CEC TEN-T ATM Task UK/96/94

ACCESS

ATN Compliant Communications
European Strategy Study

Safety Assessment and Certification

Document Reference	: ACCESS/NATS/223/WPR/044
Author	: NATS
Revision Number	: 2.0
Date	: 14/01/99
Filename	: N044I2-0.DOC

DOCUMENT CONTROL LOG

Revision Number	Date	Description of Change
0.1	7th January 1998	First Draft
0.2	9th February 1998	Updated to include further work and comments from ACCESS partners.
0.3	14th August 1998	Updated to include additional work and comments.
1.0	14th October 1998	Updated to include STNA comments.
1.1	11 November 1998	Updated following internal NATS review.
1.2	2nd December 1998	Final version for comment. Significant changes have been made to section 4.0
2.0	14th January 1999	Issue version. Minor changes have been made to section 1.3

EXECUTIVE SUMMARY

This document addresses the issues associated with the safety assessment and certification of implementing and operating the ATN in the ACCESS Region of Europe. The document is not a Safety Case for the 'Target European ATN', that is the responsibility of the relevant States and Organisations.

This document details the current work being undertaken on Safety Assessment & Certification for data link applications and the associated infrastructure. It includes a review of state procedures regarding the safety certification of systems, and identifies common trends and key issues related to the safety assessment and certification of the ATN infrastructure. Finally, there are recommendations on the practical approaches necessary to fulfil the requirements of Safety Assessment & Certification for the proposed ATN topology in the ACCESS region.

The advent of end to end data link technology and services in the ATC environment requires that the users of the technology and services provide the necessary safety assurances to the regulatory bodies prior to there certification and approval for operational use. This has resulted in a range of projects being initiated, projects whose specific aim is to provide guidance and develop 'tools' to support the approval of such systems into operational service. The EOLIA and ProATN projects have both undertaken preliminary safety assessment work to assist in the development of practical recommendations for assessing and certifying data link services and the associated infrastructure.

The objective of this work will be to allow the implementor to develop specific implementations of the data link system components e.g. routers and verify and approve them using agreed standards and methodologies. The components, providing they gain certification approval, can then be introduced into the end to end system without the need to re-certify the existing components. All the work reviewed detailed the importance of considering the institutional issues and to account for the scale of the CNS/ATM operations, i.e. it will encompass many States and Organisations.

Safety Management Systems and the Airworthiness Authorities have a major part to play in demonstrating that a safety related system is safe to be introduced into operational service. The procedures have been developed to provide assurance to the Regulatory Authorities that the potential hazards of a new system have been identified and controlled. The current procedures adopted by the majority of States rely on the ATS provider to adopt a formal Safety Management System with individual States applying their own adaptations of Safety Management. Safety Management allows organisations to implement an effective safety policy and to achieve high standards of safety thus minimising the risks as far as is reasonably practicable. The majority of States will adopt to use the 'Safety Case' methodology as the focus of their Safety Management System. The Joint Aviation Authority (JAA) is an integral part of the certification process for avionics manufacturers. It is important that any new standards and guidance material developed to address the safety implications of data link services are recognised by the regulating authorities and organisations such as the JAA.

Third Party Service Providers (TPSP) will also need to demonstrate the safety of their systems, via documented evidence, to the relevant aviation safety regulatory authority in support of their application to obtain certification for the operational use of their system.

The techniques and reference systems currently being developed by international bodies such as EUROCAE include that ATN data link services be assessed and certified as a separate entity to the ATN Communications Infrastructure (ACI). This ensures that new data link services can be developed and certified without the need to re-certify the underlying infrastructure. The safety requirements for ATN data link services can be translated into QoS requirements for the ATN Communications Infrastructure. These QoS requirements can then be distributed to the sub-systems e.g. routers and subnetworks which form the underlying infrastructure. Existing sub-systems such as communications subnetworks may need to rely on in-service history and safety cases to provide the

required safety assurance. New sub-systems such as routers will need to be designed using best practice, recognised standards and incorporate rigorous testing to include a reference facility to ensure interoperability. In all cases adequate levels of redundancy and 'fall-back' procedures will need to be demonstrated as part of the safety assurance process.

The safety assessment process will need to demonstrate that the QoS figures for the ATN Communications Infrastructure are achievable and maintainable. This can be achieved by utilising network and system management techniques to ensure that if operational changes need to be implemented this can be done in a controlled and timely manner and a safe service maintained.

In the event that the ACI QoS required to operate a safety critical application falls below the agreed target level for a defined period of time then it may not be safe to operate that application. The ATS provider will not be certified to operate the application under these conditions resulting in the application not being offered. Fall-back procedures will need to be implemented until the QoS returns to the target level.

A data link system is highly integrated and any changes no matter how minor have the potential to adversely affect the end to end performance. It is important that any SLA with a TPSP should allow for the testing and assessing of modifications by the ATS provider to minimise the impact upon the operational ATS service.

The ACCESS study has defined three transition phases, the first describes local implementation data link services which can be introduced by one state in isolation. It may be possible to provide the necessary safety assurance to the regulating authority using existing procedures adopted for other safety critical systems. In the event of a particular data link service being introduced by many States it would be beneficial for the later transition phases to coordinate and adopt consistent system acceptance criteria.

The second phase describes a coherent infrastructure offering a range of data link services covering multiple FIRs and States. This phase will require coordination of safety activities. The regulatory authorities will need to cooperate as to the role standards and tools such as CAERAF will take in the approval and certification of data link systems and services. This may require the development of an internationally agreed standard to cover specific implementations and metrics defined to ensure that consistent system acceptance criteria are employed across the institutional boundaries.

The final phase is the Target European ATN and describes a routing architecture centred around a European ATN Island. The data link services offered will consist of those identified in phase 2 and may be the introduction of more safety critical data link services. The approval of new services will be no different than the approval procedures used for existing services with the exception that more States will be involved. There is the added benefit that the ATS Providers will be able to provide evidence as to the reliability of the ACI and the associated applications from an in service history as a result of phase 2.

TABLE OF CONTENTS

1. Introduction

1.1 Scope & Document Purpose

Work package 223 will address the issues associated with the safety assessment and certification for implementing and operating the ATN in Europe. It will not produce a Safety Case for the defined ATN topology, that is the responsibility of the relevant States and Organisations.

The report will document the current work being undertaken on Safety Assessment & Certification for data link applications and the associated infrastructure. It will include a review of state procedures regarding safety certification of systems, and identify common trends and key issues related to the safety assessment and certification of the ATN infrastructure. Finally, the generation of recommendations on practical approaches necessary to fulfil the requirements of Safety Assessment & Certification for the proposed ATN topology.

1.2 Background

To date the safety assessment techniques used in the aeronautical domain have only been applied to discrete ground and airborne systems. This has ensured that the systems could be tested and developed independently. The advent of data link systems has resulted in greater use of automated exchanges between ground and air based systems blurring the functional boundaries that had previously existed. This integration of the air and ground systems has required that safety assessment techniques be applied to the end-to-end system and resulted in the evolution and development of new safety methodologies. These methodologies look at the high level end to end system requirements and ‘ripple down’ to the dependent sub-systems. This allows the potential hazards and the event sequences leading to these hazards to be determined. This makes it possible to identify the risks associated with these hazards and identify the safety requirements of the system. Once the safety requirements have been identified, criteria can be developed, e.g. the available technology and timescales, which will allow decisions to be made on whether it is feasible to meet the requirements and provide the required safety assurance.

This document is concerned with Safety Assessment and Certification it is therefore important to describe just what is meant by these terms.

1.2.1 What is Safety Assessment?

Safety Assessment is a process with two main objectives; the first is to determine the safety requirements of a safety critical system and the second is to provide assurance that the system is safe for use in an operational environment. There are three stages to the Safety Assessment process and they are described briefly below:

Functional Hazard Analysis (FHA)

This provides an analysis of the system functionality to determine the potential failure modes and to classify the hazard severity. The analysis will provide the user with categorised high level safety requirements for the system.

Preliminary System Safety Assessment (PSSA)

The safety requirements identified in the FHA are combined with the system functions to enable safety requirements to be apportioned to all of the system components. This enables the requirements for each system component to be identified. The apportionment process ensures the component requirements are traceable and may highlight previously unidentified hazards.

System Safety Assessment (SSA)

This is a rigorous evaluation of the system components to determine if the component requirements identified in the PSSA have been met. The results from this analysis will form the basis of safety cases.

It is clear from the definition of Safety Assessment and the techniques involved in the assessment process that appropriate steps are taken in the management of identified hazards. This is an on-going process and will continue throughout the lifetime of the system as modifications are made.

1.2.2 What is Certification?

Certification is the process by which an independent regulator provides formal approval that a system whether it be an engine component or a data link service is fit for purpose. The formal approval would typically result in the granting of a license for that system defining the environment and conditions in which the system can be operated. The procedures that need to be followed to achieve certification will vary depending on the system, the operational domain i.e. air or ground based and its level of safety criticality.

Currently only airborne systems are ‘certified’; ground based systems adopt a different approach, safety cases, to gain approval from the safety regulator to provide an operational ATC service. The advent of data link technology has resulted in the integration of air and ground based systems and created a number of issues which need to be addressed. For example should ground based systems be certified in order to form part of the data link system?

For the purposes of this document the meaning of the term ‘certification’ when applied to ground based systems implies the formal approval for the operational use of the ground based system by the regulator.

An important and necessary step for the development of the ATN in Europe will be the agreement and acceptance of guidelines and standard techniques by international bodies such as EUROCAE and RTCA. The techniques can then be applied by manufacturers of aeronautical equipment, Aircraft Operators, Air Traffic Service Providers and Civil Aviation Administrators to ensure that new equipment and applications provide the necessary assurance to allow their certification for operational use.

1.2.3 Accountability and Liability

Accountability and liability issues will need to be addressed particularly where third party service providers are providing services and/or equipment for the Air Traffic Service (ATS) Provider e.g. Aeronautical Mobile Satellite Service (AMSS). These aspects are not directly addressed in this document but are considered elsewhere (WP220 - Third Party Service Provision, WP224 - Institutional Issues).

1.3 References

The referenced documentation is detailed in two tables, table 1 lists the **approved documentation** and table 2 the **draft documentation**. The contents of the latter may be subject to change.

	Reference	Title
1.	[A202]	ACCESS WP 202 - Define Geographic Areas & Services - Version 2.0
2.	[A203]	ACCESS WP203 - Routing Architecture Option 1 - Version 2.0
3.	[A220]	ACCESS WP 220 - Proposed Solutions to Third Party Service Provision Issues - Version 2.0.
4.	[CAD1]	'CADAG Safety Concept Proposals' - Working Paper CADAG 4 - Shannon - 10-14/6/96
5.	[CEC12]	A Preliminary Safety Assessment of EOLIA Datalink Services - EOL/WP2/NATS/050/D22/C/1 - 12/12/97.
6.	[CEC 14]	ADS Europe 97 Final Trials Results Report, & Recommendations For Further Work - Deliverable AED03 - Issue 1 - March 1998
7.	[EAT13]	COM.ET2.ST15 - Analyse Options For Initial A/G Data Networks - Phase 1 Report: Inventory and Analysis of A/G Applications And Data Networks - Edition 0.7 - 12/04/1996
8.	[ECA1]	Guidance Material for the Establishment of Data Link Supported ATS Services - ED-78 - EUROCAE WG45 - June 1997
9.	[EUR7]	ATN Internet Project (ATNIP) - RAF User Requirements Document (URD) - DED1/ATNIP/RAF_URD/DEL/5 - Issue 3.0 - 20/06/97
10.	[EUR8]	ATN Internet Project (ATNIP) - URD Input Document Assessment - DED1/ATNIP/RAF_URD/DOC/02 - Issue 1.0 - 28/08/96
11.	[EUR9]	CAERAF Technical Requirements Specification DED6/ATN/CAERAF-CFT/DOC/05 - Issue 1.2 - 06/02/98
12.	[ICA4]	ADS Panel - ICAO Manual of Air Traffic Services (ATS) Data Link Applications
13.	[ICA16]	ICAO Doc 9705-AN/956 - Manual of Technical Provisions for the ATN- SV1 Introduction & System Level Requirements
14.	[IEC1]	IEC 16508

Table 1: Approved Documentation

	Reference	Title
1.	[CEC13]	A Preliminary Safety Assessment of two EOLIA Datalink Services: ATIS and DSC EOL/WP2/NATS/069/DE22/C/0.A - 18/03/98
2.	[CEC11]	Requirements Analysis - A Review of the Safety Aspects of the ProATN - Ref ProATN/NATS/D12.4/97/022 - Version 0.2
3.	[ECA2]	2nd JWG EUROCAE WG53/RTCA SC-189 Meeting (Seattle) - 2-6/06/97
4.	[EUR10]	ATN Implementation Task Force - European ATN Implementation Plan - DED6/ATN/ATNI-TF/DOC/37 - Issue 0.2 18/6/98

Table 2: Draft Documentation

1.4 Definitions

ATM Data Link Service A set of ATM related transactions, both system supported and manual, within a data link application, which have a clearly defined operational goal e.g. Departure Clearances. [ECA1]

Data Integrity The upper bound requirement on the probability that a transmission error in a message goes undetected to the receiving end of the application [WP202]

Data Link Application The implementation of data link technology to achieve specific Air Traffic Management (ATM) operational functionalities e.g. ADS and CPDLC [ECA1]

Data Link System This is the end to end data link system and includes the communication links and data link applications. [ECA1]

End To End Approval A process whereby the operational and interoperability requirements of a data link service as well as its safety objectives are assessed and shown to be met. This process covers the entire system, including the airborne, communications and ground domains. [ECA1]

Failure Mode A condition in which a system or component is unable to fulfil its operational requirements.

Function The action for which a system is used.

Operational Approval A process by which an authorisation is given to an organisation to operate a system, sub-system or component approved for an operational data link service. [ECA1]

Regulatory Authority The organisation responsible for the issuing of approvals in accordance with statutory requirements. [ECA1]

Safety The state in which risk is lower than the upper limit of the acceptable risk. [ECA1]

Throughput The combination of the required transit delay with the maximum message length defines the peak throughput to be provided by the communication system to the application.

Transit Delay The maximum transit delay acceptable for a message to go from the sender to the receiver

Severity The extent of the consequences of a failure mode, either in terms of the inability to provide ATC or directly upon the degradation of aircraft safety.

2. Current Safety Assessment & Certification Work

2.1 Introduction

This section will identify the current work being undertaken by the airlines, Air Traffic Service (ATS) and communication service providers, equipment manufacturers and regulators to develop safety assessment and certification methodologies. The work will result in new standards and guidance material to aid the ATC community in implementing and operating data link based communications. The importance of each study and the relevance to this work package (WP223) is assessed.

2.2 EUROCAE WG 53/RTCA 189 Activities

2.2.1 Background

The European Organisation For Civil Aviation Equipment (EUROCAE) is an international organisation with members representing users and manufacturers of aeronautical equipment and civil aviation administrations. The organisation's objectives are directed to the preparation of specifications and guidance material for civil aviation equipment. EUROCAE work closely with RTCA Inc (Requirements and Technical Concepts for Aviation) to ensure the organisation's recommendations can be adopted not only in Europe but world-wide.

WG53 was established by EUROCAE in September 1996 "to develop guidance material defining the safety and interoperability requirements for Air Traffic Services supported by data communications" [ECA2]. WG53 has representatives from aircraft and avionics manufacturers, ATC Service Providers and the Civil Aviation Authorities. There are 3 sub-groups and a CAA Advisory Group (CAG) each with their own area of responsibility:

- Sub-Group 1 - Interoperability
- Sub-Group 2 - Safety
- Sub-Group 3 - Performance
- CAA Advisory Group (CAG)

2.2.2 EUROCAE WG 53 Objectives

The objective of the Joint Working Group (JWG) is to develop the appropriate guidance material for presentation to the ATC community by October 1999. This guidance material will consist of documentation from the three Sub-Groups (SG).

SG1 - aims to produce three interoperability documents covering FANS-1/A, ARINC 623 and the ATN.

SG2 - aims to develop generic safety documentation which can then be applied to specific environments, e.g. the North Atlantic.

SG3 - aims to address communication performance.

CAG - The aim of the CAG, a creation of WG53/SC189, is to plan and prepare for recognition of the RTCA/EUROCAE publications in appropriate CAA documents. Additionally, the CAG may meet to resolve differences in policy and guidance across State boundaries and inconsistencies in commissioning of air traffic services, certification of aircraft, and operational approval. At this early stage no specific decisions have been made by the group which can be incorporated into the ACCESS work. The CAG will only be active during the lifetime of WG53/SC189.

The material produced by SG2 (Safety) is of particular interest to WP223 although interoperability and performance issues do impact upon the certification issues. The working papers of interest from WG53 include:

1. SG2 WP21 - CNS/ATM Safety Assessment Process
2. SG3 WP15 - QoS Maintenance and the Use of ATN for Safety Related Applications

Other working papers are planned but are not yet completed. These papers will provide guidance on how the certification and approval of end to end data link systems can be achieved.

2.2.2.1 Summary of SG2 WP21 - CNS/ATM Safety Assessment Process [ECA4]

This draft working paper provides an overview of the CNS/ATM safety assessment process proposed by WG53. The paper addresses the CNS/ATM operational environment from the underlying CNS/ATM infrastructure through to the aircraft, procedures and airspace characteristics in which the process will be applied. The process takes account of the scale of the CNS/ATM operations, namely inter-state and encompassing many organisations.

The methodology discussed in the working paper requires safety assessment techniques to be used to generate high level safety requirements for a specific implementation of the CNS/ATM system. These safety requirements are then mapped on to the sub-systems, procedures and airspace characteristics. The appropriate tools and techniques can then be used to demonstrate that the system meets the safety requirements and provides the appropriate level of assurance.

The process has taken account of the existing work that has been undertaken by international bodies in this area and the procedures adopted in individual states. The working paper proposes a series of recommendations including a “coordinated approach” to generate confidence in the operational use of the CNS/ATM system, and the development of metrics to ensure the acceptance criteria is consistent across the institutional boundaries.

2.2.2.2 Summary of SG3 WP15 - QoS Maintenance and the Use of ATN for Safety Related Applications [ECA5]

This working paper looks at an approach for certifying operational ATN based systems that separates the operational approval of the ATN communications Infrastructure (ACI) from the applications that will be hosted on the End Systems (ES). The benefits of this technique include not having to re-certify the ACI every time a new application is developed and implemented. The basis of the proposal is to demonstrate to the appropriate regulatory authorities and to its users that the ATN components meet specific ‘Quality of Service’ (QoS) targets. The document recommends the development of a ‘QoS Model’.

2.2.3 Relevance to ACCESS WP223

The ACCESS Final Report is due to be completed by the end of 1998 and it is unlikely that WG53 will produce any agreed proposals within this timeframe. However, it will be possible to compare the work in progress in WG53 with the other studies and provide an initial framework for WP223. In particular, the mapping of high level safety requirements onto component sub-systems can be used as a basis for further consideration in WP223.

2.3 EUROCAE WG45

2.3.1 Background

WG45 was established by EUROCAE to provide guidance material to the ATC community for the implementation of aeronautical data link services. The working group coordinated with the ‘Operational Development of Initial Applications of A/G Data Communications (ODIAC) Task Force to ensure the accuracy of the data link operational requirements listed in the guidance material. To date one document has been produced:

- EUROCAE WG45 - Guidance Material For The Establishment Of Data Link Supported ATS Services - Report ED-78 June 1997 [ECA1].

2.3.1.1 Summary of ED-78 Report

The document addresses the following topics:

1. The definition of a data link environment including applications, services and the communication media;
2. The requirements needed to design, manufacture and implement a data link service. Consideration is given to safety, QoS, operational and interoperability requirements;
3. The proposal of an end to end approval process. In particular guidance is provided on using the operational requirements to generate the data link service safety objectives and requirements.
4. Outlines the validation and verification techniques that should be adopted to ensure that all design and manufacturing requirements are met.

The process detailed in ED-78 begins with the generation and definition of the safety and interoperability requirements for the overall system. These requirements are then allocated, firstly into domain requirements, e.g. airborne and ground, and finally sub-system requirements. The sub-system requirements will then need to be proven, once this is achieved the implementor will be free to develop specific implementations of particular sub-systems and verify and approve them independently. This process will ensure the overall system still meets its performance and dependability[1] requirements. The document is well established.

2.3.2 Relevance to ACCESS WP223

EUROCAE ED-78 is currently the only completed document addressing the end to end approval of data link systems and the applications that will provide the ATM operational functions. ED-78 will provide guidance on “supporting the end to end certification and/or approval of data link based systems for Air Traffic Management (ATM) purposes” [ECA1]. ED-78 assumes that the aircraft avionics cannot be certified and approved for operational use independently of the data link infrastructure and ATS end systems in which it operates. The document is specific to ATM data link services as identified within European Airspace however, the safety methodologies developed can be applied equally to any data link service, and to any ATM application in any region of the world.

Supplementary documents also produced by WG45 include:

- EUROCAE WG45 - ACARS Departure Clearance - ED85
- EUROCAE WG45 - ATIS - ED89

These may provide additional background information for performance, interoperability and safety requirements regarding the airborne, network and ATS domains. However no formal review of these documents has been undertaken by the ACCESS project.

[1] Dependability is a generic term covering availability, reliability and maintainability.

2.4 Common American European Reference ATN Facility (CAERAF)

2.4.1 Background

The Common American European Reference ATN Facility (CAERAF) is a joint project being undertaken by Eurocontrol and the ATNSI consortium. The project is based upon the requirements developed independently by both parties for ATN testing systems. Eurocontrol were developing a Reference ATN Facility (RAF) of their own with the ATNSI consortium developing a Conformance Test Suite (CTS) and a ‘Router Reference Implementation’ (RRI). In an attempt to share the costs and to avoid unnecessary duplication, an agreement was reached by both parties to participate in a joint development and work to a joint specification. Typical users of the system will be ‘developers, users and safety regulators of ATN services and equipment’ [EUR9].

2.4.2 Objectives

The scope of the CAERAF extends beyond that of the RAF to meet as a minimum the objectives and requirements of the RAF and CTS projects. The main objective is to deliver a system that will “support the US and European approval, certification and commissioning process of operational ATN avionics and ground based ATN systems”[EUR 9].

2.4.3 Relevance to ACCESS WP223

The safety assessment and approval process for airborne and ground systems will need to be well defined if end to end approval is to be gained for ATN systems from the regulatory bodies. The CAERAF work will form part of the safety assessment process. This can be achieved by utilising the CAERAF facility to provide the necessary evidence that a “potential” ATN system is suitable for operational use by demonstrating its interoperability and its behaviour under normal and abnormal scenarios.

The CAERAF will also impact upon the development of any ATN related guidance material e.g. EUROCAE WG 53/RTCA 189 Sub-Groups (see section 2.3), and if possible, comply with any guidelines or requirements concerning the testing of ATN systems.

The aim of the CAERAF project team is to provide tools which will aid ATM operators in the certification and operational approval process of ATN systems. The tools will not certify the systems under test as safe or suitable for operational use, merely provide a first step in gaining approval from the regulatory bodies. A crucial part of this work will be the recognition and approval of the CAERAF by the safety regulation authorities.

2.5 The Pro-ATN Project

2.5.1 Background to ProATN

The **Pro**totype **A**eronautical **T**elecommunications **N**etwork (ProATN) project has as its objective the development and demonstration of a pre-operational and certifiable prototype ATN in the European region. The work of ProATN is to produce hardware and software to recognised methodologies and/or guidelines (e.g. Standard DO-178-B or IEC 16508) for the development of systems. It does not provide direct safety assurance of system safety but can, when combined with other evidence, be used to demonstrate to a certifying authority that the system is safe for operational use. ProATN is linked to the EOLIA project which is developing data link applications for Air Traffic Management (ATM).

The ProATN project is divided into two parts and within these parts there are nine work packages, four in Part 1 and five in Part 2. NATS is a ProATN consortium member and has a responsibility to produce elements of work from these work packages to ensure ProATN meets its objectives. It is the documents that have been produced as part of the 'Requirements Analysis' work package (ProATN - Part 1) that are of interest to the ACCESS Study WP223:

1. 'A Review of the Safety Aspects of the ProATN' Version 0.2 (Q3 98) [CEC11]
2. ProATN Certification Requirements Study 'Safety Case Requirements' Version 0.A - 11/09/98 [CEC15]

2.5.2 A Review of the Safety Aspects of the ProATN [CEC 11]

2.5.2.1 Document Overview

The scope of the document is to review current standards "for the certification of safety critical systems" and address "the work that must be undertaken to assess an ATN". The first part of this work is an initial Failure Modes and Effects Analysis (FMEA). It is envisaged that the FMEA could be used to guide the initial system design and be used as part of the safety assessment process once the ProATN and its use are more fully defined.

2.5.2.2 Document Methodology

The report author has identified a number of methodologies developed by ATS providers to provide safety assessment assurance; these include the NATS Safety Management Manual and Guidance Material for the Establishment of Data Link Supported ATS Services (ED-78 see section 2.3). Features common to these methodologies include the allocating of graded 'severity levels' to the identified system failure modes. These severity levels are a measure of the failure modes impact upon the aircraft and the ATC service provided. The failure modes are identified by examining the "system hardware and software, the Human Machine Interfaces (HMI), ATC and ATM procedures, system operators and the availability of the back-up systems".

The methodology used to develop the initial FMEA was based upon these techniques and involved the breakdown of the ProATN into its subsystems and components; the allocation of functions to each component and the identification of the failure modes and the severity of those failure modes associated with each component.

2.5.3 Safety Case Requirements [CEC15]

2.5.3.1 Document Overview

The document aims to capture the safety assessment and certification requirements that will need to be applied to ProATN system development to ensure it achieves an acceptable level of safety performance in operation. The approach adopted describes the safety assessment methodology (including the definition and apportionment of the safety requirements) and details the current mechanisms (e.g. certification and safety cases)used to approve avionics and ground based equipment. The importance of an adequate system design process is emphasized to ensure the safety requirements are met.

The final document will produce a series of recommendations for implementing ATN systems in general and ProATN specifically.

2.5.4 Relevance to ACCESS WP223

One of the objectives of ACCESS WP223 is to identify safety assessment techniques and the preliminary work undertaken by the ProATN consortium falls into this category. [CEC11] describes the FMEA process and can be developed further once the system description and operating environment are defined. It will also make system designers aware of the "level of safety assurance that may be required from each component".

[CEC15] describes in detail the derivation of the safety requirements and the processes required throughout the system development and implementation lifecycle to ensure these requirements are met. The document will complement WP223 which considers the application of given safety requirements to the ACCESS environment.

2.6 EOLIA

2.6.1 Background to EOLIA

The '**E**uropean Pre-**O**perational Data **Li**nk **A**pplications' (EOLIA) project is sponsored by the CEC and run as a consortium with six main partners - Aerospatiale, NATS, NLR, Thomson Airsys, Sofreavia and Airbus Industrie. The objective of the EOLIA project "is to define, develop, and demonstrate several data link services for air traffic control applications". As part of this work the EOLIA consortium is required to document "a preliminary analysis of the potential safety implications of the defined services which are being developed under the EOLIA project". To date two documents have been produced:

1. EOLIA Safety Benefits Report - A Preliminary Safety Assessment of EOLIA Datalink Services - Ref EOL/WP2/NATS/050/D22/C/1. [CEC12]
2. EOLIA Safety Benefits Report - A Preliminary Safety Assessment of two EOLIA Datalink Services: ATIS and DSC - Ref EOL/WP2/NATS/069/DE22/C/0.A. [CEC13]

2.6.2 EOLIA Safety Benefits Report - A Preliminary Safety Assessment of EOLIA Datalink Services [CEC12]

2.6.2.1 Document Overview

The first document looks at four of the services identified by the EOLIA project. They are ATC Clearances (ACL), ATC Communications Management (ACM), Dynamic Route Availability (DYNAV) and Flight Plan Consistency (FLIPCY). The document does not intend to develop fully certifiable applications, however there is a requirement for EOLIA to provide assurance that the current level of safety is maintained or enhanced prior to the introduction of the data link services. As part of the safety assurance work EOLIA developed Work Package 2.2 to generate an initial safety analysis to identify the risks associated with introducing data link services. The Work Package also addressed the need for an agreed international standard for the approval of data link services by the regulatory bodies. This is currently the major obstacle associated with the safety assessment and certification of data link services. This document therefore has two main objectives:

1. To compare the risks associated with the data link service against those risks inherent in the current R/T (Radiotelephony) procedures. (Safety Analysis Methodology)
2. To review software standards applicable to data link service development. (Review of Software Standards).

2.6.2.1.1 Safety Analysis Methodology

The report authors used the following three steps as the cornerstone for the safety analysis methodology:

Scenario Definition and Hazard Identification - The first task was the definition of a set of operational scenarios to allow the generation of a "comprehensive and representative set of hazards".

Fault Tree Analysis, Influence Diagram and Severity Categorisation - These techniques were used to look at the identified hazards in terms of causes and initiating events. This was followed by a hazard impact assessment on the data link service and finally determining how to recover from or mitigate the hazard. The risk of the data link hazards were categorised as ‘the same as’, ‘greater than’ or ‘less than’ the equivalent risk with current R/T procedures.

Comparison with Current Procedures - Using the data generated from the work above it was possible to compare the risks associated with the EOLIA data link services and the current R/T procedures.

2.6.2.1.2 Review of Software Standards

The second objective of the report was to assess the suitability of current software standards to allow the development of end to end systems containing an air/ground data path. The software standard, if it existed, would provide assurance that best practice had been adhered to during the design and development processes.

The need for this review stems from software standards only being specified for airborne systems and not for the ATC software used by the ground systems. There is a risk that the regulating authority will not certify the system for operational use because the safety assurance for the ATC ground system software is insufficient. The intention is to review the current software standards to determine if any could, when combined with other evidence, be used to demonstrate to a certifying authority that the system is safe for operational use. Thus improving the chance of ATC systems being approved by the regulatory bodies.

The work aims to identify features that are desirable in a standard and which could be applied in the development of data link software. In order to assess a standards suitability it was necessary to identify suitable criteria to allow a comparison of the selected standards. The criteria falls into three categories: safety, technical and regulatory.

The safety criteria was further developed to detail the minimum requirements the standard would need to include e.g. software safety categories used.

The report considered two standards which the authors feel would closely meet the requirements for ATC data link systems. The standards in question are DO-178B (1992) ‘ Software Considerations in Airborne Systems and Equipment Certification’. This document provides guidelines for “the production of software for airborne systems and equipment used on aircraft or engines”. The second standard is IEC 16508 ‘Functional Safety - Safety Related Systems’ it is not specific to any one domain and it covers software, electrical, electronic and programmable electronic systems. A comparison between the two standards and the minimum safety requirements was then undertaken.

It should be noted that a new sub-group (CNS/ATM SG) within the SC190/WG52 has been created and tasked with the qualification of ground software. No results are currently available from this work.

2.6.3 EOLIA Safety Benefits Report - A Preliminary Safety Assessment of two EOLIA Datalink Services: ATIS and DSC [CEC13]

This document follows a similar approach to [CEC12] and covers two further EOLIA data link services Automatic Terminal Information Service (ATIS) and Downstream Clearance (DSC). Although the services are different the methodology used to provide the risk analysis is similar and so it was not deemed necessary to address this issue further.

2.6.4 Relevance to ACCESS WP223

The EOLIA Safety Analysis is not a full risk assessment but does provide an insight into the techniques and the risks associated with data link applications. The report makes recommendations for further work that can be undertaken to mitigate and further reduce the risk associated with the data link services. These are important steps in the risk management process and may well provide the required safety assurance needed to demonstrate a data link application's suitability for operational use.

The Software Standard Review showed that no single standard met all the safety, technical and regulatory requirements. The report recommends cooperation with the European Regulatory Authorities to determine how the approvals process for data link systems will operate and secondly, the development of an internationally agreed standard for data link type systems. This standard could be based upon DO-178-B and IEC 16508.

2.7 NATIMG & CADAG

2.7.1 Background to NATIMG and CADAG

The North Atlantic Implementation Group (NATIMG) was established in January 1994. The group was created to coordinate and manage, on behalf of the NATSPG, the NAT Implementation Plan. The plan identifies and prioritises the development objectives for the North Atlantic (NAT) Region up to the year 2015.

The CADAG (Communications Automation and Datalink Applications Group) is a technical working group that reports to the NATIMG. The working group is responsible for:

1. Establishing the requirements for harmonisation of Flight Data Processing Systems within the NAT Region.
2. Defining the operational communications requirements of the NAT CNS/ATM sub-systems as they relate to the existing networks e.g. AFTN and there transition to the ATN.
3. Developing methods to monitor future communications infrastructure.

As part of this work CADAG has addressed the safety implications of introducing a data link environment into the NAT. At the fourth CADAG meeting held in Shannon in June 1996 a working paper was presented by NATS called 'CADAG Safety Concept Proposals' [CAD1]. The paper looked at proposals "for establishing the safety management concepts and approach to be adopted in the North Atlantic Data Link Programme". The paper considered related work being undertaken, in particular the proposals made by EUROCAE WG45 (See section 2.3).

2.7.2 Document Overview

The working paper proposes a practical approach to the management of safety, in particular the need to be consistent with other data link programmes, timescales permitting. It recommends that the CADAG approach should be based on EUROCAE ED-78. This being the most advanced of the safety initiatives consulted at the time (Q2 96).

In the timeframe considered it was not possible to develop a single standard or recommended practice that could be used, for both the airborne and ground domains of the data link system. The alternative is to adopt two approaches, one for the airborne systems and one for the ground based systems. The systems in the airborne domain would use current regulations and standards e.g. JAR25.1309 and RTCA/DO-178B. The ground domain, for which no agreed standards currently exist could use standard IEC 16508; a standard which is being considered for ATC ground systems. The paper proposes this dual approach as an interim measure until the development of a common standard or agreed practice for end to end data link systems. It is crucial that the two domains can be linked together to permit an overall system assessment. This will require two things:

1. Coordination between the two domains;
2. A well defined and agreed mapping between the hazard severity classes for each domain.

The paper goes on to propose an approval process for ‘End to End Certification’ describing the importance of providing safety assurance to the air space users and the ATC service providers.

The certification of equipment should be sufficiently defined to allow avionics suppliers and the Civil Aviation Authorities to demonstrate to air space users that the Air Traffic Service (ATS) meets or exceeds the target levels of safety for that region. The certifying of avionics will still be approved using the appropriate standards and requirements e.g. JAR 25.

The paper proposes that CADAG acts as the coordinating body for the NAT Region to ensure that certifying authorities provide a consistent approach when applying the certifying requirements.

2.7.3 Relevance to ACCESS WP223

The issues raised and the techniques developed are generic in nature and can be applied to different regions of airspace. The paper was presented over two years ago and further work has been undertaken since; even so, it is only the WG45 report (ED-78) that is available to provide implementors with any approved guidance material. The paper provides an interim solution that can be adopted until an agreed international standard is available for data link implementors. The need for a coordinating body for the NAT region is recommended. This would ensure a ‘custodian’ group, with the appropriate representatives, is in place to guide and coordinate activities such as working groups. The recommendation could be adopted by other areas, e.g. ECAC Region.

2.8 Additional Studies

The European Air Traffic Control Harmonisation and Integration Programme (EATCHIP) is developing a safety assessment methodology. The documentation entitled ‘Air Navigation system Safety Assessment Methodology (ref -SAF.ET1.ST03.1000-MAN-01-00) is currently at Issue 0.4. An amended version is expected in Spring 1999. The document may provide additional background information but has not been formally reviewed by the ACCESS project.

2.9 Common Trends

2.9.1 Introduction

The advent of end to end data link technology and services in the ATC environment requires that the users of the technology and services provide the necessary safety assurances to the regulatory bodies prior to their certification and approval for operational use. This has resulted in a range of projects being initiated, projects whose specific aim is to provide guidance and develop ‘tools’ to support the approval of such systems into operational service. A selection of this work has been detailed in section 2.

This section will highlight the main recommendations from section 2 and group them into distinct categories. These categories can be used as a basis for providing safety assurance and identifying important issues that need to be addressed.

2.9.2 Main Issues Arising from Section 2

1. Standards and Guidance

Safety regulators must approve and recognise the use of test facilities such as CAERAF as an acceptable means of providing evidence of a components interoperability and performance functionality.

Cooperation is required between the regulatory authorities as to the role standards will take in the approval and certification of data link systems, and the development of an internationally agreed standard.

The development of generic safety documentation for end to end approval process for data link systems is required.

Guidance to generate data link service safety objectives and requirements from the operational requirements is necessary.

2. Techniques

FMEA analysis can be used to highlight the safety criticality of services and to quantify the level of safety assurance required for each system component

3. Methodologies

The separation of the operational infrastructure certification from the application certification is one possible approach. This will necessitate the development of agreed QoS targets for the technical infrastructure.

Safety Assessment techniques to generate high level safety requirements will allow the mapping of the safety requirements on to the sub-systems, procedures and airspace characteristics.

The forming of Scenarios and Hazard Identification, Analysis and categorisation of hazards can allow the comparison of the results with current non data link procedures.

An assessment of all the system elements e.g. hardware and ATM procedures should be included in the overall system assessment.

Safety and interoperability requirements can be defined for the overall system and then allocated to the sub-systems. A necessary requirement for the completion of this process is the definition of the system description and the operating environment.

4. Tools

The CAERAF facility could assist in providing evidence that an ATN system is suitable for operational use. **Note: It will not certify the system as safe.**

The development of consistent acceptance criteria is important to ensure multi-State applicability of the ATN systems environment.

2.9.3 Conclusions

The work identifies a number of key aspects to support certification. In particular, one approach is to develop specific implementations of the system components, e.g. routers, and verify and approve them using agreed standards and methodologies. The components, providing they gain certification approval, can then be introduced into the end to end system without the need to re-certify the existing components. All the work reviewed detailed the importance of considering the institutional issues and to account for the scale of the CNS/ATM operations, i.e. it will encompass many States and Organisations. A number of important issues still require further resolution to allow the process to proceed.

3. State Procedures

3.1 Introduction

This section will outline some of the procedures and mechanisms used by Air Traffic Service Providers and equipment/avionics manufacturers, in demonstrating that a safety related system is safe to be introduced into operational service. The procedures have been developed to provide assurance to the Regulatory Authorities that the potential hazards of a new system have been identified and controlled.

In section 1.3.2 two mechanisms were identified for the safety assessment and approval of equipment these are certification and the safety case. The safety case is generally applied to ground based systems and the certification process is generally applied to avionics equipment only. The former is usually the documented evidence of adherence to an approved safety management system. A key issue will be the successful integration of the two approaches to develop the necessary methodologies for safety assurance on an end-to-end basis.

3.2 National Safety Management Systems

The current procedures developed by many States rely on the adoption, by the ATS provider, of a formal Safety Management System with individual States applying their own adaptations of the Safety Management process. Safety Management allows organisations to implement an effective safety policy and to achieve high standards of safety thus minimising the risks as far as is reasonably practicable. The majority of States already use the ‘Safety Case’ methodology as the focus of their Safety Management System.

The ‘Safety Case’ methodology covers all the lifecycle phases of the safety related system from design through to its use in operational service. The safety case defines the system safety requirements and presents the evidence, arguments and assumptions used to show the degree of compliance with the safety requirements; it is a ‘living’ document responding to changes and modifications in the target system.

The ATS Provider uses the completed ‘Safety Case’ to provide assurance to the managers who will be responsible for the system, and to the regulating bodies who will be responsible for approving the system, that it is safe for introduction into operational service.

The discussion so far has primarily focused on the ATS Provider and the avionics equipment manufacturers but has not addressed the procedures governing Third Party Service Providers (TPSP). This is an important issue given that many TPSPs are aiming to support operational ATC safety critical services. The procedure for TPSP will be no different than for the ATS Providers; they will need to demonstrate the safety of their systems, via documented evidence e.g. ‘Safety Case’, to the relevant aviation safety regulatory authority in support of their application to obtain approval to use the system in an operational environment.

The TPSP will then be entitled to offer its approved system(s) for operational use within the parameters defined by the safety case. An ATS Provider could then enter into a Service Level Agreement (SLA) with the TPSP.

The agreement might involve the TPSP supplying the ATS provider with a satellite service. This satellite service would typically be one ‘sub-system’ in a larger end to end system providing a communication’s path between the ATS Provider and suitably equipped aircraft. In the event of an incident resulting from a failure of the TPSP’s system the accountability for that incident would still rest with the ATS Provider. The liability issue is more complex and would need to be clearly defined in an SLA. (See WP220).

3.3 Equipment Certification Process

The certification process is aimed at obtaining official approval from the airworthiness authority that the avionics equipment complies with the regulatory requirements. This process is administered by individual states working to at least the baseline target requirements set by ICAO [CEC15].

To minimise the duplication of effort by European States an organisation called the Joint Aviation Authority (JAA) was formed. The JAA is an associated body of the European Civil Aviation Community (ECAC) comprising the aviation regulatory authorities of 27 countries . The purpose of the JAA is to produce common Joint Aviation Requirements (JARs) to facilitate certification of products built jointly in Europe, and .the consistent application of those agreed procedures.

The JAA is an integral part of the certification process for avionics manufacturers. Any component which is to be placed onto the airframe must undergo a safety assessment and if demonstrated to have an impact on aircraft safety will need to meet the design and testing requirements mandated by the JAA.

The equivalent body in the United States is the Federal Aviation Authority (FAA) who have developed Federal Aviation Regulations (FARs) to set minimum requirements upon the avionics equipment.

3.4 Conclusions

The procedures identified in this section highlight the role of State’s Safety Management Systems and of international regulatory activities in the certification and safety assurance of operational systems. In particular it is important that any new standards and guidance material developed to address the safety implications of data link services are recognised by the regulating authorities and organisations such as the JAA. Furthermore, it is important that developing standards and guidance material are harmonised with the Safety Management framework currently used by the States.

4. ACCESS Issues

4.1 Introduction

The information provided so far has been generic, highlighting developing methodologies and current procedures that address the safety assessment and certification of air-ground data link systems. This section aims to use this work and apply it to the air-ground and ground-ground data link systems that may be used in the ACCESS Region. This section will describe the component elements of the data link system and, where applicable, apply the methodologies and procedures identified in section 2 to generate recommendations for their certification. In addition, the recommendations will be applied to the expected ATN evolution as defined in the ACCESS study.

4.2 Proposed ACCESS Safety Methodology

There are two issues to be considered, the first is the evolutionary nature of the ATN architecture and the second is the development of new data link services; both imply change and as a result have implications for the safety assessment and certification of the data link systems of which they form a part. A perceived benefit of the ATN is that it will provide its users with a reliable and resilient communications network upon which data link applications will provide the functionality to develop Air Traffic Management (ATM) data link services. The implementors and users do not want to be constantly re-certifying systems and services.

The proposed ACCESS safety methodology is to separate the safety approval of the ATN Communications Infrastructure (ACI)[2] from that of the ATN applications and data link services supported. The ACI safety and performance requirements are then related to QoS requirements. This technique has already been proposed in [ECA5] and would require that the ATN components, e.g. routers, can meet specific ‘Quality of Service’ (QoS) targets.

In addition, the methodology recommends the development of a Data Link Application & System Document (DLASD) as defined in [ECA1] to generate the collection of all the requirements that accurately define the data link system supporting the data link services. A detailed description of the purpose of the DLASD is found in [CEC11]. One function of the document is the development of safety objectives and the generation of safety requirements for the airborne, communications and ATS domains. The safety requirements will be developed from standard safety assessment techniques, e.g. FMEA. This was based upon the work developed by ProATN and involved the breakdown of the data link system into its subsystems and components; the allocation of functions to each component and the identification of the failure modes and the severity of those failure modes associated with each component. This provides safety requirements for individual system components.

4.2.1 Quality of Service (QoS)

In general the Quality of Service (QoS) can be defined as the “totality of features, characteristics and procedures that bear on the ability of a system or service to satisfy stated or implied requirements” [ECA1]. QoS is and can be used to specify the performance of the system or service. The ICAO Manual of ATS Data Link Applications [ICA4] details general performance requirements for CNS/ATM applications in terms of <u>Availability, Integrity,</u>

[2] ACI is the ATN communications stack up to and including the application entity; it does not include the application process.

Reliability and Continuity. These requirements are defined in terms of target QoS parameters. This technique can be equally applicable to the apportionment of safety requirements to QoS targets within the ACI. The operational performance of a system or service will also be influenced by operational factors such as separation minima and traffic density and these can lead to additional target QoS parameters e.g. transit time.

[A202] recommends that Transit Delay and Throughput are useful criteria for defining the QoS. These parameters will allow QoS values to be determined for the ATN Communications Infrastructure (ACI) which can provide data link services with the appropriate level of safety and performance . It will be necessary to validate any definition of QoS and the selected QoS parameters.

The ACI can then be defined in terms of QoS capabilities which can be applied in two ways:

1. Quantifiable parameters which can fulfil the QoS needs of each data link service;

2. A measurable target which can be assured through appropriate methodologies for the design , development, implementation and operation of the ATN Communications Infrastructure (ACI).

Recommendation 1: Separate the certification of the ATN Communications Infrastructure (ACI) from the end-to-end data link services. Define QoS targets for the ATN communications service provided.

Recommendation 2: The QoS provided by the ACI can be defined using the following parameters: Availability, Continuity, Integrity, Reliability, Throughput and Transit Delay. Any definition of QoS and associated parameters will need to be validated.

4.3 ATN Data Link Services

A data link service is defined as a set of ATM related transactions, both system supported and manual, which have a clearly defined operational goal and begin and end on an operational event. The ATN will enable ATS Providers to provide data link users with a range of data link services that will provide a safe and reliable alternative to R/T procedures, and new data link services which will provide additional benefits and flexibility in the ATM system. These data link services will be derived from operational requirements and will use the underlying ATN data link applications, ATN end systems and ATN Communications Infrastructure.

[A202] describes a range of data link services that could be introduced into the ACCESS area. The work assesses the suitability of each service using criteria such as ‘operational benefit’, standardisation status, criticality of data link services and suitability of data link sub-networks. [A202] states that most ATS Providers are likely to introduce only non-critical data link services offering the most user benefit in the early implementations for European airspace. The deployment of a coherent ATN architecture could be used as the starting point for implementing less critical services such as ‘Data Link Operational Terminal Information Service (D-OTIS). This would form the foundations upon which the ACCESS target ATN architecture, as defined in [A203], would evolve and with it more sophisticated and safety critical data link services.

The ATN Implementation Task Force (ATNI-TF) has produced a draft European ATN Implementation Plan [EUR9] that aims to describe the deployment and provision of ATN equipment and data link services in the EUR Region. As part of this work the report identifies a range of ATN compliant data link services which may be provided by ATSOs to ATN equipped aircraft. The report uses criteria such as traffic density, deployment timeframe and geographical scope to categorise the identified data link services. The latter parameter has implications for safety assessment and certification given that some data link services are ‘local’ and others are ‘wide’ area services. The report provides definitions of these terms to clarify the scope of each.

Local Data Link Services - These services “may be deployed in a limited geographical area such as an airport or flight information region (FIR) and autonomously, i.e. no coordination or overlap of service coverage with adjacent areas, provide full benefits to the service users.

The Departure Clearance is a local area data link service which can be offered at airports and provide the full benefit without it being implemented throughout the EUR Region. There are some local services which require a minimum level of equipped aircraft before opportunities for service improvements and benefits become available. ADS Position reporting is such a service. The local services without such a minimum threshold are the most likely candidates for early deployment.

Area-Wide Data Link Services - These services “require a geographical service coverage which should stretch along the total flight path, in order to accrue full benefits from using the service”

The ATC Communications Management (ACM) service is a wide area data link service. This service would ideally involve all ATSUs along the total flight path i.e. from the departure to the arrival of the flight [EUR9]. This is more difficult to implement than the local services as it requires coordination between the different ATC service providers. Such services are likely to be introduced between adjacent states or in a core area such as that identified in the ACCESS study.

In addition, it will be easier to introduce the local area services with a low safety criticality. [A202] has proposed candidate data link services for the Initial European ATN based upon work described in [EAT13].

Any data link service will only be certified for operational use if the underlying ACI can meet the data link service safety and performance requirements. The operational concept and the service definition can be used to derive the safety criticality of the service.

It is important to note that various levels of QoS will be available throughout the ACI and that the appropriate level should be selected to meet the requirements of each data link service, according to its environment.

4.4 ATN Data Link Applications

The ATN data link applications, e.g. ADS, provide the communications functionality in the end systems which support the data link services. The ADS Panel [ICA4] has defined a range of application performance and transfer delay requirements reflecting their use in different operational environments.

The specific data link service will ensure appropriate safety and performance requirements to be defined. These need to be mapped onto the applications utilised by the service. The data link applications are detailed in the ATN SARPs which have been validated with experimental trials (ADS Europe) having provided valuable real time verification of the SARPs. The ATN applications are assumed to be separate from the ATN data link service and the ACI. They do not form part of the ACI and are not developed as QoS requirements. The development of the application software has been considered as part of the ES development and as such the same recommendations will apply.

Recommendation 3: Ensure the ACI QoS meets the level required to safely operate the data link service.

4.5 ATN End Systems

The ATN End System (ES) contains the seven OSI layers in its protocol stack, one or more end user application processes and an HMI interface. This provides the ATN ES with the capability to communicate with other ATN ESs to provide end to end communication services to ATN applications. The ACCESS approach only considers the ACI it does not address the user processes or the Human Machine Interface (HMI). The ATN ES must meet the overall operational performance requirements. The operational performance requirements placed upon the ES need to be apportioned on the basis of total end to end transit delay between the ultimate end users e.g. the controller and the pilot. The ATN end to end transit delay i.e. the time delay from the top of one ES stack to the top of the destination ES stack is assumed to account for 90% of this total end-to-end transit delay time [ICA16]. Thus if the ES's are to meet the performance requirements for a particular ATSC Class of traffic then each ES will be apportioned approximately 5% of the total available time to complete application processes and present the data to the user via the HMI. The safety requirements will include some performance criteria, e.g. transit delay, and these apportionment rules need to be considered in any design assessment against safety objectives.

The owners of the ES will be responsible for demonstrating that their system can support the overall performance and safety targets required to use the ES operationally. It is expected that new ES's will be designed and built using recognised standards (for hardware and software). Rigorous testing will be required to obtain failure rates and to demonstrate it is safe to use within the selected operating environment. The testing of the finished product with a reference facility such as CAERAF could be used to demonstrate interoperability and behaviour under abnormal conditions.

The high QoS that can be achieved by the ACI is a result of its distributed nature which eliminates all single points of failure. Clearly ES design needs to provide levels of availability commensurate with the performance requirements of the ES application to take full advantage of the capabilities of the ACI.

Recommendation 4. The apportionment of transit delays between ATN ESs of the ACI should be based on the 'System Level Requirements of the ATN SARPs' [ICA16].

Recommendation 5. Provide evidence of safety assurance for the End System using best practice, recognised standards and rigorous testing to include comparison to a 'recognised' reference to ensure interoperability. This will include the application software.

4.6 ATN Communications Infrastructure (ACI)

Once the ACI is 'separated' from the operational datalink services, it will be necessary to map the detailed safety requirements that exist for the data link services into safety requirements for the ACI. The network designers/administrators are responsible for designing and implementing a network that will meet the QoS requirements of the ATN data link services that use it. The ACI would need to meet these requirements as a minimum and support network management techniques to monitor and maintain the appropriate QoS for the data link services in order for it to be approved and certified. The ACI in effect would provide users with a well defined and reliable level of service appropriate for their needs.

The technique of separating the ACI from the services will make it easier for users to bring on line new services. The ACI will still be an important component in the safety assessment process since it still needs to provide its 'users' with an appropriate QoS as a sub-system contained 'within' the end to end data link system.

The ACI sub-system itself consists of components such as routers and subnetworks whose design can be demonstrated to meet the stringent QoS requirements as part of the safety assurance process. An important part of the safety assessment work will be to map the high level safety requirements on to the sub-system components and identify hazards and their severity. This information should allow the generation of QoS targets for the components so that they can provide and maintain the QoS required for the ACI. In order to provide the assurance needed for operational approval a number of measures have been identified for each component. The performance of the ACI would need to be better than that required for the overall data link service. Clearly this would need to be reflected in the target parameters for the QoS.

Recommendation 6: The overall QoS of the ACI should be derived from its individual components and their interaction architecture.

4.6.1 Routers

The ATN routers provide the connectivity to the various subnetworks and route messages across the appropriate subnetworks based on criteria such as requested class of service and availability of suitable routes. Routers will be located on the ground and aboard aircraft.

In order for the router component to provide the safety assurance needed for operational approval a number of measures can be adopted. These measures should begin in the router product development stages. A summary is provided below:

1. The development of router hardware and software should use recognised best practice as defined in standards such as IEC 16508 and DO-178B.

2. The rigorous testing of the finished product to determine failure rates and availabilities. This can provide a demonstrated level of performance for the QoS.

3. Testing of the finished product with a reference facility such as CAERAF to demonstrate interoperability and reaction to abnormal conditions.

These factors will aid in the certification and approval of the router products for operational use and ensure they meet the QoS requirements for the ACI. Additional safety assurance may be required for the aircraft based router.

The techniques identified in recommendation 8 (e.g. best practice, recognised standards and rigorous testing) can be used for the router component to provide the appropriate safety assurance for the router for certification purposes.

4.6.2 Subnetworks

The subnetwork is an independent communications network based on a particular communication technology, e.g. X25 or Frame Relay, which is used to physically transfer information between ATN systems. The ATN systems can use the subnetworks to transfer the information between air/ground and ground/ground end systems.

The ACI will utilise existing data subnetworks and typically they will already be approved for transiting operational traffic and will either have a safety case describing the parameters of their operation and/or a reliable in service history to provide details of the achieved QoS. These factors will aid the approval of the subnetworks for operational use in a data link environment and ensure they meet the QoS requirements for the ACI. This process will also highlight any performance limitations of the subnetwork that may exist and may result in a subnetwork not being able to meet the data link service performance requirements.

The ATN has been designed to allow new subnetworks to be integrated into the ATN architecture. The new subnetworks will need to provide the necessary assurance that they can meet the QoS requirements for the ATN. This can be achieved using the safety case methodology described in section 3.2 to demonstrate that the subnetwork(s) can provide the QoS needed to support ATN data link services. TPSP will also need to develop safety cases to demonstrate that their networks are able to meet the stringent QoS targets needed to transit operational ATS traffic.

The performance limitations of alternative subnetworks are inherently different because of the technology used. Therefore the performance and safety requirements needed for a data link service should be mapped onto the subnetwork options to derive the most appropriate subnetwork. Where no suitable mapping is possible re-assessment of performance requirements and other mitigation options must be considered.

Recommendation 7: Provide evidence of safety assurance for the subnetworks using existing safety cases and/or in service history. The development of new safety cases may be required for TPSP owned systems.

Recommendation 8: A comparison of the performance requirements will identify the subnetworks suitable for the service. Where no suitable subnetwork exists, requirements should be reviewed and other mitigation steps considered.

4.6.3 Management of QoS

The safety assessment process will need to provide assurance that the QoS figures for the ACI are not only achievable but maintainable to any regulating authority. Therefore it will be necessary to implement mechanisms that can be used to monitor and maintain the QoS of the ACI. This can be achieved by utilising network and system management techniques to monitor continuously the QoS parameters and ensure that if operational changes need to be implemented this can be done in a controlled and timely manner and a safe service maintained. In the event the QoS cannot be maintained at or above the target level for an application for a defined period of time then the associated service should not be offered to the users. Fall-back procedures will need to be implemented to ensure separation standards are not compromised.

Recommendation 9: Monitor the ACI performance to ensure the QoS is achieved. Network and system management tools can be used for this purpose.

Recommendation 10: If QoS target level not maintained all applications whose target level is above the actual QoS should not be offered to users.

4.6.4 Configuration Management

Given the highly integrated nature of the end to end data link system any changes no matter how minor have the potential to adversely affect the end to end performance. The ADS Europe ‘97 report [CEC14] highlighted a number of important recommendations resulting from the ADS trials experience. In particular the report recommends the role of non-ATS Provider networks in the end-end system needs to be more clearly defined. There is the potential for problems if the TPSP undertakes modifications to their networks, e.g. software upgrades, without any ATS provider coordination. This may always be a problem given that the TPSP will also have non ATS customers and forms of mitigation may need to be in place if operational safety is not to be compromised. In practice the TPSP must provide assurances that any modifications which have the potential to impact upon the ATS provider service will not be implemented until testing has been undertaken. The change control process applies equally to ATS providers and the avionics manufacturers to ensure potential problems are identified prior to the introduction of any modifications or the introduction of new systems in to the operational environment.

To limit the impact of TPSP modifications upon the ATS operational service [CEC14] recommends that a service level agreement (SLA) should be in place between the ATS provider and the TPSP to support any operational ATS service. It recommends that as part of this SLA the TPSP will notify the ATS provider of any modifications that may affect the QoS of the data link service prior to its introduction.

Recommendation 11: Define more clearly the role of the TPSP in the end to end data link system and use an SLA to establish clear responsibilities for TPSP network performance.

4.7 Transition Phases for the ACCESS Region

The ACCESS study has identified three phases in the architectural development of the ATN in the ACCESS Region. The first phase describes the current state which consists of local implementations of data link services being used for trials purposes. An example of a local implementation is the Departure Clearance (DCL) service at Airports. The second phase is known as the "Initial European ATN" and is defined as the set of services necessary to justify the evolution of the local ATN deployment (phase 1) into a coherent ATN infrastructure in the ACCESS target area necessary to support those services. The "Target European ATN" is the final phase and is the target architecture for the ACCESS region. This phase is detailed in [A203] and describes a routing architecture centred around a European ATN Island containing a high level backbone that will carry both routing and data traffic. The European ATN Island can, if required, be further divided into smaller ATN Sub-Islands containing backbones which will connect to the high level backbone.

The safety assessment and certification methodology proposed for the ACCESS Area has been detailed and addresses all the components that form the data link system. This section will look at the three phases of ATN transition identified for the ACCESS Area and will outline how States can ensure the different phases of ATN deployment are approved for operational use.

4.7.1 Transition Phase 1: Local Implementations of ATN Data Link Services

This transition phase describes the current situation in many of the States in the ACCESS Area. The local implementation data link service describes a service in one FIR or one airport for example. It may be possible to introduce the service and its users to gain the full benefit of the service without the need to cooperate or coordinate with other States. The implementing State could provide the necessary safety assurance for the data link service using safety assessment procedures that are adopted by that State for other safety critical systems. The State would not need to provide assurance to other States only to its own regulating authority. In the event of a particular data link service being introduced by many States it would be beneficial for the later transition phases to coordinate and adopt consistent system acceptance criteria. This is one of the recommendations outlined in section 2.

4.7.2 Transition Phase 2: Initial European ATN

This phase describes the evolution from local implementations to a coherent infrastructure offering a range of data link services covering multiple FIRs and States. WP202 has identified a number of candidate air-ground and ground-ground data link services that will drive this evolution. Unlike phase 1 this phase will require coordination of safety activities such as the safety criticality of a particular data link service. The regulatory authorities will need to cooperate as to the role standards and tools such as CAERAF will play in the approval and certification of data link systems and services. This may require the development of an internationally agreed standard to cover specific implementations and to ensure that consistent system acceptance criteria is employed across the institutional boundaries.

Recommendation 12: Regulatory authority cooperation across international boundaries is necessary to ensure consistent acceptance criteria is employed for standards and reference tools.

4.7.3 Transition Phase 3: Target European ATN

The Target European ATN is the final phase of evolution and describes a routing architecture centred around a European ATN Island. The data link services offered will consist of those identified in phase 2 and may be the introduction of more safety critical data link services. The approval of new services will be no different than the approval procedures used for existing services with the exception that more States will be involved. There is the added benefit that the ATS Providers will be able to provide evidence as to the reliability of the ACI and the associated applications from an in service history as a result of phase 2.

5. Conclusions

5.1 Conclusions

The purpose of this work package has been to address the issues associated with the safety assessment and certification of implementing and operating the ATN in the ACCESS Region of Europe. This document has generated a series of practical recommendations based on the current approaches being adopted for the safety assessment and certification of data link systems. The methodology used has attempted to ensure the full benefits of data link can be achieved whilst still ensuring the operational service provided is safe.

The techniques and reference systems currently being developed by international bodies such as EUROCAE include that ATN data link services be assessed and certified as a separate entity to the ATN Communications Infrastructure (ACI). This ensures that new data link services can be developed and certified without the need to re-certify the underlying infrastructure. All data link services will evolve from operational requirements and will require a service criticality to be defined. This will be a measure of the ATM system's tolerance to a failure of that service and ensures that the underlying data link applications, e.g. ADS which provide the communications functionality in the end systems, have defined safety and performance requirements.

The safety requirements for ATN data link services can be translated into QoS requirements for the ATN Communications Infrastructure. These QoS requirements can then be distributed to the sub-systems e.g. routers and subnetworks which form the underlying infrastructure. Existing sub-systems such as communications subnetworks may need to rely on in-service history and safety cases to provide the required safety assurance. New sub-systems such as routers will need to be designed using best practice, recognised standards and incorporate rigorous testing to include a reference facility to ensure interoperability. In all cases adequate levels of redundancy and 'fall-back' procedures will need to be demonstrated as part of the safety assurance process.

In circumstances where a service is being provided by a third party the procedure will be no different than for the ATS Providers; the TPSP will need to demonstrate the safety of their systems, via documented evidence e.g. 'Safety Case', to the relevant aviation safety regulatory authority in support of their application to obtain certification for operational use of their system. The TPSP will then be entitled to offer its certified system(s) for operational use within the parameters defined by the certification. An ATS Provider could then enter into a Service Level Agreement (SLA) with the TPSP.

To ensure the data link service can be offered to data link users it will be necessary to monitor performance of the ACI QoS. This can be done using network and system management tools measuring recognised QoS parameters such as integrity and reliability.

The safety assessment process will need to demonstrate that the QoS figures for the ACI are not only achievable but maintainable to any regulating authority. Therefore it will be necessary to implement mechanisms that can be used to monitor and maintain the QoS of the ACI. This can be achieved by utilising network and system management techniques and ensure that if operational changes need to be implemented this can be done in a controlled and timely manner and a safe service maintained.

Once the operational approval has been granted it is still necessary to maintain the ACI QoS at the agreed target level for a particular service. In the event that the ACI QoS required to operate a safety critical application falls below the target level for a defined period of time then it may not be safe to operate that application. The ATS provider will not be certified to operate the application under these conditions resulting in the application not being offered. Fall-back procedures will need to be implemented until the QoS returns to the target level.

Given the highly integrated nature of the end to end data link system any changes no matter how minor have the potential to adversely affect the end to end performance. There is the potential for problems if the TPSP undertakes modifications to their networks, e.g. software upgrades without any ATS provider coordination. Any SLA should allow for the testing and assessing of modifications by the ATS provider to minimise the impact upon the operational ATS service.

There are three ACCESS transition phases, the first describes local implementation data link services which can be introduced by one state in isolation. It may be possible to provide the necessary safety assurance using existing procedures adopted for other safety critical systems. The State would not need to provide assurance to other States only to its own regulating authority. In the event of a particular data link service being introduced by many States it would be beneficial for the later transition phases to coordinate and adopt consistent system acceptance criteria.

The second phase describes a coherent infrastructure offering a range of data link services covering multiple FIRs and States. This phase will require coordination of safety activities e.g. the safety criticality of a particular data link service. The regulatory authorities will need to cooperate as to the role standards and tools such as CAERAF will take in the approval and certification of data link systems and services. This may require the development of an internationally agreed standard to cover specific implementations and metrics defined to ensure that consistent system acceptance criteria are employed across the institutional boundaries.

The final phase is the Target European ATN and describes a routing architecture centred around a European ATN Island. The data link services offered will consist of those identified in phase 2 and may be the introduction of more safety critical data link services. The approval of new services will be no different than the approval procedures used for existing services with the exception that more States will be involved. There is the added benefit that the ATS Providers will be able to provide evidence as to the reliability of the ACI and the associated applications from an in service history as a result of phase 2.

5.2 Further Work

1. Mixed airspace operation will generate more hazards; work will need to be done in this area to ensure the risks can be identified and mitigated.

6. ACRONYMS

ACI	ATN Communications Infrastructure
ACL	ATC Clearances
ACM	ATC Communications Management
ADS	Automatic Dependent Surveillance
AMSS	Aeronautical mobile Satellite Service
ATIS	Automatic Terminal Information System
ATN	Aeronautical Telecommunications Network
ATM	Air Traffic Management
ATS	Air Traffic Service
CADAG	Communication Automation and Data Link Applications Group
CAERAF	Common American European Reference ATN Facility
CNS/ATM	Communications, Navigation, Surveillance / Air Traffic Management
CPDLC	Controller Pilot Data Link Communications
DSC	Downstream Clearance
DYNAV	Dynamic Availability
EOLIA	European Pre-Operational Data Link Applications
EUROCAE	European Organisation for Civil Aviation Equipment
FHA	Functional Hazard Analysis
FLIPCY	Flight Plan Consistency
FMEA	Failure Modes & Effects Analysis
ICAO	International Civil Aviation Organisation
JAA	Joint Aviation Authority
JAR	Joint Aviation Requirements
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
NATIMG	North Atlantic Implementation Group
ODIAC	Operational Development of Initial Applications of Air/Ground Data Communications
ProATN	Prototype ATN
PSSA	Preliminary System Safety Assessment
QoS	Quality of Service
R/T	Radiotelephony
RTCA	Requirements & Technical Concepts for Aviation
SSA	System Safety Assessment
TPSP	Third Party Service Provider