ATNP/WG3/WP **17-18**

20 September 1999

AERONAUTICAL TELECOMMUNICATION NETWORK PANEL

WORKING GROUP 3 (APPLICATIONS AND UPPER LAYERS)

Gran Canaria, Spain, 28 September - 1 October 1999

Agenda Item 6.4: ULCS Post Package 1 work

Draft Validation Report for ATN ULCS Enhancements

Prepared by: Tony Kerr

Presented by: Steve Van Trees

SUMMARY

This is a draft of the Validation Report for ATNP/3 relating to the draft enhancements to the Technical provisions for the ATN Upper Layer Communications Service (ULCS).

This report presents the results of the validation and implementation programmes that have been undertaken by various States and Organisations, which apply to the ULCS Enhancements. It summarises the ULCS-related results and analyses them against a set of high-level validation objectives (VOs). It is concluded that the enhanced technical provisions will be sufficiently validated for inclusion in ICAO Doc. 9705, with the possible exception of the Secure Dialogue Service.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Scope

Since the publication of the first edition of the Manual of Technical Provisions for the Aeronautical Telecommunication Network (ATN) (ICAO Doc. 9705), a number of enhancements to Sub-Volume 4 of that document, the ATN Upper Layer Communications Service (ULCS), have been progressed within ATNP/WG3. The effect of the enhancements in question is to add new functionality, and hence new technical provisions, which need to be validated before they can be published.

This is the draft ATNP/3 Validation Report for various enhancements that have been made to the ATN Upper Layer Communications Service (ULCS) by ATNP/WG3/SG3. This report presents the results of the validation and implementation programmes that have been undertaken by various States and Organisations, which apply to the ULCS Enhancements. It summarises the ULCS-related results and analyses them against a set of high-level validation objectives (VOs).

The enhancements that are the subject of this report can be summarised as:

1. Upper Layer Naming and Addressing extensions, affecting chapters 4.2.2, 4.3.2 and 4.3.3 of Sub-Volume 4,
2. The addition of the Connectionless Dialogue Service (CLDS) as chapter 4.7,
3. The addition of the Secure Dialogue Service as chapter 4.8, with consequential changes to chapters 4.1, 4.3.3 and 4.6, and
4. The addition of the Generic ATN Communication Service (GACS) as chapter 4.9.

The enhancements have been designed for backwards compatibility and interoperability with the first edition of Doc 9705, and this compatibility also needs to be validated.

1.2 Background

Each of the areas of enhancement has been progressed separately by WG3/SG3. This section summarises the history of their development and provides traceability between different evolutions of the enhancements.

1.2.1 Development of Naming and Addressing Enhancements

The ongoing development of ATN application concepts and the progress of implementation programmes have highlighted a number of restrictions in the upper layer naming and addressing published in the first edition of Doc 9705, which may cause problems in future ATN applications and implementation architectures.

These were documented in ATNP/CCB PDR 97120001, which was Forwarded by the ATNP CCB to WG3 and thence to SG3 for resolution. WG3/SG3 considered these problems at its meeting in Bracknell in April 1998, and arrived at the proposed solutions documented in WG3/WP13-11, which were presented to ATNP/WG3 at its Utrecht meeting in June - July 1998.

Following constructive comments from WG3, and further discussions in WG3/SG3 at its meeting in Toulouse in September 1998, the concepts were refined and presented to WG3 at its Bordeaux meeting in June - July 1998.

To summarise, the following issues are resolved in the proposed revision of the ATN technical provisions:

a) ATN naming and addressing to handle multiple instances of the same application type at a given location. (Requirement source: ATNP systems management, IATA verbal inputs).

b) ATN upper layers to handle AET names from name spaces other than the ICAO naming tree. (Requirement source: ATNP systems management, observation that not all ATN systems are located at ICAO-designated facilities).

It is required that the solution be backwards compatible with the first edition of ICAO Doc. 9705.

The recent change history of the UL Naming and Addressing technical provisions is summarised in the following table.

Table 1.1. NA Extensions Change History

Version	Date	Comment
1	June 1998	Input to ATNP WG3 Utrecht (WG3 WP13-11). Proposed ATN Naming and Addressing Extensions - T Kerr
2	September 1998	Input to ATNP WG3 Bordeaux (WG3 WP14-11). Proposed ATN Upper Layer Naming and Addressing Extensions - T Kerr
3	January 1999	Input to ATNP WG3 Honolulu (WG3 WP15-10). ATN Naming and Addressing - Change Pages and Examples - T Kerr
SV4 2.0p	May 1999	Input to ATNP WG3 Naples (WG3 WP16-10). Formatted as SV4 change pages.

See also:

WG3/SG3 Working Paper: Comments on ATN Naming and Addressing - Change Pages and Examples (January 1999) - F Picard

1.2.2 Development of CLDS Technical Provisions

The CLDS is an ATN infrastructure component that exploits the Connectionless Transport Service offered by the ATN Internet Communication Service in Doc 9705. It provides to ATN applications a complete connectionless protocol stack and corresponding service. The connectionless upper layer stack has been under development for a considerable time, with early drafts pre-dating ATNP/1. ATN application developers are now identifying requirements which might best be satisfied by the connectionless paradigm.

Connectionless efficiency enhancements ("fast byte" protocols) for Session and Presentation layers were developed by WG3/SG3, reviewed at their meeting in Toulouse, September 1998, and input to the ISO/IEC and ITU-T standards forums.

The recent change history of the CLDS technical provisions is summarised in the following table.

Table 1.2. CLDS Change History

Version	Date	Comment
Draft	April 1996	Input to ATNP WG3 Brussels meeting (Attachment to ATNP WG3 WP 6-25): Connectionless Upper Layer Architecture - S Van Trees

Version	Date	Comment
Final Draft	June 1996	Input to ATNP WG3 Munich meeting (Attachment to ATNP WG3 WP 7-8): Connectionless Upper Layer Architecture - S Van Trees
0.1	March 1998	Input to ATNP WG3 Rio meeting (WG3 WP12-09) ATN Connectionless Upper Layer Communication Service - S Van Trees
0.1	September 1998	Input to ATNP WG3 Bordeaux meeting (WG3 WP14-27) Connectionless Upper Layer Communication Service - S Van Trees
0.1	January 1999	Input to ATNP WG3 Honolulu meeting (WG3 WP15-35) ATN Connectionless Upper Layer Communication Service - S Van Trees
1.0	April 1999	Updated WG3/SG3 Toulouse (Jan 99) and subsequent review comments.
SV4 2.0p	May 1999	Input to WG3 Naples (WG3 WP16-10) Formatted as SV4 chapter 4.7.

See also:

WG3/SG3 Working paper: Comments on ATN Connectionless Upper Layer Communication Service (February 1999) - T Kerr

1.2.3 Development of Secure Dialogue Service

The Secure Dialogue Service is an enhancement that provides peer entity authentication and data integrity verification services for instances of communication between DS-User applications (such as ADS, CM, CPDLC, FIS, GACS). The objective was to minimise changes to the applications, and to contain the functionality as much as possible in a new Security Application Service Element (SASE).

The change history of the Secure Dialogue Service technical provisions is summarised in the following table.

Table 1.3. Secure Dialogue Service Change History

Version	Date	Comment
	Oct 97	WG3 WP11-26 ATN upper layers task outline, G M-Biron
		WG3 WP12-25 ATN upper layers security, G-M Biron
	Sep 98	Input to ATNP WG3 Bordeaux meeting (WG3 WP14-24) Secured ATN Dialogue Service, G M-Biron
1	Jan 99	Input to ATNP WG3 Honolulu meeting (WG3 WP15-43) Upper Layer Security SARPs - Version 1, G M-Biron
	May 1999	Input to WG3 Naples (WG3 WP16-34) SV4.8, G Mittaux-Biron.

	September 1999	Input to WG3/SG3 Toulouse 4.8 Security Application Service Object, G Mittaux-Biron.
	September 1999	Input to WG3 Gran Canaria (WG3 WP17-xxx)

See also:

WG3/WP15-42 Secured ATN Dialogue Service, G Mittaux-Biron

WG3/WP16-35 Recovry of Security Errors in ULCS, G Mittaux-Biron.

WG3/SG3 (Toulouse, Sep 1999) Proposed mapping of WG1/SG2 security requirements on upper layers mechanisms, G Mittuax-Biron

WG3/SG3 (Toulouse, Sep 1999) Security mechanisms for ATN Air-Ground Applications, F Picard

WG1/SG2 Flimsy 2a 25 August 1999 ULA Security Scenarios.

1.2.4 Development of GACS Technical Provisions

The Generic ATN Communications Service (GACS) is an ATN infrastructure component which presents an enhanced dialogue service which will allow future ATN applications to be developed without the need to perform connection management functions. It also plays a role in the migration of legacy application systems to the ATN infrastructure. It allows dynamic exploitation of either the Dialogue Service or the CLDS. GACS is a communications service specification in the same sense as ULCS and ICS.

The report of the 10th meeting of ATNP/WG3 states, under the agenda item Planning for Future Work Programme: “There is a need to develop future applications and/or upgrade current applications for CNS/ATM-2, for example (amongst others) simplification of ADS and FIS dialogue service.” The GACS service provides the means to accommodate this, for these and any future applications.

At the March 1998 ATNP WG meetings in Rio, the need for a simple generic end-to-end ATN communication service was recognised, and the Simple ATN Messaging (SAM) concept was broadly approved, with some reservations. WG3/SG3 was actioned to analyse the arguments and report back to WG3 in Utrecht, in July 1998.

An initial draft specification of the Simple ATN Messaging (SAM) service and protocol was produced by Eurocontrol, and formed the basis of discussion at the WG3/SG3 meeting in April 1998 in Bracknell, UK. SG3 concluded that GACS (as it became called) is a worthwhile technical addition for the next package of ATN standards to be approved by ATNP/3, and that it in no way affects the stability of the existing applications.

A number of detailed technical comments were raised on the draft GACS specification presented at Utrecht. These comments were resolved at the WG3/SG3 meeting in Toulouse in September 1998, and the specification was updated accordingly.

The recent change history of the GACS technical provisions is summarised in the following table.

Table 1.4. GACS Change History

Version	Date	Comment
0.A	12/01/98	Initial draft

0.B	21/01/98	Second draft
0.C	26/02/98	Revised after review. SAM-SEND renamed SAM-TRANSFER. Message type parameter added. PDU definitions added. Chapter 2 added.
0.D	12/05/98	Input to ATNP WG3 Utrecht (WG3 WP13-10). SAM renamed GACS. Specification restructured after review by ATNP/WG3/SG3. ASO approach added in addition to AE approach.
0.E	15/09/98	Input to ATNP WG3 Bordeaux (WG3 WP14-10). Specification updated after review in WG3/SG3, taking STNA comments into account. Former 1.3 (GACS Realisation) moved to 1.1 (Introduction). Detailed protocol description added.
0.F	28/10/98	Input to ATNP WG3 Honolulu (WG3 WP15-13). Details of mapping to PDU fields tabulated and completed in protocol description.
1.0a	01/03/99	Post ATNP/WG3 Honolulu + preliminary validation results. Renumbered as section 4.9 of ATN Technical Provisions. Guidance material split into separate document.
SV4 2.0p	May 1999	Input to WG3 Naples (WG3 WP16-10) Formatted as SV4 chapter 4.9.

See also:

WG3 WP12-19 The case for a Simple ATN Messaging Service (SAM) - D Van Roosbroek

WG3 WP15-17 Eurocontrol GACS Implementation and Validation - D Van Roosbroek

WG3/SG3 - Comments on the Simple ATN Messaging (SAM) (April 1998) - F Picard.

WG3/SG3 - STNA Comments on the Draft Specification and Guidance material for the Generic ATB Communication Service (GACS) (September 1998) - F Picard.

ATNP/CCB PDR 98100010 - added a new AE-Qualifier value for the GACS AE.

1.3 Embedded Testing

The ULCS modifications cannot be completely validated in isolation; they must be considered in combination with ATN Applications that use them. There is no requirement that the CLDS, or the GACS-ASO Service should be explicitly realised in an implementation; it serves as the abstract interface between the common ULCS and each individual ATN Application specification. It must therefore be validated for such cases that the ULCS and ATN Applications when taken together specify a complete, implementable function.

1.4 Dependencies on External Standards

The ULCS provisions incorporate by reference a number of standards produced by accredited international standards bodies. A potential advantage of using ISO/IEC or ITU-T standards is that they are pre-validated, i.e. studied and approved by national standards bodies, implemented and interoperability demonstrated between independent implementations. To benefit from such pre-validation, the validation status of each referenced standard needs to be verified. For each referenced external standard, the following points must be answered:

- What is the status of the standard (committee draft, draft or fully ratified)?
- Do implementations exist?
- Has interoperability been demonstrated?
- Are there any outstanding defect reports?
- Are the references to the standard sufficiently precise (version number, amendments and defect reports included)?

1.4.1 ASN.1/PER

The Packed Encoding Rules (ISO 8825-2) are assumed to be stable. It is proposed not to validate this standard any further in this effort.

1.4.2 ACSE (second edition)

As one element of the ULCS, the association control service element (ACSE) protocol is always embedded in an ATN Application Entity. The connection-oriented ACSE standards (second edition) are mature and stable and have not changed since the ULCS technical provisions were first validated.

New in the ULCS enhancements is the inclusion, by reference, of the connectionless ACSE protocol standard. Amendment 1 to that standard optimises the size of encoded PDUs when PER is used and also provides for the future use of security parameters. Amendment 1 is relatively recent, and has been validated by means of automated ASN.1 syntax checking. This revealed a defect in the standard, which has been input to the ISO defect handling procedure, and the agreed solution has been incorporated.

References:

ISO/IEC 10035-1:1995/Amd.1:1997 Information Technology - Open Systems Interconnection - Connectionless Protocol for the Association Control Service Element : Protocol Specification Amendment 1 : Incorporation of Extensibility Markers and Authentication Parameters.

ISO/IEC 10035-1/Amd.1 defect report 10035-1/001

ISO/IEC 10035-1/Amd.1 draft Technical Corrigendum 1 (DTC ballot pending from ISO/IEC JTC1 Maintenance Rapporteur)

1.4.3 Presentation Layer

The ULCS requires the “fast byte” efficiency enhancements to the CO presentation protocol. These are now mature and stable and have not changed since the ULCS technical provisions were first validated.

New in the ULCS enhancements is the inclusion, by reference, of the Connectionless Presentation protocol standard. The recent efficiency enhancement Amendment to that standard was raised by WG3/SG3. As the efficiency-enhanced protocol only requires a single, static octet, validation of the protocol is trivial. Validation of the wording of the standard is achieved by ensuring that unambiguous implementation of the requirements is possible.

References:

ISO/IEC 9576-1:1996/Amd.1:1998 Information Technology - Open Systems Interconnection - Connectionless Presentation Protocol : Protocol Specification Amendment 1 : Efficiency Enhancements.

1.4.4 Session Layer

The ULCS requires the “fast byte” efficiency enhancements to the CO session protocol. These are now mature and stable and have not changed since the ULCS technical provisions were first validated.

New in the ULCS enhancements is the inclusion, by reference, of the Connectionless Session protocol standard. The recent efficiency enhancement Amendment to that standard was raised by WG3/SG3. As the efficiency-enhanced protocol only requires a single, static octet, validation of the protocol is trivial. Validation of the wording of the standard is achieved by ensuring that unambiguous implementation of the requirements is possible.

References:

ISO/IEC 9548-1:1996/Amd.1:1998 Information Technology - Open Systems Interconnection - Connectionless Session Protocol : Protocol Specification Amendment 1 : Efficiency Enhancements.

2. HIGH LEVEL VALIDATION OBJECTIVES

At the lowest level of validation, every technical provision clause (“shall” and “should” statement) is validated for correctness, consistency, lack of ambiguity and lack of duplication. This is typically done as an integral stage of implementation. This report concentrates instead on high-level validation objectives. Each validation objective is categorised as:

- System Level Validation Objective (SVO), relating to the system level requirements which are based on operational requirements within the ICAO Draft Manual of ATS Data link Applications, or elsewhere.
- Functional Validation Objective (FVO), relating to the functional characteristics described in the Technical Provisions.
- Technical Validation Objective (TVO), relating to the technical details in the Technical Provisions

The following Table lists the high-level validation objectives adopted for the ULCS functional enhancements.

Table 2.1. Validation Objectives

VO	Description
SVO 1	To determine which System Level Requirements are satisfied by the functional descriptions in combination with the user requirements and recommended practices.
SVO 2	To determine if the ATN specifications are mutually consistent and that backwards compatibility is achieved.
FVO 1	To determine if the functional descriptions are compatible with the technical requirements.
FVO 2	To determine if the user requirements and recommended practices are compatible with the technical requirements.
FVO 3	To determine if the technical provisions are complete.
FVO 4	To determine if the technical provisions are unambiguous.

VO	Description
FVO 5	To determine if the technical provisions are consistent.
FVO 6	To determine if there are redundant technical provisions, i.e. requirements which would have no effect if removed. *Note: This VO should be interpreted to mean that there are no requirements that are not necessary for the defined functionality, or to achieve migration to future functionality. It is not meant to eliminate possible duplicated statements of requirement that are known to exist.*
FVO 7	To determine if provision has been made to ensure that the technical provisions are implementation independent.
TVO 1	To determine if the protocol description supports the stated end to end services.
TVO 2	To determine if the protocol description has any unacceptable behaviour
TVO 3	To determine if the abstract service interface parameters are mapped appropriately to PDU fields and/or communication service interface parameters, and vice versa.
TVO 4	To determine if protocol errors in the peer application entity are correctly handled.
TVO 6	To determine if the APDUs are correctly specified.
TVO 7	To determine if provision for QOS management has been addressed.
TVO 8	To determine if provision for future migration has been addressed.
TVO 9	To determine if efficiency requirements have been addressed, e.g. minimising size of data transfer, appropriate maintenance of dialogue.
TVO 10	To determine that the functionality described in the technical provisions is implementable.
TVO 11	To determine that independent implementations built in accordance with the technical provisions will be able to interoperate.

2.1 Grouping of Requirements

For the validation of the ULCS extensions identified in this document, the following functional groups of requirements have been identified:

Each of these groupings (“high-level requirements”) is made up of an identified set of low-level requirements (“shall” clauses) and recommendations (“should” clauses).

- D-UNIT-DATA service and supporting protocols
- G-TRANSFER service and supporting protocols
- G-TRANSFER-CONFIRMED service and supporting protocols
- G-END service and supporting protocols
- G-MULTICAST service and supporting protocols
- GACS use of Dialogue Service (connection-oriented)

- GACS use of CLDS
- GACS behaviour when requested connection mode unavailable
- GACS realisation as an Application Entity
- GACS realisation as an embedded ASO supporting an application ASE
- Use of Presentation Addresses in CODS, CLDS and GACS services
- Use of System-ID parameters in CODS, CLDS and GACS services
- Addressing duplicate applications at the same location
- Backwards compatibility with naming and addressing in Doc 9705 first edition
- Secure Dialogue Service – successful establishment
- Secure Dialogue Service – unsuccessful establishment
- Secure Dialogue Service – data integrity
- Secure Dialogue Service – integrity failure
- Secure Dialogue Service – backwards compatibility with Dialogue Service in Doc 9705 first edition.

3. VALIDATION MEANS

The following generic means of validation have been identified, and are used in Table 4.1.

a) Two or more independently developed interoperating implementations validated by two or more states/organisations.

b) Two or more independently developing interoperating implementations validated by one state/organisation.

c) One implementation validated by more than one state/organisation.

d) One implementation validated by one state/organisation.

e) Partial implementation validated by one or more state/organisation.

f) Simulation, analysis using tools e.g. ASN.1 compiler, modelling tools.

g) Analysis and inspection.

4. FUNCTIONAL VALIDATION ACHIEVED BY STATES AND ORGANISATIONS

The validation programme has employed a number of validation methods including inspection and desk checking, the specification of an API based on the abstract service interface, simulation and modelling of the CF protocol machine, as well as multiple interoperating implementations.

The following table summarises the validation activities that have completed to date. The letters in the table correspond to the validation means given in section 3.

Note.— In the present draft, the matrix is incomplete. It will continue to be updated as the validation programmes listed in Section 5 progress.

Table 4.1. Validation Activities Summary

Group	ATNP/WG3/SG3	Eurocontrol	CENA CHARME	FAA
D-UNIT-DATA service and supporting protocols	g) f)	d)	d)	?
G-TRANSFER service and supporting protocols	g)	d)		
G-TRANSFER-CONFIRMED service and supporting protocols	g)	d)		
G-END service and supporting protocols	g)	d)		
G-MULTICAST service and supporting protocols	g)	e)		
GACS use of CLDS	g)	d)		
GACS use of CODS	g)	d)		
GACS behaviour when requested connection mode unavailable	g)	d)		
GACS realisation as an Application Entity	g)	d)		
GACS realisation as an embedded ASO supporting an application ASE	g)	e)		
Use of Presentation Addresses in CODS, CLDS and GACS services	g)	d)	d)	?
Use of System-ID parameters in CODS, CLDS and GACS services	g)	d)	d)	?
Addressing duplicate applications at the same location	g)	d)	d)	?
Backwards compatibility with naming and addressing in Doc 9705 first edition	g)			
Secure Dialogue Service – successful establishment	g)		d)	?
Secure Dialogue Service – unsuccessful establishment	g)		d)	?
Secure Dialogue Service – data integrity	g)		d)	?
Secure Dialogue Service – integrity failure	g)		d)	?
Secure Dialogue Service – backwards compatibility with Dialogue Service in Doc 9705 first edition.	g)			?

5. SUMMARY OF ACTIVITIES SUPPORTING VALIDATION

5.1 EUROCONTROL GACS Project

EUROCONTROL has instituted a project to realise the draft Generic ATN Communication Service (GACS) Technical Provisions as a software implementation. The software produced will not only provide application developers with easy access to the full 7-layer ATN infrastructure, but also contributes to the validation of the ULCS extensions for GACS, the connectionless ATN upper layers and Dialogue Service (CLDS), and upper layer naming enhancements.

The GACS implementation project produced independent software implementations of the following components:

- The ATN Connection-oriented Upper Layers (CO Session layer efficiency enhancement option, CO Presentation layer efficiency enhancement option, CO ACSE edition 2 and Control Function).
- The ATN Connectionless Upper Layers (CL Session layer efficiency enhancement option, CL Presentation layer efficiency enhancement option, CL ACSE edition 2 and Control Function).
- The Generic ATN Communications Service (GACS), providing a well-defined interface for applications to the full ATN protocol stack.
- A demonstration HMI.

The contract for the development of the GACS software was let in November 1998, and the software was delivered in August 1999. The project produced two major software modules:

- the Upper Layer Stack (ULS), which includes both connection-oriented and connectionless Dialogue Service, and interfaces to the ATN Transport Service.
- The GACS component, which is an implementation of the GACS-AE, providing a well-defined API to allow easy access to the full 7 layers of the ATN.

The GACS implementation project will consist of three phases:

I. The development of GACS software and the demonstration of its functionality (complete);

II. The integration of an example ATSC application (In progress);

III. Possible flight trials of the application from Phase II.

There is work in progress to perform interoperability trials with other, independent implementations.

The EUROCONTROL GACS implementation project has played a major role in ATNP/3 SARPs validation as well as providing a migration path for non-ATN (e.g. ACARS-based) applications and a rapid prototyping platform for the development of ATM applications. It will be important for ATN trials and exploitation in the future and will be available for free distribution under licence for non-commercial experimental use to EUROCONTROL Member States to assist in their ATN evaluation and trials activities.

5.2 CENA CHARME project

The objectives of CHARME are to provide the French DGAC with:

a) an ATN platform for data-link experiments on Package-1 applications,

b) a base for the prototyping of future air/ground data-link applications,

c) an infrastructure for the validation of some of the ATN Package-2 features, with a priority on: security services, naming and addressing extension, system management related to security, and key management mechanisms by CM ASE.

The CHARME developments consist of commercial off the shelf (COTS) products, and CENA-originated components. The COTS components are: the CO Session and Presentation layers, an ASN.1 compiler and associated PER runtime libraries, and the development environment for the CENA components. This COTS environment provides testing and integration facilities, and proved to enable the porting of CHARME components to various hardware platforms and operating systems. CENA developments for CHARME include: the CL Session, Presentation and CO/CL Application layers, together ASEs issued from OSI (CO/CL ACSE/Ed 2, ROSE, CMISE) or ICAO Package-1 specifications (ADS, ADS Report Forwarding, CM, CPDLC, and FIS). APIs are provided for each ASE, and for the Dialogue Service.

CHARME has successfully been integrated with the ProATN air-ground BIS, and an implementation of the ATN Transport Layer. This integration resulted in:

a) a Package-1 connection oriented full ATN stack,

b) a Package-2 connection oriented, and connectionless ATN stack (complete up to the Dialogue service).

The Package-2 stack includes the ATN ASEs, ROSE and CMISE for system management, and the Security ASO for upper-layers security.

CHARME is part of the simulated data-link infrastructure of CENA, which includes:

a) simulated sub-networks (Mode S, AMSS and VDL mode 2) access, real sub-network access (X.25 WAN, LAN) and loop-back facilities.

b) air traffic simulator, cockpit simulator and pseudo-pilot interface,

c) experimental ground control facilities.

The following CHARME developments are completed:

a) a full package 1 connection oriented ATN stack: CO Session and Presentation layers, ACSE and Dialogue control function, together with APIs,

b) CO and CL Session and Presentation layers,

c) ROSE and CMISE ASEs integrated in Package 1 upper-layers.

For CENA's ATN activities, the on-going CHARME developments are:

a) CO/CL package 2 dialogue control function, which should be finished before mid-99,

b) Security ASO for upper-layers security, which should be finished during the third quarter of 99.

Future CHARME activities should address:

a) System management for the management of security,

b) Prototyping activities (X.500),

c) Future ATN applications (e.g. CM server).

5.3 FAA Validation Activities

The FAA currently has two programs underway for the validation of the enhancements to Doc. 9705.

The FAA Technical Center with the assistance of the Mitre Corporation has a project underway to implement and test the security changes. The FAA Technical Center is modifying its ATN router to incorporate the security mechanisms added to Doc. 9705, Sub-Volume 5. This security work will include work in using the ATN directory for the purpose of testing certificate retrieval. Mitre will also be involved in testing the security modifications and in providing assistance in implementing the ATN directory.

The FAA AND-370 organization has a project underway to modify the previously developed prototype implementations of the applications and ULCS to incorporate the enhancements. These implementations will be available for interoperability testing with other organizations. This validation project is also implementing the ATN directory services for validation purposes. The validation project is also planning to implement the ATN system management enhancements.

5.4 Analysis and Conclusions

(To be completed)

6. DEFECT REPORT SUMMARY

This section summarises the defect reports raised during the validation programme.

6.1 Naming and Addressing Enhancements

- Encoding of LOC + SYS fields not defined unambiguously (CENA).

6.2 CLDS

- Error in ASN.1 definition of CL ACSE - tag missing for calling-authentication-value (CENA)
- Error in ASN.1 definition of CL ACSE - semicolon missing from IMPORTS statement (OSS, Bancroft Scott, ASN.1 compilation).

6.3 Secure Dialogue Service

Note.— This component is not at present considered stable enough to be placed under configuration control. It is anticipated that a stable draft will be produced once WG1/SG2 (Security subgroup) has resolved outstanding issues relating to algorithm selection, key length and distribution, and detailed security mechanisms (symmetric, asymmetric, hybrid).

6.4 GACS

The following tables list the changes proposed for and made to the draft SARPs document for the Generic ATN Communication Serice (GACS), since it was distributed in its first stable version: "Specification for Generic ATN Communication Service" V0.F. The change proposals come from a number of sources:

- ATNP/WG3/SG3 meeting, Toulouse, Jan 1999 - structure of Sub-Volume 4 additions for ATNP/3
- ATNP/WG3 meeting, Honolulu, Jan 1999 - avoidance of confusion with AMHS SARPs, clarification of CM usage.
- Sub-Volume 4 editor - alignment with SV4 Naming and Addressing enhancements, various clarifications.
- CENA CHARME project - format of LOC + SYS
- Airtel ATN - User Data removed from D-END, note on G-END request when multiple dialogues. Various clarifications resulting from implementation.

6.4.1 Changes to GACS Specification V0.F

Ref.	Section	Description of change
1	general	• Document title changed to indicate proposed positioning in Sub-Volume 4 • Abstract updated • Document version updated to V1.0
2	2	Guidance Material (chapter 2) moved to separate document.

Ref.	Section	Description of change
3	All	Alignment with Doc 9705 Sub-Volume 4: • Font changed to Times New Roman • Section numbering starts at 4.9, so prefix "1." replaced with "4.9." in all section numbers, figure and table captions, and cross-references. • All paragraphs in section 1.1 which do not contain "shall" or "should" to become Notes, or to be reworded. • Conversion to WordPerfect 8 from MS Word 6/7.
4	general	Avoidance of confusion with AMHS in Doc 9705 Sub-Volume 3: • all use of the word "message" reviewed, and replaced with appropriate synonyms where possible.
5	1.1.3 Note 5	Clarification that CLTS may not support multicast
6	1.1.5	Clarification of the use of CM
7	1.1.5	Object Identifier aligned with naming & addressing enhancements
8	1.1.6	Object Identifier aligned with naming & addressing enhancements
9	1.2.3.1 Note 3	Recipient list entries may also include Sys-ID
10	1.2.3.1 Note 4	Sender may also include Sys-ID.
11	1.2.3.1 Note 8	List of parameter values replaced with ref to [ICS] Table 5.6-1.
12	1.2.3.1 Note 9	List of parameter values replaced with ref to [SV1] Table 1-2.
13	1.2.4.1 Note 4	Sender may also include Sys-ID - refer to G-TRANSFER for syntax.
14	1.2.5.1 Table 1.2-4	Airtel ATN 15.02.99: User Data parameter deleted from G-END service
15	1.2.5.1	Airtel ATN 15.02.99: New note 4 to state that if there is more than one dialogue open with the specified peer then it is a local implementation matter how the G-END request is associated with the correct dialogue.
16	1.2.5.1 Note 5	Sender may also include Sys-ID - refer to G-TRANSFER for syntax.
17	1.2.5.1 Note 8	Delete note, as User Data parameter deleted from G-END service
18	1.3.6.1	CENA CHARME 02.02.99: Add ASN.1 comment to ULCSPeerId.sysID to indicate that the INTEGER is formed by the concatenation of the LOC and SYS octets from the NSAP address, with LOC as the most significant.
19	1.3.8.3 Table 1.3-6	Airtel ATN 15.02.99: Allow G-END request when in STA 0 or STA 3 (no action, no state change).
20	1.3.9.1	Add note describing layout of this section, i.e. each input event is considered in turn.
21	1.3.9.2.3 Table 1.3-8	Change Status of Called Peer ID to (U) and add Called Sys-ID (C), Called Presentation Address (U) - all take values from one item of Recipient List.
22	1.3.9.2.3 Table 1.3-8	Add Calling Sys-ID (C), Calling Presentation Address (U) - Not used.
23	1.3.9.2.5 Table 1.3-10	Change Status of Called Peer ID to (U) and add Called Sys-ID (C), Called Presentation Address (U) - all take values from one item of Recipient List.
24	1.3.9.2.5 Table 1.3-10	Add Calling Sys-ID (C), Calling Presentation Address (U) - Not used.

Ref.	Section	Description of change
25	1.3.9.3.3 Table 1.3-12	Change Status of Called Peer ID to (U) and add Called Sys-ID (C), Called Presentation Address (U) - all take values from one item of Recipient List.
26	1.3.9.3.3 Table 1.3-12	Add Calling Sys-ID (C), Calling Presentation Address (U) - Not used.
27	1.3.9.3.5 Table 1.3-14	Change Status of Called Peer ID to (U) and add Called Sys-ID (C), Called Presentation Address (U) - all take values from one item of Recipient List.
28	1.3.9.3.5 Table 1.3-14	Add Calling Sys-ID (C), Calling Presentation Address (U) - Not used.
29	1.3.9.4.2 Table 1.3-15	Add format of sender in “end” APDU - ULCSLocationType if available, otherwise absent.
30	1.3.9.4.2 Table 1.3-15	userData is always Absent, as User Data parameter deleted from G-END service.
31	1.3.9.4.	Airtel ATN 15.02.99: Add new para 1.3.9.4.4: “If a G-END request primitive is invoked and the GACS entity for the Dialogue which corresponds to the Recipient List entry is in the Idle state (STA 0) or the Ending state (STA 3), then the GACS entity shall take no action and remain in the same state.”
32	1.3.9.5.2 Table 1.3-18	Add format of sender in confirmation APDU - local ULCSLocationType value if available, otherwise absent.
33	1.3.9.5.2 Table 1.3-19	Change Status of Called Peer ID to (U) and add Called Sys-ID (C), Called Presentation Address (U) - all take values from received D-UNIT-DATA ind
34	1.3.9.5.2 Table 1.3-19	Add Calling Sys-ID (C), Calling Presentation Address (U) - Not used.
35	1.3.9.5.3 Table 1.3-20	Sender not always present in APDU. Add format of sender in confirmation primitive - ULCSLocationType value if present in received APDU, otherwise peer PSAP address.
36	1.3.9.6.3 Table 1.3-25	Add format of sender in confirmation APDU - local ULCSLocationType value if available, otherwise absent.
37	1.3.9.7.2 Table 1.3-27	Sender not always present in APDU. Add format of sender in confirmation primitive - ULCSLocationType value if present in received APDU, otherwise peer PSAP address.
38	1.3.9.7.2 Table 1.3-28	Add format of Sender - same format as original D-START req.
39	1.3.9.8.1 Table 1.3-29	Sender not always present in APDU. Add format of sender in confirmation primitive - ULCSLocationType value if present in received APDU, otherwise peer PSAP address.
40	1.3.9.9.1 Table 1.3-32	Syntax of sender parameter in G-END ind. Peer ULCSLocationType value if available, otherwise PSAP address.
41	1.3.9.9.1 Table 1.3-32	Delete User Data row, as User Data parameter deleted from G-END service.
42	1.3.9.11.1 Table 1.3-33	Syntax of sender parameter in confirmation primitive - peer ULCSLocationType value if available, otherwise PSAP address.
43	1.3.9.11.1 Table 1.3-34	Syntax of sender parameter in G-END ind. Peer ULCSLocationType value if available, otherwise PSAP address.
44	1.3.9.11.1 Table 1.3-34	Delete User Data row, as User Data parameter deleted from G-END service.
45	1.3.9.12.1 Table 1.3-35	Add format of sender in “end” APDU - ULCSLocationType if available, otherwise absent.

Ref.	Section	Description of change
46	1.4.3.1 Table 1.4-1	Table replaced with ref to [ICS] Table 5.6-1.
47	1.4.3.2 Table 1.4-2	Table replaced with ref to [SV1] Table 1-2. Transport priority rather Network priority used - sense is opposite.
48	1.4.3.3	Add description of Called Sys-ID and Called Presentation Address.
49	1.4.3.4	Replace para by "The Calling Peer ID, Calling Sys-ID and Calling Presentation Address parameters of the D-START and D-UNIT-DATA services shall be unused."
50	1.5	Airtel ATN 15.02.99: Add new para 1.5.2: Recommendation.— The GACS user should set the Message Type parameter in GACS primitives to a value which unambiguously identifies the abstract syntax used by that GACS-User.

6.4.2 Changes to GACS Specification V1.0a

51		Airtel ATN 16.03.99: G-END in start-multi state. In 4.9.3.9.4.3 of the GACS specification, a G-END request is received in the start multi state. What happens to any data that was waiting to be sent once the dialogue was established? G-END should not disrupt the data transfer. The previous G-TRANSFER(-CONFIRMED) request would have completed successfully and the GACS-User would therefore think that the transfer had succeeded. If the connection set-up is taking too long and the user data cannot be transferred, this should be caught by the recommended timer in section 4.9.3.3.6. The GACS spec should be changed so that G-END req is IGNORED when in the Start-multi state. This should be indicated to the G-END invoker via a suitable API return code.
52		Airtel ATN 19.03.99: GACS security parameter for a G-TRANSFER in multishot mode. If there is an existing dialogue with the same QOS paramaters it must also be ensured that it has the same security value before it can be used for this transfer.

7. RESULTS AND ANALYSIS

7.1 SVO 1

To determine which System Level Requirements are satisfied by the functional descriptions in combination with the user requirements and recommended practices.

As determined by inspection, all the system level requirements relevant to ULCS are satisfied by the revision of Sub-Volume 4 as presented. (g)

(Assuming that Secure Dialogue Service will be integrated into Sub-Volume 4 before ATNP/3)

7.2 SVO 2

To determine if the ATN specifications are mutually consistent and that backwards compatibility is achieved.

Study of the CLDS, and implementation of CLDS alongside the CO dialogue service, ensures it has been specified in a manner consistent with the existing connection-oriented Dialogue Service. (d)

No applications other than GACS have yet been specified to use the CLDS, so backwards compatibility is not at issue. (g)

Implementing the CLDS and/or GACS has no effect on implementations of the technical provisions of the first edition of Doc 9705. (g, d)

Study and implementation of the GACS service and protocol has ensured that they have been specified in a manner consistent with other ATN application and ULCS specifications. (g, d)

It is noted that great care has been taken to minimise the impact of the naming and addressing enhancements on existing implementations. (g, d)

The Secure Dialogue Service has been designed from the outset to be consistent with the existing connection-oriented dialogue service. Fallback provisions have been defined in order to achieve backwards compatibility. (d)

7.3 FVO 1

To determine if the functional descriptions are compatible with the technical requirements.

The technical requirements have been examined and trials have been performed to ensure they provide the intended functionality. (g, d)

(Technical requirements for Security ASO are still under development)

7.4 FVO 2

To determine if the user requirements and recommended practices are compatible with the technical requirements.

The “User Requirements” correspond to the requirements at the GACS, DSI and CLDS service boundaries. Inspection has shown that all user requirements result in appropriate protocol requirements, and specification of APIs has shown that such requirements can be conveyed. (g)

7.5 FVO 3

To determine if the technical provisions are complete.

All statements in the sections on protocol have been analysed, syntax-checked and implemented in prototype form, and care was taken not to make any assumptions in the event that there were no “shall” statements. (d)

(Technical requirements for Security ASO are still under development)

7.6 FVO 4

To determine if the technical provisions are unambiguous.

It has been demonstrated that the technical provisions are implementable. Interoperability testing will demonstrate that different implementers have interpreted them in the same way. In the mean time, independent supervision of system tests, and desk-checking of encoded data steams has validated the interpretation of technical provisions by implementer and independent tester (for GACS, CLDS and Naming enhancements).

(Pending results of implementation projects and interoperability testing)

7.7 FVO 5

To determine if the technical provisions are consistent.

All statements in the sections on protocol have been analysed, syntax-checked and implemented in prototype form. All inconsistencies found have been removed. (d)

(Technical requirements for Security ASO are still under development)

7.8 FVO 6

To determine if there are redundant technical provisions, i.e. requirements which would have no effect if removed.

Note: This VO should be interpreted to mean that there are no requirements that are not necessary for the defined functionality, or to achieve migration to future functionality. It is not meant to eliminate possible duplicated statements of requirement that are known to exist.

All statements in the sections on protocol have been analysed, syntax-checked and implemented in prototype form, and care was taken not to make any unnecessary over-specification. (g)

(Technical requirements for Security ASO are still under development)

7.9 FVO 7

To determine if provision has been made to ensure that the technical provisions are implementation independent.

All statements in the sections on protocol have been analysed, syntax-checked and implemented in portable software that is independent of environment. The use of ASN.1 for syntax definition ensures that the resulting encoded data steams are machine-independent. Care has been taken not to over-prescribe implementation approaches. Implementers have not found themselves to be constrained when defining the implementation approach. (d)

(Technical requirements for Security ASO are still under development)

7.10 TVO 1

To determine if the protocol description supports the stated end to end services.

All statements in the sections on protocol have been analysed, syntax-checked and implemented in prototype form. Testing has shown that the stated end-to-end services are indeed supported. (d)

(Protocol description for Security ASO is still under development)

7.11 TVO 2

To determine if the protocol description has any unacceptable behaviour

All statements in the sections on protocol have been analysed, syntax-checked and implemented in prototype form. Testing has shown that the protocol description has no unacceptable behaviour. (d)

(Protocol description for Security ASO is still under development)

7.12 TVO 3

To determine if the abstract service interface parameters are mapped appropriately to PDU fields and/or communication service interface parameters, and vice versa.

Fully validated by inspection of the Technical Previsions. Note there is no requirement for implementations to expose parameters defined in abstract services, and equally they are free to add implementation-specific parameters. Nonetheless, implementation projects have produced APIs, which map closely to the defined ASIs for CLDS and GACS, and the fact that they are encoded efficiently has been validated by inspection of traces and logs. (g).

7.13 TVO 4

To determine if protocol errors in the peer application entity are correctly handled.

Inspection has shown that protocol definitions include appropriate error handling. Interoperability testing with artificially induced errors will demonstrate this in practice.

(Pending results of implementation projects and interoperability testing)

7.14 TVO 6

To determine if the APDUs are correctly specified.

The APDU definitions have been inspected and syntax-checked using an ASN.1 compiler. (f, g)

(Pending further results for Secure Dialogue Service)

7.15 TVO 7

To determine if provision for QoS management has been addressed.

Inspection shows that the ICS QoS parameters are carried in CLDS primitives and DSI QoS parameters are exposed in GACS primitives, the conclusion being that existing validated provisions for QOS management are unaffected. (g)

7.16 TVO 8

To determine if provision for future migration has been addressed.

A version number has been included for GACS-users as an aid to future migration. All significant protocol elements are extensible. There are no significant restrictions on name or address space. The ULA was designed to be extensible, and this has been demonstrated by the addition of the Security ASO. Further ASOs could be added in future. All syntax definitions have been made in ASN.1, with appropriate extensibility markers to ensure that the protocols are extensible in a controlled way. (g)

(Security ASO to be checked when stable)

7.17 TVO 9

To determine if efficiency requirements have been addressed, e.g. minimising size of data transfer, appropriate maintenance of dialogue.

ASN.1 Packed Encoding Rules (PER) are invoked, and PER-visible constraints have been specified for optimal encoding. GACS avoids the use of DSI fields that lead to inefficient OID encoding, and provides the user with options to maintain the dialogue where appropriate. Efficiency enhancements for the CL Session and Presentation protocols were input to the ISO/IEC and ITU-T standardisation process and subsequently ratified as international standards. (g)

(Security ASO to be checked when stable)

7.18 TVO 10

To determine that the functionality described in the technical provisions is implementable.

Implementations have been produced. (d)

(Pending further results of implementation projects and interoperability testing)

7.19 TVO 11

To determine that independent implementations built in accordance with the technical provisions will be able to interoperate.

(Pending results of implementation projects and interoperability testing)

8. CONCLUSIONS

It is concluded that the enhanced technical provisions in Sub-Volume 4 will be sufficiently validated for inclusion in ICAO Doc. 9705, with the possible exception of the Secure Dialogue Service.

It should be noted that interoperability testing between independent implementations is still required as an urgent item.

States and Organisations are requested to provide information regarding any validation activities that have not been covered in this draft report.