in den Meldungsformaten ITA-2 oder IA-5 vor. Der Unterschied in diesen Formaten liegt im Wesentlichen in der Zulässigkeit von zusätzlichen Steuerzeichen in IA-5. Diese Zeichen dienen der vereinfachten programmtechnischen Handhabung. So wird beispielsweise dem Meldungskopf das ASCII-Zeichen³¹ <SOH>³² vorangestellt und vor Meldungsinhalt das ASCII-Zeichen <STX>³³ eingefügt. Im Format ITA-2 waren dagegen nur mit dem Fernschreiber erzeugbare Zeichen wie die ASCII-Zeichen <CR>³⁴ und <LF>³⁵ zulässig.

Wird eine ATS-Meldung via AFTN übertragen, so besteht diese aus den Teilen:

- Kanalbezeichnung und Laufnummer der Meldung
- Kopf mit Prioritätsvermerk, Adressaten und dem Absendezeitpunkt, sowie der Absenderkennung
- Eigentlicher Meldungsinhalt mit Kennung der Type der ATS-Meldung.

3.3.1 Kanalbezeichnung und Laufnummer einer ATS-Meldung

Die Kanalbezeichnung stellt die dezidierte Verbindung zwischen den beiden Bodenstationen dar. In Verbindung mit der Laufnummer (Sender erhöht diese mit jeder weiteren Meldung um eins) kann jede einzelne Meldung identifiziert werden. Werden Meldungen nicht empfangen, können dies durch ein durch organisatorische Eingriffe (meist manuell), neu angefordert werden.

3.3.2 Adressierung einer ATS-Meldung

Im Meldungskopf einer Meldung ist unter Anderem der Adressat enthalten. Nach dem Vorrangvermerk sind eindeutige Adressen deren semantische Bedeutung normiert [ICA102] ist, mit jeweils acht Buchstaben anzubringen.

³¹ American Standard Code for Communication Interchange, 7-bit Zeichencode

³² Start-of-Header, Dezimal 01

³³ Start-of-Text, Dezimal 02

³⁴ Carriage Return, Dezimal 13

³⁵ Line Feed, Dezimal 10

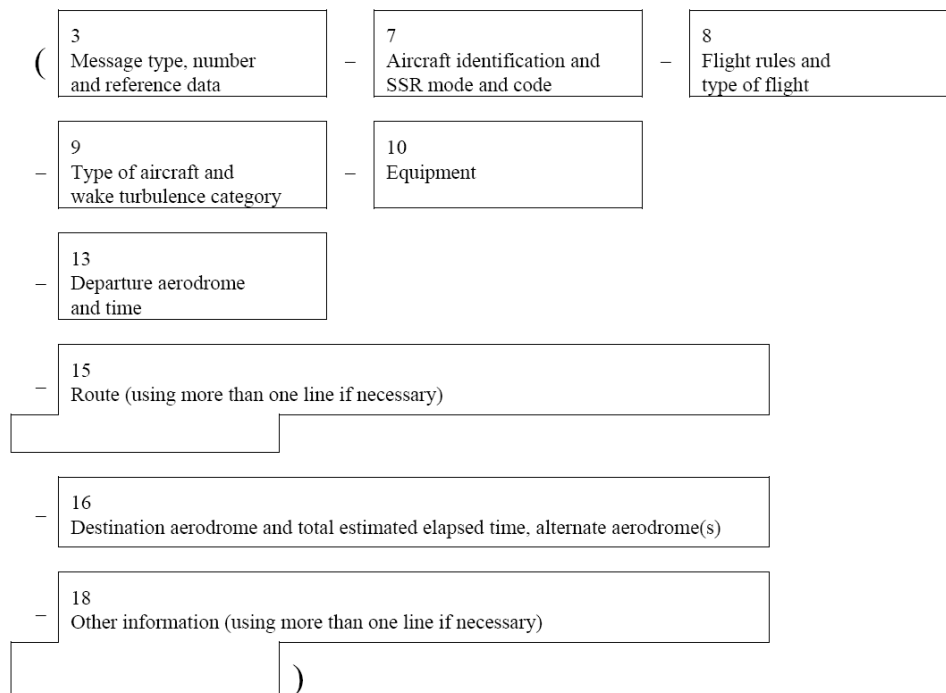
Eine Erklärung am Beispiel eine Empfängeradresse LGATZTZX [ICA01, 4-10]:

L	Regionscode	Südeuropa
G	Länderkennung	Griechenland
AT	Flughafen	Athen
ZTZX	Kontrollturm	

Wird beispielsweise eine „Air Traffic Service“ (ATS)-Meldung in Österreich erstellt, so bestehen für die zwischen Österreich und Griechenland liegenden ATC die oben angeführten „store-and-forward“-Prinzipien.

3.3.3 ATS-Flugplan

Der Meldungsinhalt ist in Syntax und Semantik definiert [ICA07, A3-35], wobei im Folgenden Beispielhaft die Struktur des Meldungsinhalts eines Flugplanes dargestellt wird:



Beispiel:

(FPL-TPR101-IS
-B707M-CHOPV/CD
-EGLL1400
-N0450F310 G1 UG1 STU285036/M082F310 UG1 52N015W
52N020W 52N030W 50N040W 49N050W
-CYQX0455 CYR
-EET/EISN0026 EGGX0111 20W0136 CZQX0228 40W0330
50W0415)

Bedeutung:

Filed flight plan message — aircraft identification TPR101 — IFR, scheduled flight — a Boeing 707, medium wake turbulence category equipped with Loran C, HF RTF, VOR, Doppler, VHF RTF and SSR transponder with Modes A (4 096 code capability) and C — ADS capability — departure aerodrome is London, estimated off-block time 1400 UTC — cruising speed and requested flight level for the first portion of the route are 450 knots and FL 310 — the flight will proceed on Airways Green 1 and Upper Green 1 to a point bearing 285 degrees magnetic and 36 NM from the Strumble VOR. From this point the flight will fly at a constant Mach number of .82, proceeding on Upper Green 1 to 52N15W; then to 52N20W; to 52N30W; to 50N40W; to 49N50W; to destination Gander, total estimated elapsed time 4 hours and 55 minutes — alternate is Goose Bay — captain has notified accumulated estimated elapsed times at significant points along the route, they are at the Shannon FIR boundary 26 minutes, at the Shanwick Oceanic FIR boundary 1 hour and 11 minutes, at 20W 1 hour and 36 minutes, at the Gander Oceanic FIR boundary 2 hours and 28 minutes, at 40W 3 hours and 30 minutes and at 50W 4 hours and 15 minutes. [ICA07, A3-36]

Kapitel 4

Ziel - Systeme und Protokolle

4.1 AMHS

Betrachtet man die aktuell standardisierten Implementierungen nach ICAO und EUROCONTROL, so ist das „Aeronautical Message Handling System“ AMHS zur Kommunikation im ATN als Nachfolger für das standardisierte AFTN definiert.

Ishibashi [Ish05, 1.D.1-2] beschreibt, dass ATN mit MHS³⁶ durch ICAO festgelegt wurde. Dieser Standard basiert auf der X.400 Netzwerkprotokollfamilie, die wiederum mehrere Protokollausprägungen standardisiert. Die funktionellen Komponenten für den Datenaustausch zwischen Endsystemen im ATN sind wie folgt definiert:

- MTA Message Transfer Agent
- UA User Agent
- MS Message Store

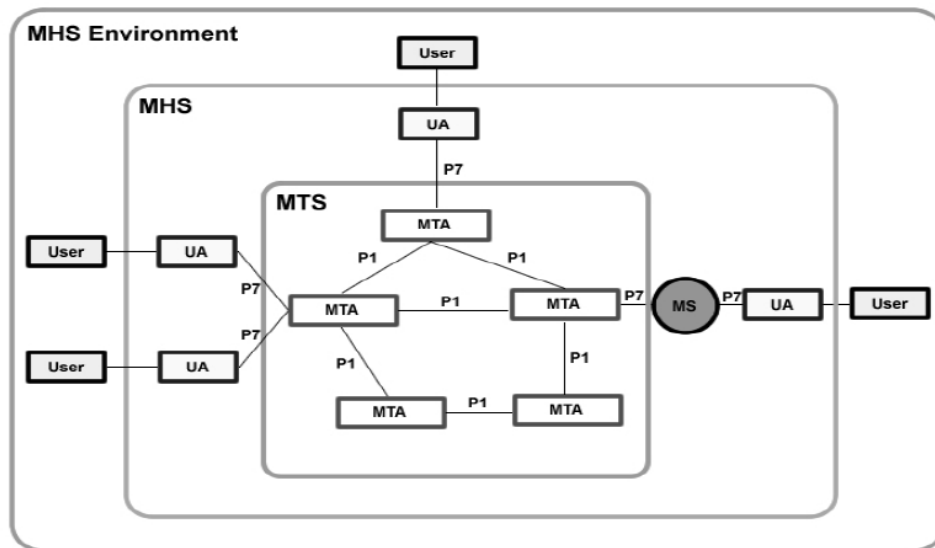


Abbildung 11: Funktionale Übersicht MHS [Ish05, 1.D.1-3]

³⁶ Message Handling System nach ISO

MTA dient dabei als „Message Switch“ und hat die Aufgabe Meldungen entsprechend der Adressierung weiterzuleiten. UA stellt das „User Interface“ zur Verfügung und verarbeitet die Meldungen, die vom MTA kommen. MS dient zur Zwischenspeicherung der Meldungen zwischen MTA und UA.

In der Abbildung 11 stellt *Ishibashi* funktionale Übersicht des MHS und die verwendeten Protokollausprägungen dar. P1-Protokoll dient als Routing-Protokoll zum Meldungs austausch zwischen den MTA, um eine Weiterleitung der Meldung ohne Öffnen des Meldungsinhaltes zu ermöglichen. Das P7-Protokoll dient zur syntaktisch und semantisch richtigen Verarbeitung der Meldungen zwischen UA und MTA.

4.2 Anforderungen an AMHS

Die mit der Implementierung zu berücksichtigenden Anforderungen werden in zwei signifikante Gruppen geteilt und sind durch ICAO [EUR11, 17ff] genau festgelegt:

- Basic Requirements Anforderungen müssen durch alle AMHS Implementierung bereitgestellt werden
 - Sicherstellung der Interoperabilität zu AFTN (Abwärtskompatibilität)
 - Die Meldungslänge darf nicht beschränkt werden.
 - Keine Limitierung der Anzahl der Empfänger
 - Automatisierte Übermittlung von Nicht-Zustellungsmeldungen
- Functional Groups Anforderungen, die auf Grund der prozeduralen betrieblichen Abläufe oder auch durch Besonderheiten unterschiedlich implementiert sein können. Als Beispiele werden angeführt:
 - Implementierung von IPv4 oder IPv6
 - Anforderungen an die IT-Security wie Authentifizierungs- oder Autorisierungsmechanismen

4.3 AMHS over TCP/IP

Nach der Definition des ISO/OSI-Schichtenmodells ist AMHS am „Application Layer“ anzusiedeln.

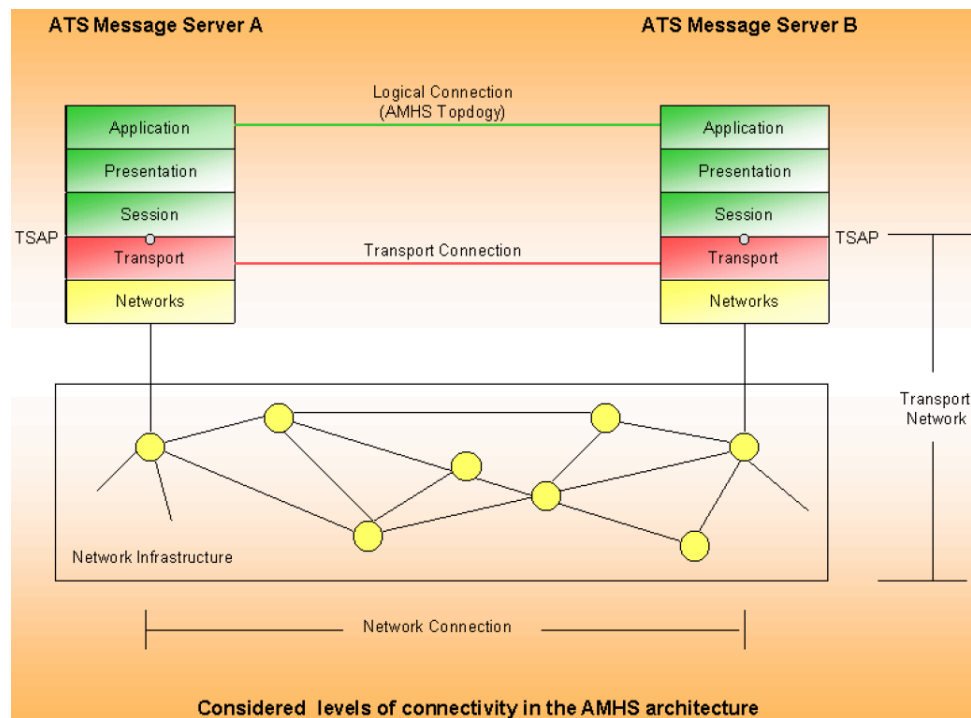


Abbildung 12: Netzwerk-Layer mit AMHS [EUR11, 50]

In dieser Abbildung sieht AMHS eine logische Trennung der Netzwerk und Applikations-Schichten vor:

- Eine Anbindung der Netzwerke über TCP/IP ermöglicht auch die Anbindung an Netze, welche nur AFTN vorsehen.
- Die Verbindungen zwischen den ATC können unabhängig von der Implementierung von AMHS bestehen bleiben.

4.3.1 Meldungszustellung in AMHS

Die Adressierung von Meldungen in AMHS erfolgt mit Hilfe eines eigens festgelegten und in der ICAO EUR-Region [EUR11, 26] verwalteten „AMHS Addressing Plan“.

In diese Datenbank werden jene Adressen aufgenommen, die den Umstieg von AFTN auf AMHS tätigen. Ab diesem Zeitpunkt erfolgt die Zustellung als AMHS-Meldung. Eine Konvertierung einer zuzustellenden AFTN-Meldung erfolgt automatisiert auf Basis des definierten „XF-Addressing Scheme“.

Beispiel einer XF AMHS Address für Southampton Tower

C/=XX/A=ICAO/P=EG/O=AFTN/OU1=EGHIZTZ³⁷

³⁷ C..Country-Name, A..Admin Domain, P..Private Domain, O..Organisation, OU1..Unit

4.4 Protokollfamilie X.400

4.4.1 Entstehung

Auch das X.400³⁸ Protokoll ist schon seit längerem ein fester Bestandteil der Kommunikationsprotokolle. Bereits 1984 wurden die ersten Dokumente dazu publiziert, die derzeit aktuelle Version wurde im Juni 1999 veröffentlicht [Wik123]. Die Grundidee war für die Kommunikation das ISO OSI Schichtenmodell als Basis zu nutzen. Ursprünglich sollte es als Email Protokoll verwendet werden, wurde aber durch das SMTP³⁹ Protokoll [pos82] verdrängt und spielt heute nur noch eine Rolle im militärischen Bereich sowie in der Luftfahrt. Grund dafür sind die in X.400 vorgesehenen Sicherheits- und Integritäts- Features.

4.4.2 Aufbau

Der Aufbau des X.400 Protokolls basiert auf dem ISO OSI Schichtenmodell. Protokollbezogen gibt es jedoch 2 weitere Layer [Kil85]. Diese sind der Message Transfer Layer und der Inter Personal Messaging Layer. Je nach Betriebsart unterscheidet sich die daraus resultierende Protokollstruktur wie folgt [Duc92].

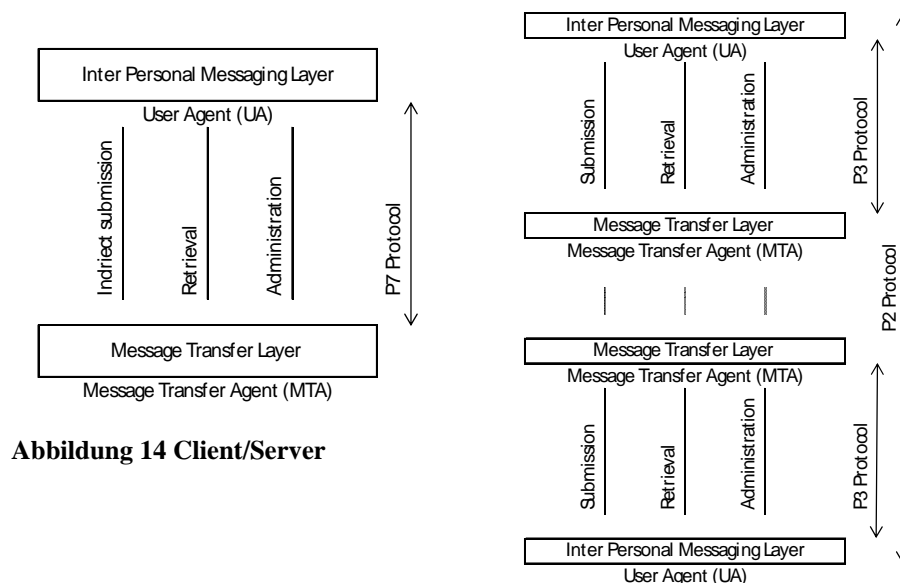


Abbildung 14 Client/Server

Abbildung 13 Peer-to-Peer

³⁸ ITU-T Non-Telephone Telecommunication Services. F.400/X.400 (1999)

³⁹ Simple Mail Transfer Protocol, RFC821

Jedem User Agent (UA) wird eine global eindeutige ID zugeordnet. Ein Originator/Recipient Name wird auch den Message Transfer Agents (MTA) zugewiesen [Kil85].

Je nach Struktur werden diese Schichten durch Management Domains (MD) zur Verfügung gestellt. Diese werden im Protokoll als Organisation Unit bezeichnet. Des Weiteren gibt es im Protokoll auch noch die sogenannte Billing Authority um gegebenenfalls Leistungen abrechnen zu können.

Die Ziele dieser beiden Betriebsarten sind:

- Einheitliche Struktur bei der Nachrichten Speicherung
- Einheitliche Struktur beim Versenden einer Nachricht
- Direkte Anwendbarkeit bei allen X.400 Systemen
- Flexibilität bei der Auswahl der Betriebsart des Protokolls
- Vollständigkeit der Elemente im Protokoll

Für die Sicherheit sind folgende Voraussetzungen definiert:

- Die Kontrolle zur vertrauenswürdigen Kommunikation ist in der MTA Schicht zu implementiert, da die Message Transfer Agent's vertrauenswürdige Entitäten sind, die User Agent's nicht.
- Die Verbindungen zwischen den MTA's müssen gesichert sein und den aufrufenden MTA korrekt identifizieren.
- Die Autorisation muss für jeden Bereich der UA/MTA implementiert werden.

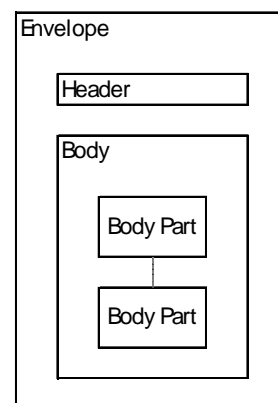
Die Autorisation muss für jede Management Domain implementiert werden.

4.4.3 Kommunikationstelegramme

Aufgrund der einheitlichen Struktur beider Betriebsarten muss im Folgenden nicht weiter unterschieden werden wie die Struktur der Nachrichten aufgebaut ist.

Die Nachrichten sind so aufgebaut, dass sie durch ein Envelope adressiert werden und die eigentliche Nachricht kapseln [ITU99][ITU991].

Die Nachricht wiederum hat einen Header gefolgt von einem Message-Body, der wiederum aus mehreren Teilnachrichten bestehen kann (Body Parts). Diese Nachrichten Teile können von unterschiedlicher Art sein, wie beispielsweise Textnachrichten und Files.



**Abbildung 15 X.400
Nachrichten Struktur**

Für die Adressierung sind spezielle Tags definiert die angefangen bei den Adressaten bis hin zur Organisation alle notwendigen Informationen kennzeichnen [Har92].

4.4.3.1. Directory names (DL)

Jeder Benutzer eines Message Handling Systems (MHS) kann über einen Namen identifiziert werden. Dieser Directoryname muss in einem Verzeichnis eingetragen sein und ermöglicht so den entsprechenden OR-name zu finden.

4.4.3.2. Originator/Recipient names (OR-names)

Jeder Benutzer eines MHS oder eines DL hat einen oder auch mehrere OR-names. Über diesen OR Namen findet sich die dazugehörige OR Adresse.

Wird für den angegebenen OR Namen keine OR Adresse gefunden wird die im Envelope angegebene Adresse verwendet.

4.4.3.3. Originator/Recipient addresses (OR-addresses)

Die OR Adresse ermöglicht es dem MHS die Nachricht an genau den User zuzustellen für den sie bestimmt ist. Diese OR-adresse besteht aus mehreren Attributen die das exakte Ziel spezifizieren.

4.4.4 Kommunikationsablauf

Eine Nachricht wird vom User mittels UA an den ursprünglichen MTA weiter gereicht und wird solange an den nächsten MTA weitergeleitet bis sie beim MTA des Adressaten angelangt ist, dort kann sie der Empfänger mittels seines UA abrufen.

Dabei werden vom System sowohl Zustellbestätigungen (wenn vom Absender gewünscht) als auch Fehlermeldungen (z.B. Zustellung nicht möglich) an den Absender zurück gemeldet.

Je nach Betriebsart übernehmen verschiedene Protokolle den Transfer der Nachrichten. So ist zwischen den MTA Schichten das P1-Protokoll, zwischen UA und MTA im Peer 2 Peer Mode das P3-Protokoll, zwischen UA und UA das P2-Protokoll und zwischen UA und MTA im Client/Server Mode das P7-Protokoll zuständig.

Diese Protokolle bieten die Grundfunktionen:

- MTA-bind
- MTA-unbind
- Message-transfer
- Probe-transfer
- Report-transfer

Mit Hilfe dieser Grundfunktionen kann die Verbindung zur jeweiligen Gegenstelle aufgebaut werden, um dann entsprechend des Bedarfs die Daten zu übertragen. Wenn die Übertragung beendet ist und keine weiteren Übertragungen anstehen kann die Verbindung dann abgebaut werden.

4.5 Funktionalitätserweiterung durch AMHS

Ishibashi [Ish05, 1.D.1-3] beschreibt funktionelle Erweiterungen im AMHS. Voraussetzung jeder Implementierung ist jedoch die Erfüllung der „Basic Requirements“ wie in 4.2 Anforderungen an AMHS beschrieben.

Funktionalitätserweiterungen sind demnach in jeder Implementierung zulässig. Hierbei soll in der EU hinsichtlich der „IT-Security“ [BKA07, 15] der technische Standard wie ihn EUROCONTROL [Eur09, Anx D, D-6] fordert, erreicht werden.

4.5.1 IT-Security

In Zusammenhang mit AMHS erfolgt ein Ausblick zur Integration folgender „Features“:

- **Public-Key-Infrastructure** Ein modernes Schlüsselmanagement wird durch die Integration einer „Public Key Infrastructure“ auf Basis von X.509 Zertifikaten [ICA02, 8.4.3] ermöglicht. Diese Forderung wird von EUROCONTROL [Eur09, 43ff] definiert und in ihrer Organisation festgelegt.
- **Kryptografische Verschlüsselungsfunktionen** ATN Security [ICA02] empfiehlt die Implementierung eines „Elliptic Curve Cryptosystems“ (ECC) in Verbindung mit ATN- „Public Key“-Algorithmen.
- **Hashfunktionen und Signaturen** ATN Security empfiehlt die Verwendung von digitalen Signaturen aus der nach NIST⁴⁰ definierten SHA-2⁴¹ Familie als „Secure Hash Standard“.

⁴⁰ American National Institute of Standards and Technology, 1993

⁴¹ Spezifikation durch NIST mit FIPS 180-3, 2007

Kapitel 5

Schlusswort

5.1 Fazit

Die Erfüllung der vorgegebenen Standards stellt die Interoperabilität der dem weltweiten Luftverkehr zu Grunde liegenden „Air Traffic Service“ Meldungen sicher. Neben den Datenkommunikationsstandards sind auch die organisatorischen und administrativen Abläufe durch Organisationen wie ICAO bzw. EUROCONTROL normiert.

Das primäre Ziel mit der Einführung des „*Aeronautical Telecommunication Network*“ (ATN) ist die Sicherstellung der Rückwärtskompatibilität zu AFTN, welche durch Einhaltung der Vorgaben für die „Transitionphase“ (siehe 2.1.3 Übergangsphase) gewährleistet wird.

Auf Grund der weitgehenden Anlehnung an Industriestandards wird eine langfristige technische Unterstützungs- bzw. Versorgungssicherheit gewährleistet.

Zur Sicherstellung der Verfügbarkeit sind neben den technischen Gegebenheiten auch die implementierten prozeduralen und administrativen Abläufe zu prüfen, um auch Alternativen der Kommunikation zur Verfügung zu haben.

Bei der Umstellung von AFTN auf das Zielsystem AHMS als Basis des ATN sind folgende Basiserfordernisse wie sie durch *Smith* [Smi01, 7.A.6-2] festgelegt wurden, erfüllt:

- Bestehende Infrastruktur insbesondere der Netzwerkinfrastruktur bleibt weiterhin verwendbar.
- Eine Hochverfügbarkeit auf Netzwerkebene durch redundante Verbindungen auf Basis X.400 sichergestellt.
- Eine Priorisierung der Meldungübermittlung kann auf Basis von X.400 festgelegt werden.
- Die Meldungszustellung ist nicht mehr von Leitungsverbindungen und Personen abhängig, sondern durch „Policy basiertes Routing“ bestimmt.
- Die Verwendung von COTS-Hardware sowie eingeführter Netzwerktechnologie ist jederzeit möglich.

5.2 Empfehlungen und Ausblick

Im Rahmen der funktionalen Erweiterungen sind für AMHS die Vorgaben zur Sicherstellung der IT-Sicherheit durch EURCONTROL definiert und werden eindringlich empfohlen.

Diese Erweiterungen sollen auf Basis technischer Sicherheitsmaßnahmen wie Authentifizierung, Verschlüsselung, Schlüsselspeicherung, u.a. implementiert werden, um die primären Sicherheitsziele Vertraulichkeit, Integrität, Verfügbarkeit [Pfl07, 10] zu gewährleisten.

Die Integration und Überprüfung digitaler Signaturen, der Schlüsselverteilung sowie weiterer Mechanismen, sind über eine zumindest europaweite „Public-Key Infrastructure“ bereit zu stellen und das notwendige organisatorische und technische Umfeld zu definieren. Dadurch werden zusätzliche Sicherheitsziele wie Zurechenbarkeit, Authentizität und Zuverlässigkeit [BKA07, 57] erreicht.

Die Vorgabe der europäischen Kommission, die Planung eines weitgehend vereinheitlichten europäischen Luftraumes aufzunehmen, wird durch die Implementierung des „*Aeronautical Telecommunication Network*“ zumindest auf technischer und operationeller Ebene unterstützt.

Literatur

- [Ois01] Oishi Roy T., *Future Applications and the Aeronautical Telecommunication Network*, Aerospace Conference, ⁰³2001, IEEE Xplore.org, Conference publications, <http://ieeexplore.org/arnumber=931364>, Zugriff vom 18.03.2011
- [Ish05] Ishibashi R, Anzaloni A., *An Agent Development Framework for data exchange at ATN Environment*, Digital Avionics Systems Conference, ¹⁰2005, DASC 2005 The 24th, Print ISBN: 0-7803-9307-4, IEEE Xplore.org, Conference publications, <http://ieeexplore.org/arnumber=01563306>, Zugriff vom 18.03.2011
- [Smi01] Smith Phil, *IPSKY: IPV6 for the Aeronautical Telecommunications Network*, Digital Avionics Systems Conference, ¹⁰2001. DASC 20th Conference, IEEE Xplore.org, Conference publications, <http://ieeexplore.org/arnumber=964186>, Zugriff vom 18.03.2011
- [ICA01] ICAO Annex 10 Volume II, *Aeronautical Telecommunication – Communication Procedures*, International Standards, Recommended Practices and Procedures for Air Navigation Services, Ed. 6.0, July 2001, + Amendments 78-86 applicable on 17.11.2011
- [ICA02] ICAO Doc. 9705-AN/956 – *Manual of Technical Provisions for the Aeronautical Telecommunications Network (ATN)*, Third Edition (2002), Sub- Volume VIII – ATN Security
- [ICA07] ICAO Doc 4444-ATM/501, *Air Traffic Management*, Procedures for Air Navigation Services, Fifteenth Edition, 22 Nov 2007, ICAO
- [ICA10] ICAO Doc 9880-AN/466, *Manual on detailed Technical Specification for the Aeronautical Telecommunication Network (ATN) using ISO/OSI Standards and Protocols*, Ed. 1.0 - 2010, Approved by ICAO Secretary General
- [ICA101] ICAO Doc 9896-AN/469, *Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocols Suite (IPS) Standards and Protocols*, Ed. 1.0 - 2010, Approved by ICAO Secretary General

- [ICA102] ICAO Doc 7910/138 – *Location Indicators*, Edition 138, Dec 2010, Approved by ICAO Secretary General
- [EUR11] EUR Doc 020, *EUR AMHS Manual*, ICAO Regional Manual, Version 6.0, 14.04.2011, Author: AFSG Planning Group, download http://icao.paris.int/documents_open, Zugriff 08.05.2012
- [EUR111] EUR Doc 021, *ATS Messaging Management Manual*, ICAO Regional Manual, Version 6.0, 14.04.2011, Author: AFSG Planning Group, download http://icao.paris.int/documents_open, Zugriff 08.05.2012
- [EUR12] EUR Doc 020 App D, *EUR AMHS Manual Appendix D*, ICAO Regional Manual, Version 7.0, 26.04.2012, Author: AFSG Planning Group, download http://icao.paris.int/documents_open, Zugriff 08.05.2012
- [Eur07] Eurocontrol Specification-0107, *Eurocontrol Specification for ATS Data Exchange Presentation (ADEXP)*, Released Ed. 3.0, Date 20.10.2007
- [Eur09] Eurocontrol Specification-0136, *Eurocontrol Specification on the Air Traffic Service Message Handling System (AMHS)*, Released Ed. 2.0, Date 18.09.2009
- [BKA07] ÖSiHB, „*Österreichisches Informationssicherheits-Handbuch*“, 2007, Verlag: Österreichische Computer Gesellschaft, Band 226
- [Pfl07] Charles P. Pfleeger Shari Lawrence Pfleeger, „*Security in Computing*“, Fourth Edition, 2007, Verlag Pearson Prentice Hall, ISBN: 0-13-239077-9
- [Ryb77] Rybczynski, A, *Datapac X.25 service characteristics*. In : Proceedings of the fifth symposium on Data communications SIGCOMM '77. ACM, New York, NY, USA (1977)
- [Tan81] Tanenbaum, A.: Network Protocols. ACM Comput. Surv. 13(4), 453-489 (1981)
- [Cos77] Cosell, B.: X.25 link access procedure. SIGCOMM Comput. Commun. Rev, 7(4), 15-35 (1977)
- [ITU96] ITU-T Telecommunication Standardization Sector of ITU: Series X: Data Networks and Open System Communication. Technical Report X.25, ITU-T, Genf (1996)

- [ITU99] ITU-T Telecommunication Standardization Sector of ITU: Series F: Series F: Non-Telephone Telecommunication Services. Technical Report F.400/X.400, ITU-T, Genf (1999)
- [ITU991] ITU-T Telecommunication Standardization Sector of ITU: Series X: Data Networks and Open System Communication. Technical Report X.419, ITU-T, Genf (1999)
- [Kil85] Kille, S.: A model of message flow control. SIGCOMM Comput. Commun. Rev. 15(5), 40-49 (1985)
- [Duc92] Duchien, L.: X.400-based distributed application design methodology. In : Proceedings of the 1992 ACM annual conference on Communications CSC '92. ACM, New York, NY, USA (1992)
- [Har92] Hardcastle-Kille, S.: Mapping between X.400(1988) / ISO 10021 and RFC 822. RFC 1327, University College London, London (1992)
- [Pos82] Postel, J.: SIMPLE MAIL TRANSFER PROTOCOL. RFC 821, University of Southern California (1982)
- [Cis12] Cisco Systems, Inc., „Cisco DocWiki,“ [Online]. Available: <http://docwiki.cisco.com/wiki/X.25>. [Zugriff 04 2012].
- [Wik123] Wikimedia Foundation, Inc., „X.400 “ [Online]. Available: <http://en.wikipedia.org/wiki/X.400>. [Zugriff 04 2012].
- [Wik122] Wikimedia Foundation, Inc., „X.25 “ [Online]. Available: <http://en.wikipedia.org/wiki/X.25>. [Zugriff 04 2012].

Abbildungsverzeichnis

Abbildung 1: Flightplan	7
Abbildung 2: X.25 WAN	10
Abbildung 3: X.25 Layer	11
Abbildung 4 Call Request packet	1
Abbildung 5 Control packet	1
Abbildung 6 Data packet	1
Abbildung 7: Schema der Netzstruktur	14
Abbildung 8: Call Request	14
Abbildung 9: Clear Request	14
Abbildung 10: Data Transfer	15
Abbildung 11: Funktionale Übersicht MHS	19
Abbildung 12: Netzwerk-Layer mit AMHS	21
Abbildung 13 Peer -to-Peer	1
Abbildung 14 Client/Server	22
Abbildung 15 X.400 Nachrichten Struktur	1

Erfolgt bei der Beschriftung einer Abbildung keine Quellenangabe, so ist der Autor dieses Dokuments zugleich der Urheber der Abbildung.