AEEC
Together “We Set the Standard.”

To	Internet Protocol Suite (IPS) Subcommittee	**Date**	June 22, 2017
From	P. J. Prisaznuk pjp@sae-itc.org tel 1-240-334-2579	**Reference**	17-069/IPS-006 lth

Subject **Draft 1 of ARINC Project Paper 658:** *Internet Protocol Suite (IPS) for Aeronautical Safety Services – Roadmap Document*

Summary

The IPS Subcommittee is preparing an Industry Roadmap for ATN/IPS standards development. ATN/IPS has the potential to improve aviation safety services communication infrastructure. The guidance applies to air/ground communication and ground/ground communication.

ARINC Project Paper 658 is organized as follows:

Action This document will be reviewed by the IPS Subcommittee at its next meeting to be held July 25-27, 2017 in London, England. The ARINC Industry Activities staff invites comments on this document before July 14, 2017.

cc AGCS, AMX, DLK, NIS, SAI

SAE ITC
An SAE International Affiliate
16701 Melford Blvd., Suite 120, Bowie, Maryland 20715 USA
http://www.aviation-ia.com/aeec

SAE Industry Technologies Consortia (SAE ITC)
16701 Melford Blvd., Suite 120
Bowie, Maryland 20715 USA

DRAFT 1
OF
ARINC PROJECT PAPER 658
INTERNET PROTOCOL SUITE (IPS) FOR AERONAUTICAL SAFETY SERVICES
ROADMAP DOCUMENT

This draft dated: June 22, 2017

ARINC PROJECT PAPER 658
TABLE OF CONTENTS

ATTACHMENTS

APPENDICES

1.0 INTRODUCTION

1.1 Purpose

It is generally agreed by aviation stakeholders that the future aviation network communication infrastructure will be based on selected commercial Internet Protocol (IP) standards. This future aviation communication network has been referred to in ICAO as ATN/IPS[1] (Aeronautical Telecommunication Network/Internet Protocol Suite) and is considered as the successor in the long term of the previously defined ICAO network infrastructure based on the Open Systems Interconnection (OSI) model and referred to as ATN/OSI. The ATN/IPS network will be implemented onboard an aircraft and the ground infrastructure to support safety related services, including Air Traffic Services (ATS) and Aeronautical Operational Control (AOC).

Therefore, the Airlines Electronic Engineering Committee (AEEC) has initiated the development of the required avionics standards to support ATN/IPS. AEEC has acknowledged that ATN/IPS standards development is complex and it needs to be coordinated with other organizations such as ICAO, EUROCAE and RTCA. Furthermore, the exact scope and the potential impact on aircraft communication functions, such as applications and communication media, need to be understood. In addition, there may be interdependencies with related industry standards and those that need to be developed by other organizations.

Therefore, the AEEC has agreed to proceed in two steps for the development of the ATN/IPS avionics standards.

The first step is the analysis and capture of the high-level user requirements for ATN/IPS focusing on the airline, but also considering when possible the ground users (ANSPs), requirements, investigating what is needed for ATN/IPS standardization for aviation, taking into account the current and/or expected plans of the other standardization organizations, and focusing in identifying what exactly needs to be developed by AEEC for ATN/IPS. The outcome of this first step is a detailed plan for the work to be carried out by AEEC in the second step defining also the perimeter of the necessary ARINC Standards for ATN/IPS, as well as general recommendations for the general ATN/IPS standardization work that is required in aviation. The recommendations will be a valuable input/feedback to the ATN/IPS standardization groups in ICAO, EUROCAE, and RTCA.

The second step will be the execution of the recommendations coming out of the Step 1 work in relation to the effort to develop ARINC Standards for ATN/IPS.

This document is the outcome of the activities under the first step above. As such it provides a so called “roadmap” for the development of the aviation standards for ATN/IPS for Aeronautical Safety Services. This document recognizes the broad use of the existing datalink infrastructure components and protocols. It describes the steps necessary to transition to ATN/IPS. The recommendations are intended to be evolutionary and are expected to be implemented in a step-wise fashion.

In addition, this document describes data communication services necessary for operation in the evolving Communications Navigation Surveillance/Air Traffic

---

[1] In this document the term “ATN” is used to refer generically to the Aeronautical Telecommunications Network and could be either ATN/IPS or ATN/OSI. Furthermore, if only “IPS” is used, this is considered equivalent to referring to “ATN/IPS”.

Management (CNS/ATM) environment expected for the FAA NextGen, the European Single European Sky ATM Research (SESAR) and the Japan Collaborative Actions for Renovation of Air Traffic Systems (CARATS) ATM modernization Programmed, whose capabilities and functionalities are intended to satisfy the industry’s long-term requirements and in line with the International Civil Aviation Organization (ICAO) planning.

ICAO is developing an Aviation System Block Upgrade (ASBU) plan to harmonize the Air Traffic Management (ATM) improvement programs across the globe. The ASBU defines target implementation timelines organized in four blocks: Block 0 – up to 2018, Block 1 – up to 2024, Block 2 – up to 2030, and Block 3 – 2030 onward. Each Block addresses four aviation performance areas:

- Airport operations
- Globally-interoperable systems and data
- Optimum capacity and flexible flights
- Efficient flight paths

The Blocks contain Modules which define the Communication, Navigation, and Surveillance (CNS) information management functions required for the aircraft and ground components. Descriptions of the ASBU Blocks and Modules can be found in the ICAO Global Air Navigation and Capacity Enhancement Plan (GANP), whose 2nd edition was issued in 2016. The ATN/IPS work relates to Blocks 2 and 3 and potentially the last part of Block 1.

The ICAO ATM modernization plans emphasize broad use of datalink communication, Global Navigation Satellite System (GNSS), and the various surveillance capabilities to improve flight deck situational awareness and enhance performance-based operations. This document assesses the impact of airspace modernization plans to airborne avionics equipment and architectures, recognizing that the benefit from equipping aircraft may depend on coordinated changes to regulations, procedures, ground infrastructure, and other factors. The equipage analyses contained herein are intended to represent a high-level system view that can be broadly disseminated to airlines, airspace planners, Air Navigation Service Providers (ANSPs), airframe manufacturers, avionics suppliers and others who participate in the development process.

This document refers to **ARINC Report 660B**: CNS/ATM Avionics Architectures Supporting NextGen/SESAR Concepts. Content from ARINC Report 660B may be included in this document for emphasis and to facilitate reading of the document.

The challenges to the industry set forth by this document requires cooperation among international standards organizations and the development of complementary standardization material. The working relationships and the various standardization deliverables to be produced are summarized in Section 5 of this document.

1.2 Scope

This document represents the consensus of industry. This document describes airline objectives (while also considering the ground side when possible) towards the development and introduction of advanced data communication protocols and services that meets the safety and performance requirements of aviation for the year 2020 and beyond.

1.0 INTRODUCTION

Previous analysis has recognized that in the implementation of data communications, there are three distinct elements which need to be considered: 1) the applications, 2) the communication network(s) over which the applications are running and 3) the physical link(s)[2] the network(s) interface to as shown in the following figure.

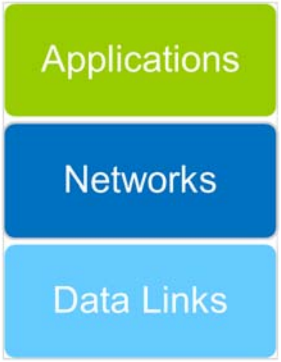


Figure 1-1 – Distinct Elements in Data Communications

The AEEC ATN/IPS activity addresses exclusively the 2nd element of the figure above, the communication network(s). However, this report provides some information for the other two elements as required for reference.

Currently aviation uses two networks: The Aircraft Communications Addressing and Reporting System (ACARS) network and the Aeronautical Telecommunication Network (ATN) infrastructure. These two existing networks are aviation-unique and the need for improvements has already been identified. The aviation industry desires a modern, off-the-shelf, efficient, and robust network infrastructure common to both Air Traffic Services (ATS) and Aeronautical Operational Control (AOC) safety[3] services.

A new network infrastructure for safety services, the ATN Internet Protocol Suite (ATN/IPS), based on commercial IP will meet this need. Accordingly, the industry is preparing ARINC Standards that will define the ATN/IPS for aeronautical safety services. The resulting documents are expected to be based upon updated versions of the ICAO Doc. 9896 defining the agreements in ICAO for ATN/IPS and on prevalent commercial IP network technology (e.g., IETF RFC 2460 for IPv6) with the modifications necessary to support aeronautical safety services.

It is anticipated that ATN/IPS will use multiple line-of-sight and beyond-line-of-sight subnetworks that operate in the protected spectrum allocated by ITU and ICAO for safety services, including Inmarsat SwiftBroadband, Iridium NEXT, AeroMACS, future Satcom and LDACS systems, and possibly VDL Mode 2. It is desired that ATN/IPS will also provide application level backward compatibility with traditional ACARS ATS (e.g., FANS) and AOC (e.g., ARINC 702A flight plans) as well as Link

---

[2] The physical links are also referred to as communication media or subnetworks.

[3] The International Telecommunication Union (ITU) defines a “safety service” as any radio communication service used for the safeguarding of human life and property. ICAO Annex 10 refines that definition to a “service reserved for communications relating to safety and regularity of flights”, specifically ATS and AOC “safety communications” as defined in ICAO Doc 9718.

2000+ (ATS B1) and ATS B2 applications, so the applications will remain unchanged. Figure 1-2 shows the connectivity between the aircraft applications in the ACD and AISD domains via the various communication networks to the ground applications of the ANSPs and airlines. As shown in the figure, ATN/IPS will cover ATS and AOC data in the ACD as well as AISD domains for both Airlines and ANSPs.

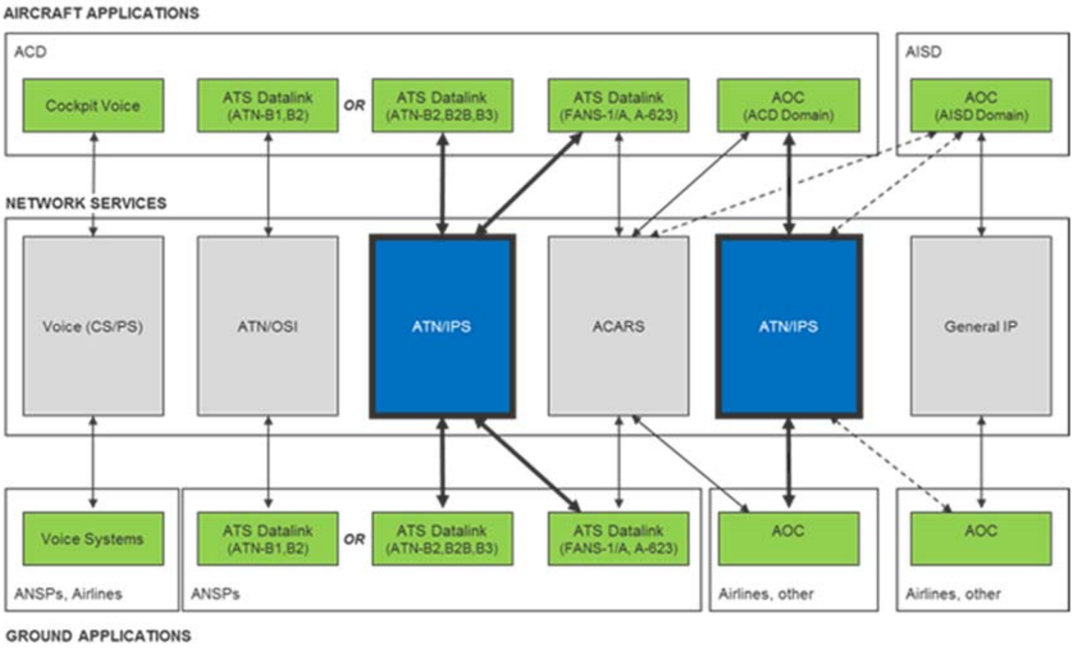


Figure 1-2 – Applications and Networks

For the development of the ATN/IPS standards, the AEEC has initiated a two-step approach as outlined below.

1.2.1 Step 1: ATN/IPS Standardization Roadmap and Main Architecture Impacts

The outcome of step 1 is covered by this document: ARINC Report 658. This document describes the roadmap for the standardization of ATN/IPS (air-to-ground and end-to-end) and the timeline for elements to be standardized by the relevant Standards Development Organizations (SDO), e.g., ARINC Industry Activities, RTCA, EUROCAE, ICAO. The report includes an identification of ATN/IPS requirements (e.g., performance, information security) and ATN/IPS overall standardization needs. It also includes a description of the avionics architecture impacts of ATN/IPS as well detailing the scope of the ARINC ATN/IPS standard to be developed in Step 2.

1.2.2 Step 2: Development of an ARINC Standard for ATN/IPS

An ARINC Standard will be prepared to define the avionics architecture, functions, and an IPS profile which describes implementation options and constraints as well as higher level details regarding the accommodation of different applications. The scope of this standard will correspond to the CMU (or equivalent avionics).

As in Step 1, coordination with aviation SDOs will continue in the Step 2 activities.

1.3 Expected Benefits of ATN/IPS

ATN/IPS will provide multiple benefits to aviation. A number of benefits relate primarily to operational improvements of the NextGen/SESAR/CARATS airspace system and individual airline operations. The benefits may vary by geographic region, depending on the level of ATM capability and approved method of operation. The airborne CNS equipment should provide the flexibility needed to take advantage of regional benefits.

Internet Protocol Suite (IPS) will introduce an efficient protocol stack that will benefit airlines, airframe manufacturers and avionics equipment suppliers.

IPS will be designed to support existing and future ATS and AOC applications, while enabling new CNS/ATM applications to be developed for the airline community and to be updated as necessary for the life of the airplane.

Airline benefits will accrue in the form of greater data communications performance compared to ACARS and ATN/OSI. ATN/IPS will be designed to support both ATS and AOC applications, provide backward compatibility with traditional ACARS ATS (e.g., FANS) and AOC (e.g., ARINC 702A flight plans) applications, and use both line-of-sight and beyond-line-of-sight subnetworks, all of which will further increase its effectiveness and applicability. ATN/IPS will support a wide range of future applications and enable a transition to high-speed links for safety services.

Airframe manufacturer and avionics equipment supplier benefits will accrue in the form of moving towards future datalink technologies providing more bandwidth and capabilities. IPS protocols (IP, TCP, and UDP) have been exhaustively tested in the commercial domain and are widely available for adaptation for aeronautical use.

1.4 Document Organization

This document is generally organized in six sections as follows:

- Section 1 – Introduction

  This section introduces the work that needs to be performed for the ATN/IPS development. It explains AEEC's approach toward standardization. It focuses on step 1 activities and report structure.

- Section 2 – ATN/IPS Overview

  This section provides an overview of IPS for safety services in the context of how IPS elements integrate within the aircraft, networking services, and ground systems. Existing and future ATS and AOC applications expected to be supported by IPS are presented in terms of key services supported by IPS, key application characteristics that may impact IPS, and the potential impact that IPS may have on applications. This section also introduces the broadband, IP-based safety datalinks – airport surface, terrestrial, and satcom – that IPS is expected to leverage, in addition to the potential use of existing safety communication infrastructure such as VDLM2.

- Section 3 – ATN/IPS Architectures

  This section provides a high-level overview of ATN/IPS airborne possible architecture options, forming a framework to refine standardization needs. To this objective, main assumptions are listed, and a first set of Data security, Safety and Performance requirements is identified. A particular emphasis is placed on the data security process (security risk analysis) which allows elaborating this first set of requirements. Based on these assumptions and requirements, some avenues on how ATN/IPS could be integrated in legacy equipment (ARINC 429 based) and current (ARINC 664 based) architectures are described.

- Section 4 – ATN/IPS Work Scope Considerations

  This section describes other non-architectural areas that need definition in order for ATN/IPS to serve its intended role. This includes upper layer protocol interface considerations for current and future applications, naming and addressing, mobility, ATN/IPS administration, and how ATN/IPS would fit within a larger security context.

- Section 5 – ATN/IPS Standardization Roadmaps

  This section presents a proposed roadmap and timeline for ATN/IPS standardization. Using the work scope identified and discussed in Section 4, a gap analysis captures known in-progress and planned standardization work and then identifies areas where new and/or additional standardization activities are required. Recommendations are offered for allocation of the to-be-completed standardization to various standards development organizations, with an emphasis on AEEC standardization activities. A graphical roadmap illustrates the expected timing and interdependencies among recommended AEEC activities, and it highlights key dependencies with other standards organizations developing ATN/IPS standards. The roadmap is intended to serve as a communication tool for inter-organization coordination, particularly where key dependencies are identified. Finally, this section provides information in relation to the planned ATN/IPS Validation Activities in US and Europe.

- Section 6 – Summary Recommendations

  This section summarizes the outcome of the report and provides go-forward recommendations.

- Attachment 1 – List of Acronyms

  This appendix lists and for easy reference the acronyms used in the report.

- Attachment 2 – Glossary

  This appendix explains the precise meaning of terms used in this report to avoid ambiguity and confusions.

- Appendix A – Notional ATN/IPS Timelines

  This appendix includes roadmaps developed by various organizations to document their perspective on the timing of ATN/IPS standardization, validation, implementation, deployment, and initial operational capability. These roadmaps, which served as an input to the development of the standardization roadmap in Section 5, include:

  - The ICAO Global Air Navigation Plan (GANP),
  - A harmonized FAA-EUROCONTROL data communications roadmap, and
  - Airframe Manufacturer roadmaps, including Airbus and Boeing datalink implementation roadmaps.

- Appendix B – Avionics Architectures

This appendix identifies the key elements of the current avionics architectures, which are based on ARINC 429 and ARINC 664, and the key architecture components that need to be considered in the context of introducing ATN/IPS in these architectures.

- Appendix C - High Level Risk Assessment and Security Objectives

  This appendix provides additional details regarding the high-level security risk assessments for ARINC 429 and ARINC 664 architectures presented in Section 3.1.

- Appendix D – Standardization Gap Analysis Worksheet

  This appendix contains a current “snapshot-in-time” of the spreadsheet used to capture the status of ATN/IPS work areas and to identify gaps.

1.5 Document Development and Objectives

This document was prepared for the airline community and all aviation stakeholders. It presents the scope and the level of detail necessary to achieve ATN/IPS standardization. It defines the long-term needs for ATN/IPS for aeronautical safety services including:

- The users ATN/IPS datalink services (ATC, AOC)
- The functional, performance and safety and information security requirements
- The desired applications and means of communication

This document also provides deployment information including the transition phase during which ACARS, ATN/OSI, and ATN/IPS will co-exist. It describes how aircraft equipped with ACARS, ATN/OSI and aircraft with ATN/IPS will be accommodated.

2.0 ATN/IPS OVERVIEW

2.1 Introduction

ATN/IPS is intended to provide an efficient and robust network infrastructure common to both Air Traffic Services (ATS) and Aeronautical Operational Communications (AOC) safety service applications.

Figure 2-1 illustrates a high-level ATN/IPS diagram showing the potential aircraft applications, the network stack, the network services, and expected air/ground subnetworks, and the ground applications and network stack. ATN/IPS elements are shaded blue.

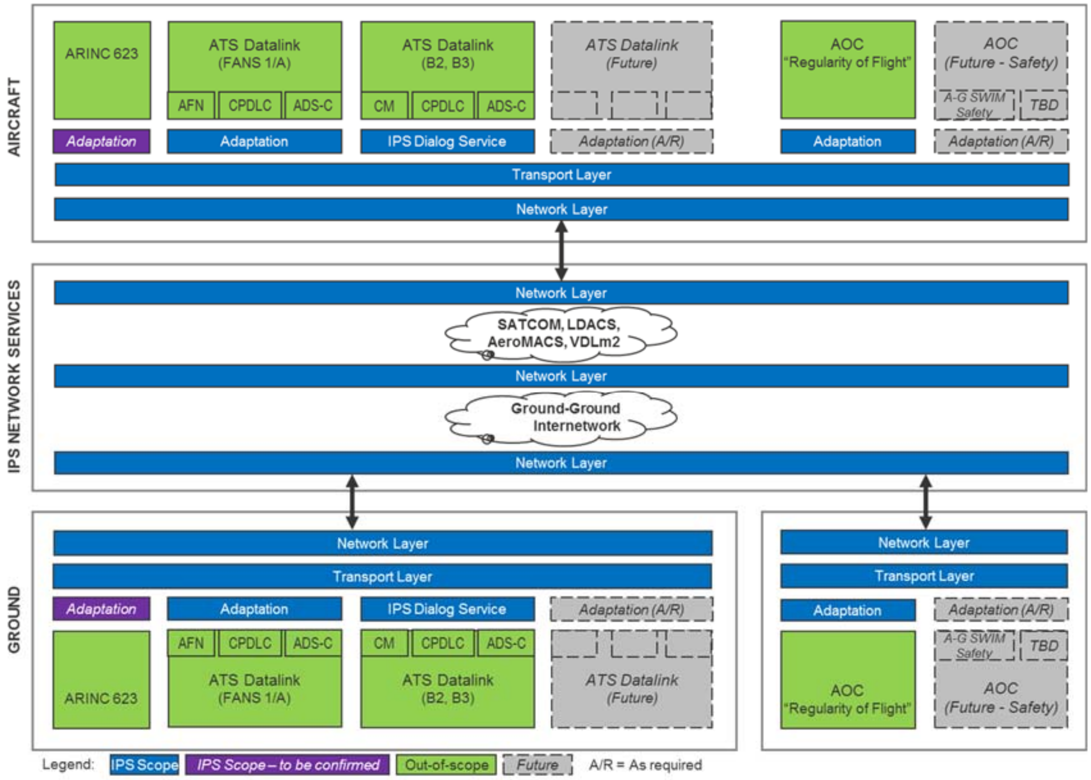


Figure 2-1 – ATN/IPS Overview

As shown in Figure 2-1, IPS supports both legacy applications, which require adaptation (e.g., using the ATN/IPS Dialog Service described in ICAO Doc. 9896), and future applications, which could be extensions of adapted legacy applications or new native IP applications not yet covered by ICAO Doc. 9896.

The following points summarize the target applications:

- ATS datalink applications supporting integrated air traffic control services in continental and oceanic airspace as part of the future Aeronautical Telecommunication Network (ATN). This includes Baseline 2 and Baseline 3 applications that support initial and full 4D trajectory based operations respectively. IPS may also provide a network service for aircraft equipped with legacy ARINC 623 or FANS-1/A, and further investigation is part of the work plan described in this document, particularly with respect to transition.
- AOC applications supporting safety and regularity of flight. This includes AOC services currently supported over ACARS (and adapted to support

transmission over IP). Candidate AOC applications include flight plans, weather reports and forecasts, weight and balance information, Aircraft Condition Monitoring System (ACMS) reports, and aircraft position reports.

The ATN/IPS network service must be designed and developed to support the safety, performance and security requirements for these applications in the airspaces in which it is deployed and for all phases of flight: airport, terminal maneuvering area, enroute, and oceanic/remote.

The ATN/IPS network connects air and ground assets over an internetwork comprising a series of interconnected networks, which use the IPv6 protocol suite specified within ICAO Doc. 9896 [*planned updated pending output of WG-I Mobility Sub-group*]. The design of the ATN/IPS network needs not only to consider which network layer protocols are required to support air/ground mobile connectivity, but also how the upper communications layers provide the necessary end-to-end service required by each of the applications listed above. There may also be requirements that ATN/IPS would impose on Layer 2 (link layer) radio networks, and the work plan described in this document addresses activities to consider these requirements. This includes selection of a suitable transport protocol and any adaptation required to support legacy applications over the selected transport protocol.

Air/ground subnetworks, operated by one or more Communications Service Providers (ACSPs), provide communications between aircraft and ground entities. As examples, the diagram shows Satcom, L-band terrestrial radio, and AeroMACS systems. Section 2.5 provides further detail regarding candidate communication systems.

On the ground, ANSPs, airlines, and other organizations (e.g., engine manufacturers) use their own ground network and connect directly to ACSPs or via intermediate ground service providers. For simplicity, the connectivity between ground end user networks and ACSPs may be viewed as a homogeneous ground/ground internetwork, where each air/ground subnetwork may present one or more “points of presence” onto the ground/ground internetwork, through which communications to connected aircraft can be routed.

Although not shown in Figure 2-1, the transition to ATN/IPS must address interoperability among aircraft and ground entities exchanging messages among different networks. Aircraft may have dual protocol stacks for ATN and ACARS operation (e.g., OSI+ACARS or IPS+ACARS). Similarly, ground centers may not support all OSI and IPS variants. Therefore, ground gateways may be required to support interoperability, as further described in Section 3.6.

2.2 ATN/IPS Applications and Services

The aviation community, in concert with NextGen and SESAR programs, is expected to introduce ATN/IPS for a number of applications and services. The following applications and services are discussed in the context of the implications of introducing ATN/IPS.

2.2.1 ATS Data Communications

2.2.1.1 ARINC 623

ARINC 623 specifies character-oriented ATS messages that are transmitted over ACARS via VHF, HF, and Satcom datalinks.

Primary references for character-oriented ATS messages include:

- EUROCAE ED-85A, Data Link Application System Document for the Departure Clearance Data Link Service
- EUROCAE ED-89A, Data Link Application System Document for the ATIS Data Link Service
- EUROCAE ED-106A, Data Link Application System Document for the Oceanic Clearance Data Link Service
- ARINC Specification 623, Character-Oriented Air Traffic Service (ATS) Applications.

An adaptation layer is necessary to accommodate the exchange of ARINC 623 application messages over ATN/IPS. Note that although the current EU/US Data Communications Harmonization Roadmap (Section A.2) does not reference ARINC 623 over ATN/IPS, the ATN/IPS technical solution should not preclude this functionality if stakeholders and a business case support it.

2.2.1.2 FANS

The Future Air Navigation System (FANS) was the first operational ATS datalink service use for transmitting datalink messages over the ACARS network and VHF, HF, and Satcom subnetworks.

FANS was introduced in the mid-1990s. Boeing introduced FANS 1 services and Airbus developed a similar product called FANS A. Collectively the products are known as FANS 1/A. FANS 1/A+ is an improved version of FANS 1/A and includes a message latency detection function. New installations typically support FANS 1/A+. However, older installations may not have FANS 1/A+.

Primary references for FANS 1/A and 1/A+ are:

- EUROCAE ED-100 / RTCA DO-258A, Interoperability Requirements for ATS Applications Using ARINC 622 Data Communications.
- ARINC Specification 622, ATS Data Link Applications over ACARS Air/Ground Network.

In addition, there is a large collection of documents that define functions and characteristics of the avionic and ground based systems.

FANS 1/A uses ACARS subnetworks including: VHF (VDL Mode 0/A using the “Plain Old” ACARS (POA) protocol and VDL Mode 2 using the ACARS over Aviation VHF Link Control (AVLC), or AOA, protocol); HF (using the HF Data Link (HFDL) protocol); and Satcom (using the Data-2 protocol for Inmarsat Classic Aero Satcom and the Short-Burst Data (SBD) protocol for Iridium NEXT). The worldwide coverage includes oceanic RNP-4 routes which require data communications; consequently, FANS 1/A is implemented on many aircraft that fly internationally. The FAA Data Communications program has chosen FANS 1/A+ for use in domestic operations, including the introduction of Departure Clearance (DCL) operations in 2015 and plans to extend CPDLC services for enroute operations in 2019.

As shown previously in Figure 2-1, an adaptation layer is necessary to accommodate the exchange of FANS 1/A application messages over ATN/IPS.

2.2.1.3 Baseline 1 (B1)

ATN is a communication architecture developed by ICAO to provide a global air/ground and ground/ground data link application and communications standard for air traffic services. ICAO Doc. 9705-AN/956 specifies the initial ATN technical provisions, and ICAO Doc. 9880-AN/466 amends and supersedes Doc. 9705 based on the results of ongoing validation and operational experience gained during implementation and deployment. These ICAO technical manuals specify the operation of ATN applications and the ATN End Systems (application entities). In addition, it specifies the Communication Service (including ULCS and ICS), which uses the OSI protocol stack.

B1 is a subset of the ICAO ATN applications that support initial enroute datalink services. Specifically, B1 specifies the following datalink applications: Context Management (CM), Automatic Dependent Surveillance-Contract (ADS-C), Controller-Pilot Data Link Communications (CPDLC), and Flight Information Services (FIS). Note: Avionics and ground systems currently implement the B1 CM and CPDLC applications. However, they do not implement the B1 ADS-C and FIS applications.

The following EUROCAE/RTCA documents standardize B1:

- ED-110B/DO-280B, Interoperability Requirements Standard for Aeronautical Telecommunication Network Baseline 1 (ATN B1 Interop Standard)
- In addition, the interoperability between FANS 1/A and B1 is specified in ED-154A/DO-305A, Future Air Navigation System 1/A – Aeronautical Telecommunication Network Interoperability Standard (FANS 1/A – ATN B1 Interop Standard).

In Europe, the Data Link Services Implementing Rule (DLS-IR) requires airspace users operating above Flight Level 285 and Air Navigation Service Providers (ANSPs) operating in the EU region to equip for operation of B1 over VDL Mode 2. Implementing Rule EC 2015/310 amends the initial regulation EC 29/2009 and is applicable from February 2018. The DLS-IR mandates specific ATS services under the CM application (DLIC) and the CPDLC application (ACM, ACL and AMC), which were validated by the EUROCONTROL Link 2000+ Programme. The ETSI Community Specification (ETSI EN 303 214) and the EUROCONTROL Specification on Data Link Services (EUROCONTROL SPEC-0116) defines the compliance for B1 systems.

ICAO Doc. 9880-AN/466 specifies technical provisions for B1 operation over the OSI protocol stack. To facilitate transition from OSI to IPS, ICAO Doc 9896 defines provisions for an adaptation layer (shown previously in Figure 2-1) that mimics the Dialog Service interface to support B1 operation over ATN/IPS. Note that the Dialog Service interface is the same for B2 as it is for B1, so the adaptation layer functions equivalently for both B1 and B2.

As noted in Appendix C-2.3, the long-term EU and US harmonization strategy includes the B2 application set and ATN/IPS. Therefore, as ATN/IPS implementations are fielded, it is expected that B2 will be the current data communications application standard. However, as ground systems transition to ATN/IPS, there will be a need to support B1 applications where they are deployed (currently only continental Europe). ATN/IPS-based ground systems using either B1 or B2 may communicate with OSI-based aircraft using either B1 or B2 (and vice versa) via an accommodation function similar to the Gateway discussed in Section 3.3.

2.2.1.4 Baseline 2 (B2)

Baseline 2 (B2) represents a significant expansion of B1 services aimed at supporting the totality of ICAO ATN applications that enable 4D trajectory based operations and airports services.

Compared to B1, B2 modifies the subset of datalink applications, which include CM, ADS-C, and CPDLC. The following EUROCAE/RTCA documents specify the applicable B2 standards:

- ED-228/DO-350, Safety and Performance Standard for Baseline 2 ATS Data Communications (Baseline 2 SPR Standard)
- ED-229/DO-351, Interoperability Requirements Standard for Baseline 2 ATS Data Communications (Baseline 2 Interop Standard)
- ED-230/DO-352, Interoperability Requirements Standard for Baseline 2 ATS Data Communications, FANS 1/A Accommodation (FANS 1/A - ATS Baseline 2 Interop Standard)
- ED-231/DO-353, Interoperability Requirements Standard for Baseline 2 ATS Data Communications, ATN Baseline 1 Accommodation (ATN Baseline 1 - Baseline 2 Interop Standard)

At the time of this writing, Revision A to the B2 standards referenced above has been published but not yet validated. Revision A adds Advanced Interval Management (AIM), Dynamic RNP (D-RNP), and ATC Winds. B2 Revision ”n” will incorporate corrections resulting from validation; however, it will not contain any new functionality.

EUROCONTROL under SESAR, and FAA under NextGen, have B2 capability in the future implementation roadmap. B2 is intended to support B1 ATS services, plus additional services under the CPDLC application (DCL, D-TAXI, ITP, IM, OCL, IER, 4DTRAD, D-RNP) and the ADS-C application (PR, IER, 4DTARD, D-RNP).

As shown previously in Figure 2-1, an adaptation layer is necessary to accommodate the exchange of B2 application messages over ATN/IPS.

2.2.1.5 Beyond Baseline 2

Beyond B2, yet-to-be-defined Baseline 3 (B3) services are foreseen to support longer-term operations in the 2030+ timeframe (i.e., Block 3 per ICAO’s Aviation System Block Upgrades (ASBU) plan). Definition of B3 may include applications of more stringent technical performance characteristics for the existing B2 services, as well as the definition of new services. The European SESAR 2020 Programme will be offering proposals for potential new services. The interface to ATN/IPS may use the dialog service or another interface may be defined.

2.2.2 AOC Data Communications

AOC applications support services that generally fall into flight planning, weather, dispatching, and messaging categories. ATN/IPS is intended to support these AOC applications, which in turn support safety and regularity of flight.

2.2.2.1 Current AOC Data Communications

Current AOC applications operate over the ACARS network and are consequently character-oriented. This means that an adaptation layer is necessary to accommodate exchange of character-oriented AOC messages over ATN/IPS without changing the applications implemented by both avionics and ground systems.

2.2.2.2 Future AOC Data Communications

Future AOC applications should be designed to operate over the ATN/IPS network and consequently would be bit-oriented. This means that only a minimal adaptation layer, if any, would be necessary to accommodate exchange of bit-oriented AOC messages over ATN/IPS, although it also implies development and implementation of complementary new AOC applications by both avionics and ground systems.

2.2.3 Aeronautical Information Management (AIM)

2.2.3.1 AIM Services

RTCA SC-206 and EUROCAE WG-76 are in the process of developing Airborne Meteorological (AMET) and Aeronautical Information Management (AIM) Services including:

- Airspace Information Update
- Digital notice to airmen (NOTAM)
- Digital in-flight weather (VOLMET)
- Winds and temperature aloft
- Winds and temperature data for flight management
- Aerodrome weather
- Hazardous weather
- Environmental conditions in critical flight phases
- Weather imagery
- Runway visual range
- Digital automatic terminal information service (ATIS)
- Runway, taxiway, and obstacle information
- Special aircraft weather reports (AIREP/AUTOMET)
- Exchange of real-time aircraft derived data
- Others

The associated service message definitions are generic, technology agnostic, and can utilize both safety services protected spectrum as well as non-safety service broadband air/ground communications. Most of these new services will leverage the native internet protocol application-layer interfaces. Depending on the outcome of operational performance, safety assessment, and data quality requirements, some of these services may utilize ATN/IPS, when deployed.

2.2.3.2 System Wide Information Management

The ICAO Global Air Traffic Management Operational Concept describes System Wide Information Management (SWIM) as the integration of ATM information using a many-to-many information distribution model. Many geographically dispersed sources collaboratively update information that is then shared among relevant stakeholders to maintain situational awareness and improve operational decision-making.

At the time of this writing, air/ground SWIM is not intended to carry safety-critical data such as aircraft trajectory and tactical command and control. Current air/ground SWIM offerings support the exchange of non-safety-critical, advisory information such as weather and AIM that the aircraft flight crew uses to enhance situational awareness. The scope of ATN/IPS safety services does not include these non-safety air/ground SWIM information exchanges. If air/ground SWIM safety services are deployed in the future, these applications may leverage the native ATN/IPS application-layer interfaces or they may implement an adaptation layer, as illustrated previously in Figure 2-1.

2.2.4 Voice Services

While certain aeronautical mobile communication technologies may offer voice services, cockpit voice services are assumed to be outside the scope of the ATN/IPS standardization activity. If air/ground VoIP services over ATN/IPS are deployed in the future, further analysis will be required to ascertain requirements (e.g., performance, architecture, networking, and security) and whether ATN/IPS can support those requirements.

2.3 Networks

2.3.1 ACARS

The Aircraft Communications, Addressing and Reporting System (ACARS) is an air/ground data communications system deployed initially by ARINC in 1978 to support message exchanges between aircraft and airline operation center. ACARS uses aviation-unique, character-oriented, air/ground communications protocols (per ARINC Specifications 618, 619, and 620) to exchange messages no larger than approximately 3.5 kilobytes. ACARS supports both ATS and AOC message exchanges.

ACARS has evolved to use multiple subnetworks globally including the following

- VDL Mode 0/A (using the “Plain Old” ACARS (POA) protocol)
- VDL Mode 2 (using the ACARS over Aviation VHF Link Control (AVLC) or AOA protocol
- Inmarsat L-band Satcom
- Iridium L-band Satcom
- High Frequency Data Link (HFDL)

Since ACARS use is expected to continue beyond initial deployments of ATN/IPS, it may be necessary for aircraft equipage to support both ACARS and IPS networks (“dual-stack”), similar to current equipage that supports both ACARS and OSI.

In an ATN/IPS environment, no changes to the ACARS protocol stack are necessary. ATN/IPS may offer an alternate means for communicating ACARS messages, by carrying either the ACARS messages themselves (i.e., ARINC 618 blocks) or the data contained in an ACARS message (i.e., the payload data in ARINC 618 blocks). Ground gateways will be necessary to provide translation services.

2.3.2 OSI

The current deployment of Link 2000+ datalink services in Europe that began in the early 2000's implements the bit-oriented ATN Open Systems Interconnection (OSI) network protocols specified in ICAO Doc. 9880 (originally Doc. 9705 Ed. 2 plus correcting actions specified in the EUROCONTROL DLSIR). The aviation-unique OSI protocol stack includes the ISO 8208 Packet Layer Protocol (PLP), ISO 8473 Connection-Less Network Protocol (CLNP), ISO 8073 TP4 Connection-Oriented Transport Protocol (COTP), and "fast-byte" session and presentation layers. OSI is deployed only in Europe, supports only B1 ATS message exchanges, and uses only the VDLM2 subnetwork (although use of Inmarsat SBB as an additional subnetwork is in development/testing under the Iris Precursor Programme).

Initial B2 implementation in Europe (SESAR Very Large Scale Demonstration) will also be based on OSI over VDLM2 subnetwork (and possibly over Inmarsat SBB).

In a mixed OSI-IPS environment, ground gateways may be necessary to provide accommodation of OSI-equipped aircraft communicating with IPS-based ground systems and/or IPS-equipped aircraft communicating with OSI-based ground systems. Reference Section 3.3, which presents ground segment and transition accommodation considerations.

2.3.3 IPS

The IPS protocol stack will eventually replace both the ACARS and OSI networks, and provide a convergence point for current and future applications. Various aviation standards organizations are planning to specify or in the process of specifying the IPS protocol stack. The current version of ICAO Doc. 9896 specifies some initial considerations for the IPS protocol architecture, which include the connection-oriented Transmission Control Protocol (TCP) and extensions per RFC 793 and RFC 1323 (respectively); connectionless User Datagram Protocol (UDP) per RFC 768; and general Internet Protocol inter-networking based on IPv6 per RFC 2460. The ICAO technical manual further specifies Internet RFCs for mobility, addressing, inter-domain routing, quality-of-service, security, and so forth. However, these specifications are subject to change based on ongoing analyses of mobility and security alternatives, as well as recommendations for additional standardization identified in this roadmap document.

2.4 Candidate Communication Links

ATN/IPS will use multiple subnetworks that operate in protected aeronautical spectrum allocated by ITU and ICAO for safety services. This section addresses candidate subnetworks including: terrestrial-based communications that provide Line of Sight (LOS) coverage (i.e., range of about 200 NM), satellite communications that provide Beyond Line of Sight (BLOS) coverage, and airport surface communications, which are a form of LOS used only when the aircraft is on the airport surface. Systems such as VHF Digital Link Mode 0/A, current aeronautical HF Datalink, and Performance Class C Satcom are not considered to support ATN/IPS due to performance limitations.

The subnetwork descriptions in this section are summaries from ARINC Report 660B, to which the reader is referred for additional background information.

2.4.1 Terrestrial-based Communications

Terrestrial-based communications support voice and datalink operations within line-of-sight coverage of ground stations. Most modern aircraft are forward-fit with ARINC 750 radios and are therefore capable of VHF datalink operations. Operations in areas that are not within VHF coverage (e.g., oceanic operations) depend on Beyond Line-Of-Sight (BLOS) communications such as satcom.

2.4.1.1 VHF Digital Link Mode 2 (VDLM2)

VDLM2 supports both B1 (OSI) and FANS 1/A (ACARS) services, and B2 services are expected to operate initially over VDLM2. It operates with a Common Signaling Channel (CSC) of 136.975 MHz, at the top of the aeronautical VHF band, with a channel width of 25 kHz using Differential 8-Phase Shift Keying (D8PSK) modulation to provide digital communications at a nominal data rate of 31.5 kbps. ICAO Doc. 9776 specifies the VDLM2 technical provisions, supported by the following documents:

- RTCA DO-224, Minimum Aviation System Performance Standards (MASPS) for Advanced VHF Digital Data Communications,
- ARINC 631, VHF Digital Data Link (VDL) Mode 2 Implementation Provisions.

European and US organizations are working together to identify terrestrial-based alternatives to VDLM2 (e.g., LDACS, reference Section 2.4.1.2). Until those new communication means are defined and deployed, the number of VHF carrier frequencies has been increased for VDLM2, resulting in what is known as multi-frequency VDLM2.

ATN/IPS protocols are expected to work with existing VDLM2 similar to the way in which the ACARS over AVLC (AOA) protocol works with VDLM2, meaning that unlike OSI, IPS would not use the ISO 8208 Subnetwork Access Protocol (SNAcP). In addition, current VDLM2 optimization investigations, including initial laboratory and flight tests, show promising results. Pending further investigation, this optimization may yield a connectionless variant (e.g., using Unnumbered Information (UI) frames) that may offer better RF efficiency and robustness than current connection-oriented operation, and which can support ACARS and OSI, in addition to IPS. Protocol multiplexing is possible using the Initial Protocol Identifier (IPI), which tags the AVLC Frame content as being IPS, ACARS, or OSI, as needed. Further investigation should assess the need for reliability mechanisms to provide robust data transmission. As is the case for introduction of any new protocol, addressing transition requirements is necessary so that aircraft and ground systems can deal easily with different protocols simultaneously.

2.4.1.2 LDACS

The L-band Digital Aeronautical Communications System (LDACS) is an integral component of the Future Communications Infrastructure (FCI) identified in the FAA and EUROCONTROL Future Communications Study and endorsed by ICAO in 2008.

LDACS in considered, particularly in Europe, to complement VDLM2 data link operations (B2 services) when additional capacity will be required as well as to enable new services with more stringent performance requirements (e.g., B3 including B2 with more stringent performance requirements).

The LDACS protocols utilize modern commercial technologies based on Frequency Division Duplex (FDD) with OFDM modulation. (In the past, this was termed LDACS1, which was one of two candidate LDACS technologies considered previously).

To date, Europe is taking the lead with LDACS definition and development efforts. Under the SESAR1 activities, the LDACS system specifications were further refined, a transmitter prototype was built, and spectrum compatibility tests against DME and TACAN were performed. Work on LDACS will continue in SESAR 2020, including the development of complete prototypes (i.e., transmit and receive functionality) and testing to investigate and ascertain spectral compatibility with other existing L-band systems.

LDACS will operate as a native ATN/IPS air/ground subnetwork. As of December 2016, ICAO initiated a group to develop the SARPs and Technical Manual for LDACS by the 2020 timeframe.

2.4.2 Satellite Communications (Satcom)

2.4.2.1 Satcom Performance Class B – Medium Term

As background, Satcom Performance Class C covers performance requirements included in the current ICAO SARPs, and it supports oceanic datalink operations. Class C is applicable to existing systems, such as Inmarsat Classic Aero/I3, MTSAT, and Iridium, which have already been standardized by ICAO.

Satcom Performance Class B has more stringent performance requirements (as compared to Class C), such as those necessary to support initial 4D trajectory based operations, for both oceanic and continental operations. Class B will be applicable to existing Satcom systems, such as Inmarsat SBB/I4 and Iridium NEXT, and which are expected to be considered for standardization in ICAO.

2.4.2.1.1 Inmarsat SBB

Inmarsat provides land, maritime, and aviation services with geo-synchronous satellites at an altitude of approximately 22,000 NM. Its coverage is from 80° N to 80° S with no polar coverage.

Inmarsat SwiftBroadband Safety (SB Safety) uses digital high-speed and secure IP broadband to support a host of new safety and operational applications. This is a natural evolution of Inmarsat Classic Aero services, which have served airlines for over 25 years.

SB Safety supports simultaneous voice and broadband data, with IP data at up to 432 kbps, and IP data streaming on demand at 32, 64, and 128 kbps. The SB Safety architecture, shown in Figure 2-2, illustrates the high-level SB-Safety system architecture; although not shown, the architecture includes redundancy, with primary operation over the SwiftBroadband link, and fallback operation over the Classic Aero satellite network. This enables a highly available, high priority link for the reliable and safe transfer of FANS/ACARS messages meeting RCP240 and RSP180 performance requirements, while also providing voice and non-safety IP data services to the cockpit.

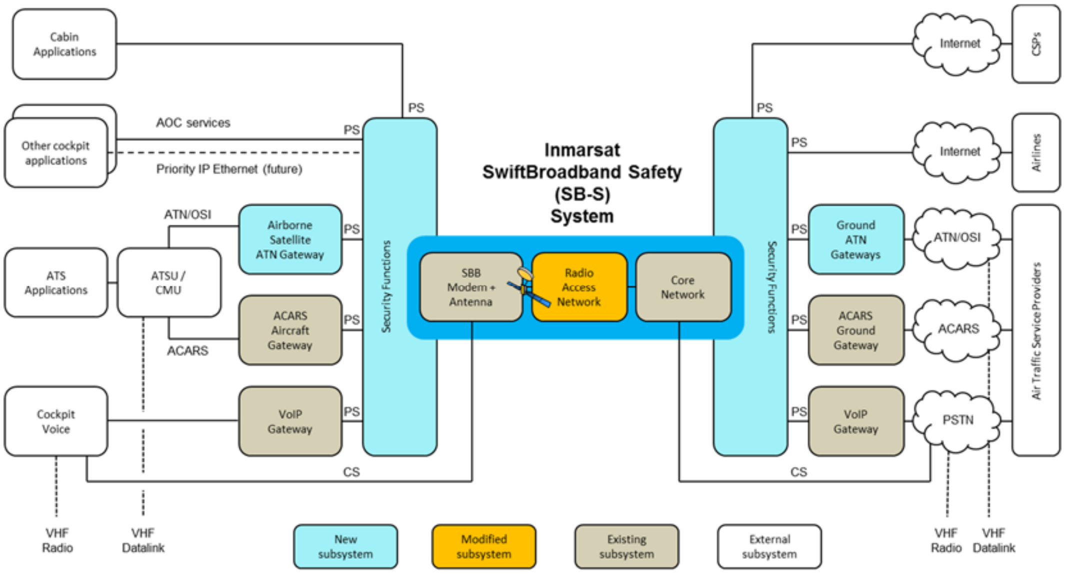


Figure 2-2 – SwiftBroadband Safety High-level Architecture

The Inmarsat SBB safety services ensure that existing onboard avionics systems for the voice and ACARS services do not require changes to the system interfaces used for Classic Aero today.

Note: For Class B, air/ground datalink standards development will extend RTCA SC-222 material considering EUROCAE ED-228 and ED-229 to cover continental airspace performance requirements, with support from SESAR P15.2.5 and the ESA Iris Precursor Programme (Inmarsat SBB evolution).

Inmarsat is now working on a program of upgrades to SwiftBroadband that will meet RTCA/EUROCAE performance standards for terrestrial ATS datalink. This service, which is currently under development in the context of the European Iris Precursor program with links to SESAR will enter pre-operational flight trials with Airbus in the 2017/2018 timeframe. The operational objective is to support initial 4D applications within both oceanic domains (e.g., for sequenced arrivals) and European continental domain as a complement to the datalink capabilities provided by VDLM2. The service will also provide an additional capacity to support the growth of Airline Operational Communications (AOC) as required.

The proposed Iris system architecture is a natural evolution of the SB-Safety system developed for Oceanic Safety services, which itself is an adaptation of the commercial SwiftBroadband (SBB) system in service today. As shown previously in Figure 2.2, Iris Precursor introduces ATN/OSI and Security gateways in both the air and ground segments. ATN Gateways encapsulate ATN/OSI traffic into the SBB IP data connection. The gateways present standard interfaces defined in the ICAO ATN Manual (ICAO 9705) for integration into ground/ground networks within the European ATM Network and, through minor modification, to the ATSU/CMU on board the aircraft. The Security gateways create an IPsec VPN to protect ATS datalink traffic against potential controller masquerade and replay/modification attacks. Additional mechanisms deployed on the air and ground mitigate denial of service attacks and prioritize SBB access for ATS services.

While the current datalink deployment in Europe is ATN/OSI-based, parallel industry initiatives are defining the approach to ATN/IPS for future datalink systems.

Inmarsat has initiated a new program/study that is investigating potential Iris Precursor upgrades to support integration of ATN/IPS communications service into existing infrastructure. To achieve the objective of a globally interoperable service, international standards are required for future developments. The study will contribute key principles, design approaches, and proposed standards to the technical specifications of ICAO CP and AEEC standards committees.

Inmarsat's aim will be to introduce ATN/IPS functionality by upgrading the Iris system with the introduction of an ATN/IPS gateway.

2.4.2.1.2 Iridium NEXT

The Iridium NEXT constellation, which completely replaces the Iridium Block 1 constellation, consists of 66 operational satellites, 6 in-orbit spares, and 9 ground spares. Iridium NEXT will offer the Iridium Certus Broadband Service with dramatically increased data speeds ranging from 88 kbps to 1.4 Mbps and with global pole-to-pole broadband service coverage. The initial launch of Iridium NEXT satellites started in January 2017, with targeted completion by early 2018.

The Iridium satellites are located in six distinct planes in near-polar orbit at a Low Earth Orbit (LEO) of approximately 780 km and circle the Earth approximately once every 100 minutes, travelling at a rate of roughly 27,088 km/h. The 11 mission satellites within each plane are spaced approximately every 32.7 degrees and perform as nodes in the communications network. Satellite positions in adjacent odd and even numbered planes are offset from each other by one-half of the satellite spacing. This constellation ensures that at least one satellite covers every region at all times.

Each Iridium satellite has four cross-link antennas to allow it to communicate with and route traffic to the two satellites that are fore and aft of it in the same orbital plane, as well as to neighboring satellites in the adjacent co-rotating orbital planes. These inter-satellite links operate at approximately 23 GHz. Inter-satellite networking is a significant technical feature of the Iridium Satellite Network that enhances system reliability and capacity and reduces the number of gateways or Ground Earth Stations (GESs) required for global coverage. As part of the Iridium NEXT program, all GES locations have been updated and an encrypted teleport network has been built to interconnect GES locations.

Iridium NEXT satellites are classified as replacement satellites as they support the current Block 1 services as well as offer new waveforms for the Iridium Certus Broadband capability. Therefore, all legacy Iridium Block 1 devices will continue to operate under the Iridium NEXT constellation without interruption nor impact to certification as the EIRP, G/T and RF frequencies are unchanged.

Iridium Certus is a multi-service platform offering simultaneous voice and broadband data services in five classes. Table 2-1 summarizes the data rates along with associated antenna, LGA (Low Gain Antenna, Active LGA (ALGA), and High Gain Antenna (HGA). Note that the TX/RX speeds are usable data rates and exclude the headers required in the Iridium system.

Table 2-1 – Iridium Certus Service Class

Service Class	TX Speed (max)	RX Speed (max)	Antenna Type
Iridium Certus 100	176 kbps	88 kbps	LGA
Iridium Certus 200	176 kbps	176 kbps	LGA/ALGA
Iridium Certus 350	352 kbps	352 kbps	HGA
Iridium Certus 700	352 kbps	704 kbps	HGA
Iridium Certus 1400	524 kbps	1408 kbps	HGA

Services offered on each Iridium Certus terminal will include three independent voice lines, background IP data, streaming IP data, standard IP data, and short burst data. The use of simultaneous services will be limited to the maximum transmit/receive speeds of the transceiver.

Figure 2-3, illustrates the high-level Iridium Certus safety system architecture. It is planned that Iridium NEXT will operate as both an ATN/OSI and ATN/IPS air/ground subnetwork in addition to traditional voice and ACARS services.

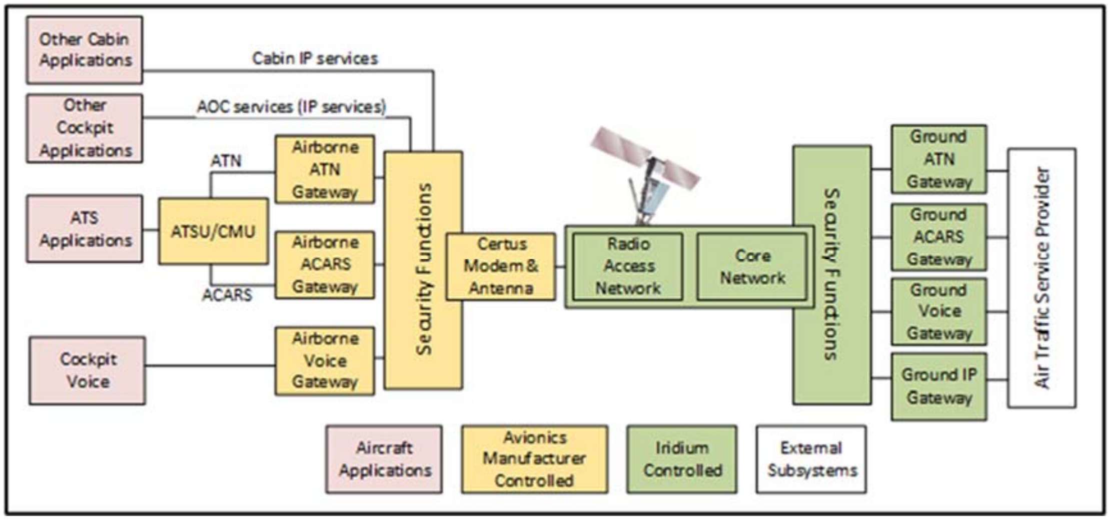


Figure 2-3 – Iridium Certus Safety High-level Architecture

2.4.2.2 Satcom Performance Class A – Longer Term

Satcom Performance Class A will cover more stringent performance requirements (as compared to Class B), such as those required to support full 4D trajectory based operations and future operational concepts being defined by SESAR and NextGen, and it will support both oceanic and continental operations. Class A is applicable to future Satcom systems that are not available today.

The Performance Class A requirements are important since they serve as design drivers and guidelines for the development of the future Satcom systems. In addition, it is desired to develop a global (ICAO) standard for a Satcom system supporting the Class A requirements and allowing different service providers using the same set of avionics to avoid interoperability/interference issues and stimulate equipage.

An input to the definition of the Satcom Performance Class A air/ground datalink standard will be from the work undertaken in the ESA Iris Programme.

It is expected that a Satcom Performance Class A system will operate as an ATN/IPS air/ground subnetwork.

2.4.3 Airport Surface Communications

2.4.3.1 AeroMACS

AeroMACS is a radio IP subnetwork that supports ATC and AOC applications for safety and regularity of flight on the airport surface. It operates on globally reserved ITU spectrum in the C-band (5091-5150 MHz) with locally optional extensions in the 5000-5091 MHz spectrum. ICAO Doc. 10044-AN/514 specifies the AeroMACS technical provisions, supported by the following EUROCAE/RTCA documents:

- ED-222/DO-345, Aeronautical Mobile Airport Communications System (AeroMACS) Profile
- ED-223/DO-346, Minimum Operational Performance Standards (MOPS) for the Aeronautical Mobile Airport Communication System (AeroMACS)
- ED-227, Minimum Aviation System Performance Standards (MASPS) for the Aeronautical Mobile Airport Communication System (AeroMACS)

AeroMACS is based on WiMAX, a cellular technology using a communications profile of the IEEE 802.16-2009 standard that enables the access of Mobile Stations (MS) to user applications on the surface. The Access Service Network (ASN) is provided by a number of Base Stations (BS) that operate in dedicated 5 MHz bandwidth channels and manage the access of the MSs to the common channel accessing configured channels in radio cells. An ASN Gateway (ASN-GW) manages the data path with the Connectivity Service Network (CSN) and handover within the access network.

An AeroMACS network provides an IP convergence sublayer to interface to IPv4 and IPv6 networks and applications on the ground. It supports QoS configuration, traffic prioritization, and AAA security infrastructure.

It is expected that AeroMACS (IPv6) will operate as an ATN/IPS aircraft-to-ground subnetwork.

3.0 ATN/IPS ARCHITECTURES

This section presents general ATN/IPS airborne architecture considerations forming an architectural framework to discuss standardization needs. The level of impact to existing avionics is dictated by the generation of aircraft in a given fleet.

The scope of the on-board ATN/IPS router is shown in the following Context Diagram. Figure 3-1 shows the main functions of the system of interest and the interfaces to the most important external systems.

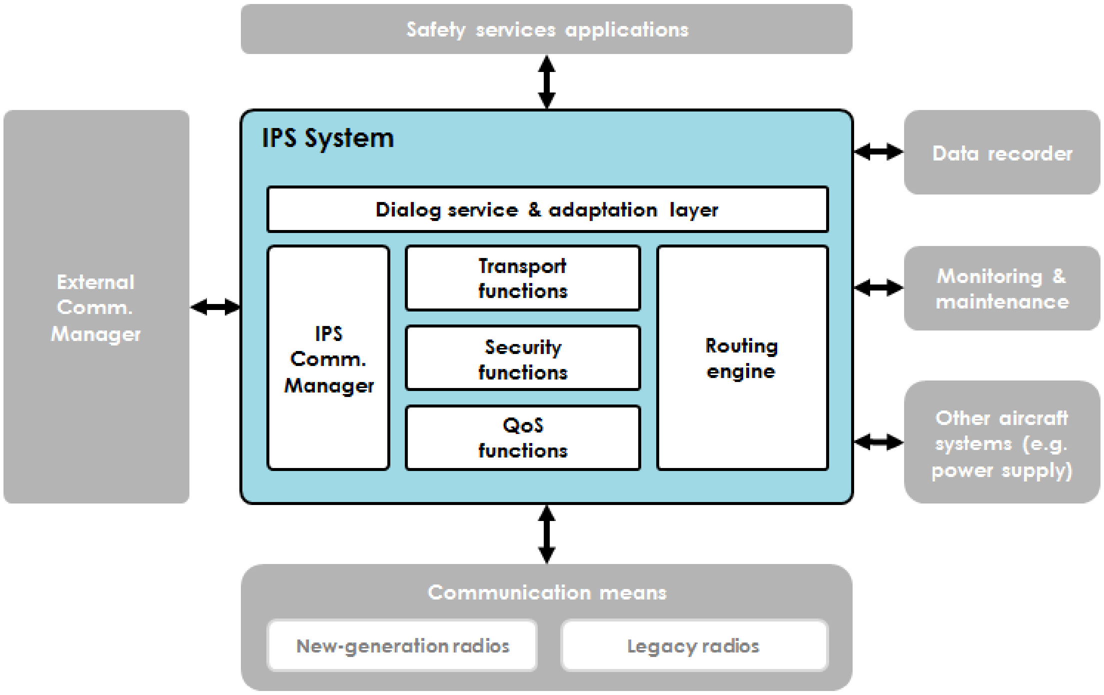


Figure 3-1 – ATN/IPS System Context Diagram – Avionics Perspective

The ATN/IPS system consists of the following main functions:

- **Dialog service and adaptation layer**: Applications may require an adaptation (service) layer over the Transport (e.g., using the ATN/IPS Dialog Service described in ICAO Document 9896 or MIAM over IP for AOC per ARINC Specification 841)
- **Routing engine**: The function of the routing engine is to transfer incoming traffic flow to an outgoing interface directed towards the next-hop interface.
- **Transport function:** It consists of the Transport protocols (UDP, TCP).
- **Security functions**: This entity implements all security functions required to secure the traffic (e.g., authentication, firewall, encryption).
- **QoS functions:** Methods used to optimize and guarantee the performances of high-priority traffic.
- **ATN/IPS Communication Manager:** This function manages the selection of the radio bearer for a dedicated traffic flow and the associated mode of communication. This function works in correlation with the routing module of

the Network and Transport protocols as the routing paths may also depend on the radio bearer.

The ATN/IPS system interfaces with multiple systems in the aircraft, including:

- **Communication means:** Sub-networks connected to Aircraft Control Domain (ACD) can be divided into two categories:
  - Legacy radio systems: Current systems used in aircraft for safety-related operations (VHF).
  - Native IP solutions: Next generation radio systems that are part of the Future Communication Infrastructure (FCI): e.g., AeroMACS, Performance Class A and Class B Satcom, LDACS.
- **Safety services applications:** Entity supporting the Air Traffic and Aeronautical Operational Control Services (ATS and AOC)
- **Data recorder:** Device that records datalink information
- **Monitoring and maintenance:** On-board system performing status monitoring as well as maintenance of the aircraft systems
- **External communication manager:** Function performing router selection and associated vertical handover decisions. This entity may be extended to include the management of multi-domain link selections.

Aircraft may be fitted with dual-stack ATN and ACARS operation (ATN/OSI+ACARS or ATN/IPS+ACARS), but it is not anticipated that aircraft will accommodate both ATN/OSI and ATN/IPS stacks. It is noted that ATN/OSI and ACARS will continue to be used for ATS datalink services in areas that have not migrated to ATN/IPS. This section focuses on ATN/IPS + ACARS dual airborne capability.

The allocation of the ATN/IPS function to the avionics systems will have some similarities on most of the aircraft types of the same generation but differences exist in terms of avionics architecture. Also, several updates may have occurred during the life of certain aircraft, and this has resulted in a large variance in avionics architectures implemented today on aircraft in production and on aircraft in service.

Two main architecture options are considered, as the ATN/IPS implementation on each of them may have significant differences:

- ARINC 429 legacy architecture, based on point-to-point ARINC 429 data buses
- ARINC 664 based architecture, which may also include some ARINC 429 data buses

As shown in Figure 3-1, ATN/IPS is aviation-specific Internet Protocol utilized by aviation communication safety services and related airborne systems. ATN/IPS provides similar functionality offered by ACARS and ATN/OSI protocols.

While many airborne systems use ARINC 429 as the primary interface to the air/ground media link radios, ATN/IPS will interface with various radios using ARINC 429 as well as ARINC 664 Ethernet interfaces. The ATN/IPS networks may support all existing applications which are being deployed using ACARS and ATN/OSI protocol. ATN/IPS also supports future capabilities such as ATN B2 applications and beyond.

The hardware platform hosting ATN/IPS services may vary based on specific implementation and aircraft type. The ATN/IPS system boundaries are shown in

Figure 3-1. The larger system architecture impacts should not propagate beyond the scope of the ATN/IPS message router. The ATN/IPS Roadmap (this document), describes the perimeter where impacts are contained within ATN/IPS network.

3.1 High-Level Requirements and Assumptions

As described in Section 2, the ATN/IPS network infrastructure aims at supporting a wide set of applications. This includes AOC to ATC (ATN B2 and beyond, identified as “ATN B3” in SESAR 15.2.4 documents referred in this document or as ATN B2B in other documents). ATN/IPS is expected to support future ATM applications not defined yet, and therefore must be ready to encompass growing capabilities.

Driven by the support of these applications, a set of general requirements applicable to the ATN/IPS network has been identified and listed in the following sub-sections.

Note: In this section, the “ATN/IPS system” refers to set of equipment that hosts all or part of the airborne functions.

3.1.1 General Requirements

This ATN/IPS Roadmap document identifies high-level target requirements that are expected to be detailed in subsequent industry standards development activities.

<u>Requirement 1:</u> The ATN/IPS system shall provide connectivity to ATS applications via an ATN/IPS air/ground network infrastructure.

Note: These applications are CM, CPDLC, ADS-C and potentially others (for ATN Baseline 2 and future applications ATN B2B or B3).

<u>Requirement 2:</u> The ATN/IPS system shall provide connectivity to AOC safety applications hosted in avionics via an ATN/IPS air/ground network infrastructure.

> Note: Any AOC application considered as Safety (ICAO definition) should have access to ATN/IPS. These applications will be connected to ground AOC applications hosted at Airline premises or by third parties.
>
> Note: The ATN/IPS system may provide connectivity to AOC applications hosted in AIS domain (e.g., EFB) via an ATN/IPS air/ground network infrastructure. This capability may not be possible on each type of architecture (e.g., due to data security considerations).

<u>Requirement 3:</u> The ATN/IPS system shall be able to utilize multiple communication means.

> Note: Several communication means are candidate to support ATN/IPS, e.g., AeroMACS, LDACS, future Satcom.
>
> Note: The ATN/IPS system must be able to utilize multiple communication means simultaneously. This concept will be defined in ICAO Document [TBD].

<u>Requirement 4:</u> The ATN/IPS system shall support mobility management.

> Note: The goal is to minimize the complexity of this capability on the aircraft.

<u>Requirement 5:</u> ATN/IPS mobility solution shall minimize the volume of routing/connectivity information exchanged on the air/ground segment.

Note: The goal is to and optimize air/ground links performance.

Requirement 6: The ATN/IPS system shall support QoS and Airline policy driven media selection.

Main assumptions:

Assumption 1: ATN/IPS system is part of dual (ACARS and ATN/IPS) stack airborne architecture

Note

1. Triple stack (ATN/OSI, ATN/IPS and ACARS) is not envisaged.
2. ACARS/ATN/IPS system may replace the existing ACARS/OSI router for retrofit.

Assumption 2: Functional interface between ATC applications and the ATN/IPS system should be same as for ATN/OSI (Dialogue Service Interface on top of the Transport layer)

Rationale: The introduction of ATN/IPS for replacing ATN/OSI in an existing architecture should have limited or no impact on the ATC applications.

Note: As CM application manages ATN addresses (OSI or IPS) several options need to be assessed.

Assumption 3: ATN/IPS system will be IPv6 only

Note: IPv6 communication stack offers all the necessary addressing, mobility and security mechanisms.

3.1.2 Safety Requirements

While ATN B1 and B2 safety and performance requirements are well-known, only preliminary requirements are available for beyond B2 (delivered by SESAR). The future ATS operational concepts are not yet mature.

Nevertheless, as ATN/IPS aims at supporting B2 and applications beyond B2, the ATN/IPS specification needs to consider all the relevant requirements and the feasibility of the most stringent should be at least assessed.

When supporting B2 applications, ATN/IPS replaces or provides the alternative network layer and transport layer communication protocols. Failure condition does not change or remains the same as existing communication management Software/System. Safety and design assurance level is same as the ATN/OSI per RTCA DO-178C, DO-278 or EUROCAE ED-12C Design Assurance Level D (DAL D).

For other services and in particular, beyond ATN B2 applications, a higher design assurance level may be required.

A preliminary study for future ATM services (beyond ATN B2) has been conducted in the scope of the SESAR 15.2.4 project. In particular, with the support of these services, ATN/IPS is expected to contribute to functions with minor to major safety impact:

In this section, the considerations below are relevant for beyond ATN B2 ATM services.

Table 3-1 shown below provides a summary of expected performances:

Table 3-1 – Qualitative Safety Requirements Anticipated for Future ATM Services (Extract from SESAR 15.2.4-D4)

Hazard (per EUROCAE ED-228)		**ATN-B2**	**ATN-B3/IP**
OH-CPDLC-1	Detected loss of CPDLC capability [single aircraft]	SC4 (Minor)	SC3 (Major)
OH-CPDLC-2	Detected loss of CPDLC capability [multiple aircraft]	SC4 (Minor)	SC3 (Major)
OH-CPDLC-4	Detected reception of corrupted CPDLC messages [multiple aircraft]	SC4 (Minor)	SC3 (Major)
OH-CPDLC-6	Detected reception of unintended CPDLC message [multiple aircraft]	SC4 (Minor)	SC3 (Major)
OH-CPDLC-8	Detected unexpected interruption of CPDLC transactions [multiple aircraft]	SC4 (Minor)	SC3 (Major)
	Undetected unexpected interruption of CPDLC transactions [multiple aircraft]	SC4 (Minor)	SC3 (Major)

Operational Hazard “OH-CPDLC-1” (Detected loss of CPDLC capability [single aircraft]), could have a Severity Level SC3 (Major) in the future, which would be one level more than the severity of the same OH considered in the scope of ATN Baselines 1 and 2, where this OH is classified “SC4 – Minor”.

The “OH-CPDLC-1” event may happen at Aircraft level due to one of the following basic causes:

- A detected loss of the Aircraft ATC applications
- A detected loss of the aircraft ATN/IPS communications, which should encompass all failure cases on aircraft ATN/IPS routing system that lead to an ATN/IPS communication failure

This second cause applies to the ATN/IPS system itself which is therefore part of the fault tree supporting this major failure condition.

Other causes linked to the detected and non-detected loss of the communication means can also be identified. This is outside the scope of this document.

Note: Underlying communications bearers themselves would contribute to all detected hazards identified in Table 3-2, not just loss of capability.

The fault tree of “OH-CPDLC-1” allows identifying the following safety objectives onto the ATN/IPS network:

Table 3-2 – Safety Objectives for the ATN/IPS Network

The likelihood of a detected loss of ATN/IPS communication due to a failure of the Aircraft ATN/IPS routing system shall be less than 1x10^{-6} flight hours.
The detected loss of ATN/IPS communications, due to a failure of the aircraft ATN/IPS routing system, and which leads to a situation where it can be determined that CPDLC should not be used anymore, shall be considered MAJOR.
Loss of the ATN/IPS routing system shall be considered MAJOR

The quantitative safety objective for the ATN/IPS routing system implies that the likelihood of a failure of the aircraft ATN/IPS routing system shall be less than 1x10^{-6} flight hours. Such an objective is difficult to achieve with one single airborne ATN/IPS router, because, with current technology, availability of complex avionics equipment items is generally known to be lower than 1x10^{-5} flight hours.

Therefore, aircraft may be equipped with two redundant ATN/IPS routers to meet the safety requirements. This will have an impact on the ATN/IPS system design and all its interfaces.

The loss of ATN/IPS routing capability is to be considered as a Major failure condition. This will translate, by following ARP4754 guidelines, into a choice of several options regarding the Development Assurance Level of the ATN/IPS router equipment as follows:

- Two dissimilar redundant ATN/IPS routers, which are DAL D
- Two identical ATN/IPS routers, which are DAL C
- A single ATN/IPS router, which is DAL C, and which reliability meets the targeted quantitative safety objective (1x10^{-6} flight hours)

In a global safety analysis including the communication means (e.g., future Satcom, LDACS) multi-link concept may also need to be considered.

Even if this safety study is preliminary and future ATM services are not yet fully specified, the following requirements should be considered:

Requirement 9: ATN/IPS system architecture shall allow a redundant ATN/IPS routing function.

Assumption 4: For beyond ATN B2 applications support, ATN/IPS router may be developed to DAL C.

3.1.3 Security Requirements

This section contains information security considerations that are intended for the system designers involved in the development of IPS for Aeronautical Safety Services, including Air Traffic Services (ATS) and Aeronautical Operational Communications (AOC).

It provides guidance and constraints that will assist in the development of ATN/IPS airborne architectural designs (see Section Section 3.2 ATN/IPS Implementation Considerations) that is intended to satisfy regulatory requirements by providing adequate risk mitigation against threats.

The increasing use and importance in new airplane designs of airborne networks based on standard ARINC 664 Ethernet and IP protocols results in a significant new arena of information systems security risks that must be understood and adequately mitigated or controlled.

From a security perspective, aircraft network systems are divided into three domains as described in ARINC 664 Part 5 Network Domain Characteristics:

- Aircraft Control Domain (ACD)
- Airline Information Services Domain (AISD)
- Passenger Information and Entertainment Services Domain (PIESD)

It should be noted that these domains are primarily defined for functional purposes, and do not necessarily imply or correlate to specific assurance requirements.

The ATN/IPS system must satisfy security requirements. This is particularly the case when it is providing ACD services and to a lesser extent to AISD services. FANS services (e.g., ADS-C and CPDLC) and AOC safety services are viewed as ACD while EFB and non-safety AOC services are viewed as AISD.

The security requirements must ensure that the functions (shared or independent) contained within the airborne ATN/IPS system can provide adequate segregation between domains and withstand potential threats that are introduced by its use in an open air/ground network environment.

Security Process

The airworthiness security process defined in RTCA DO-326A / EUROCAE ED-202A (Airworthiness Security Process Specification) helps to ensure that all potential security threats have been accounted for and that the threats are adequately mitigated when there is a potential safety impact due to a security failure. It is intended to align closely with SAE ARP4754A: Guidelines for Development of Civil Aircraft and Systems.

At a high level, it defines the following steps in the security process:

1. Identify the security scope to determine the points of entry to the system
2. Identify the security threats that can attack those entry points
3. Develop the security architecture
4. Assess the preliminary security risk
5. Assess the final security risk
6. Verify the implementation
7. Ensure the security of the final product

3.1.3.1 High-Level Security Objectives

When designing a secure system, it is important to first document the overall security objectives.

These objectives are typically based on the experience of the system designer and security experts, and guided by an understanding of the functional role of the system, the threat environment in which it will operate and its criticality level. These general objectives are intended to be augmented through the risk assessment conclusions (see Appendix E) and further refined into both avionics and ground security requirements (see Sections 3.1.3.3, 3.1.3.4, and 3.1.3.5).

3.0 ATN/IPS ARCHITECTURES

The following high-level objectives have been identified for the design of the airborne system supporting ATN/IPS. They are not in ranked order and should all be taken into consideration for a system design:

- The ATN/IPS system should use protocols and systems that are commonly used to provide security controls (e.g., IPSec, firewall), and minimize the numbers and types of protocols to the greatest extent possible;
- The ATN/IPS system should ensure that security threats targeting the ATN/IPS system or using the ATN/IPS system as an attack vector cannot cause any safety impact to the aircraft;
- The ATN/IPS system should use separate physical interfaces for administrative functions and regular communications;
- The ATN/IPS system should provide a means for verifying the integrity of the running software image;
- Security controls must be effective at performing their intended security functions during all operational modes, while not unduly interfering with the safe aircraft operations or not unduly complicating maintenance and airline operations activities;
- Security controls selected should induce minimal or no impact on existing systems. They need to support an environment with either native IPv6 future applications or with legacy applications;
- Security controls must not introduce overhead and latency to safety communications such that satisfaction of RCP requirements is negatively impacted;
- Security controls must be designed to be field-updatable, so that components like encryption algorithms can be updated or replaced when required by a changing threat environment;
- Security functions, such as those using encryption, should support flexibility in configuration to enable global use, i.e., including over and in countries with more restrictive controls on the use of cryptography;
- Security functions, such as those using digital certificates, should be able to leverage existing implementations on the aircraft network versus creating new instances that result in higher operational overhead;
- Robustness of security functions should be based on open standards, and not depend on security through obscurity;
- Security functions must leverage existing standardized logging formats and facilities whenever possible, e.g., ARINC 852-compliant;
- Careful consideration should be given to security controls that would otherwise “fail closed”, when there would be a safety impact resulting from this;
- Digital certificate formats used for ATN/IPS must comply with the profiles defined in ATA Spec 42;
- The digital certificate management lifecycle for ATN/IPS must comply with ARINC 842;
- Data loading functions should be designed to preclude the creation of new vulnerabilities that could be exploited by an attacker or malware directed at the system software or that of any connected system;

- Data loading operations should be performed only when explicitly enabled by authorized maintenance personnel;
- The ATN/IPS system should employ security controls that authenticate the message source and mitigate message alteration and message replay attacks through each safety-related communication link;
- The ATN/IPS system should employ security controls to prevent attacks that would result in the decreased or loss of availability of services (e.g., denial of service).

3.1.3.2 Design Principles for Secure Airborne Architectures

Introduction of ATN/IPS will require the applicants to demonstrate that security risks linked to this new capability are identified, assessed and mitigated.

In particular, it is expected that any new application for aircraft systems that directly connect to external services and networks will have to comply with Special Conditions identified by FAA and/or EASA.

For instance, the FAA Special Conditions applicable to Airbus Model A350-900 (similar for Boeing Model B787 and B747-8) are the following:

- Airbus Model A350-900 Airplane; Electronic System-Security Protection from Unauthorized External Access [Docket No. FAA-2013-0909; Special Conditions No. 25-533-SC]:
    - Extract: The applicant must ensure airplane electronic system-security protection from access by unauthorized sources external to the airplane, including those possibly caused by maintenance activity.
- Airbus Model A350-900 Airplanes; Isolation or Protection of the Aircraft Electronic System Security from Unauthorized Internal Access [Docket No. FAA-2013-0910; Special Conditions No. 25-534-SC]:
    - Extract: The applicant must ensure that the design provides isolation from, or airplane electronic system security protection against, access by unauthorized sources internal to the airplane. The design must prevent inadvertent and malicious changes to, and all adverse impacts upon, airplane equipment, systems, networks, or other assets required for safe flight and operations.

This is a strong driver for the airborne and global architecture.

To meet these regulations, the following rules and best practices apply:

- Provide two security barriers (or one simple device) in front of critical assets
- Ensure that no common vulnerability can affect the two barriers
- Provide at least one security barrier on each identified attack path
- Security barrier shall be fail-secure and not possible to bypass
- System shall be delivered free of malicious code
- Provide the capability to recover the aircraft in normal operation after security event

Therefore, the following key architecture drivers should be considered. Aircraft security architecture shall be based upon layered protection capabilities:

- This principle of defense-in-depth enhances system resilience by helping to ensure continued secure operation in the event of individual security control failure or in response to changes in the threat environment (e.g., time for security patches)
- It also contributes to regulatory compliance and safety objectives by eliminating common mode and single-point of failures

At least one on-board security barrier shall be implemented on each threat attack path between threat sources and the assets

- The number of security barriers required is defined by value of the asset to be protected and the related aircraft safety impact
- The assets with the highest safety impact (strong and very strong safety impact, corresponding to hazardous and catastrophic impact as per FAR 25.1309) will require two barriers of protection or an equivalent simple device, based on simple hardware, limited source code and exhaustive security evaluation

Guidance material is available that provides a minimum set of security guidance for airworthiness certification based on the latest version of the following industry standards:

- Airworthiness Security Process Specification, RTCA DO-326 / EUROCAE ED-202
- Airworthiness Security Methods and considerations, RTCA DO-356 as harmonized with EUROCAE ED-203.
- ARINC Report 811: Commercial Aircraft Information Security Concepts of Operation and Process Framework

3.1.3.3 General Security Requirements

Based on the preliminary risk assessment shown in Appendix E, the following general security requirements are defined:

Security Requirement 1: Air/ground authentication through secure links shall be ensured in order to mitigate spoofing threats and provide a message recipient with assurance that the source of a message is as claimed.

Based on ICAO recommendations, the aircraft shall not be denied service by the ground, but the ground could be denied service by the aircraft. Mutual authentication may be required:

- Airborne segment: The ATN/IPS system shall request authentication from ground systems (i.e., ATC center and Airline Operations Centers) to aircraft entity
- Ground segment: The ground ATN/IPS infrastructure shall request authentication from aircraft entity to ground systems (i.e., ATC center and Airline Operations Centers)

  Note: Datalink Service Provider sub-network access is outside the scope of this document.

Security Requirement 2: Air/ground dataflow integrity through secure links shall be ensured to prevent message alteration threats (including unauthorized message modification, insertion, substitution, replay, and/or deletion attacks).

Commentary: ICAO SARPS are viewed to be applicable to all countries rules and regulations including technical specification and guidance on Air Navigation Cyber Security; ICAO Document 9985, ATM Security Manual (2020) Amendment to Annex 10 Volumes II and III. Deviations may have an adverse impact on ATN/IPS services.

Security Requirement 3: Air/ground dataflow confidentiality should be ensured if needed to protect some specific data exchanged.

Note: As security countermeasures are specified and developed, consideration must be given to variations in regulations from country to country on use of tools like cryptography.

Note: However, while more flexibility is desirable in many cases (e.g., adapt to in regulations from country to country, response to changes in the threat environment), less flexibility and limited options may be necessary to achieve aircraft certification.

Security Requirement 4: The ATN/IPS system shall be developed with requirements identified by the appropriate Security Assurance Level (SAL). The SAL will be confirmed by a detailed security risk analysis based on the final architecture.

Note: In particular, security controls selected shall be developed in a manner that supports a high degree of confidence that the control is complete, consistent, and correct.

Note: Security assurance requirements define the following classes of assurance processes for an avionics system: configuration, management, maintenance of assurance, development, life cycle support, tests, delivery and operation, guidance documents and vulnerability assessment.

Security Requirement 5: Security controls put in place by the overall ATN/IPS infrastructure should be designed in such a manner as to maximize the likelihood of an intrusion detection and identification of the threat agents responsible.

Security functional requirements will include requirements for audit function (including its management), cryptography management (certificates and keys management, algorithms agility), data protection, other potential authentication needs, security management, potential privacy issues, and protection of security functions.

3.1.3.4 Avionics Security Requirements

The assessment of the airborne ATN/IPS system architecture is based on the following assumptions and key operational requirements for its security environment:

- The ATN/IPS system software parts are assumed to be RTCA DO-178 / EUROCAE ED-12 Level C or Level D design assurance levels (see Section 3.1.2 Safety Requirements)
- Maintenance personnel will follow approved procedures including MRO personnel
- The system designer, operator, and regulator agree on a characterization of the likelihood and severity of maintenance personnel errors, including the

possibility that malware may be unknowingly carried to the airplane on a maintenance terminal or any mass storage device

- Flight crews will follow approved procedures
- The system designer, operator, and regulator agree on a characterization of the likelihood and severity of flight crew errors, including the possibility that malware may be unknowingly carried to the airplane on a portable crew device (e.g., EFB laptop, tablet, USB sticks)
- Physical access to the ATN/IPS system items is controlled to the same degree as physical access to other installed on-board electronic systems in general (i.e., avionics E/E bay). That is, there are no special access physical control requirements, nor is access control requirements relaxed
- ATN/IPS router is not logically mixed with AISD router or PIESD router
- The security requirements of the ground infrastructure and communication links networks are an important part of the overall end-to-end security
- Interfaced systems at higher level of trust do not serve as a launching point for attacks on the ATN/IPS system:
  - Higher-assurance systems are not corrupted by attackers;
  - Such systems may not provide any protection to the ATN/IPS system if attacks are simply passed through them to the ATN/IPS system, thus enabling the attack vector;
- Any such dependencies should be evaluated for each installation.

Based on the preliminary risk assessment shown in Appendix E and the assumptions above, the following avionics security requirements are defined:

<u>Security Requirement 6:</u> In case of implementation of air/ground secure links through PKI authentication. ICAO Documents 9880 and 9896 have recommended PKI as the chosen method for security. The ATN/IPS system shall implement certificate validity verification checks (e.g., expiration dates, non-revoked certificate) along the overall trust path from the end-users to the root CA.

<u>Security Requirement 7:</u> The ATN/IPS system shall ensure by design that all management flows associated with the air/ground authentication set-up (e.g., CSR, CRL) will not provide the opportunity for an attacker to upload malevolent data.

> Note: CSR and CRL could be non-fully authenticated dataflows. Thus, to prevent bypass of the mutual authentication, the supplier should provide a design that protects the system against malevolent data coming over these channels.

<u>Security Requirement 8:</u> The ATN/IPS system shall be protected by a filtering function allowing only a defined subset of communication on its interfaces (i.e., whitelist of authorized IP addresses and protocols).

<u>Security Requirement 9:</u> The ATN/IPS system shall provide protection against flooding to mitigate denial-of-service attacks.

<u>Security Requirement 10:</u> The ATN/IPS system shall provide protection against replay attacks to avoid replay-based masquerading attacks.

<u>Security Requirement 11:</u> The ATN/IPS system shall be fault tolerant and have no security flaws in case of partial or total failure. During these non-nominal conditions,

security protections of ATN/IPS system shall not degrade performance or interfere with the safe, continued operation of aircraft.

Security Requirement 12: Security protections implemented for the ATN/IPS system should minimize administrative and operational overhead. In particular, specific actions by cockpit or cabin crew during operation should be not required.

Security Requirement 13: The ATN/IPS system shall issue security audit logs in order to give capabilities to investigate and contribute to identify security root causes.

3.1.3.5 Ground Security Requirements

Based on the preliminary risk assessment shown in Appendix E the following ground security requirements are defined:

Security Requirement 14: Only authorized entities should be able to access ground ATN/IPS infrastructure:

- Ground ATN/IPS systems shall employ security controls that limit access to users, services and devices authorized to access air traffic services and interact with ATS systems;
- Ground ATN/IPS systems shall employ security controls that limit access to users, services and devices authorized to access AOC services and interact with AOC systems.
- Ground ATN/IPS systems and networks shall ensure that flooding attacks do not reach the forward links to the aircraft.

3.1.4 Performance Requirements

When supporting ATN B1 or B2 applications, allocated RSP-180, RCP-130 and RCP-240 are applicable. Performance related to timing and continuity requirements remain the same.

For future applications (beyond ATN B2), a preliminary study for future ATM services has been conducted in the scope of the SESAR 15.2.4 project. Table 3-3 shown below provides a summary of expected performances:

Table 3-3 – Performances Requirements of Future ATM Services (extract from SESAR 15.2.4-D04)

Performance Parameter	**ATN B1 ED120 SPR Standard published Based on Eurocontrol Generic ACSP Requirements doc.**	**B2 ED-228 SPR Standard published Based on most stringent RCP130/RSP160**	**B3 SESAR 15.2.4 predicted (no standards started) Based on most stringent RCP60/RSP60**
Transaction Time One way (sec)	4 – 95% of messages 12 – 99.9% of messages	5 – 95% of messages 12– 99.9% of messages	2 – 95% of messages 5 – 99.9% of messages
Transaction Time Two way (sec)		10 – 95% of messages 18 – 99.9% of messages	4 – 95% of messages 8 – 99.9% of messages
Availability - CSP	0.999	0.9995	0.999995 (maybe reduced by multi-link)
Availability - Aircraft		0.99	0.999
Integrity	1-10-5	Not specified Must be good enough to meet RCP/RSP	Not specified Must be good enough to meet RCP/RSP
Security	Physical protection Unauthorized access	Not specified but Unauthorized access protection needed, ICAO requirements	Technical security requirement likely

It is expected that apportionment of these performance requirements on the airborne segment will **be as a minimum similar to ATN B2 applications**, but likely more stringent.

Assumption 1: QoS functions will be required to meet the timing performance with acceptable overhead and without over-dimensioning the network.

Rational: In particular, AOC traffic shall not affect ATC performances. Quality of service requirements can be met by over-provisioning the infrastructure so that data flows never encounter congestion at any layer (even during rate peak loads) and always have an available alternative routing option if a link fails, even in unusual circumstances. Such an approach may not be practical. The more practical approach is to dimension the infrastructure based on typical requirements and manage load peaks and capacity drops (e.g., link failures) through in-network QoS management mechanisms.

Assumption 2: The mobility solution will have an impact on the timing performance during handovers.

Rational: Mobility management will cause re-routing of data within the ATN/IPS inter-network as the connectivity of the aircraft to the ground networks changes. The ability of the mobility solution to minimize or avoid end-to-end connectivity outages during these handovers is an important performance indicator as this could be a significant factor towards the maximum end-to-end delay through the network.

Assumption 3: The multilink solution will be introduced to improve the timing and availability performances (depending on the definition of multilink).

Rational: In many cases the aircraft will have multiple air/ground links available for a given data flow. In general, the airborne ATN/IPS system will select the best link to be used at any given time. There are however cases where:

- The choice of best link changes. In such cases, an efficient handover mechanism should aim to minimize loss of availability (and therefore delay) of end-to-end connectivity.
- The performance (availability, bandwidth) of any one of the available links on its own is not sufficient for the flow's required service level. In such cases, it may be advantageous to use multiple links in parallel (e.g., duplicating packets to improve availability or load sharing to improve bandwidth and lower queues).

Assumption 4: The air/ground datalink capacities represent a constraint for service availability, i.e., if the "high priority" messages load consistently exceeds link capacity there will be loss.

Rational: Quality of service mechanisms enable efficient use of existing resources, but do not improve the performance of the resources themselves. The burst nature of most traffic means that the available bandwidth can generally only be characterized by a mean and peak load values. The system must be dimensioned to accommodate at least the mean rate. QoS mechanisms then ensure the most important traffic gets serviced preferentially when the offered load exceeds capacity.

3.2 Integration of ATN/IPS in Avionics Architectures

Current architectures, before the introduction of ATN/IPS, are described in APPENDIX D.

3.2.1 Integration of ATN/IPS in ARINC 429 Avionics Architectures

First thoughts on ATN/IPS implementations are provided below. These considerations aim at clarifying the detailed scope of AEEC standardization needs.

General and security considerations:

- ATN/IPS system architecture shall provide means for guaranteeing a not to exceed delay for messages processing. It shall be deterministic in order to demonstrate the required performances (transaction time).
- The ATN/IPS system could be hosted either in the ATSU/CMU or in dedicated/standalone equipment, taking into account that segregation is likely required for providing a layered security solution.
- In this architecture, a first security barrier would be the trusted channel (e.g. VPN) implemented between the airborne and ground gateways (assumed that the ground infrastructure is trusted and the ground gateway is certified), and a second barrier (if necessary) could be a security device between the ATN/IPS router and the CMU/ATSU. Other options could be envisaged for this second barrier.

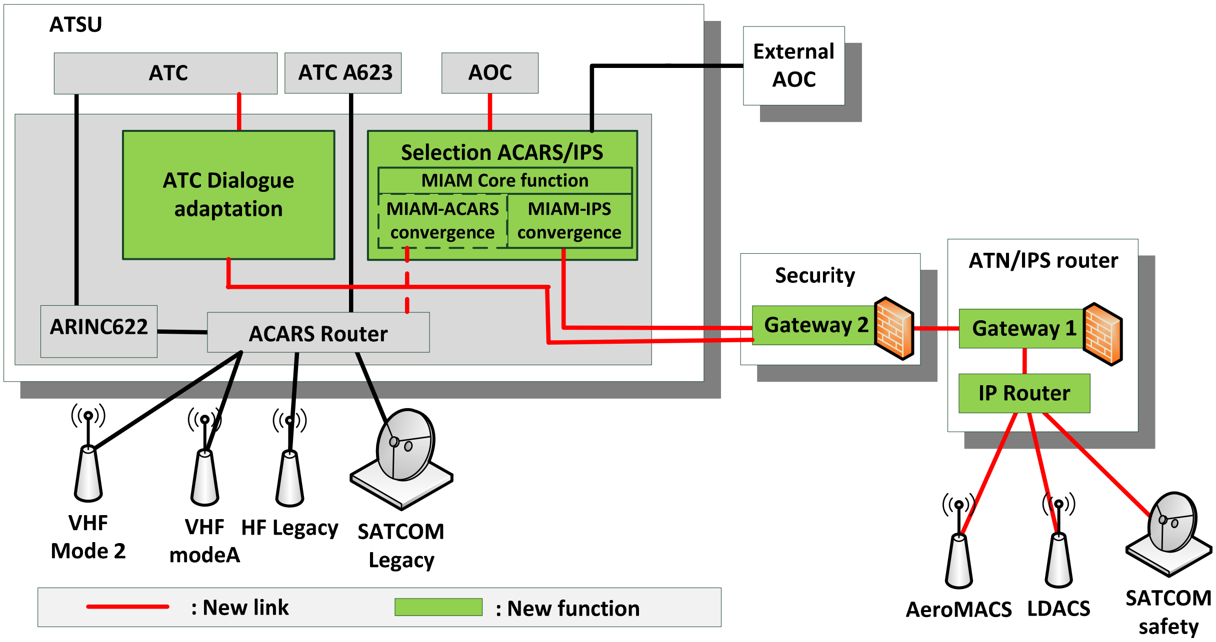


Figure 3-2 – Example ATN/IPS High-Level Architecture in ARINC 429 Legacy Environment

- The ATN/IPS system may interface with AOC applications through a simple and dedicated messaging service (e.g., MIAM over IP)
- Selection between ACARS and ATN/IPS is implementation dependent. There is no need for standardization.
- The ATN/IPS system architecture and security design will take the assumption that communication means are secured (e.g., VPN). Current definition of SBB safety “Light Cockpit Satcom” can be considered for a first layer of defense if the ground gateway is certified. See ARINC Characteristic 781, Supplement 8 and later. Other media (e.g., AeroMACS, LDACS) would implement similar mechanisms and will be certified.
- End-to-end security (e.g., between airborne and ground ATC systems) should be implemented in the ATN/IPS system rather than in the applications.
- The ATN/IPS system must segregate the flows between ATC and AOC. ATC communications should not be compromised by AOC traffic.

Physical interface considerations:

- Interfaces with the communication means (radios) should be based on Ethernet and standard protocols (e.g., PPPoE)

  Note: ARINC 429 could also be used on legacy aircraft (as for Iris Precursor Satcom and new types of L-Band Satcom services).

- Interfaces with the ARINC 619 peripherals (e.g., FMS, FWS) should be based on ARINC 429
- Interfaces with the AOC applications (using MIAM protocol) could be based on ARINC 429 or ARINC 664 Ethernet.

- If implemented in a different equipment, interface with the ATC applications (hosted on ATC) should be based on ARINC 429 or ARINC 664 Ethernet

Logical interface considerations:

- If implemented in a different equipment, the functional interface between CMU/ATSU and the ATN/IPS system could be at Dialogue Service level.

  Note: In ATN, this Dialogue Service is almost similar to the Transport Service.

- For IHM purpose, the airborne ATN/IPS system should use an ARINC 739 MCDU to interface with the CDU.
- The airborne ATN/IPS system may use VDLM2 via ARINC 429 for IP communication, using a dedicated IPI value to multiplex IP data and AOA and ISO8208.

3.2.2 Integration of ATN/IPS in ARINC 664 Avionics Architectures

ATN/IPS implementation considerations include the following:

General and Security Considerations:

- The ATN/IPS system architecture shall provide the means for guaranteeing a not to exceed delay for messages processing. It shall be analyzable and measurable to determine that it is meeting the required performance.
- The ATN/IPS system could be hosted either in an IMA (Integrated Modular Avionics) partition or in dedicated equipment, taking into account that segregation is likely required for providing a layered security solution. Moreover, it is preferable to have a multi-program approach for the ATN/IPS network. Even if integrated in a different way depending on the aircraft type, it is suitable that the ATN/IPS router is common to all aircraft types. This could justify the preference for a dedicated equipment.
- In this architecture, a first security barrier would be the trusted channel (e.g. VPN) implemented between the airborne and ground gateways (assumed that the ground infrastructure is trusted and the ground gateway is certified). A second barrier could be a security device between the ATN/IPS router and the IMA module hosting the ATC applications. Other options could be envisaged for this barrier.

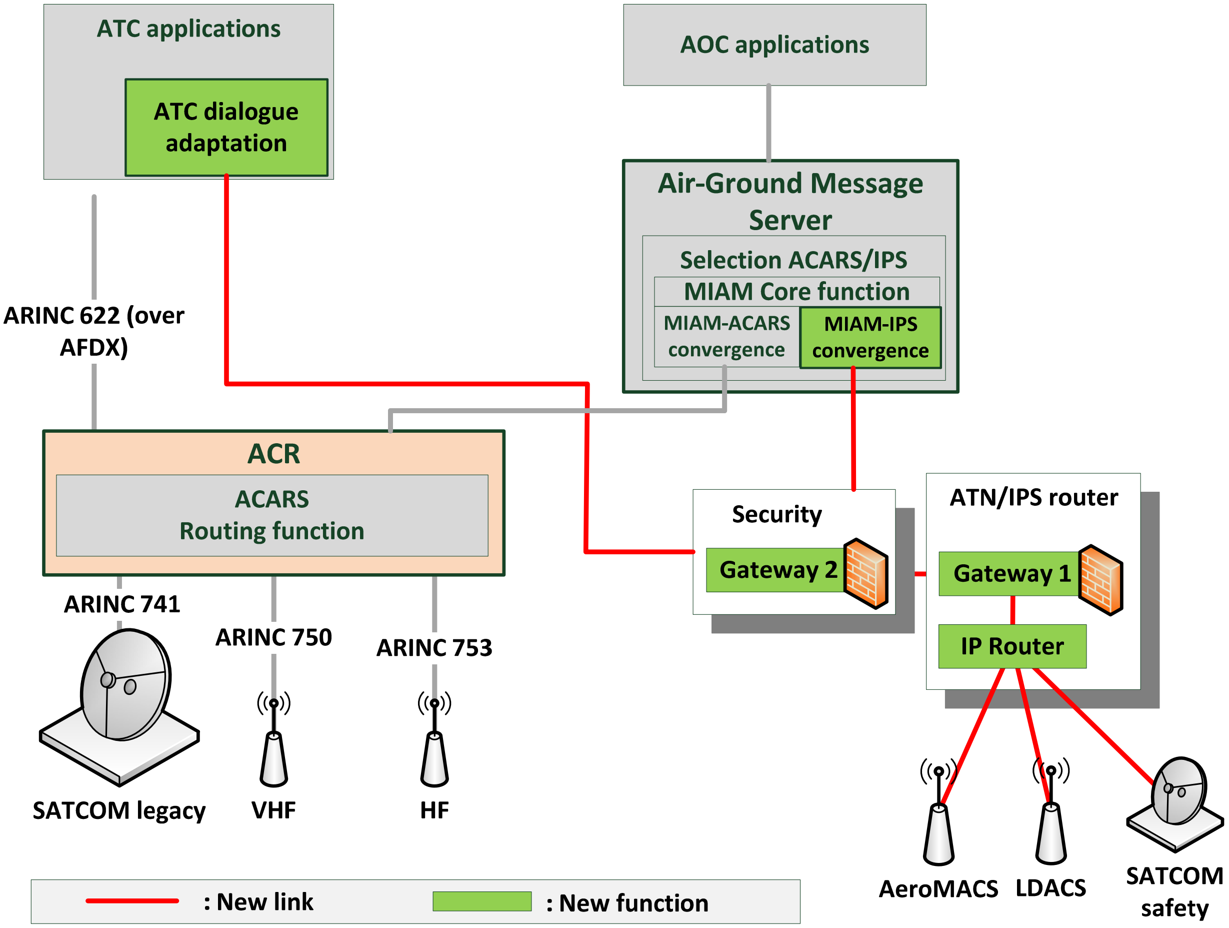


Figure 3-3 – Possible ATN/IPS high level architecture in ARINC 664 environment

- Systems hosting ATC and AOC applications on the ACD network shall be reachable from the ground, but security mechanisms need to be in place to control flow of traffic from the ground to systems on the ACD network.
- ATN/IPS network could interface with the AOC applications through a new simple and dedicated messaging service (e.g., MIAM over IP)
- Selection between ACARS and ATN/IPS should remain implementation dependent (no need for standardization)
- The ATN/IPS network architecture and security design will assume that communication means are secure (e.g., VPN). The definition of Inmarsat SBB safety services can be considered for a first layer of defense if the ground gateway is certified. See ARINC Characteristic 718 Supplement 8 and later. Other media (e.g., AeroMACS, LDACS) will implement similar mechanisms and will be certified.

To protect the Aircraft Control Domain (ACD) from malicious IP traffic, the ATN/IPS implementation must provide the following:

- Prevent, at the earliest moment possible, unauthorized IP traffic from entering the ACD
- Prevent unauthorized IP traffic to reach any aircraft systems directly interfaced with the aircraft radios and with the airborne ATN/IPS router

- Offer at least two independent security barriers

End-to-end security (e.g., between airborne and ground ATC systems) should be implemented in the ATN/IPS system. The ATN/IPS network must segregate the flows between ATC and AOC (ATC communications should not be threatened by AOC traffic). Use of the Secured Dialogue Service solution may provide end-to-end security, but it may be insufficient from the perspective of network security.

<u>Physical interfaces considerations:</u>

- Interfaces with the communication means (radios) should be based on ARINC 664 Ethernet and standard protocols (e.g., PPPoE)
- Interface with the ATC applications should be based on ARINC 664 Ethernet or point-to-point
- Interface with the AOC applications should be based on ARINC 664 Ethernet or ARINC 664 Part 7.

3.2.3 Considerations for Future Avionics Architectures

The concept of aircraft network domains (ACD, AISD, PIESD) may evolve.

With the emergence of new radio technologies (e.g., SDR), new concepts of communication cabinets with a more integrated Data Link function could be considered.

The continuous need for more aircraft data communications and the overall modernization of Air Traffic Management, with the introduction of new radio bearers such as AeroMACS, LDACS and Iris, will certainly necessitate a significant evolution of the aircraft communication systems in the following decade and beyond. SESAR has identified the need for new “supporting capabilities” with in particular:

- Multilink management, which is a key part of the ATN/IPS standardization effort,
- Flexible Communication Avionics, which refers to the development of Software Defined Radio (SDR) terminals.

Major European research projects, including SANDRA, SESAR and Clean Sky 2, have made clear that the legacy communication systems have strong limitations. The introduction of new capabilities in the so-called federated architectures implies penalties for the airlines including additional weight, power consumption and volume.

Those projects, as well as Eurocontrol, express the need to investigate the use of Software Defined Radio technology in avionics systems. It is envisaged that SDR will increase the flexibility of the system, especially allowing easier radio capability upgrades. In addition, when coupled with advanced distributed architectures, SDR can bring additional benefits in terms of SWaP (Size, Weight and Power) by integrating multiple functions on the same processing platform.

The deployment of those new radio-communication systems in the aircraft may have an impact on the overall architecture and, in particular, on the installation of future IPS routers.

3.3 Ground Segment Considerations

This section provides a high-level description of ground gateways and accommodation considerations. Current ground system deployments supporting air/ground data communications with aircraft are as follow:

- FANS: Oceanic Centers and FAA Data Comm
- European CPDLC Mandate for ATN-B1
- European CPDLC Mandate for ATN-B1 with FANS Accommodation

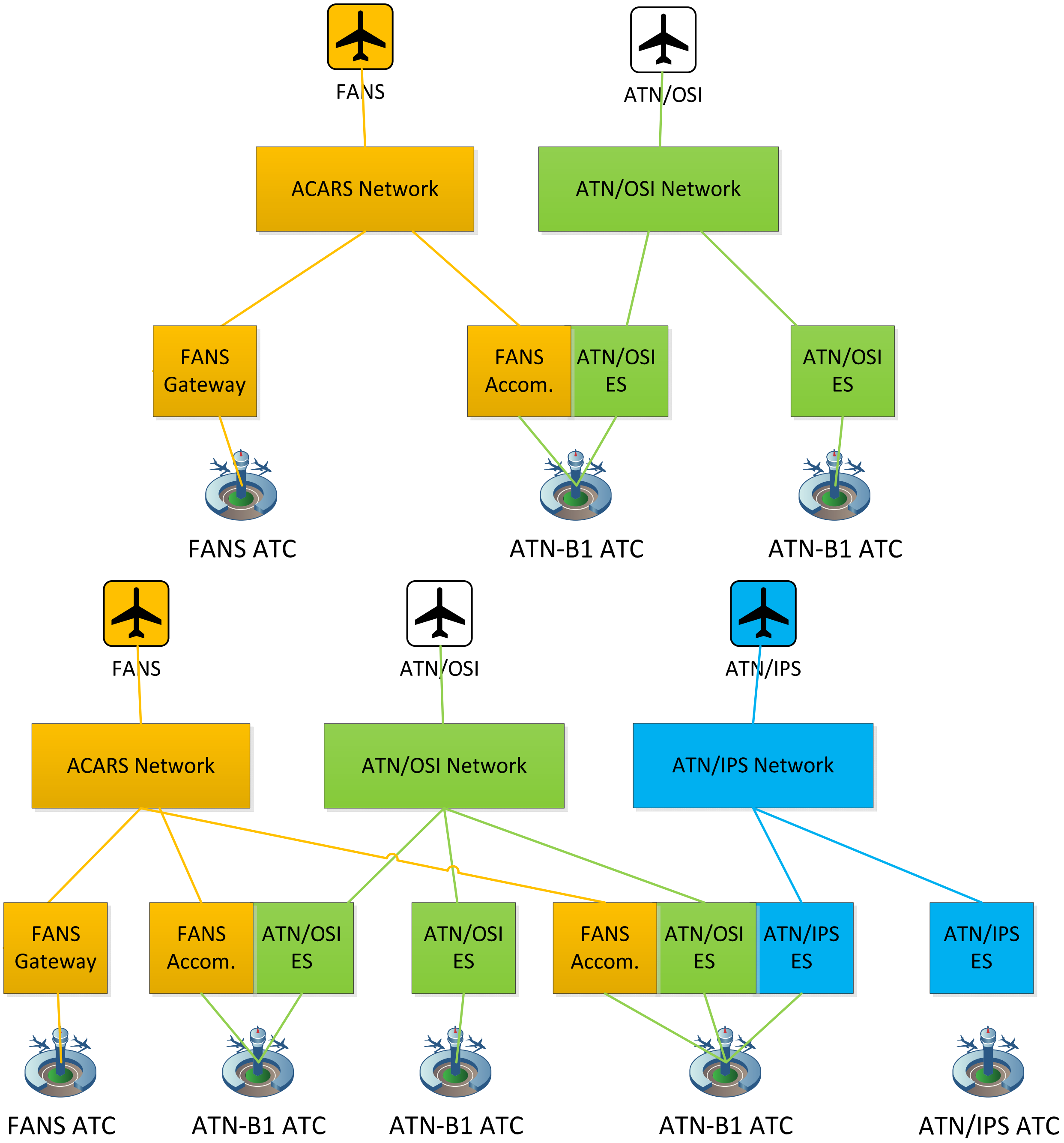


Figure 3-4 – Future Ground Deployment

Table 3-4 shown below presents the different combinations possible when ATN/IPS aircraft are available. Three different technology equipped aircraft could be flying in the same airspace. New ATN/IPS aircraft and legacy aircraft (ATN-B1 or FANS).

Note: For dual stack aircraft, the interoperability should be read by combining the two applicable columns.

Table 3-4 – Aircraft Equipage as a Function of Airspace

GROUND CENTER	FANS	ATN/OSI	ATN/IPS
Single FANS ATC	Yes	No	No
Single ATN-B1 ATC	No	Yes	No
Single ATN/IPS ATC	No	No	Yes
Dual FANS ATC + ATN-B1	Yes	Yes	No
Dual FANS ATC + ATN/IPS	Yes	No	Yes
Dual ATN/OSI + ATN/IPS	No	Yes	Yes
Triple FANS ATC + ATN/OSI + ATN/IPS	Yes	Yes	Yes

Transition criteria need to be addressed as well as the ground deployment of ATN/IPS systems (for example in Europe) will not be done at the same time.

Ground gateways could also be considered to bridge the gap for ground deployments

- For ATN-B1 OSI aircraft to ATN/IPS ATC systems
- For ATN/IPS aircraft to ATN-B1 OSI ATC systems

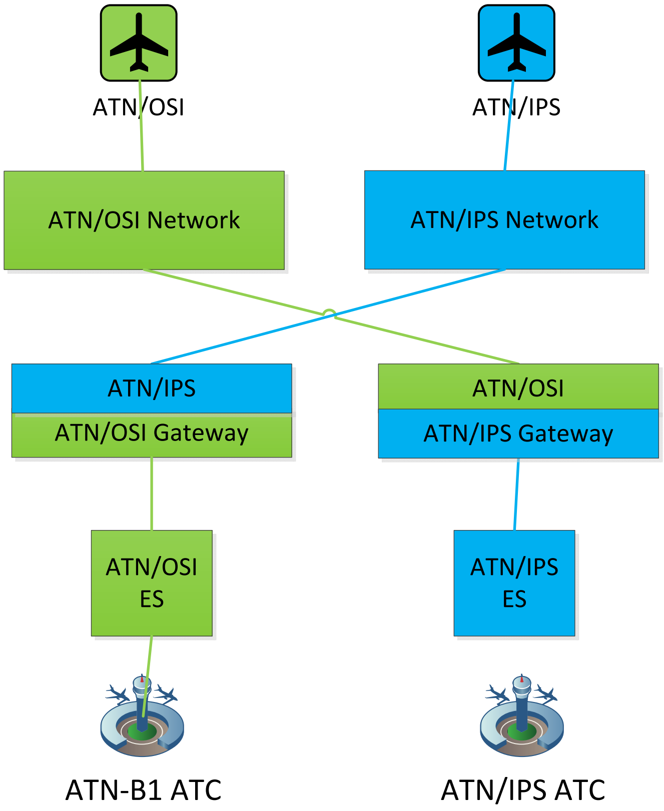


Figure 3-5 – Ground Gateways

Note: For both cases, the ATN/OSI and ATN/IPS network components operating in the same region must be deployed in that country or region.

4.0 ATN/IPS WORK SCOPE CONSIDERATIONS

4.1 Basic Technical Requirements

This section describes some considerations for basic capabilities and needs for IPS. Figure 4-1 depicts the IPS domain from this perspective. Note that architectural considerations are described in Section 3.

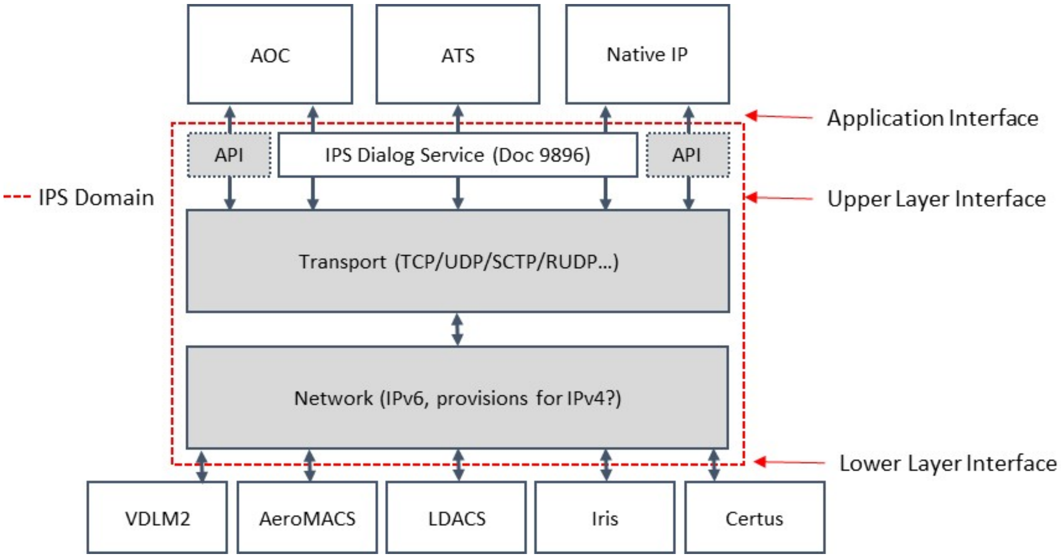


Figure 4-1 – Interface Demarcations

4.1.1 Application Interface Definition

ATN/IPS is intended to provide an efficient and robust network infrastructure common to both Air Traffic Services (ATS) and Aeronautical Operational Communications (AOC) safety service applications.

To properly use the ATN/IPS system, applications will need to have a compatible interface definition. Some legacy applications are not native-IP, and therefore may need to make use of a specialized interface in order to communicate to peers and preserve maximum application compatibility. Other applications may be native IP (i.e., designed to take advantage of IP via TCP or UDP, so will not necessarily need to make usage of the dialog service as per ICAO Document 9896), and therefore adapt more easily to the communication stack, making use of existing provisions for transport layers. These differing needs must be considered and clear, unambiguous implementation guidance must be provided. Specifically, it must be targeted to support the following applications:

- **ATS datalink applications** supporting air traffic control services in continental and oceanic airspace, including both current applications such as ARINC 623, FANS-1/A and B1 applications as well as future B2 and B3 applications.
- **AOC applications** supporting safety and regularity of flight. This includes AOC services currently supported over ACARS (adapted to support transmission over IP) and future Aeronautical Information Services (AIS) and Meteorological (MET) services supported by the air/ground SWIM system.

AOC applications serving airline operations supported by general IP services to the aircraft are assumed outside the scope of ATN/IPS. Cockpit voice is also assumed outside the ATN/IPS standardization effort.

The application interface presented by the ATN/IPS network needs to provide support for:

- B1, B2 and, potentially, FANS-1/A applications through use of an adaptation layer. The adaptation layer needs to ensure that existing aircraft and ground application behavior is supported without modification, providing means to map existing application-level parameters (e.g. application addresses, port numbers) to ATN/IPS equivalents.
- Legacy ACARS AOC applications through use of an adaptation layer or IP-based messaging solution (for example Media Independent Aircraft Messaging – MIAM, ARINC 841)
- New ATS, AOC and air/ground SWIM applications developed to support future safety services and native IPv6. Standard profiles and interfaces need to be developed to support different application types, including reliable / non-reliable transport, unicast and/or multicast delivery, and support for application-specific QoS.

4.1.1.1 Legacy Applications – OSI

The original purpose of the ICAO Document 9896 was to allow a replacement of the upper layer communication service (ULCS) specified in the original ICAO Document 9705 to something that could be mapped to TCP and UDP. This was done with an intent of not requiring any changes of the applications themselves; from the application point of view the communication with the peers would be exactly the same as if the applications were using OSI protocols.

This was achieved by the combination of defining the IPS Dialog Service (DS) and the ATNPKT format. The IPS DS provides the dialog service interface to the ATN applications, replacing the ULCS DS primitives in a compatible way. The purpose of the ATNPKT is to convey information between peer applications. It is carried in the data part of the transport protocol (either TCP or UDP) and is used to convey parameters of the service primitives that cannot be mapped to existing IP or transport header fields. The ATNPKT will also convey information to indicate the Dialogue Service protocol function (e.g. the type of DS primitive).

In order to make use of IPS, OSI-based ATN applications should adhere to the Legacy ATN Applications section of the Part II of ICAO Doc 9896. Interoperability between OSI-based implementations and IPS-based implementations is discussed in Section 3.6.

4.1.1.2 Legacy Applications – ACARS

IPS is also intended to be capable of support for legacy, ACARS-based applications such as FANS-1/A and AOC messaging. The ACARS structure has a message payload (such as CPDLC, ADS-C, or AOC messages) that is put into a communication envelope. The envelope may be defined by ARINC 622 for ATS messages or ARINC 702A for some types of AOC messages. For IPS, these payloads may be put into the contents of an ATNPKT. However, there are still a number of questions that need to be answered:

- Should the original ACARS messages be preserved in such a way that it can still be injected into the ACARS network?
- Should only the payload of the message be included, and not the header?
- How will the subsequently received encapsulated messages be processed at the peer (e.g. is there a need to preserve some aspects like SMI)
- Can this be handled within the ATNPKT format, or would there be a new format necessary?
- The ATNPKT format has a number of other supporting parameters that are specified by ICAO Document 9896. These would need to be reviewed to see if there are additional values that would need to be defined in order to convey information other than the ICAO Document 9896 CM, CPDLC or ADS-C defined port numbers for application data.

Aside from the data content itself, the use of the dialog service primitives would also need to be investigated. ACARS applications are connectionless by nature, and do not employ the same dialog service structure that ATN applications use. Given that, would the transfer of ACARS messages lend itself to an overlay onto the IPS DS for connection-oriented or connectionless operations, or would there need to be new primitives defined, or something different altogether.

Additionally, there are other aspects of ACARS communications like message assurance (MAS) and intercepts that may need to be taken into consideration. Similar mechanisms in the IPv6 domain may need to be taken into consideration to provide equivalent functionality.

4.1.1.3 Legacy Applications – Other

Different types of applications can also potentially be served by IPS. These are existing applications that use various protocols and communications links to exchange data between the aircraft and the ground using existing safety links. Below are some examples of potential applications:

- QAR data
- Engine and maintenance data
- Data from interface to on-board LRUs, e.g. intent data from the FMS extracted by a third party device such as an EFB and subsequently downlinked to the ground by the EFB.

4.1.1.4 Future Applications – Native IP

Deployment of ATN/IPS provides the opportunity to enable various future native IP applications. Application may utilize socket like API interface or lightweight native API interface to access transport and network layer. Following applications or capabilities may utilize native IP interface in future:

- FIS applications (Digital NOTAM, Aerodrome Weather, Special AIREP/AUTOMET, Winds and Temperature ALOFT, VOLMET, SIGMENT, ATIS, OTIS, Runway Visual Range, Hazardous Weather)
- Wind/Temp Data for FMS
- Runway and Taxiway Information
- Aircraft Realtime Data

- On-board video surveillance sent to the ground for improved security and, passengers and crew medical assistance
- Airport, airway or airspace information status updates
- Obstacle Information
- Aircraft Trajectory Optimization and Environmental conditions in critical flight phases

4.1.2 Mobility Requirements

The aircraft will, depending on its location, be able to connect to one or more of the available air/ground Subnetworks. The aircraft will receive a stable IPv6 Mobile Network Prefix (MNP) that that travels with the aircraft through all mobility events. The network mobility mechanisms implemented within the ground/ground internetwork need to be able to deliver traffic to the aircraft irrespective of its changing air/ground connectivity and therefore changing point(s) of attachment on the ground network.

The following mobility scenarios need to be considered:

- **Mobility within subnetworks**: **('micro' or 'local' mobility)**: As the aircraft moves between radio coverage areas within the same air/ground subnetwork, it will need to establish link layer connectivity with the next ground radio station. As long as the network point of attachment does not change, handover mechanisms remain specific to the air/ground subnetwork and should be supported at the subnetwork level, but mobility support at the network level may be required if the handover results in a change of point of attachment on the ground/ground internetwork.
- **Mobility between subnetworks ('macro' or 'global' mobility)**: As the aircraft moves between one air/ground subnetwork and another (for example between LDACS and Satcom), its point of attachment on the ground network will change and mobility support at internetwork level will be required in order to ensure that application traffic continues to be correctly routed towards the aircraft.
- **Mobility between network regions**: The future ground/ground internetwork will likely comprise a number of interconnected regional networks, each independently administered and serving a defined geographical area / set of FIRs (for example, ECAC). Most domestic flights would be served within a particular network region; intercontinental flights however may cross multiple network boundaries. The requirements for mobility between network regions need further definition – for example, is a seamless handover required or is it sufficient for the aircraft to establish a new communications context when entering a new region?

The mobility solution selected needs to work hand-in-hand with the solution adopted for multilink in Section 4.5.3.

The ATN/IPS design needs to pay particular attention to the following areas:

- Scalability of the routing solution adopted within the ground/ground internetwork, for example avoiding performance issues that may occur through dynamically flooding routing updates through the network.

- Complexity, e.g. in terms of amount of software, of the mobility solution within the aircraft, and the traffic load that this might impose on the air/ground communications link.
- Compatibility with existing ATN and AOC application behavior. Existing ATN applications allow ground facilities to initiate application sessions with aircraft using IPv6 network addresses from the aircraft's MNP. The mobility solution chosen needs to be able to support ground-initiated application sessions and route traffic towards the aircraft at this advertised network address, irrespective of the air/ground subnetwork(s) the aircraft is connected to.
- Performance of the handover mechanisms in each of the mobility scenarios, i.e., the speed with which changes in air/ground connectivity and point of attachment can be promulgated and take effect within the ground/ground internetwork. The aim is to achieve handover seamlessly[4] from the point of view of the applications being served, and trade-offs between complexity and performance are needed.
- Optimization of the selected route, considering that the ground facility with which the aircraft is communicating may be distant from the aircraft's 'home' network – particularly when operating in a different network region[5]. The optimized route should be such that it can be dynamically updated as a result of changes to aircraft air/ground connectivity.
- Mobility management technique must not impose undue control-plane messaging traffic over performance-limited aviation data links
- The air/ground control plane traffic (e.g., routing exchanges, keepalives, link initiation, handoffs, mobility signaling) must be minimized, e.g. network based mobility could be considered for optimization (both numbers of messages and size of messages must be considered)
- Message and header compression are valuable tools in minimizing network traffic overhead; compression complexity should be considered as a tradeoff to traffic overhead and security vulnerabilities
- The mobility solution should be able to operate over existing links (e.g., VDLM2)
- The aircraft multilink function is responsible for link connectivity change detections and proper hand offs between various terrestrial and satellite subnetworks.
- Make maximum use of existing RFCs and COTS when possible

The airborne ATN/IPS system is connected to multiple providers. Avionics IPS air/ground subnetwork configuration has more than one air/ground links and more

---

[4] *Seamless* means the ability to support changes in radio network interconnection (e.g., result of handover) or routing within the internetwork without adversely affecting the application behavior or user experience. Technically this requires that the network supports the applicable Safety and Performance Requirements (SPRs) for the application, in terms of service continuity and maximum number of operationally significant outages per annum. Some packet loss can be accepted and applications should be resilient to this packet loss and temporary communication outages.

[5] This specifically becomes a concern with the more stringent targets for Required Communications Technical Performance (RCTP) and Required Surveillance Technical Performance (RSTP) projected for 4D trajectory based operations.

than one subnetwork service provider. Each subnetwork provider (e.g., satellite service provider, VDLM2 service provider) may operate with different global prefix. See Section 4.2 for further addressing discussion.

4.1.3 Lower Layer Interfaces

The means by which traffic is delivered over the air/ground subnetwork and how that network delivers its required availability and performance is a subnetwork design matter and is required to be transparent to operation at the ATN/IPS internetwork level.

Ideally a common interface should be presented by each air/ground subnetwork towards the neighboring aircraft and ground ATN/IPS systems. The details will be specific to the selected design of the ATN/IPS network.

The design of the interface between subnetwork layer and ATN/IPS internetwork layer needs to consider (at least):

- Means by which the subnetwork indicates that connectivity becomes available / unavailable to each aircraft in a timely manner to support mobility and multilink routing decisions.
- Mechanisms to support the delivery of IPv6 traffic services to/from the upper layers, including whether unicast and multicast are supported.
- Indication of the required Class of Service (CoS) associated with each packet in order that the subnetwork can apply the required traffic prioritization to meet QoS requirements.

The air/ground subnetworks present one of the principal vectors for security attacks on the ATN/IPS system and applications within the Aircraft Control Domain. Security of air/ground subnetwork and its interface with higher layers therefore needs careful consideration in the design. This includes the link level for subnetworks such as VDLM2, which needs further investigation.

In particular, the ATN/IPS system must be secured against Internet-based or Subnetwork-based Distributed Denial of Service (DDoS) attacks that could disrupt or shut down critical communication services. (see Section 4.4)

The need for IP multicast support within air/ground subnetworks requires further investigation and substantiation. There are potential aeronautical information / meteorological services (e.g. D-VOLMET) which require large amounts of common data to be transmitted to all aircraft e.g. within an FIR. Network efficiency and overall performance could be substantially improved by delivering this application data using IP multicast: the potential need for multicast for these applications has been highlighted by SESAR 15.2.4 and EUROCAE WG-76. Nevertheless, further study is required on the overall concept of operation and how IP multicast should be supported by the IPS network, including whether multicast should statically/dynamically routed and whether seamless mobility is required.

4.1.4 Upper Layer Interfaces

Upper layer interfaces are logical interfaces. These are the ATN/IPS system interfaces that act as a router, providing functionality to local and peer applications.

The ATN/IPS upper layer interfaces need to be able to support a range of legacy and new applications, as described in Section 4.1.1.3.

In designing the upper layer interface, consideration needs to be given to:

- The transport layer requirements of each “native IPS” application, e.g., reliable versus non-reliable transport, data checksum, congestion avoidance, multi-homing, ordered delivery, streaming delivery. This will help indicate choice of transport layer protocol (e.g., TCP, UDP, MP-TCP, SCTP).
- Adaptation required for existing non-native IP applications, specifically including support for existing ATN and FANS-1/A applications. For ATN, use of an IPS variant of the ATN/OSI Dialog Service is foreseen in ICAO Document 9896 for this purpose.
- Security needs at the transport layer, including authentication, confidentiality, and integrity

Some applications may require multiple transport interfaces.

In selection of the transport protocol, consideration needs to be made of not only application requirements but also of suitability of the proposed protocols operating over the proposed subnetworks, for example, known throughput problems with TCP over high-latency links.

The choice of transport protocols needs to be compatible with the overall architecture and mobility solution.

The ATN/IPS protocols will need to provide various options that can be selected to implement a detailed specification, likely via protocol implementation conformance statement (PICS) or IPS profiles (e.g., RTCA profile definition).

For the IPS dialog service, applications are assigned port numbers that are registered with IANA. This was done for CM, CPDLC, ADS-C and FIS (note that FIS is no longer considered part of the B2 application set). These ports numbers are expected to be carried forward. Additionally, there may be a number of standard ports that are necessary as well. As the protocol details of IPS are defined, these ports will need to be identified so that access to those ports can be configured. This would include both air and ground initiation, depending on the service (some services may not be bi-directional, e.g., an ICMP echo may be allowed from the aircraft to the ground system but not vice-versa).

The handling of other existing and new applications will also need to investigated and defined. Should new ports for applications like FANS-1/A applications be identified and registered, or should a generic “ACARS” port be defined and registered that would serve all legacy ACARS-based applications? And how would the introduction of new applications be handled? It may not be convenient to continually register new port numbers; maybe there would need to be generic ports for application type with further discriminators to identify the specific application within the ATNPKT format (or other format, as applicable). This will need to be better defined before specific requirements can be identified.

4.1.5 Connection Establishment

Consideration needs to be given to the establishment of connectivity to the aircraft. Previously, depending on the application, either air and/or ground-initiated connections were possible. For example, CM was air-initiated while CPDLC was ground-initiated. However, enabling ground-initiated connections in an IP-based environment raises concerns about increasing the potential for attacks to the aircraft, since there is a greater potential for malicious attacks to be initiated from the ground that violate assumptions on session state.

ATN/IPS internetworks should not place restrictions on how connections are established. However, CPDLC and other applications that rely on ground initiation may need to employ different solutions in order to operate. There may need to be provisions for a generic mechanism to enable trusted session state to be maintained across interruptions in the physical air/ground connections. Additionally, if connectionless services are employed, these mechanisms would also need to be expanded to cover these types of services.

Requirement: Mechanisms shall be in place that will allow both air and ground initiated connections to be established.

4.2 Naming and Addressing

ICAO Document 9896 edition 2.0 (2015) lists the requirements related to the IPS addressing for air/ground communications.

The airborne ATN/IPS system is connected to multiple downstream and upstream networks via multiple service providers. IPv6 addresses can be allocated by service providers to end-users. The aircraft IPv6 addressing scheme should be finalized in the standardization phase, and should comply with ARINC Standards [TBD] on this subject. IPS node IPv6 addresses are assigned by each respective service provider resulting in nodes with multiple global scope IPv6 addresses with different prefixes. As each subnetwork service provider is allocated a different address space from its Internet Registry it in turn assigns a different address space to the airline or operator network or IPS node.

For IPS avionics IPv6 addressing and basic connectivity, there are a few options: a) having multiple IPv6 global addresses within the same prefix, b) multiple addresses within the multiple prefix c) single address with multiple prefixes. All globally aggregatable IPv6 addresses are provider-assigned. Even though it is possible to assign multiple IPv6 prefixes to networks and hosts, having assigned multiple prefixes to a network allows that network to connect to multiple service providers which simplifies the avionics multihoming configuration. Multiple addresses introduce complexity problems. Having a single global address with network managed multiple prefixes may simplify the deployment.

IPS nodes will use globally scoped IPv6 addresses when communicating over the Safety service IP network.

Recommendation A1: ICAO should coordinate with IANA to reserve the block of address to be used for civil aviation. ICAO should be an Internet Registry for aviation who can delegate the regional responsibility to ICAO region or organization such as EUROCONTROL as Local Internet Registry.

Recommendation A2: ICAO should update and finalize the addressing scheme, taking into account input from multiple groups include the ICAO Mobility Subgroup.

4.3 IPS Administration

It should also be recognized that the ATN/IPS solution may need to work in different deployment configurations in different geographic regions, including:

- A centralized architecture, whereby a regional entity anchors ATS datalink services on behalf of ANSPs - for example the datalink infrastructure service (CS-9) proposed as part of future Centralized Services in Europe

- A service provider oriented architecture whereby an air/ground communications service provider (ACSP) is the preferred service provider for an airline and provides the necessary air/ground services – including handing over to an alternate service provider if the preferred service fails (e.g., existing ACARS and ATN/OSI service provision).
- A distributed architecture, whereby each ANSP is connected to multiple ACSPs and can set its own routing preferences.

The ATN/IPS protocols may need to accommodate additional deployment architectures.

Each of these deployment options may have implications on a number of areas of network design, including administration of aircraft network addresses/prefixes, quality of service policy, and selection of appropriate routing / mobility protocols.

4.4 Security Roadmap

This section presents the cyber security-related elements that need to be addressed as part of the overall ATN/IPS system standards definition.

Development of security requirements is an integral part of the functional requirements development process. This ensures that security as a property is baked into the end-to-end ATN/IPS system. As the overall architecture and specific technical elements of the system are defined, the security analysis process can begin to identify the specific threats and vulnerabilities and appropriate countermeasures. This may be an iterative process, where functional changes driven by security needs in turn drive other dependent functional changes.

Four main areas should be developed for the security-related portions of ATN/IPS standards:

1. Comprehensive security architecture
2. End-to-end security analysis
3. Security requirements
4. Operational security guidance

Consideration should also be given to development of an overall high-level security policy document for the ATN/IPS system.

4.4.1 Comprehensive Security Architecture

ATN/IPS, a large and complex network communications system, will require a comprehensive security architecture document be developed and maintained over time. Such a document will define all of the elements of the ATN/IPS system that contribute to the overall security posture, how they interact with each other to maintain security, and the role played by the various operational processes and procedures for security. Such a document will help ensure that as the system evolves, gaps do not develop that may present an uncontrolled expansion of the attack surface. It will also define the roles and responsibilities of all of the entities in the system in maintaining security. Additionally, it should lay out the rationale and tradeoffs for either link-layer (hop-by-hop) or network layer (end-to-end) security.

The primary objective of the ATN/IPS security architecture is the establishment, maintenance, and transfer of trust among all the assets within the system and trust among the assets in which the system interfaces. Trust is maintained by the ability to verify the authenticity and integrity of data and the system.

The security measures implemented for the ATN/IPS system must take into account critical performance requirements (e.g., RCP) and be able to protect the system even while being constrained by low bandwidth air/ground subnetworks and avionics systems with limited processing and memory resources.

Business rules are used to describe various configuration items for the ATN/IPS system and how the various actors will interact with the aircraft. This provides the framework for suppliers, ANSPs and airlines to create business rules considering the following content:

- Entity Authentication framework
- Allowed Content Types
- Trust relationships
- Algorithms and protocols to be used potentially based on aircraft location
- Aircraft Home Location

4.4.2 Security Analysis

The IPS security architecture will form the basis for the security analysis process, which will comprehensively identify threats, vulnerabilities, impacts, and countermeasures.

The overall analysis approach to define required security assurance levels should be consistent across the ATN/IPS system. It is recognized, however, that there do not exist yet any security assurance analysis approaches that are applicable for both airborne and ground components. While processes and methodologies have been developed by RTCA and EUROCAE for the airborne side (and are under further development), equivalent ones do not yet exist for the ground portion of an IP-based safety communications system. Careful consideration must be given to how the different assurance analyses will map to each other to ensure there are no gaps in the end-to-end security of the system.

Security assurance approaches for ground components can follow an internationally approved scheme based on elements such as ISO 15408 (Common Criteria) and ISO 27001/27002 (ISMS). Based on experience developing the processes for the airborne side, this may prove challenging.

Alternatively, nation-specific schemes can be considered, such as those endorsed by the various country CAA’s. The security risk management approach should remain flexible enough to allow for more than one valid approach. However, this can be difficult when outputs and requirements generated by the respective processes differ from each other and don’t have a clear way to normalize them.

4.4.3 Security Requirements

The output of the security analyses will drive definition of security requirements for the ATN/IPS system. As stated earlier in this document, this should be developed closely alongside the general technical requirements.

4.4.4 On-going Operational Security

System security needs to be managed through a continuous process of risk assessment and improvement (Plan-Do-Check-Act process) requiring system upgrades to be made on a regular basis to counter any newly identified threats or vulnerabilities in the system.

The airworthiness certification process and equivalent approval processes for ground systems need to recognize that this cycle of continuous improvement is necessary for the overall security architecture to remain valid. This is a major change from how things work for type certification process, and would be welcomed by almost no one. However, there is not yet any framework for re-certification of airplanes after the original type cert.

Operational security management processes for the system must be flexible enough to be able to respond rapidly to an evolving threat landscape.

The idea is to enable the necessary security updates to be installed without changing the aircraft type certification. Section 5.2 provides additional detail.

4.4.5 Country-Specific Regulatory Considerations for Security

As security countermeasures are specified and developed, consideration must be given to variations in regulations from country to country on use of tools like cryptography. Consistent compliance across multiple different regulatory regimes is also an important consideration.

4.5 Other Considerations

This section describes other considerations that must be flexible to meet user requirements.

4.5.1 Quality of Service (QoS)

Specific mechanism should be defined to map the QoS parameter to a specific links as well as specific channel within the same link so that message are routed based on the QoS priority.

4.5.2 Compression Requirements

This section discusses the need for data compression, and also looks at where compression should be done. The ATN/IPS system can support both types of QoS services:

Differentiated Service (diff-serv): This is coarse-grain (per-class), qualitative promises (e.g., higher priority), no explicit signaling.

Integrated Service (int-serv): This is fine-grain (per-flow), quantitative promises (e.g., x bits per second), uses RSVP signaling

IPv6 header has two QoS-related fields:

- (20-bit Flow Label): Used by a source to label sequences of packets for which it requests special handling by the IPv6 routers. This is geared to IntServ and RSVP.
- 8-bit Traffic Class Indicator: Used by originating nodes and/or forwarding routers to identify and distinguish between different classes or priorities of IPv6 packets. This may be initialized by source or by router enroute; may be rewritten by routers enroute. Service provider can utilize this capability to determine what air/ground link they should route particular message (e.g., VHF, HF, Satcom). Traffic Class value of 0 used when no special QoS requested (the common case today).

4.5.3 Multilink Considerations

A key concept embodied within the future communications infrastructure is the use of multilink in order to improve availability and performance of datalink communication. Multilink is a desirable feature of ATS datalink services and may become essential given the more stringent safety and performance requirements associated with the migration to full 4D trajectory based operations and the increased reliance on data communication.

Multilink in this context refers to the ability of a router to be able to select a communication path from one of multiple different communication links. The router selects a communication path from the available links for any given packet transmission. The communication session may be maintained at the application, transport or network level. Packets may arrive simultaneously from the multiple links, however, there should only be a single path for a given packet. Therefore, the concept of simultaneous transmission of the same packet on multiple links should not be considered “multilink” in this context.

Multilink requires the aircraft network node (host, router) to be able to connect to multiple air/ground subnetworks where multiple air/ground subnetworks are available and be able to switch between these dynamically in response to loss and re-establishment of communications on any one of the links as detected by the involved subnetwork entities (airborne radio, ground station).

The ATN/IPS design needs to pay particular attention to the following areas:

- Means by which the aircraft node can connect to multiple air/ground subnetwork interfaces simultaneously (multi-homing) and what criteria should be applied to select the interface that downlink traffic is sent on if multiple are available (e.g., airline preference, routing policy) in order to meet the RCP/RSP.
- Means by which the ground/ground internetwork connects to multiple air/ground subnetworks (e.g., where is the aggregation point, or the point where a ground decision is about which path to take is made) and what criteria should be applied to select the air/ground subnetwork that uplink traffic is sent on if multiple available in order to meet the RCP/RSP. Which organization should set routing policy, will the policy be different for different services (ATS datalink, AOC services) and do the same routing preferences/policy need to be applied on the uplink and downlink?
- Means by which the air/ground subnetworks can notify the neighboring airborne and ground routers of their availability and QoS.
- The safety assurance level associated with the multilink switching mechanism and the implications on switch design and safety requirements imposed on the air/ground subnetworks to provide reliable and timely notification of subnetwork availability.

Potential routing of traffic through multiple air/ground subnetworks simultaneously to potentially increase overall datalink performance. This prompts a broader question regarding how multilink services would be charged generally and the commercial sustainability of “non-preferred” air/ground subnetworks. Additionally, this would result in more requirements on the on-board routing to handle multiple copies of messages over multiple links. There will need to be investigations into the increased bandwidth usage across multiple link types.

5.0 ATN/IPS STANDARDIZATION ROADMAPS

5.1 Introduction

This section presents a high-level roadmap for ATN/IPS standardization, also known as IPS for safety services. Using the work scope identified in Sections 3 and 4, an analysis of known in-progress and planned standardization efforts identified areas where new and/or additional standardization activities are required. The analysis also considers standards necessary for certification of ATN/IPS systems, as well as validation efforts that may provide feedback into ATN/IPS standards. While the emphasis is on identifying ARINC standards, a gap analysis has been performed to identify areas of standardization pertinent to other standards development organizations.

A summary-level graphical roadmap presents recommended AEEC activities, as well as the work efforts of other standards organizations developing ATN/IPS standards. The roadmap serves as a useful communication tool for intra- and inter-organization coordination, particularly where there may be dependencies.

5.2 Regulatory and Certification Considerations

The introduction of ATN/IPS as a transport/network protocol for safety services presents new certification considerations that will require discussion and collaboration among regulators (e.g., FAA and EASA) and industry stakeholder organizations, including aircraft OEMs and avionics suppliers. An initial step will be to bound the problem by identifying the intended functions, services, notional architectures, and performance requirements. Foundational activities may include the development of a Concept of Operations, deployment considerations and transition plan for ATN/IPS, a preliminary system safety assessment, preliminary system security risk assessment, and development of profiles, MOPS, and MASPS.

A published MOPS will support development of a Technical Standard Order (TSO) for ATN/IPS Network Equipment. The TSO’s apply to avionics equipment intended to provide safety services by means of communications between aircraft avionics, corresponding subnetworks, and ground communication stations.

Regulators will develop an advisory circular (AC) for ATN/IPS as used within Required Communication Performance (RCP) environment for airport surface communication, terminal communication, domestic enroute communication, and communication in procedural operations along international air routes. The ATN/IPS AC is expected to provide guidelines on what is required for ATN/IPS systems to be compliant with providing protection against misleading and corrupted messages.

As highlighted in the architecture discussions in Section 3, comprehensive and layered data security approach (e.g., link level, network level, and application level) will be critical to ATN/IPS certification and deployment. Current policy statements, such as FAA PS-AIR-21-16-02, address designs of aircraft systems that include connectivity to “non-governmental services” (e.g., internet) that are not certified and accredited for secure operations by a government authority. Since the use of these services can introduce cyber security vulnerabilities, special conditions are applied to address cyber security vulnerabilities in aircraft certification programs. It is expected that ATN/IPS implementations designed specifically to support aeronautical safety services will be subject to current special conditions and/or future rulemaking that addresses cyber security vulnerabilities.

As part of this process and based on the outcome of a security risk assessment, it will be important to consider end-to-end security and whether aircraft certification of ATN/IPS systems can assume shared responsibility by the ground; in other words, reliance on the cyber security protections implemented by the ground, with ground accountability for proper operation of those protections. This will drive a new framework and processes to certify ATN/IPS as an end-to-end capability, in both aircraft and ground certifications.

The RTCA Aviation Rulemaking Advisory Committee (ARAC) may be the appropriate forum to define this environment.

In addition, EUROCAE ED-246, *Process Specification for Wireless On-board Avionics Networks*, provides guidance on the airworthiness certification process for electronic aircraft equipment installed or integrated on board an aircraft, featuring a wireless communication function to allow for exchange of information with other equipment on the airport grounds or on board the same aircraft. These wireless communication functions are part of the aircraft configuration and their proper functioning will require approval through airworthiness certification authorities.

5.3 Standardization Gap Analysis

Standardization is critical to the successful implementation, certification, and deployment of globally interoperable ATN/IPS systems. Given this importance, the industry stakeholders who participated in the development of this document conducted a detailed analysis to understand and assess ATN/IPS-related standardization activities. For each of the ATN/IPS work areas identified in Sections 3 and 4, the analysis documented the status (e.g., complete, in-progress, planned, and proposed) of ATN/IPS-related standards from aviation standards development organizations including ICAO, EUROCAE, RTCA, and AEEC. A key output of the analysis was the identification of gaps, where the industry stakeholders believe that a standard is required but an associated standardization activity is not yet identified.

The primary objective of the analysis was to identify the need for new ATN/IPS-related ARINC Standards and to identify existing ARINC Standards that may require modification to support ATN/IPS. However, having a comprehensive picture of ATN/IPS-related standardization efforts across standards organizations also helps to minimize duplication of effort and facilitates the identification of topics that might benefit from cross-organization coordination. Appendix D is a snapshot of the spreadsheet used to capture the gap analysis.

5.4 Standardization Activity Summary and Recommendations

The following sub-sections summarize the standardization analysis findings for each standards development organization contributing to ATN/IPS standards. This includes a description of ATN/IPS standardization efforts that are in progress, planned, or proposed and identification of potential new and/or additional standards activities.

5.4.1 ARINC Standards

All new ARINC Standards pertaining to data communication should fuly consider the applicablity of ATN/IPS and the recommendations of this document.

5.4.1.1 Work of the AEEC IPS Subcommittee

The AEEC Executive Committee formed the IPS Subcommittee to develop an ATN/IPS Roadmap (this document) as an initial task. The current and future role of the IPS Subcommittee is further outlined below.

5.4.1.1.1 IPS Coordination

The initial work of the AEEC IPS Subcommittee is to create this ATN/IPS Roadmap document, which identifies: 1) the areas that will require further definition in order to implement ATN/IPS; and, 2) potential groups that are best suited to address identified gaps. However, not all identified gaps are suited to an existing external standardization group, new work items may arise during ATN/IPS standardization, and there will likely be questions from other standards groups regarding interpretations of ARINC Report 658. Therefore, an ongoing coordination role is necessary to maintain an overall high-level view that supports continued and efficient ATN/IPS standardization progress. This role would include monitoring ATN/IPS-related developments and standardization work, maintaining the roadmap (including updates to the gap analysis and activity timing), and organizing and executing work on ATN/IPS that is not being done elsewhere.

Section 6.0, Summary Recommendations, provides additional information.

5.4.1.1.2 Architecture-driven Work Scope

Based on general assumptions and high-level requirements, Section 3 provides initial considerations for the integration of ATN/IPS in legacy equipment (ARINC 429 based) and current ARINC 664 based architectures.

A primary outcome of architecture discussions in Section 3 is the acknowledgement that there will be multiple implementations of the airborne ATN/IPS function, based on: different types of interfaces; different data network architecture design and their associated security requirements; and different levels of cockpit integration (e.g., displays, centralized maintenance and aircraft condition monitoring, data-loading, navigation other cockpit functions). Therefore, as shown in Figure 5-1, the airborne ATN/IPS system can be divided in two parts:

- A “Core” ATN/IPS stack that is architecture-independent (shown as the red-shaded box in the figure), and
- Supplementary ATN/IPS functions, that are highly dependent on the avionics environment and interfaces (shown as the blue-shaded box in the figure).

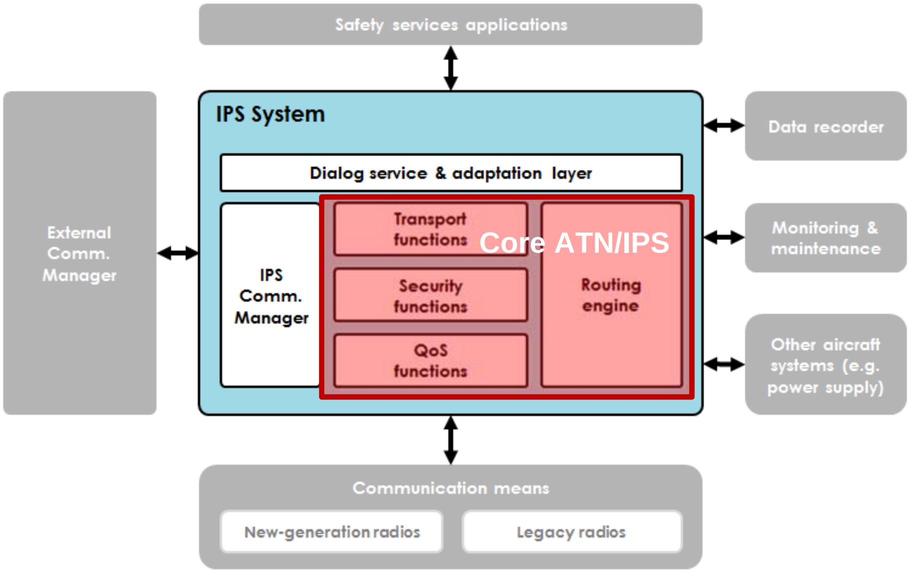


Figure 5-1 – ATN/IPS Core Functions Scope – Notional

The AEEC IPS Subcommittee should focus its standardization efforts on scoping and defining the software-based, functional "Core" ATN/IPS stack and interfaces, based on the technical provisions specified by ICAO and IP profiles specified by RTCA/EUROCAE. This Core ATN/IPS stack:

- Would be abstracted from the different communication means
- Would be platform (hardware and interfaces) independent (i.e., portable)
- Would offer standard functional interfaces (i.e., for sending/receiving messages, monitoring, and configuration
- Could be implemented as "COTS-based" stack that is reusable in different architectures, thereby benefiting multiple industry stakeholders, including airframe manufacturers, avionics suppliers, and operators

If necessary, the way in which that stack is used through its functional interfaces could be documented in appendixes (e.g., "Airbus ATSU profile", "Boeing CMF profile", "CMU profile"). The "Supplementary" ATN/IPS functions are expected to be implementation dependent. As part of its continuing efforts, the IPS Subcommittee will further refine the dividing line between Core and Supplementary functions and continue to elaborate the ATN/IPS scope to be standardized.

5.4.1.1.3 Gap Analysis-driven Work Scope

In addition to coordination among various standards groups progressing ATN/IPS as described in Section 5.4.1.1.1 and addressing core ATN/IPS stack and interface considerations as detailed in Section 5.4.1.1.2, the AEEC IPS Subcommittee is also envisaged to have an on-going role in specific areas of ATN/IPS standards development. Section 6.0, Summary Recommendations, provides additional information.

As identified by the gap analysis, the following topics are assigned notionally to the AEEC IPS Subcommittee for further investigation:

- Encapsulation of FANS and ACARS messages,

- QoS mechanisms for segregating ATS and AOC traffic,
- Compression considerations,
- Multi-link definition,
- IPS router definition and specification, and
- ACARS-IPS ground gateway functionality.

As part of its ongoing efforts in these areas, the AEEC IPS Subcommittee may identify the need to engage other groups that are better suited to address some aspects of the standardization work. As an example, further analysis may determine that the definition of FANS encapsulation is best addressed by ICAO in Doc. 9896 (which defined the original ATNPKT format with provisions for multiple application types), along with complementary updates to ARINC 618 by a relevant AEEC Subcommittee (e.g., Datalink Systems responsible for ACARS standards). The IPS Subcommittee would coordinate the analysis results and recommendations with the appropriate standards groups, and the results of these efforts may become part of the ATN/IPS standards generated by the IPS Subcommittee.

5.4.1.2 Work of Other AEEC Subcommittees

As noted in the previous section, the AEEC IPS Subcommittee will provide coordination of AEEC standardization activities that are relevant to ATN/IPS. For each of the following standardization activities identified as part of the gap analysis, the IPS Subcommittee will coordinate with industry stakeholders and AEEC Subcommittees to ensure that the timing and scope of project proposals consider the “need-by” dates of specific industry programs as well as dependencies on other AEEC Subcommittees and/or other standards development organizations.

5.4.1.2.1 IPv6 Airborne Naming and Addressing

As specified in ICAO Doc. 9896, the ATN/IPS uses Internet Protocol inter-networking based on IPv6 (per RFC 2460). In terms of architecture and addressing, this means that one or several airborne software/hardware components will have to be reachable via an IPv6 format network address.

ARINC Specification 664, which defines airborne addressing definition (internal and external interfaces), currently considers only IPv4 format addresses. Updates to this specification, including descriptive and guidance sections, are necessary to support any of the possible options to host ATN/IPS components on aircraft data networks. In particular, the scope of an AEEC activity to incorporate ATN/IPS naming and addressing in ARINC 664 may require modifications to the following ARINC 664 parts:

- Part 1 – General introduction of ATN/IPS and its expected network performance allocation (Appendix A);
- Part 3 – A more detailed description of IPv6, including options for dealing with potential mixed IPv6 and IPv4 systems. (Note: The AEEC Executive Committee has approved an activity to elaborate the IPv6 migration strategy for all air/ground connectivity, including but not limited to ATN/IPS);
- Part 4 – Naming and addressing definitions, in accordance with what will be proposed by ICAO;
- Part 5 – Data security considerations, linked to the migration from IPv4 to IPv6 in general, but also specific to ATN/IPS hosting in the ACD;

- Part 8 – A global description of ATN/IPS interactions with other protocols (ACARS, ATN/OSI) to improve material in the existing document that may be obsolete based the evolving ATN/IPS standards.

5.4.1.2.2 Communications Management Unit / Function

Supplement 4 (and later) to ARINC Characteristic 758 [date TBD] contains material that enables the CMU hardware design and system / hardware interface to support 100 Mbps Ethernet protocol and interface per ARINC 664 Part 2. With these updates, which will be consistent with ARINC Characteristic 781 (Inmarsat SBB), the CMU will support Ethernet interface with the Internet Protocol for air/ground communication and other on-aircraft communications.

ARINC Characteristic 758 includes provisions for transferring ACARS messages to/from a transceiver using one or two “super” blocks, instead of the traditional sized ACARS blocks, and the use of IP to send and receive messages. In addition, planned ARINC 618 modifications include a section on ACARS messaging over IP using Ethernet interface(s) between the CMU and transceiver(s). ACARS messaging over IP is an interim solution that provides some benefit before ARINC Standards for ATN/IPS are available.

Once ATN/IPS standards are available, ARINC Characteristic 758 may be updated accordingly to include ATN/IPS service specifications. This is expected to serve existing and future native IP applications and peripherals.

5.4.1.2.3 VDL Mode 2

As described in Section 2.5.1.2, VDL Mode 2 (VDLM2) may operate as an ATN/IPS air/ground subnetwork while also continuing to operate as an air/ground subnetwork for ACARS and ATN/OSI. The scope of an AEEC standardization effort for IPS-over-VDLM2 will include updates to ARINC Specification 631 to accommodate the exchange of IP packets in Aviation VHF Link Control (AVLC) frames. Specifically, the update will define the Initial Protocol Identifier (IPI) value, which is contained in the Information Field of an AVLC frame to indicate that the frame carries an IP packet (i.e., that IP is the network layer protocol) per ISO 9577:1999(E). (Note: The use of an Extended Initial Protocol Identifier (EIPI) is unnecessary with an IPI other than 0xFF. The protocol identifiers specified currently indicate that an AVLC frame carries an ACARS-over-AVLC (AOA) packet or an ISO 8208 packet.)

At the time of this writing, the AEEC is standardizing the implementation provisions for a connectionless variant of VDLM2 that would allow aircraft and ground stations to exchange AVLC frames without first having to establish an explicit connection, similar to the way in which VDL Mode 0/A (“Plain Old” ACARS) operates. While the intent of this activity is to address further the datalink performance of current ACARS and ATN messages, it also includes consideration for ATN/IPS messages given that the robustness and efficiency improvements expected with connectionless VDLM2 may benefit ATN/IPS as well, subject to validation. The current work scope includes updates to ARINC Specification 631 and coordination with related standards (e.g., RTCA DO-224C) to accommodate: indication of DSP support for exchanging data using UI frames via the AVLC specific options parameter in its GSIF; indication of support for UI frames in the HDLC optional functions XID public parameter; and use of the ground station broadcast address of a particular DSP as the destination address of a downlink UI frame. Methods to secure VDLM2 (e.g., authentication) data exchanges needs to be investigated.

VDLM2 implementation details are provided in ARINC Specification 631.

5.4.1.2.4 AeroMACS

As described in Section 2.15.2 of ICAO Doc. 10044, AeroMACS Technical Manual, IP packets are carried directly over the AeroMACS link. The AeroMACS Radio Unit (ARU), as defined in ARINC Characteristic 766, connects to the aircraft edge IP router. The ARU establishes both Layer 2 and Layer 3 connectivity with the terrestrial ASN Gateway.

Per the current definition in ARINC 766, AeroMACS is expected to support and to be compatible with ATN/IPS. However, changes to ARINC 766 may be necessary, based on the outcome of further AEEC IPS standardization activities. Any required changes would be the subject of a future supplement.

5.4.1.2.5 LDACS

As described in Section 2.4.1.2, LDACS will operate as a native ATN/IPS air/ground subnetwork. The scope of a potential AEEC LDACS standardization effort is expected to include development of an avionics specification that defines standards for interchangeability and interoperability, including the definition of physical form/fit, electrical interfaces, and functions of an LDACS radio. The specification is also expected to include the following guidance: avionics architectures (e.g., segregation from unrelated functions, integration with other systems); implementation options (e.g., a physical unit or a function that is integrated in other equipment to provide embedded LDACS functionality); and aircraft installation (e.g., antennas, cabling). The effort will leverage various industry documents (when developed) that specify LDACS functional and performance requirements, including an ICAO Technical Manual currently under development.

COMMENTARY

> Depending on the region, LDACS deployment may be a prerequisite for achieving ATN/IPS Initial Operational Capability (IOC). LDACS standardization timing and ATN/IPS standardization timing are independent.

5.4.1.2.6 Satcom

As described in Section 2.4.2, Satcom is one of the main media candidates to support ATN/IPS. The Satellite Data Unit (SDU) as defined in ARINC 771 (Iridium NEXT) and ARINC 781 (Inmarsat SBB safety services), will connect to the aircraft edge IP router. The SDU establishes both Layer 2 and Layer 3 connectivity with the terrestrial Satcom gateways.

Both ARINC 771 and ARINC 781 include provisions for ACD Ethernet access, e.g., Priority IP service. However, changes to both ARINC 771 and ARINC 781 may be necessary based on the outcome of further AEEC IPS standardization activities. Any required changes would be the subject of a future supplement to those documents. Changes may include an update of the interfaces (e.g., Ethernet, ARINC 664 Part 7, other), as well as architecture design considerations for segregation between aircraft domains, where ATN/IPS is part of the ACD (e.g., Attachment 8 to ARINC 781 and a similar attachment to ARINC 771).

5.4.1.2.7 Media Independent Aircraft Messaging (MIAM)

The preliminary and high-level architecture studies in Section 3 highlight the need for an adaptation layer between AOC applications (in particular ARINC 620 formatted messages) and the IPS transport/network layers. The existing ARINC Specification 841, MIAM, provides an overall concept and protocol for exchanging AOC messages over multiple protocols. MIAM uses a layered approach that includes a Core layer, which is fully independent of the underlying technologies, and a set of convergence sub-layers, which define simple and efficient adaptation to the available transmission protocols. Together, the core and convergence layers define a comprehensive end-to-end messaging service.

The current version of ARINC 841 available today defines ACARS and IP Middleware convergence layers. The scope of an AEEC standardization effort to update ARINC 841 will include definition of a new and specific convergence layer that supports an AOC messaging service over the native IP protocol, including:

- Provides avionics domain AOC applications (e.g., ACMS, CMS, FMS) with an asynchronous messaging service over IP by encapsulating Core MIAM messages into IP packets
- Interfaces with ATN/IPS at transport or network layer
- Accommodates the expected performance characteristics (e.g., latency) associated with the candidate ATN/IPS links (e.g., Satcom, AeroMACS, and LDACS)
- Provides an end-to-end service that complies with the overall ATN/IPS network infrastructure

5.4.1.2.8 Key Loading and Key Management

The current version of **ARINC Report 842:** *Guidance for Usage of Digital Certificates*, serves as a companion to ATA Spec 42, Aviation Industry Standards for Digital Information Security. ARINC 842 provides guidance to aircraft manufacturers, equipment suppliers, and operators regarding the life cycle management of private keys and digital certificates in an aircraft environment. It includes reference to ICAO Doc. 9896, ATN/IPS, as an example application of public key cryptography that requires life cycle key management. Future AEEC standardization activities will include the review of requirements in an ICAO-developed Public Key Infrastructure (PKI) Certificate Policy (CP) for ATN/IPS with respect to ARINC 842. Where necessary, updates to ARINC 842 will include new and/or revised guidance to address specific procedural and operational requirements for key management that are contained in the CP but not addressed in the existing guidance.

COMMENTARY

The AeroMACS Technical Manual, ICAO Doc. 10044, includes a PKI CP that is consistent with a reference CP for aviation specified in ATA Spec 42. The AeroMACS CP defines the procedural and operational requirements for managing public and private keys in a PKI environment. This includes requirements for key generation and storage, certificate generation and distribution, and secure distribution of trust anchor certificates. It is important to note that the development of the AeroMACS CP included input from and consideration of ATN security, including the Secure Dialog Service, which offers application-layer security for ATN applications operating over IPS or OSI networks. Consequently, the AeroMACS CP will serve as the basis for an ATN CP, and the ICAO PT-I Security Subgroup has a stated action item to “develop a policy document based on the AeroMACS PKI policy.”

At the time of this writing, the AEEC is updating ARINC 842 to maintain synchronization with recent changes to ATA Spec 42. As part this activity, the AeroMACS CP is being reviewed to ascertain potential improvements to the ARINC 842 guidance.

5.4.2 RTCA Standards

The RTCA Program Management Committee (PMC) assigned Special Committee (SC) 223 to develop the ATN/IPS Profiles and the ATN/IPS Minimum Operational Performance Standards (MOPS). The Terms of Reference (TOR) call for completion of IPv6, Transport, Mobility, Security and Multilink Profiles by December 2017 and the MOPS by end of 2019. Recognizing the interdependency of the protocol requirements definition with ICAO PT-I, the SC-223 started with the development of the IPv6 functional Profiles first and then recommend RFCs for other functions to ICAO PT-I. Once ICAO establishes high-level requirements, SC-223 will proceed with detailed requirements profiles for those functions. MOPS activities are not expected to begin before 2018.

In addition to ATN/IPS standardization efforts in progress and/or planned by RTCA, the following are potential additional activities identified as part of the standardization gap analysis:

- Extension of RTCA DO-262 MOPS and DO-343 MASPS to accommodate future Satcom and ATN/IPS, specifically definition of subnetwork interfaces to support standardized IPS network layer functions.
- Updates for VDLM2 support of ATN/IPS, such as modifications to RTCA DO-224C VDLM2 MASPS and DO-281B/ED-92B VDLM2 MOPS, to address explicitly the exchange of IP packets in Unnumbered Information (UI) frames. Includes coordination with AEEC on updates to ARINC 631 and with ICAO on updates to ICAO Doc. 9776.
- Updates to Safety and Performance Requirements Standard for Baseline 2 ATS Data Communications, for safety services beyond B2.
- Development of overall ATN/IPS security processes that address incident management, security logging and analysis, and coordination with an Aviation Information Sharing and Analysis Center (A-ISAC).

In addition to the work efforts of RTCA SC-223 on ATN/IPS profiles and MOPS, SC-216, Aeronautical Systems Security, has an effort underway to harmonize RTCA DO-356 with EUROCAE ED-203, which is the work product of EUROCAE WG-72. These harmonized Airworthiness Security Methods and Considerations documents will provide guidance on aircraft, system, and item level security requirements, which will drive design requirements for IPS systems.

5.4.3 EUROCAE Standards

Per EUROCAE, the EUROCAE Council and Technical Advisory Committee (TAC) are required to approve the engagement of the organization in a new activity, such as ATN/IPS. Both decision bodies were informed in the third quarter of 2016 about the developments in this area, and it is expected that the TAC will hold initial discussions about it during their April 2017 meeting.

In addition, the EUROCAE standard making process requires members' support to engage in any standardization activity. This is due to the member-driven system that forms the basis of the organization, as the members will have to commit the resources to complete the development of industry standards.

Currently, three EUROCAE Working Groups (WGs) – namely WG-82, WG-78, and WG-92 – deal with related subjects. More specifically, WG-92, VDL Mode 2 Working Group is working on VDLM2 standards, and a Terms of Reference (ToR) update is ongoing with finalization expected in April 2017. WG-78, Standards for Air Traffic Data Communication Services is dormant, having finished the deliverables as per their approved ToR; however, the group could be reactivated and start working on a new activity should the TAC and the Council approve it. Regarding WG-82, New Air-Ground Datalink Technologies, so far ATN/IPS is out of the scope of the current ToR. If WG-82 is tasked with the delivery of a standard for ATN/IPS, additional expertise would be required and a new Call for Participation issued to this end.

EUROCAE coordinates closely with RTCA regarding these three joint WGs, and it will maintain this coordination to ensure global interoperability.

EUROCAE reports that it will initiate the relevant process to identify the EUROCAE activities when ARINC Report 658 is available. This may include appropriate deliverable types, the appropriate organization, and so forth. The technical context will be analyzed fully at that time.

5.4.4 ICAO Standards

The ICAO Communications Panel (CP) Infrastructure Specific Working Group (ISWG) work program currently includes two approved ATN/IPS-related job cards, summarized in Table 5-1.

Table 5-1 – Approved ATN/IPS Standards Activities – ICAO[6]

Job Card	Activity Description	Assigned Project Team	Artifact(s) and Dates
CP-DCIWG 006.01 Provisions on the exchange of information using the ATN over IPS	An IP-based network for ATM is a key enabler for developments such as SWIM, FF/ICE, TBO and many others. However, there are complex issues that need to be addressed to ensure network security and efficiency. Some of these include stringent performance requirements (especially for air/ground; higher availability requirements, accommodation of the ICAO 24-bit aircraft address, a robust network architecture and interfaces, naming conventions unique to aviation, which must be globally consistent, and unique addressing to provide protection from random intrusions.	PT-I (Inter-networking)	Doc. 9896, ATN IPS (2020) Amendment to Annex 10 Volume III (2020)

---

[6] Reference ICAO Working Paper CP/2-WP/02, *Data Communications Infrastructure Working Group (DCIWG) Work Programme*, October 2016.

Job Card	**Activity Description**	**Assigned Project Team**	**Artifact(s) and Dates**
CP-DCIWG 007.01 SARPS and guidance on Air Navigation Cyber Security	SARPS and guidance will be needed across a whole range of areas, especially those related to Information Management (IM) and Communications. In addition to this, the automated systems used to support operational improvements such as FF/ICE, CDM and 4D TRAD will require protection against external intrusion.	PT-I (Inter-networking) with support from the Operational Specific Working Group (OSWG)	Doc. 9985, ATM Security Manual (2020) Amendment to Annex 10 Volumes II and III (2020)

During the second meeting of the ICAO CP in October 2016, the ISWG proposed new ATN/IPS-related job cards, summarized in Table 5-2. These are to subject to further definition and approval by the ISWG.

Table 5-2 – Proposed ATN/IPS-related Standards Activities – ICAO[7]

Job Card	**Activity Description**	**Proposed Project Team**	**Artifact(s) and Dates**
CP-DCIWG XXX.01 Future Satellite Systems	New Satellite systems are being developed which will provide greater performance and capacity than is available today. ICAO standards for AMS(R)S need to be updated in order to support their use for ATM operations. As the development of these systems will be developed in phases, each phase will need to be evaluated and ICAO provisions updated. This will also require a transition plan.	PT-T with support on PBCS by OSWG	Doc. 9925, AMS(R)S (TBD) Doc. 9869, PBCS (TBD) Amendment to Annex 10 Volume III (2020)
CP-DCIWG YYY.01 Future Terrestrial Datalink System (LDACS)	Future terrestrial communications systems are being developed which have greater performance and capacity than the systems in use today. ICAO standards and guidance need to be developed to support their use for ATM operations. Future operations based on TBO with support by SWIM will require the performance provided by such systems.	PT-T with support on PBCS by OSWG	Doc. YYYY, AMS(R)S (TBD) Doc. 9869, PBCS (TBD) Amendment to Annex 10 Volume III (2020)
CP-DCIWG ZZZ.01 Multi-link	Definition/standardization of the multilink concept in support of the operational requirements in various airspaces, taking into account the ground and airborne architectures and network infrastructure interoperability aspects of the communication systems.	TBD – to be assigned by ISWG	TBD

---

[7] Reference ICAO Working Paper CP/2-WP/02, *Data Communications Infrastructure Working Group (DCIWG) Work Programme*, October 2016.

During the seventh meeting of the ICAO ISWG PT-I Security Sub-group held in December 2016, the Security Sub-group Rapporteur presented a working paper[8] that proposed the following ATN/IPS security tasks:

- Consideration for using the Secure Dialog Service (sDS) for air/ground access network security,
- Development of an ATN/IPS security Concept of Operations that includes a notional architecture, identification of roles and responsibilities, a generic risk assessment for the notional architecture, and identification of technical security solutions, and
- Development of an ICAO security policy, PKI architecture, and guidance document for ATN/IPS.

In addition to ATN/IPS standardization efforts in progress and/or proposed by ICAO ISWG, the following are potential additional activities identified as part of the standardization gap analysis:

- Mapping between OSI addresses and IPS addresses. (A potential extension of the work scope included under Job Card CP-DCIWG 006.01)
- Updates to ICAO Doc. 9896 technical provisions to support accommodation of FANS messages, as well as support for future native IP (e.g., non-DSI-based) applications. (A potential extension of the work scope included under Job Card CP-DCIWG 006.01)
- Extension of the AeroMACS PKI CP in ICAO Doc. 10044 to support ATN/IPS security.
- Processes for administration of IP names and addresses. (A potential extension of the work scope included under Job Card CP-DCIWG 006.01)
- Updates for VDLM2 support of ATN/IPS, e.g., modifications to the Doc. 9776 VDL Tech Manual to address connectionless VDLM2 exchanges and use of IP packets in VDLM2.
- Guidance describing the information shared between OSI and IPS in order to maintain correlation of the ATN applications.

ICAO's ATN/IPS standardization plans may already include these activities; however, they are offered for ICAO consideration where current job cards do not identify these activities explicitly.

5.4.5 Other Standards and Activities

In addition to ARINC Industry Activities, RTCA, EUROCAE, and ICAO IPS standardization efforts, the standardization gap analysis identified potential additional activities that may require coordination with other organizations.

- In concert with ICAO activities to administer IP names and addresses for safety services, complementary processes may be necessary for the administration of IP names and addresses for non-safety airline communications. This could be managed in the same way the ICAO 24-bit addresses are managed.

---

[8] Reference ICAO Working Paper CP-SDS SWG/07-WP/03, *Future Security Plan*, December 2016.

- Each regional Civil Aviation Authorities (CAA) will need to define an ATN/IPS network topology that supports the regional implementation of ATN/IPS based on ICAO Doc. 9896.

5.5 ATN/IPS Validation Activities

The following sub-sections provide a description of ATN/IPS validation efforts that are in progress, planned, or proposed by various organizations.

5.5.1 FAA Secure Dialog Service Validation

The ATN/IPS Security sub-group of ICAO ISWG PT-I recently completed the technical provisions for the Secure Dialog Service (sDS), which may be implemented by airborne and ground ATN/IPS nodes to provide interoperable application layer security at the dialog service boundary. The FAA is validating the sDS provisions in FY17 and FY18.

The FAA sDS validation uses simulated air and ground systems with the ATN/IPS Dialogue Service running over IPv6 via local Ethernet interface. The validation prototype is an extension of an existing ATN/IPS DS implementation developed for the Tower Data Link System (TDLS) Departure Clearance application. This implementation provides the ATN/IPS connectionless service primitives (D-UNITDATA and D-ACK) only. It is being extended to provide the connection-oriented primitives operating over UDP with the IPS DS reliability extensions.

Once the ATN/IPS DS implementation is tested successfully, the sDS primitives for air-initiated and ground-initiated applications are being implemented using the ASN.1 wrappers for each sDS service. Finally, the sDS cryptographic primitives, using the latest defined domain parameters, are being implemented and integrated with the sDS primitives. Validation of the sDS implementation leverages simulated air and ground applications and X.509 certificates generated by open-source utilities.

5.5.2 SESAR ATN/IPS-related Validation Activities

In SESAR 2020, there are activities related to the definition and validation of the proposed solutions for ATN/IPS. Under project PJ14, which addresses CNS aspects in general, there are five “solutions” (effectively sub-projects), addressing COM aspects. Four of these COM sub-projects focus on further development of the Future Communications Infrastructure (FCI), including:

- PJ14-02-04 – FCI Network Technologies: Addresses general FCI aspects and the overall architecture, as well as specific focus on the Multilink Concept and the use of ATN/IPS.
- PJ14-02-01 – FCI Terrestrial Data Link: Development and standardization of LDACS through the prototype development and testing.
- PJ14-02-02 – Future Satellite Communication Means: Definition of the Long Term Satcom system (Performance Class A), considering the available Inmarsat Precursor capabilities (Performance Class B).
- PJ14-02-06 – Completion of AeroMACS Development: Verification of AeroMACS with ATN services starting with ATN/OSI and its integration in a multilink environment with handover to and from VDLM2.

In relation to ATN/IPS, all four solutions will develop prototypes and perform testing and verification (technical validation) activities including ATN/IPS functionality and selected protocols. Solution PJ14-02-04 will consolidate the common ATN/IPS requirements considering ongoing work at ICAO and other groups, including the AEEC IPS Subcommittee, and provide the requirements as input to the other three solutions, which address specific technologies for datalink. The three technology solutions will perform technical validation activities integrating the ATN/IPS functionality over LDACS, Satcom and AeroMACS. In addition, solution PJ14-02-04, with the support of the other three technological datalink solutions, will perform verification activities of the Multilink Concept in an ATN/IPS environment, with handover from one datalink to the other.

These four SESAR 2020 solutions initiated their technical work in Q1 of 2017, and the planned completion date is Q3 of 2019. The intent is to present the outcome of the SESAR 2020 ATN/IPS verification activities to relevant standardization groups, including AEEC, as they become available.

5.5.3 Iris Programme ATN/IPS-related Validation Activities

The Iris Programme includes activities related to the definition and validation of the proposed solutions for ATN/IPS. The issue, which has several dimensions, will set requirements for future developments in airborne and ground systems. Since the objective is a globally interoperable service, international standards are required for future developments, Iris will develop key principles, design approaches and proposed standards and technical manual contributions that feed into the ICAO and ARINC Standards. Inmarsat and consortium members who are partners of the SESAR Joint Undertaking will undertake additional European coordination with SESAR work.

Within the Iris Programme, this work will be coordinated by the ATN/IPS Coordination Team, which will study transition options and produce transition plans for both ground and air segments, ensuring co-existence and interoperability with ATN/OSI implementations are maintained. In addition, an ATN/IPS Coordination Forum will coordinate among the Iris activities led by various industrial partners that rely on the definition of ATN/IPS. The Forum will maintain a work plan/schedule that will define and scope all activities that relate to the definition of ATN/IPS, and it will provide oversight and coordination to ensure that there is a harmonized approach and roadmap for global implementation.

The ATN/IPS Co-ordination Forum and will coordinate standardization activities with the appropriate SDOs, namely ICAO, AEEC and others as required. The Iris effort will be aligned with AEEC IPS Subcommittee guidance, which is expected to produce a new ARINC Standard containing an ATN/IPS profile that specifies implementation options and constraints as well as details regarding the accommodation of different applications.

The activities associated with the early definition of ATN/IPS under the Iris project commenced in Q1 2016 and the initial activities are planned to be completed in Q4 2017. It is expected that the Iris activities, and potentially other developmental activities, will lead to further work in the standards arena. However, it should be noted that follow-on work is anticipated to continue into 2019 to formalize the work being done in the standardization arena.

5.5.4 Clean Sky2 ATN/IPS-related Validation Activities

Clean Sky2 is a European Joint Technology Initiative (JTI) aiming at enhancing environmental impact of aeronautical technologies and supporting modernization of the aircraft architectures. As part of this European initiative, two major programs integrate activities related to ATN/IPS:

- Large Passenger Aircraft IADP (Innovative Aircraft Demonstrator Platforms) led by Airbus and focused on the ATN/IPS airborne router,
- Systems ITD (Integrated Technology Demonstrators) led by Thales.

Those programs intend to consolidate the industry requirements for ATN/IPS and develop prototypes that will be used to perform validation of the network and communication management functions over multiple sub-networks.

Such activities have been associated with European Calls for Core Partners, enabling a further widening and engagement of the European aeronautics industrial and research base in the ATN/IPS developments:

- JTI-CS2-2015-CPW02-LPA-03-01: Maturation, validation and integration with the airframers of cockpit functions and avionics technologies (Call Topic Leader: Airbus)
- JTI-CS2-2016-CPW04-SYS-01-01: Networking solutions for future cockpit communications (Call Topic Leader: Thales)

5.6 Standardization Timing and Coordination

Appendix C presents notional roadmaps developed by various organizations to document their perspective on the timing of ATN/IPS standardization, validation, implementation, deployment, and initial operational capability (IOC). Table 5-3 summarizes IOC dates presented in each of the Appendix C roadmaps with respect to applications/services leveraging ATN/IPS, the ATN/IPS network, and subnetworks supporting ATN/IPS.

Table 5-3 – Summary of Notional Timelines in Appendix A

		Notional IPS Timeline Summary (Appendix C references)				
Elements	**Enabler**	**ICAO ASBU (A-1)**	**FAA Continental (A-2)**	**EU Continental and US/EU Oceanic (A-2)**	**Airbus (A-3.1)**	**Boeing (A-3.2)**
Application/Servcies (over IPS)	FANS 1/A (US only)		Mid-Term (~2024+)			(not shown separately)
	B2	Block 2 (2024-2030)	Mid-Term (~2024+)	Long-term (~2028+)	2028-2030+	2024+
	B3	Block 3 (2030+)	(not shown separately)	(not shown separately)	2028-2030+	(not shown separately)
Network	IPS	Block 2 (2024-2030)	Mid-Term (~2024+)	Mid-Term (2024+ ramping to 2028+)	2028-2030+	2024+
Physical Links (supporting IPS)	VDLM2 (US only)		Mid-Term (~2024+)			2024+
	Satcom Perf. Class B	Block 2 (2024-2030)	Mid-Term (~2024+)	Mid-Term (2024+ ramping to 2028+)	2028-2030+	2028+
	AeroMACS	Block 2 (2024-2030)	Mid-Term (~2024+)	Mid-Term (2024+ ramping to 2028+)	2028-2030+	2024+
	LDACS	Mid-Block 2 (2028+)	(not planned)	Long-term (~2028+)	2028-2030+	2030+
	Satcom Perf. Class A	(not shown separately)	Long-term (~2030+)	Long-term (~2030+)	2028-2030+	(not shown separately)

As shown, the IOC dates for the ATN/IPS network, which is the focus of this document, is in the 2024 to 2028+ timeframe, and this serves as a key input to ATN/IPS standardization timing.

Using the 2024+ to 2028+ IOC timeframe as a starting point, which aligns with ICAO ASBU Block 2, Figure 5-2 presents a notional summary-level reverse plan for standardization/validation and productization/certification activities that are predecessors to ATN/IPS IOC. As suggested in the figure, having complete and validated standards by 2020 allows necessary time for product development and certification to support the earliest IPS IOC date of 2024+.

COMMENTARY

> While 2020 represents the standardization schedule to which the industry is currently working, the reader should not interpret the notional summary timeline as a commitment. The overall feasibility of the notional timing, particularly with respect to product development and certification, is subject to evolving industry stakeholder strategies and product introduction plans.

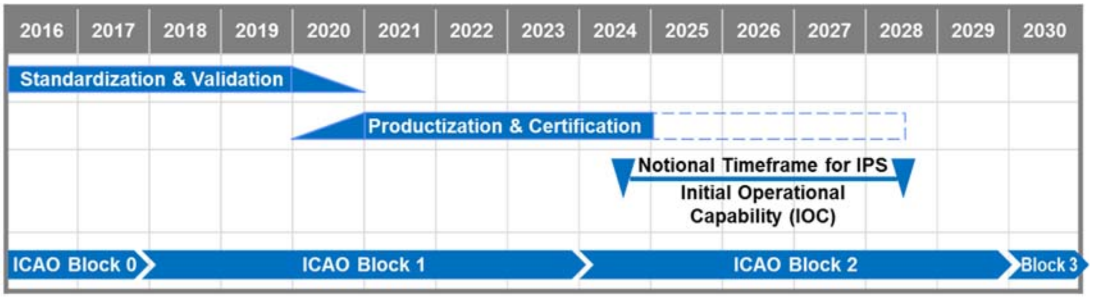
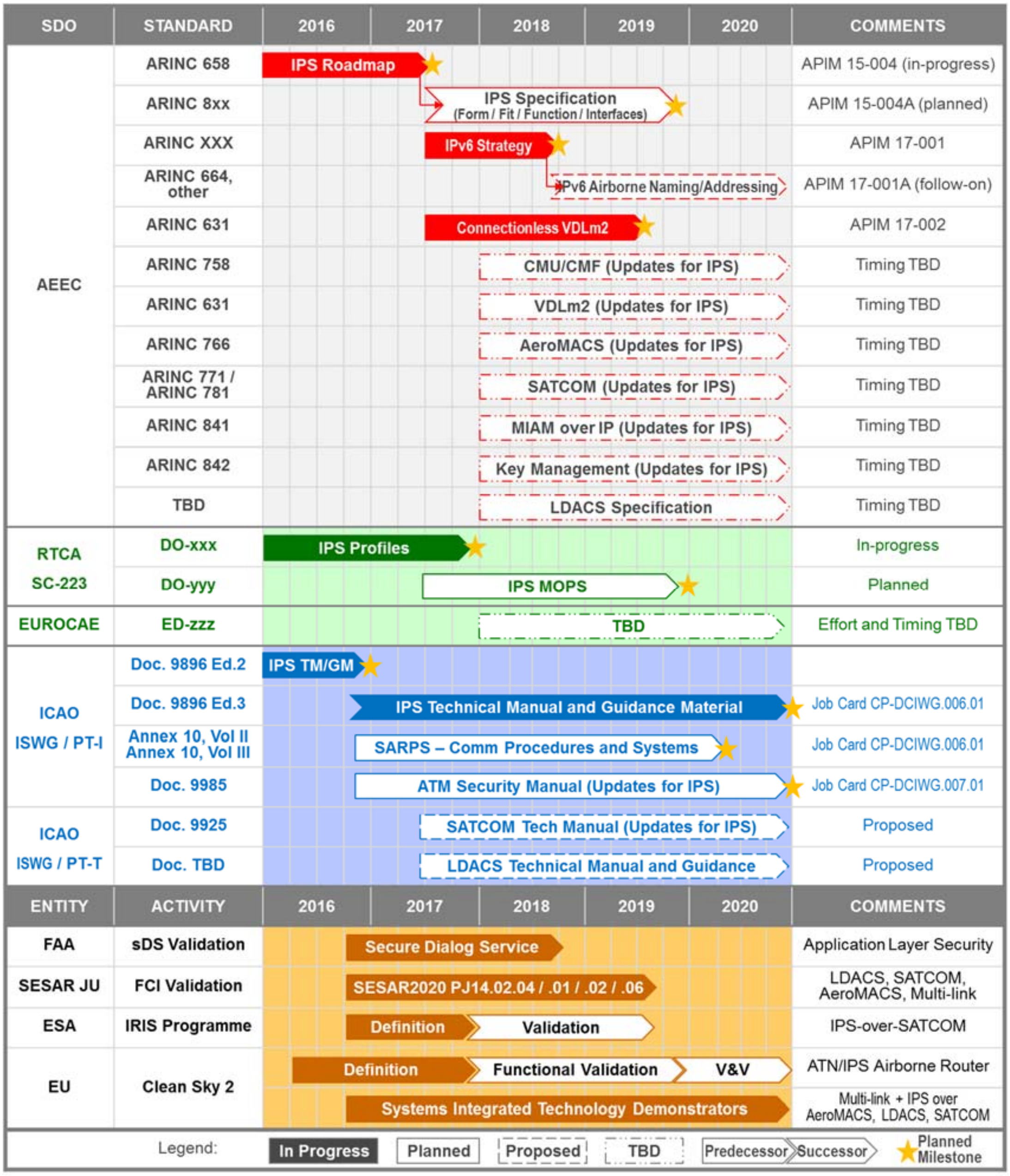


Figure 5-2 – Notional Standardization Timeframe

Figure 5-3 expands upon the “Standardization and Validation” phase (2016 to 2020) and graphically illustrates the timing of specific activities described in Section 5.4 for each of the standards development organizations. The ongoing work of the AEEC IPS Subcommittee will include coordination with industry stakeholders and other AEEC subcommittees to provide necessary timing and scope fidelity for AEEC standardization activities currently shown as “Timing TBD,” subject to evaluation and confirmation that the activity is necessary. As AEEC projects are proposed and approved, the IPS Subcommittee may update the roadmap in order to facilitate intra- and inter-organization coordination, particularly where there may be dependencies.

5.0 ATN/IPS STANDARDIZATION ROADMAPS



SDO	STANDARD	2016	2017	2018	2019	2020	COMMENTS
AEEC	ARINC 658	IPS Roadmap ★					APIM 15-004 (in-progress)
	ARINC 8xx		IPS Specification (Form / Fit / Function / Interfaces) ★				APIM 15-004A (planned)
	ARINC XXX		IPv6 Strategy ★				APIM 17-001
	ARINC 664, other			IPv6 Airborne Naming/Addressing			APIM 17-001A (follow-on)
	ARINC 631		Connectionless VDLm2 ★				APIM 17-002
	ARINC 758			CMU/CMF (Updates for IPS)			Timing TBD
	ARINC 631			VDLm2 (Updates for IPS)			Timing TBD
	ARINC 766			AeroMACS (Updates for IPS)			Timing TBD
	ARINC 771 / ARINC 781			SATCOM (Updates for IPS)			Timing TBD
	ARINC 841			MIAM over IP (Updates for IPS)			Timing TBD
	ARINC 842			Key Management (Updates for IPS)			Timing TBD
	TBD			LDACS Specification			Timing TBD
RTCA SC-223	DO-xxx	IPS Profiles ★					In-progress
	DO-yyy		IPS MOPS ★				Planned
EUROCAE	ED-zzz			TBD			Effort and Timing TBD
ICAO ISWG / PT-I	Doc. 9896 Ed.2	IPS TM/GM ★					
	Doc. 9896 Ed.3	IPS Technical Manual and Guidance Material ★					Job Card CP-DCIWG.006.01
	Annex 10, Vol II Annex 10, Vol III	SARPS – Comm Procedures and Systems ★					Job Card CP-DCIWG.006.01
	Doc. 9985	ATM Security Manual (Updates for IPS) ★					Job Card CP-DCIWG.007.01
ICAO ISWG / PT-T	Doc. 9925		SATCOM Tech Manual (Updates for IPS)				Proposed
	Doc. TBD		LDACS Technical Manual and Guidance				Proposed
ENTITY	**ACTIVITY**	**2016**	**2017**	**2018**	**2019**	**2020**	**COMMENTS**
FAA	sDS Validation	Secure Dialog Service					Application Layer Security
SESAR JU	FCI Validation	SESAR2020 PJ14.02.04 / .01 / .02 / .06					LDACS, SATCOM, AeroMACS, Multi-link
ESA	IRIS Programme	Definition	Validation				IPS-over-SATCOM
EU	Clean Sky 2	Definition	Functional Validation		V&V		ATN/IPS Airborne Router
		Systems Integrated Technology Demonstrators					Multi-link + IPS over AeroMACS, LDACS, SATCOM

Legend: In Progress | Planned | Proposed | TBD | Predecessor › Successor | ★ Planned Milestone

Figure 5-3 – ATN/IPS Standardization Roadmap

6.0 SUMMARY RECOMMENDATIONS

6.1 Recommendations to the AEEC IPS Subcommittee

The AEEC IPS Subcommittee should:

- Maintain the IPS standardization roadmap (including updates to the gap analysis and standardization activity timing), developed as part of the AEEC IPS Phase 1 activity and presented in Section 5 of this document.
- Serve as the coordination focal for all AEEC IPS-related activities, including:
  - Coordinate with industry stakeholders and other AEEC Subcommittees to ensure that the timing and scope of ATN/IPS-related project proposals consider the “need-by” dates of specific industry programs as well as dependencies on other AEEC Subcommittees and/or other standards development organizations.
  - Address questions from other AEEC Subcommittees regarding interpretations of ARINC Report 658.
  - Monitor AEEC IPS-related developments and standardization work, including cyber security
- Coordinate with other IPS standardization development organizations, including:
  - Engage AEEC IPS industry participants, particularly those who support multiple SDOs, to develop and present working papers to other SDOs regarding the status of AEEC ATN/IPS efforts.
  - Leverage the ATN/IPS standardization roadmap as a communication tool for inter-organization coordination, particularly where there may be dependencies.
  - Based on updates to the gap analysis, provide recommendations for potential additional work to be considered by the other SDOs.
- Organize and execute ATN/IPS standards development efforts to address the work scope allocated to the IPS Subcommittee, as described in Section 5.4.1.1 of this document, Work of the AEEC IPS Subcommittee.
  - Prepare ARINC Project Paper 8xx, Standardization of ATN/IPS for Aviation (working title) per APIM 15-004A approved by the AEEC Executive Committee.

6.2 Recommendations to Regulatory Bodies

The regulatory bodies (e.g., FAA and EASA) should:

- Collaborate with industry stakeholder organizations, including aircraft OEMs and avionics suppliers, to identify new certification considerations driven by the introduction of ATN/IPS as a transport/network protocol for safety services.
- Support development of foundational documentation necessary for certification. This documentation may include:
  - Concept of Operations for ATN/IPS safety services,
  - Preliminary system safety assessment,
  - Preliminary system security risk assessment, and
  - MOPS and MASPS.

6.0 SUMMARY RECOMMENDATIONS

- Support development of a Technical Standard Order (TSO) for ATN/IPS Network Equipment.
- Develop an ATN/IPS advisory circular (AC) that provides guidelines on what is required for ATN/IPS systems to be compliant with providing protection against misleading and corrupted messages.
- Develop and/or update policy statements to address cyber security vulnerabilities in aircraft certification programs. Considerations should include:
    - End-to-end security requirements for ATN/IPS,
    - Assumptions regarding shared responsibility by the ground (i.e., to what extent can aircraft certification of ATN/IPS systems rely on the cyber security protections implemented by the ground).

ATTACHMENT 1 LIST OF ACRONYMS

4DT	Four Dimensional Trajectory
4DTRAD	Four Dimensional Trajectory Datalink
A-G or A/G	Air-to-Ground
A-ISAC	Aviation Information Sharing and Analysis Center
AC	Advisory Circular
ACARS	Aircraft Communications Addressing and Reporting System
ACD	Aircraft Control Domain
ACL	ATC Clearance
ACM	Aircraft Communications Message
ACMS	Aircraft Condition Monitoring System
ACR	Avionics Communications Router
ACSP	Air/Ground Communications Service Provider
ADS-C	Automatic Dependent Surveillance-Contract
ADS-C EPP	ADS-C Extended Projected Profile
AEEC	Airlines Electronic Engineering Committee
AeroMACS	Aeronautical Mobile Airport Communications System
AFN	ATS Facilities Notification
AIM	Aeronautical Information Management
AIREP	Aircraft Report
AIS/MET	Aeronautical Information Services/Meteorological
AISD	Aircraft Information Services Domain
ALGA	Active Low Gain Antenna
AMC	ATC Microphone Check
AMET	Airborne Meteorological
ANSP	Air Navigation Service Provider
AOA	ACARS Over AVLC
AOC	Airline Operational Control
ARAC	Aviation Rulemaking Advisory Committee
ARU	AeroMACS Radio Unit
ASBU	Aviation System Block Upgrade
ASN	Access Service Network
ASN-GW	Access Service Network Gateway
ATA	Air Transport Association
ATC	Air Traffic Control
ATM	Air Traffic Management
ATN	Aeronautical Telecommunication Network
ATS	Air Traffic Services
ATSP	Air Traffic Service Provider
ATSU	Air Traffic Services Unit

ATTACHMENT 1
LIST OF ACRONYMS

AUTOMET	Automatic Meteorological (report)
AVLC	Aviation VHF Link Control
BLOS	Beyond Line Of Sight
BS	Base Station
CA	Certificate Authority
CAA	Civil Aviation Authority
CARATS	Collaborative Actions for Renovation of Air Traffic Systems (Japan)
CDU	Control Display Unit
CDM	Collaborative Decision Making
CLNP	Connectionless Network Protocol
CM	Context Management
CMF	Communications Management Function
CMU	Communications Management Unit
CNS/ATM	Communications Navigation Surveillance/Air Traffic Management
CoS	Class of Service
COTP	Connection Oriented Transport Protocol
COTS	Commercial Off The Shelf
CP	Communications Panel (ICAO)
CP	Certificate Profile (PKI)
CPDLC	Controller Pilot Data Link Communications
CPU	Central Processing Unit
CRL	Certificate Revocation List
CSN	Connectivity Network Service
CSP	Communication Service Provider
CSR	Certificate Signing Request
D8PSK	Differential 8-Phase Shift Keying
D-ATIS	Digital Automatic Terminal Information Service
D-OTIS	Datalink Operational Terminal Information Service
D-TAXI	Digital TAXI
DAL	Design Assurance Level
DCL	Departure Clearance
DCNS	Data Communications Network Service
DDoS	Distributed Denial of Service
DLIC	Data Link Initiation Capability
DLS-IR	Data Link Services Implementing Rule
DME	Distance Measuring Equipment
DoD	Department of Defense
DoS	Denial of Service
D-RNP	Dynamic Required Navigation Performance
DS	Dialog Service
DSP	Data Link Service Provider

ATTACHMENT 1
LIST OF ACRONYMS

EASA	European Aviation Safety Agency
ECAC	European Civil Aviation Conference
EFB	Electronic Flight Bag
EIPI	Extended Initial Protocol Identifier
EIRP	Equivalent Isotropically Radiated Power
ESA	European Space Agency
EU	European Union
FAA	Federal Aviation Administration
FANS	Future Air Navigation System
FCI	Future Communications Infrastructure
FDD	Frequency Division Duplex
FEP	Front End Processor
FF/ICE	Flight and Flow Information for a Collaborative Environment
FIR	Flight Information Region
FIS	Flight Information Service
FMF	Flight Management Function
FMS	Flight Management System
FY	Fiscal Year
G-G or G/G	Ground-to-Ground
GANP	Global Air Navigation Plan
GATM	Global Air Traffic Management
GES	Ground Earth Station
GHz	Gigahertz
GNSS	Global Navigation Satellite System
HDLC	High-level Data Link Control
HF	High Frequency
HFDL	High Frequency Data Link
HGA	High Gain Antenna
ICAO	International Civil Aviation Organization
ICS	Internet Communication Service
IER	Information Exchange and Reporting
IETF	Internet Engineering Task Force
IM	Information Management
IMA	Integrated Modular Avionics
IMS	Information Management Services
IOC	Initial Operational Capability
IP	Internet Protocol
IPI	Initial Protocol Identifier
IPS	Internet Protocol Suite
IPsec	Internet Protocol Security
IPv4 / IPv6	Internet Protocol Version 4 or Version 6

ATTACHMENT 1
LIST OF ACRONYMS

IS	Information Services
ISO	International Standards Organization
ISWG	Infrastructure Specific Working Group
ITP	In-Trail Procedure
ITU	International Telecommunication Union
LDACS	L Band Digital Aviation Communication System
LEO	Low Earth Orbit
LGA	Low Gain Antenna
LOS	Line of Sight
MAS	Message Assurance
MASPS	Minimum Aviation System Performance Standards
MCDU	Multi-purpose Control and Display Unit
MET	Meteorological
MHz	Megahertz
MIAM	Media Independent Aircraft Messaging
MOPS	Minimum Operational Performance Standards
MP-TCP	Multi-Path Transmission Control Protocol
MRO	Maintenance Repair and Overhaul
NAS	National Airspace System
NextGen	Next Generation Air Transportation System
NM	Nautical Miles
NOTAM	Notice to Airmen
OCL	Oceanic Clearance
OEM	Original Equipment Manufacturer
OFDM	Orthogonal Frequency Division Multiplexing
OSWG	Operational Specific Working Group
OTIS	Operations Terminal Information System
PFIS	Passenger Flight Information Systems
PGW	Protocol Gateway
PIESD	Passenger Information Services Domain
PKI	Public Key Infrastructure
PLP	Packet Layer Protocol
PMC	Program Management Committee
POA	Plain Old ACARS
PPPoE	Point to Point Protocol over Ethernet
PR	Position Reporting
PS	Policy Statement
PT	Project Team
QAR	Quick Access Recorder
QoS	Quality of Service
RCP	Required Communication Performance

ATTACHMENT 1
LIST OF ACRONYMS

RCTP	Required Communication Technical Performance
RF	Radio Frequency
RFC	Request For Comment
RNP	Required Navigation Performance
RSP	Required Surveillance Performance
RSTP	Required Surveillance Technical Performance
SAL	Security Assurance Level
SARPS	Standards and Recommended Practices
Satcom	Satellite Communications
SBB	Swift Broadband
SBD	Short Burst Data
SCTP	Stream Control Transmission Protocol
SDO	Standards Development Organization
SDR	Software Defined Radio
sDS	Secure Dialog Service
SDU	Satellite Data Unit
SESAR	Single European Sky Air Traffic Management (ATM) Research
SIGMET	Significant Meteorological Information
SNAcP	Subnetwork Access Protocol
SPR	Safety and Performance Requirement
SWaP	Size Weight and Power
SWIM	System Wide Information Management
TAC	Technical Advisory Committee
TACAN	Tactical Air Navigation
TBD	To Be Determined
TBO	Trajectory Based Operations
TCP	Transmission Control Protocol
TDLS	Terminal Data Link System
ToR	Terms of Reference
TSO	Technical Standard Order
UDP	User Datagram Protocol
UI	Unnumbered Information
ULCS	Upper Layer Communication Services
US	United States
USB	Universal Serial Bus
V&V	Verification and Validation
VDL	VHF Data Link
VDLM2	VHF Data Link Mode 2
VHF	Very High Frequency
VOLMET	Vol (flight) Meteo (weather)
VPN	Virtual Private Network

ATTACHMENT 1
LIST OF ACRONYMS

WG	Working Group
WiMAX	Worldwide Interoperability for Microwave Access
WoW	Weight on Wheels
XID	eXchange Identification

ATTACHMENT 2 GLOSSARY

AAC – Aeronautical Administrative Communications

Communication used by aeronautical operating agencies related to the business aspects of operating their flights and transport services. This communication is used for a variety of purposes, such as flight and ground transportation, bookings, deployment of crew and aircraft or any other logistical purposes that maintain or enhance the efficiency of over-all flight operation.

ACARS – Aircraft Communications Addressing and Reporting System

A digital datalink network providing connectivity between aircraft and ground end systems (command and control, air traffic control).

ACD – Aircraft Control Domain

It consists of systems and networks whose primary functions are to support the safe operation of the aircraft. This domain connects to high-priority Air Traffic Services (ATS) and some Airline Operational Control (AOC) communications.

ADS-C – Automatic Dependent Surveillance-Contract

ADS-C is the same as ADS-A. Automatic Dependent Surveillance-Addressed is a datalink application that provides for contracted services between ground systems and aircraft. Contracts are established such that the aircraft will automatically provide information obtained from its own on-board sensors, and pass this information to the ground system under specific circumstances dictated by the ground system (except in emergencies).

Airborne ATN/IPS Router

It is an airborne device that supports ATN/IPS packet forwarding in the air/ground environment.

AISD – Aircraft Information Services Domain

This domain provides general purpose routing, computing, data storage and communications services for non-essential applications. The AISD domain can be subdivided into two sub-domains;

- Administrative sub-domain, which provides operational and airline administrative information to both the flight deck and cabin,
- Passenger support sub-domain, which provides information to support the Passengers

AOA – ACARS Over Aviation VHF Link Control

AOA is an attempt at gaining some early benefits of digital technology without the full risk of ATN. It is a step between full ACARS and full ATN. The most significant near-term benefit is the reduction of VHF congestion problems by transitioning traffic to the VDLM2 air/ground network. AOA allows airborne and airline host applications to remain unchanged (character format). The airborne AOA process packages the data so that it can be routed over the digital VDLM2 network. At some point on the ground, the data is restored to its original format for processing by legacy airline host applications. VDLM2 operates at 31.5 kbps versus ACARS at 2.4 kbps.

ATTACHMENT 2
GLOSSARY

AOC – Airline Operational Control (Aeronautical Operational Control)

Operational messages used between aircraft and airline dispatch centers or, by extension, the DoD to support flight operations. This includes, but is not limited to, flight planning, flight following, and the distribution of information to flights and affected personnel.

APC – Aeronautical Passenger Communications

Communication relating to the non-safety voice and data services to passengers and crew members for personal communication.

Application

Functions that provide the services needed by the users. Applications are grouped into Application sets that are associated to specific network protocols. In the ACD domain the Applications sets are providing air traffic and operational control services.

ATN – Aeronautical Telecommunications Network

An internetwork architecture that allows ground/ground, air/ground, and avionic data subnetworks to interoperate by using common interface services and protocols based on the ISO OSI Reference Model.

ATN/IPS Node

An ATN/IPS node is a device that implements IPv6. There are two types of ATN/IPS nodes; the ATN/IPS router that forwards Internet Protocol (IP) packets not explicitly addressed to itself and ATN/IPS host, which does not have the capability to route traffic flows.

ATN/IPS System

Internetwork consisting of ATN/IPS nodes and networks operating in a multinational environment in support of Air Traffic Services (ATS) as well as aeronautical industry service communication such as Aeronautical Operational Control (AOC) and Aeronautical Administrative Communications (AAC).

ATS – Air Traffic Services

A generic term meaning variously, flight information service, alerting service, air traffic advisory service, air traffic control service. The latter is a service provided for the purpose of preventing collisions, expediting and maintaining an orderly flow of traffic.

ATSU – Air Traffic Services Unit

A unit established for the purpose of receiving reports concerning air traffic services and flight plans submitted before departure. It is a generic term meaning air traffic control unit, flight information center, or air traffic service reporting office.

ATTACHMENT 2
GLOSSARY

CM – Communication Manager

This function manages the connectivity of the aircraft with the ground system. It is decomposed into two sub-functions:

- ATN/IPS Communication Manager, which manages in the ATN/IPS system the selection of the radio bearer for a dedicated traffic flow and the associated mode of communication.
- External Communication Manager, which performs router selection and associated vertical handover decisions. This entity may be extended to include the management of multi-domain link selections.

CMU – Communication Management Unit

The CMU performs two important functions: it manages access to the various datalink sub-networks and services available to the aircraft and hosts various applications related to datalink. It also interfaces to the flight management system (FMS) and to the crew displays.

CNS/ATM – Communication, Navigation, Surveillance/Air Traffic Management

CNS/ATM is a system based on digital technologies, satellite systems, and enhanced automation to achieve a seamless global Air Traffic Management. Modern CNS systems will eliminate or reduce a variety of constraints imposed on ATM operations today.

CPDLC – Controller-Pilot Data Link Communications

The CPDLC application provides for the exchange of flight planning, clearance, and informational data between a flight crew and air traffic control. This application supplements voice communications and, in some areas, data may supersede voice.

DS – Dialogue Service

The Dialogue Service serves as an interface between the ATN applications and the ATN/OSI or ATN/IPS upper layer protocols via the control function.

FANS-1/A – Future Aircraft Navigation System 1/A

A set of operational capabilities centered around direct datalink communications between the flight crew and air traffic control. Operators benefit from FANS-1/A in oceanic and remote airspace around the world.

FMF – Flight Management Function

A collection of processes or applications that facilitates area navigation (RNAV) and related functions to be executed during all phases of flight. The FMF is resident in an avionics computer and automates navigational functions reducing flight crew workload particularly during instrument meteorological conditions. The Flight Management System encompasses the FMF.

FMS – Flight Management System

A computer system that uses a large database to allow routes to be preprogrammed and fed into the system by a means of a data loader. The system is constantly updated with respect to position by reference to designated sensors. The sophisticated program and its associated database insure that the most appropriate aids are automatically selected during the information update cycle. The flight management system is interfaced/coupled to cockpit displays to provide the flight crew situational awareness and/or an autopilot.

Ground ATN/IPS Router

A ground device that is used to support ATN/IPS packet forwarding in both air/ground and ground/ground environments.

Infrastructure

This is a general term corresponding to the communication systems that support the application sets. It consists of the Network and Sub-networks functions.

LINK 2000+ – The EUROCONTROL LINK 2000+ Program

Packages a first set of enroute controller-pilot data-link-communication (CPDLC) services into a set for implementation in the European Airspace using the ATN and VDL Mode 2 (Aeronautical Telecommunication Network and VHF Digital Link).

MASPS – Minimum Aviation System Performance Standards

High-level documents produced by RTCA that establish minimum system performance characteristics.

MOPS – Minimum Operational Performance Standards

Standards produced by RTCA that describe typical equipment applications and operational goals and establish the basis for required performance. Definitions and assumptions essential to proper understanding are included as well as installed equipment tests and operational performance characteristics for equipment installations. MOPS are often used by the FAA as a basis for certification.

Multilink

Concept that defines the use of concurrent, existing and future communication links between air and ground (e.g., AeroMACS, LDACS and Satcom), depending on the defined criteria (performance needs).

NAS – National Airspace System

One of the most complex aviation systems in the world that enables safe and expeditious air travel in the United States and over large portions of the world’s oceans.

Network

The Network function is decomposed into two main sub-functions; a router that routes data packets from a source to a destination and the communication manager, which is responsible for the network and link selections.

Network Layer

The Network Layer is based on Internet Protocol (IP) ensuring global routing over interconnected packet-switched communication networks.

ATTACHMENT 2
GLOSSARY

Physical and Link Layers

They are associated with the Sub-networks and handle the physical interface with the transmission medium (i.e., radio links).

PIESD – Passenger Information and Entertainment Services Domain

It is characterized by the need to provide passenger entertainment and network services. Beyond traditional IFE systems, it may also include passenger device connectivity systems, Passenger Flight Information Systems (PFIS), broadband television or connectivity systems.

SARPS – Standards and Recommended Practices

Produced by ICAO, they become the international standards for member states. As the name implies, they are only “recommended” practices. It is up to each member states to decide how/if to implement them.

Satcom – Satellite Communications

Communication service providing data, voice, and fax transmission via satellite. Allows aircraft to communicate in BLOS areas.

SESAR – Single European Sky ATM Research

European air traffic control infrastructure modernization program. SESAR aims at developing the new generation ATM system capable of ensuring the safety and fluidity of air transport worldwide over the next 30 years.

Sub-network

The sub-networks correspond to all radio systems that are used to communicate between the aircraft and the ground.

Transport Layer

The transport layer protocols are used to provide reliable or unreliable communication services over the ATN/IPS System. Those include TCP for reliable transport services and UDP that is used to provide best effort service.

VDL – VHF Data Link

Also known as VHF Digital Link, VDL is the LOS sub-network supporting data communications that are sent over VHF frequencies. The traditional VHF voice radio can be used in conjunction with a data modem to send data messages over VHF frequencies.

VDLM2 – VHF Data Link Mode 2

A datalink-only service designed to digitize VHF and improve the speed of the VHF link. VDLM2 is intended for use within the US and Europe as an interim datalink solution for enroute ATC functions. VDLM2 provides a 31.5 kbps channel rate.

APPENDIX A NOTIONAL ATN/IPS TIMELINES

A-1 ICAO Global Air Navigation Plan

The ICAO Global Air Navigation Plan (Doc. 9750) presents a strategic Aviation System Block Upgrade (ASBU) framework that facilitates harmonization of global ATM modernization objectives and operational improvements. The ASBU defines target implementation timelines organized in four six-year blocks. Block 0 represents technologies and capabilities implemented and deployed in many parts of the world today. Block 1 (2018) represents both existing and new technologies necessary to support operational improvements that are well understood through prior research, development, and trials/validation. Block 2 (2024) represents a natural progression of operational improvements from Block 1, with the potential need for further development and standardization. Block 3 (2030) represents an end-state as envisaged in the Global ATM Operational Concept.

Technology roadmaps complement the ASBU by providing timelines for the technologies that support Communications, Navigation and Surveillance (CNS), Information Management (IM), avionics and ground requirements. Figure A-1 illustrates the technology roadmap for air/ground datalink communications, which is relevant to ATN/IPS. Block 0 reflects the current datalink service implementations, e.g., FANS 1/A and Baseline 1, that leverage existing communication systems, e.g., VHF and VDLm2. In Blocks 1 and 2, ATS services continue to exploit existing technologies, and a key goal is harmonization of regional datalink implementations through implementation of next generation datalink service (Baseline 2). It is in these blocks that the ATN is expected to adapt to operate over new aeronautical broadband systems, such as AeroMACS and broadband Satcom. In Block 3, datalink will supplant voice for air/ground communications supporting routine and complex exchanges (e.g., full 4D trajectory based operations).

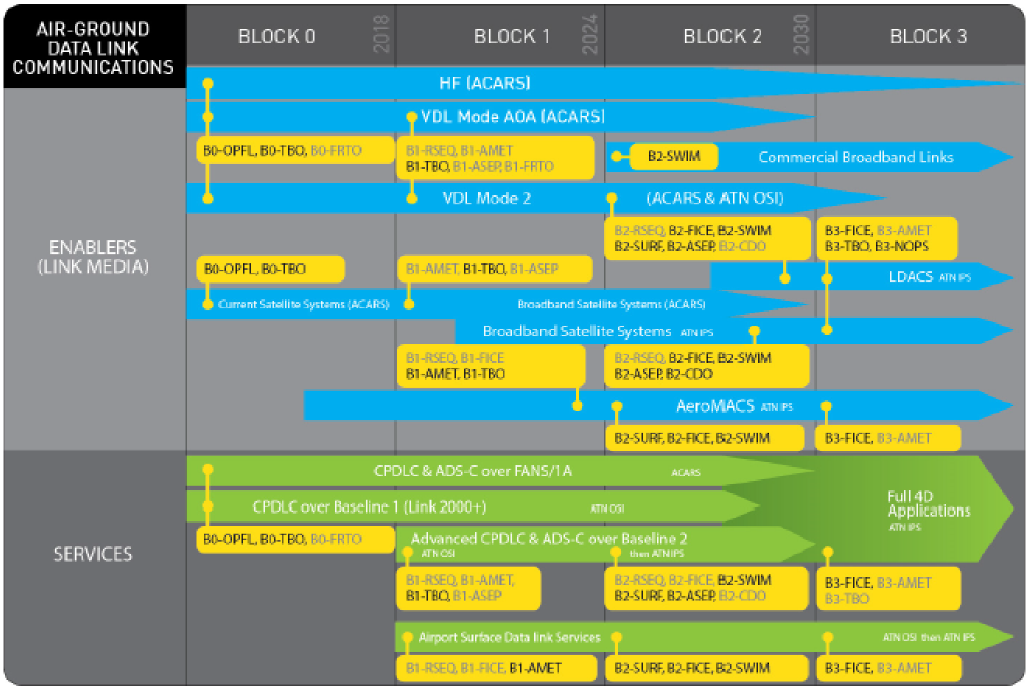


Figure A-1 – ICAO Technology Roadmap – Air/Ground Datalink Communications

A-2 EU and US Data Communications Harmonization Roadmaps

COMMENTARY

> The text in this section is adapted from ICAO Information Paper CP/2-IP/01, *EU and US A/G Data Communications Strategy*, 30 September 2016 (Rev.1) prepared and presented jointly by Eurocontrol and the FAA.

Beyond initial regional implementations and deployment of air/ground data communications capabilities, both the EU and the US recognize the benefits of addressing harmonization challenges identified previously in the *Eurocontrol-FAA Action Plan 17 Future Communication Study* (2007). Consequently, the SESAR Joint Undertaking (SJU) and the FAA are coordinating to develop a joint data communications strategy that focuses on areas where harmonization and interoperability between regions is required or desirable.

The strategy leverages existing EU and US roadmaps developed to achieve regional requirements and proposes a path for driving the regional roadmaps toward a more harmonized solution with respect to three principal elements: applications, networks and physical links. The strategy balances long, medium and short-term requirements with respect to current deployment plans, interoperability needs, and harmonization challenges/opportunities related the operational needs of data communications in the target trajectory based environment. While there are differences in the regional plans, the EU and US agree on a long-term harmonization strategy, which includes the Baseline 2B (B2B) application set and IPS network technology.

Figure A-2 provides the current, consolidated Air/Ground Data Communications Roadmap that represents the short, medium and longer term planned and ongoing developments and implementations in the EU and US with respect to applications, networks and physical link elements.

APPENDIX A
NOTIONAL ATN/IPS TIMELINES

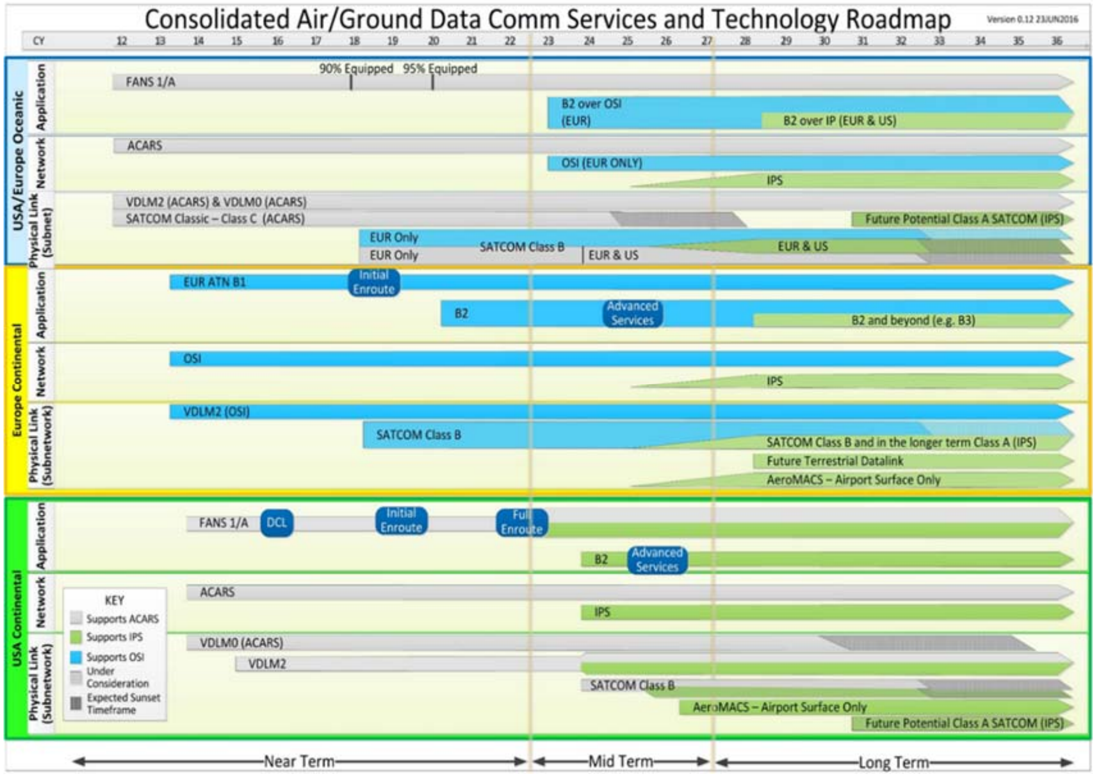


Figure A-2 – Consolidated US and Europe Air/Ground Data Communications Roadmap (dated 30 January 2017)

This consolidated roadmap is a work in progress, with identified challenges and opportunities that require further coordination in order to converge on the long-term target (B2B and IPS). The SJU and the FAA continue to develop the strategy and roadmap to achieve a harmonized approach that presents clear benefits and maximizes common equipage.

A-3 Airframe Manufacturer Roadmaps

A-3.1 Airbus Datalink Implementation Roadmap

The true benefits of ATN/IPS protocols will come in synchronization with the deployment of future wide scale air/ground Communication Systems (LDACS, Future Satcom), and with the development of future router equipment and architectures designed to take into account the future Required Communication Performance levels projected from the experience gained with the initial B2 deployments.

Before deployment of these services, the investment and costs linked to the development of an ATN/IPS protocol stack on aircraft (in particular to cope with the increasing need of data security containment measures) comes with no operational incentives to the airlines. While recognizing that ATN/IPS is based on state-of-the-art, proven, and widely deployed protocols for public commercial usage, using TCP/IP over VDLM2 for ATC communications would not bring any particular benefits from an operational standpoint. In addition, it would not resolve the difficulties currently observed in Europe with the VDLM2 link better than possible adjustments to current OSI protocols.

APPENDIX A
NOTIONAL ATN/IPS TIMELINES

In Europe, the ATN/OSI protocols defined in ICAO technical manuals support the first set of data link services covered by the Data Link Services Implementing Rule (DLS IR). It is currently envisaged that Europe will continue with ATN/OSI over VDLM2 for ATN B2 applications with possible adaptations and/or complements (e.g., ATN/OSI over Satcom), and consider ATN/IPS only for the next generation of data links (e.g., ATN B3). In other regions, datalink programs are based on FANS 1/A over ACARS without yet known established plans to deploy ATN/IPS for air/ground communications.

Given the envisioned datalink networks roadmap as shown on Figure A-3, Airbus' short-term priorities are to:

- Secure and improve VDLM2 infrastructure robustness to ensure simultaneous availability for ACARS and ATN/OSI, and
- Support deployment of alternatives to VDLM2 in order to secure sufficient bandwidth for ATC communications (e.g., AOC over IP, ATN/OSI over Satcom).

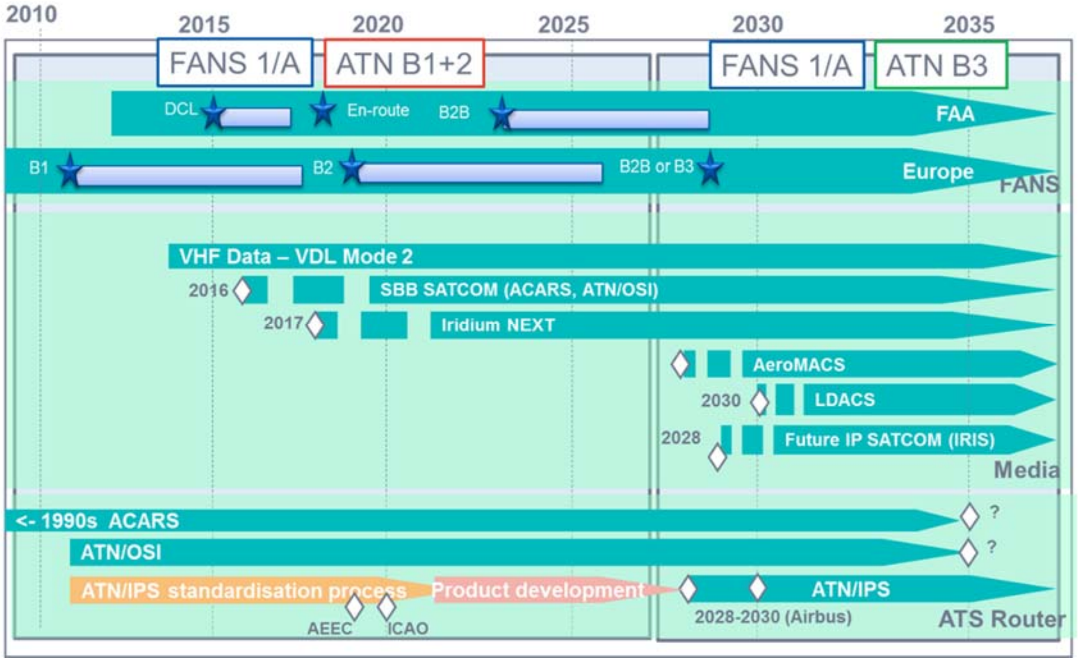


Figure A-3 – Airbus Datalink Implementation Roadmap

In practical terms, Airbus will participate in ATN B2 validation via SESAR Very Large scale Demonstrations with the FANS A+C product, which represents a single, integrated solution, for worldwide interoperability, including:

- FANS 1/A+ (ACARS)
- FANS B ATN B1 (ATN/OSI over VDLM2)
- FANS C ATN B2 (ATN/OSI over VDLM2)

This product also supports AOC traffic migration to non-safety IP links, ATN/OSI protocol simplification (e.g., air/ground IDRP inhibition), and provisions for a possible extension to ATN/OSI over Satcom.

Airbus assumes that the next upgrade steps regarding the evolution of the safety-related communication systems on aircraft and the transition to ATN/IPS will therefore progress along two main phases:

- A transitory phase, between 2018 and 2028, where the focus will be on:
  - Gaining experience and initial benefits of the deployment of B2 services,
  - Taking full benefit of existing and matured communication networks (ACARS and ATN/OSI),
  - Possibly taking advantage of new emerging communication means to experiment or extend FANS A and B2 services benefits in oceanic/remote airspaces (e.g., ACARS and possibly ATN/OSI over SBB or Iridium), and
  - Preparing for the transition to ATN/IPS and Future Communication Systems, with contributions from all stakeholders on the definition, trials, and validation of these new systems.
- Transition to ATN/IPS after 2028, where the introduction of ATN/IPS protocols on the aircraft is justified by the deployment of future IP-based communication systems (e.g., LDACS, future Satcom) and next generation ATS datalink services (e.g., ATN B3).

In order to support this roadmap, Airbus will support ATN/IPS standardization activities and participate in research and technology and validation initiatives through various projects such as SESAR 2020, Iris Service Evolution, and Clean Sky II.

A-3.2 Boeing Datalink Implementation Roadmap

The roadmap in Figure A-4 shows the current Boeing-envisaged roadmap for the introduction of ATN/IPS and supporting technologies related to the Airborne ATS Router. The roadmap includes three sections: Legacy Comm means, Future Comm means and Airborne ATS Router. The Legacy and Future Comm means sections represent subnetworks, and the Airborne ATS Router section represents network and transport layer technologies for the aircraft. Of course, the Airborne ATS Router also assumes availability of peer systems on the ground to support those technologies. Note that this diagram does not include the applications; that is a different, independent subject.

The diamonds represent significant milestones and associated milestone dates, which are notional target dates (for Boeing and the industry at large) for technology introduction. Additionally, schedule bars with a color gradient represent a continuum from a developmental period, shown in the lighter color, to a more mature, prolific implementation state, shown with the darker color.

APPENDIX A
NOTIONAL ATN/IPS TIMELINES

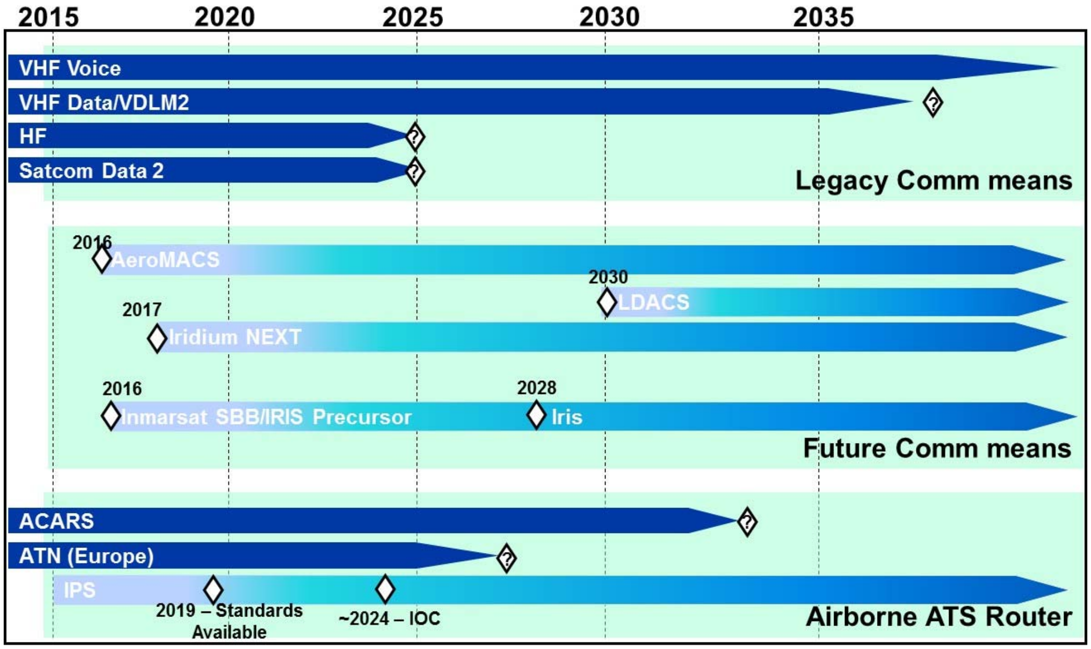


Figure A-4 – Boeing Datalink Implementation Roadmap

Boeing believes that the ATN/IPS standards should be available in the 2019-2020 timeframe, which should provide sufficient time to define many of the areas that are lacking maturity, and allowing an implementation target date of mid-2020’s. Accordingly, as ATN/IPS matures and implementations increase, other router technology implementations will start to decrease. Note that the depicted phase-out of ACARS and ATN is from the router perspective, not the application perspective, since ATN/IPS will include adaptation that provides application-level compatibility with existing ACARS and ATN applications. Legacy communication technologies will also eventually phase out, being replaced by the technologies shown under the Future Comm means section.

Finally, while the Future Comm means acknowledges Iris Precursor, Boeing prefers to move directly to ATN/IPS and skip this interim step, which Boeing believes would add additional cost and complexity for an as-of-yet unknown benefit. Moving directly to ATN/IPS will facilitate technology convergence, and speed the industry and ICAO goal of moving to IP-based technology for aviation safety services.

APPENDIX B AVIONICS ARCHITECTURES

This appendix was included to provide the reader with some background and insight of the various avionics architectures that are candidate for ATN/IPS services based on the timeframe of introduction.

Some ATS end systems may be integrated in the FMS. This architecture does not have any significant impact on the deployment of ATN/IPS services.

B-1 Avionics architectures – 2000'S

ARINC Specification 429: *Digital Information Transfer System (DITS)* defines the Air Transport Industry's standard for the transfer of digital data between avionics systems.

Legacy data comm architecture uses ARINC 429 interfaces between on-board functions.

In the existing mainline based on ARINC 429, as represented on Figure B-1B-1, the central element is the CMU/ATSU equipment, which includes the following functions:

- ACARS routing function,
- ATN/OSI routing function,
- Possibly ATS applications, including CPDLC,
- Hosted AOC applications.

Note: ATSU units are installed on Airbus Single Aisle and Long Range commercial aircrafts families (A32x and A330/340).

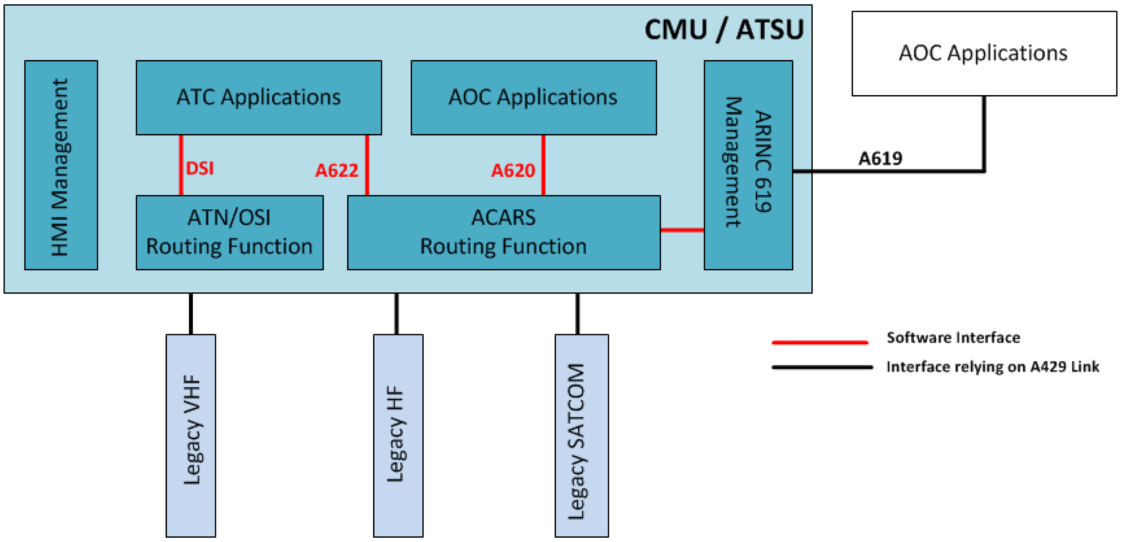


Figure B-1 – Current Architecture based on ARINC 429

All functions are implemented as software products hosted on CMU/ATSU equipment, based on ARINC 758 standard concept. Interfaces between functions are thus also software-based.

The ATSU has also the capability to provide ACARS communication to AOC applications located outside the ATSU, through an ARINC 619 interface supported by ARINC 429 data buses. This capability is for instance provided to the FMS AOC on existing Airbus aircraft.

ATS applications can be hosted in the CMU/ATSU equipment, but also outside (e.g.,FMS). Usually each ATS application is dedicated to one routing function (ACARS or ATN).

On Continental Airspace configurations, ATN B1 applications are connected to the ATN/OSI routing function, and optionally ARINC 623 applications (DCL, ATIS) are connected to the ACARS routing function.

On Remote or Oceanic Airspace configurations, FANS 1/A applications and optionally ARINC 623 applications (OCL, DCL, ATIS) are connected to the ACARS routing function.

Moreover, dual configurations are possible.

ARINC 429 data buses connect avionics equipment is installed on most commercial transport aircraft. However, ARINC 429 data buses are limited in bandwidth to 100 kbps.

B-2 Avionics Architectures – 2010'S

ARINC Specification 664 defines the network that establishes the architecture framework for IP-based aircraft. It contains a detailed implementation specification for the Ethernet physical layer. ARINC 664 also provides aeronautical profiles for IPv4 and an IP address allocation scheme using private IP address space.

ARINC 664 architectures are based on Integrated Modular Avionics (IMA) and rely on ARINC 664 network and switches defined in ARINC 664 Part 7.

The ARINC 664 standards defines a number of elements of a generic aircraft architecture which may support functions relying on an ARINC 664 Part 7 switched network, but also a domain based on "standard" ARINC 664 Ethernet network.

The ARINC 664 network starts from IP and Ethernet standards for defining a deterministic network which is certified for being used in the context of cockpit avionics functions.

The IMA equipment provides a hardware platform allowing safety-compliant sharing of hardware resources (CPU, Memory, network access) between several software functions hosted on the same IMA module.

The combination of these two technologies leads to building an architecture optimizing weight and volume by reducing the number of hardware modules in the cockpit avionics.

A sample of such architecture is shown below.

APPENDIX B
AVIONICS ARCHITECTURES

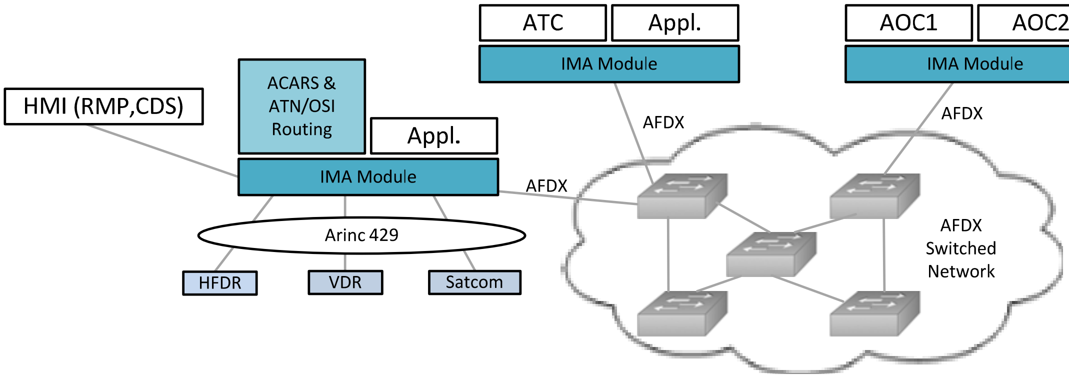


Figure B-2 – Current Architecture Based on ARINC 664 Part 7

The ACARS and ATN/OSI routing function (ACR) is a software element hosted on an IMA module. VDLM2 and Satcom systems use standardized interwiring. Several ARINC Standards apply.

The communications between applications using the datalink functions (i.e., the services provided by the ACARS and ATN/OSI router) rely on the ARINC 664 Part 7 switched network, thanks to the services provided by the IMA module.

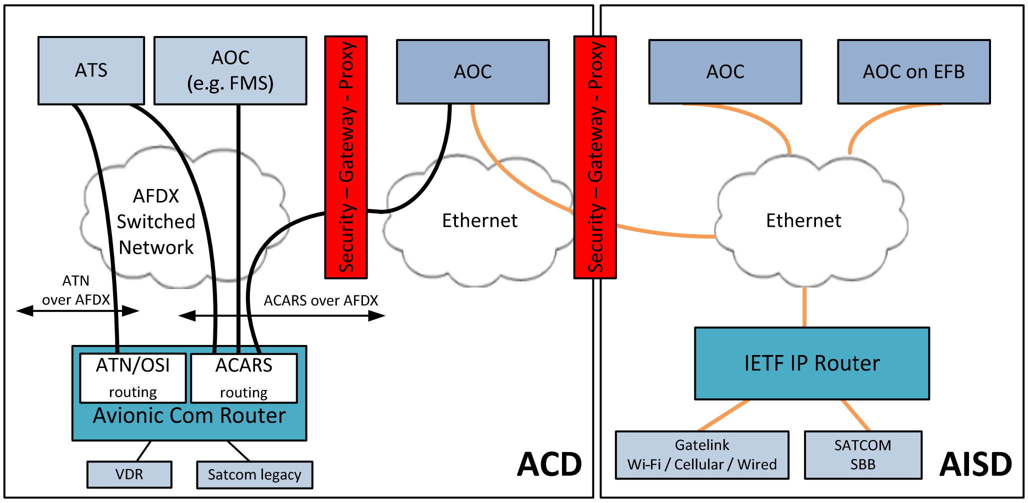


Figure B-3 – Example of ARINC 664 based architecture

The architecture is ARINC 664 compliant with security domains segregated one from another by security gateways controlling the information flows to prevent threats related to security attacks.

In Airbus implementations, the datalink communication functions are hosted as follows:

- Access network functions (e.g., VDLM2, Satcom, Gatelink) may be implemented in federated equipment connected via ARINC 429.
- The ACR (ATN, ACARS routing function) is implemented as a software function hosted on an IMA module.

- The ATC applications are implemented as software functions hosted on an IMA module

One important subject in this architecture is the security considerations. Namely, the architecture includes several levels of security equipment, especially on all data flows between airborne security domains.

APPENDIX C HIGH-LEVEL RISK ASSESSMENT AND SECURITY OBJECTIVES

C-1 Introduction

This appendix contains a *preliminary* risk assessment based on some anticipated ATN/IPS architectures that serves to highlight issues and considerations for security of both the airborne and ground segments for the ATN/IPS system. Taking security into account at the beginning of a design process is vastly preferable to doing so later in the process, since doing so can result in needing to make difficult or expensive changes to systems and processes that have already been developed (and even certified). The preliminary nature of this assessment therefore implies that a full and comprehensive risk assessment on the end-to-end IPS system will need to be done by the appropriate party when the system definition is completed. It should be anticipated that there will be an iterative process whereby design changes will be made in response to discovered vulnerabilities, until all identified risks have been sufficiently mitigated.

The risk assessment should be based on the airworthiness security process defined in the latest version of RTCA DO-326A and EUROCAE ED-202A, and referencing the guidance published in RTCA DO-356A / ED-203A (expected to be published by 2018). However, it should be noted that these documents are intended to apply only to airplanes and airborne systems, and that they will need to be tied to an appropriate risk assessment process for the ground side. NIST or ISO documents may be useful in this area. Further work is needed to define what the end-to-end assessment methodology will look like, since ATN/IPS is entering new territory in its use of open Internet Protocols for safety communications.

C-2 Security Scope Definition

As defined in RTCA DO-326A / EUROCAE ED-202A (Airworthiness Security Process Specification), the security scope of a system is defined by its security perimeter, data assets requiring protection, and the environmental external dependencies that contribute to the overall security of the system under analysis but are outside the perimeter of the system.

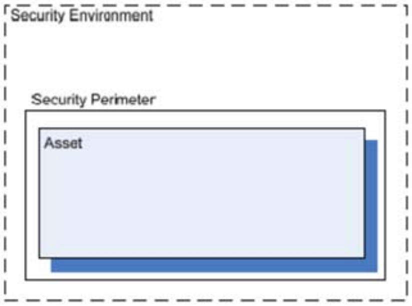


Figure C-1 – General Definition of the Security Scope

The assets are the logical and physical items that characterize the system well enough to identify all the potential targets of attack. It includes functions, data and resources that, if attacked, will cause an adverse effect on aircraft safety or operations.

The purpose of the security perimeter is to identify and trace points of entry to the assets (e.g., external network interfaces and data flows). The security perimeter does not bring functionalities by itself, and is not an asset. It contains the assets and is crossed by logical and physical interfaces, possible interactions, and information exchanges with external systems.

The external dependencies are the environmental elements, functions, systems, or processes that contribute to the overall security but are outside the perimeter of the system.

The security process defined in RTCA DO-326A / EUROCAE ED-202A is comprehensive and is intended to cover the end-to-end airplane design process from the airplane level down to the system and item levels.

This section focuses on the system level as shown in Figure C-1

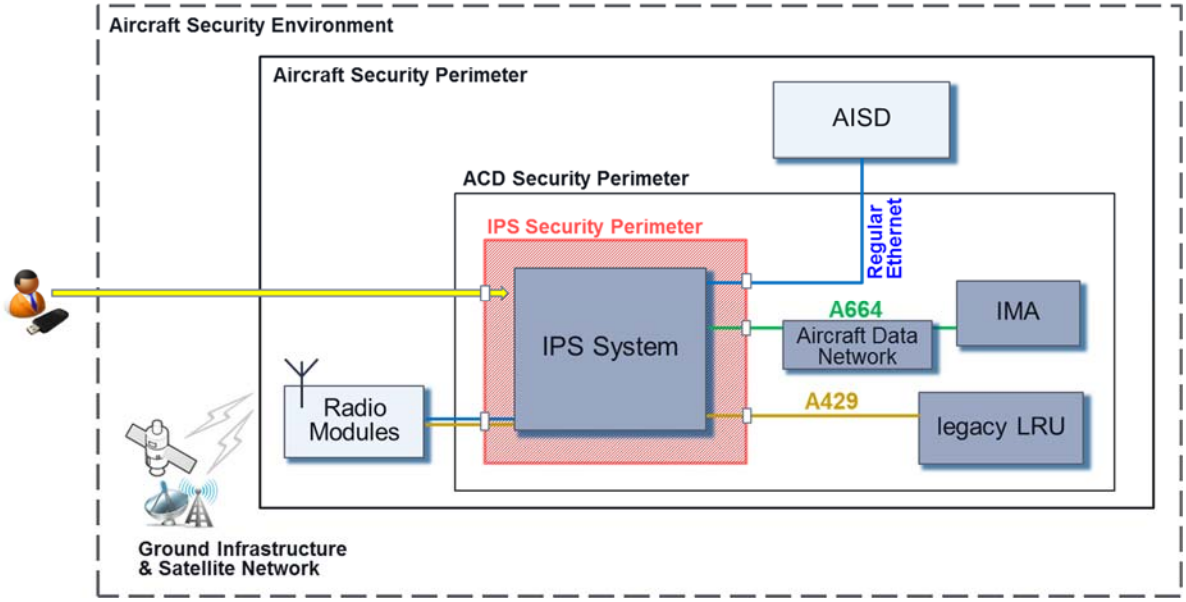


Figure C-2 – ATN/IPS System Security Scope

C-2.1 Interfaces

All interfaces on the ATN/IPS airborne system should be treated as part of the ATN/IPS security perimeter since they are potential points of entry for malicious attacks.

Possible network interfaces on ATN/IPS system are:

APPENDIX C
HIGH LEVEL RISK ASSESSMENT AND SECURITY OBJECTIVES

Table C-1 – ATN/IPS System Security Scope

		PHYSICAL INTERFACES				Aircraft Domain	Threat source	To be protected
		A664-P7	A429	Discrete	Regular Ethernet			
LOGICAL INTERFACES	ATS applications	x	x			ACD	No	Yes
	AOC safety applications	x	x			ACD	No	Yes
	Non-safety AOC applications (e.g., EFB)				x	AISD	Yes	No
	Aircraft Monitoring and Maintenance	x	x		x	ACD	No	Yes
	Other Aircraft Systems, if any	x	x			ACD	No	Yes
	Radios		x		x	External	Yes	No
	Ground					Ground	Yes	No
	Aircraft Environmental Data (e.g. ADIRS, WoW)	x	x	x		ACD	No	Yes
	Front-face (e.g., USB port)					External	Yes	No

C-2.2 Assets

A threat path is the way that an attacker might follow from an origin (the physical interface and logical connection where the attack starts) to the target.

The purpose of identifying the assets is to define all the potential targets of attack, so that the threats against them can be identified and mitigated.

Assets are physical (e.g. a LRU) or logical resources (e.g. software, data) of the ATN/IPS system under consideration. For logical assets, the dependencies on the implementing physical assets should be considered (see Section 3.2).

For purpose of this analysis, the assessment has been performed by focusing on the ATN/IPS capability managed by the ATN/IPS system on the airplane, but with the goal to highlight the end-to-end risk including the avionics systems directly connected to the ATN/IPS system:

1. Functional assets that are of:
   - Ground-ACD data flows using ATN/IPS communication means
   - Embedded applications supporting ATS or AOC safety
2. Connected avionics systems supporting the ATN/IPS system (e.g., Flight Warning, Maintenance, Dataloading)
3. Parts of the ATN/IPS system itself (see Section 3.0 introduction)

Ground systems are expected to implement security provisions independent of the airborne equipment. Ground systems are treated as external dependencies for purposes of aircraft certification.

C-2.3 External Dependencies

External dependencies are elements, functions, systems, or processes that contribute to the overall security of the ATN/IPS system but are outside the airborne ATN/IPS system perimeter. These include:

1. Access networks and ground stations of the Datalink Service Providers (Satcom safety, LDACS and AeroMACS)
2. Assuming that these infrastructures are trusted, ATN/IPS system should take advantage of ground activities put in place to ensure that the datalink service will be safely and securely delivered:
   - Regulatory approval of ground gateways (e.g., Inmarsat IP AeroRack or Iridium Gateway)
   - Trustworthiness of interfaces (e.g. secured channels with ATSP/ACSP)
   - Monitoring processes
3. Ground infrastructures and private networks of the Air Traffic Services Providers (ATSP) and Airline Operations Communication Service Providers (ACSP)
4. These major actors should adhere to aviation industry best practices for mission critical IT systems (e.g. NIST), and shall ensure by all needed means (e.g. vulnerability monitoring and management, procedures, user and administrative accounts, filtering) that:
   - No external threat can access to the equipment used to deliver ATS or AOC services
   - No internal threat can degrade the security level
5. Data loaders and portable maintenance terminals
6. Airlines and MROs should have processes in place to ensure that data loaders and maintenance terminals do not become infected with malware and are access-restricted to authorized and licensed maintenance personnel only.

C-3 Threat Conditions

To assess security risks induced by threat scenarios, the threat conditions must be identified.

A threat condition results when safety or operation of the aircraft is adversely affected due to a security failure on a specific asset (i.e., successful attack executed by a threat through the existence of vulnerabilities).

Two main threat conditions are identified for an ATN/IPS system:

1. **Loss of Integrity** through undetected corruption of ATN/IPS messages
2. A function is used in a legal but unintended manner (includes spoofing, man in the middle attacks). Possible consequences are lack of integrity of

information, misleading function, unexpected behavior of the equipment or function

3. **Loss of Availability** of ATS and/or AOC safety services

A function or data is temporarily or permanently not available (includes Denial of Service (DoS)).

C-4 Risk Assessment in ARINC 429 Avionics Architecture

This section provides a summary of the airborne risk assessment analysis conducted by Airbus (based on existing Airbus architectures), and consequent security objectives, including identification of security risk factors.

C-4.1 Threat Scenarios

Threat scenarios lay out all the elements necessary for an attack to be successful and cause an impact to aircraft safety or operation.

The two scenarios below are mapped to the threat conditions for ATN/IPS system. They include multiple attack vectors that map to the same threat condition:

Table C-2 – ATN/IPS Security

Group 1 Malevolent crafted ATN/IPS messages leading to coherent corruption	
Element	**Description**
Assets involved	• Ground-ACD dataflows either through: - Satcom - LDACS - AeroMACS • ATN/IPS system • ATSU (hosting or being connected to ATN and AOC applications) • Communication radio means • Other avionics systems connected to ATN/IPS system or ATSU
Threat condition that results from attack	Loss of integrity through malevolent ATN/IPS messages injected into systems (undetected corruption)
Vulnerabilities involved	Inadequate or insufficient technical and operational processes to prevent from ground impersonation
Potential attacks	An attacker sends especially crafted messages in order to take control of ATN/IPS system, ATSU or ATN/AOC applications either through: • ACSP/ATSP impersonation • DSP impersonation In case of ATN/IPS system or ATSU corrupted, attacker could launch additional attacks through avionics systems

Group 1 Malevolent crafted ATN/IPS messages leading to coherent corruption	
Element	**Description**
Security countermeasures intended to intervene	• Datalink service providers' networks and ground stations hardening • Secured ground ACSP/ATSP enclave and environment • Light Cockpit Satcom security functions • ATN/IPS system security functions • End-to-end security

Table C-3 – ATN/IPS Security

Group 2 Malevolent crafted ATN/IPS messages leading to loss of availability	
Element	**Description**
Assets involved	• Ground-ACD dataflows either through: - Satcom - LDACS - AeroMACS • ATN/IPS system • ATSU (hosting or being connected to ATN and AOC applications) • Communication radio means • Other avionics systems connected to ATN/IPS system or ATSU
Threat condition that results from attack	Denial of service through malevolent ATN/IPS messages injected into systems
Vulnerabilities involved	Inadequate or insufficient technical and operational processes to prevent from ground impersonation
Potential attacks	• An attacker sends especially crafted messages in order to inflict software crashes of ATN/IPS system, ATSU or ATN/AOC applications either through: - ACSP/ATSP impersonation - or DSP impersonation • An attacker sends an excessive number of messages in order to lead to a denial of service of ATN/IPS system, ATSU or ATN/AOC applications either through: - ACSP/ATSP impersonation - or DSP impersonation

Group 2 Malevolent crafted ATN/IPS messages leading to loss of availability	
Element	**Description**
Security countermeasures intended to intervene	• Datalink service providers' networks and ground stations hardening • Secured ground ACSP/ATSP enclave and environment • Light Cockpit Satcom security functions • ATN/IPS system security functions • End-to-end security

C-4.2 Security Objectives

At the output of the risk assessment, security objectives come in addition to general objectives detailed in Section 3.1.3.1.1 and help to define what is needed to counter the threat scenarios that have been identified as needing mitigation:

- Attempts to inject malevolent ATN/IPS messages should be prevented (unauthorized message modification, insertion, substitution and/or deletion);
- Attempts to flood or inflict a software crash to reduce availability of ATS and/or AOC safety services should be prevented.

These scenarios cannot be fully secured by security protections on-board the aircraft (described in Sections 3.1.3.3 and 3.1.3.4) since attack vectors cannot be addressed by the aircraft in isolation. Joint airborne and ground security protections are needed to mitigate security risks. In particular:

- Certification of ground gateways (e.g. Inmarsat IP AeroRack) at embedded standards level;
- Trustworthiness of interfaces between ACSP/ATSP and DSP through secure links;
- Use of air/ground secure links providing integrity, authentication and confidentiality (if needed);
- End-to-end secured exchanges at software application level (through cyphered communication over all "backbone" secure links) providing integrity, authentication and confidentiality.

Ground segment analysis should extend these threat scenarios identified at aircraft level to determine how these attacks could be mounted from the ground segment and determine the effectiveness of ground security measures in combatting these attacks.

C-5 Risk Assessment in ARINC 664 Avionics Architectures

An attacker-centric risk assessment evaluates risks in terms of the probability that an attacker (i.e., malicious threat actor) is able to successfully accomplish a given threat condition over a given time period. This type of assessment is utilized by RTCA DO-356 or ED-203.

A system-centric risk assessment evaluates risks in terms of the probability that a system provides the necessary robustness to prevent a given threat condition over a given time period.

A system-centric risk assessment utilizes the composition of the system (e.g. partitioning, assurance levels, layers of security) to evaluate specific risks.

This section provides a summary of the airborne risk assessment analysis conducted by Airbus (based on existing Airbus architectures), and consequent security objectives, including identification of security risk factors.

C-5.1 Threat Scenarios

Threat scenarios lay out all the elements necessary for an attack to be successful and cause an impact to aircraft safety or operation.

The two scenarios described in Section C-4.1 for ARINC 429 avionics architectures are also valid for ARINC 664 avionics architectures, and thus security objectives are applicable.

Nevertheless, due to avionics general ACD architecture, threats on the ARINC 664 network may have a significant impact and must be considered. As a consequence, two security barriers (or a simple device) shall be implemented to protect the ARINC 664 network.

C-5.2 Security Objectives

At the output of the risk assessment, security objectives come in addition to general objectives detailed in Section 3.1.3.1.1 and help to define what is needed to counter the threat scenarios that have been identified as needing mitigation:

- Security objectives similar to the ones identified for ARINC 429 architectures
- Any attempts to impair ARINC 664 network operation should be prevented through defense in depth best practices.

APPENDIX D STANDARDIZATION GAP ANALYSIS DATA

As noted in Section 5.3, industry stakeholders who participated in the development of this roadmap document conducted a detailed analysis to understand and assess ATN/IPS-related standardization activities. In particular, the analysis identified gaps where the industry stakeholders believe that a standard is required but an associated standardization activity is not yet identified. This appendix contains a snapshot-in-time of the spreadsheet used to capture the gap analysis input data.

COMMENTARY

> The reader is cautioned that the data contained in this appendix reflects an understanding of ATN/IPS standardization activities just prior to the completion of this document. This data is subject to change over time as standardization activities progress and evolve to meet the needs of the industry stakeholders. As part of its coordination activities (see Section 5.4.1.1.1), the AEEC IPS Subcommittee plans to monitor overall ATN/IPS standardization progress and update the working copy of the gap analysis spreadsheet, as appropriate.

The gap analysis spreadsheet contains three primary sections:

- Columns A and B – Work Area and Sub-work Area: These columns organize the standardization activities with respect to the ATN/IPS work areas identified in Sections 3 and 4 of this document.
- Columns C thru K – IPS-related Standardization Activities: These columns summarize the status of ATN/IPS standardization activities.
- Column L – Additional Comments: This column provides additional commentary, clarification, or observations offered by industry participants.

The following details are captured for each of the IPS-related Standardizations Activities:

- Column C – Work Type, which may take one of the following values:
    - STD – Standard or specification
    - GM – Guidance Material
    - ANA – Analysis
    - PRO – Prototype Implementation
    - VAL – Validation
    - OPR – Operational Standard or Guidance.
- Column D – Work Status, which may take one of the following values:
    - Complete
    - In-Progress
    - Planned
    - Proposed
    - *GAP*.
- Column E – The ARINC 658 section where potential actions to address an identified gap are described.

- Columns F and G – Standards Development Organization and the associated working group and sub-working group (optional) associated with the specified standardization activity.
- Column H – Description of the standardization activity (normal font, black text) OR a description of an identified gap (italicized font, red text).
- Column I – Artifact: A document number, if known, for the planned output of the standardization activity.
- Column J – Dependencies: Other activities on which the standardization activity may be dependent.
- Column K – Planned Completion Date, if known, when the output of the standardization activity is expected.

Note: The gap analysis spreadsheet is a draft input provided for formatting illustration. It will be replaced by the version that results as an output of the London IPS meeting and reviewed prior to adoption and publication of ARINC 658.

APPENDIX D
STANDARDIZATION GAP ANALYSIS DATA

A	B	C	E		F	G	H	I	J	K	L
		IPS-related Standardization Activities									
Work Area	**Sub-work Area**	**Work Type**	**Work Status**	**A658 Section where Gap is Addressed**	**Standards Organization**	**Working Group / Sub-group**	**Activity Description / *Gap Description***	**Artifact**	**Dependencies**	**Planned Completion Date (MMM-YYYY)**	**Additional Comments**
Application Interfaces	DSI (legacy)	**STD**	In-Progress		ICAO	PT-I	ATNPKT definition for backward compatibility with existing dialog service-based OSI applications	Doc. 9896	Doc. 9880	Nov-2020	Job Card: CP-DCIWG.006.01
		STD	***GAP***	**5.4.4**	ICAO	PT-I	*Mapping between OSI addresses and IPS address (see comment)* *Updates to DSI (?)*	Doc. 9896	Doc. 9896 (IPS addressing)		1. Consider multi-phased approach, where initial deployments use address mapping from OSI to IPS, but future deployments may be IPS addresses only. 2. May start in ICAO and move to RTCA/EUROCAE (SC-214/WG-78)
	ACARS (legacy)	**STD**	***GAP***	**5.4.4**	ICAO	PT-I	*Provisions for accommodation of FANS messages*	Doc. 9896			
		STD	***GAP***	**5.4.1.1**	AEEC	IPS	*Encapsulation of FANS (e.g., A618) for IPS (e.g., mapping of FANS to IPS DS), including what parts of the ACARS message are included (e.g., SMI)*	ARINC 758 ARINC 618 (?)	Doc. 9896 (above)		
		STD	***GAP***	**5.4.1.2.7**	AEEC	DLK	*Standardization of air-ground messaging layer for AOC (A620 non-safety) applications over IP (MIAM over IPS)*	ARINC 841			
	Native IP (future)	**STD**	***GAP***	**5.4.4**	ICAO	PT-I	*Support for native IP applications*	Doc. 9896			
Mobility	Access Network	**ANA**	In-Progress		ICAO	PT-I / MSG	Mobility sub-group to analyze Mobility options for the Access Sub-Networks (Terrestrial (VDL-2 and LDACS), AeroMACS, and Satellite) and protocols (e.g. PMIPv6, other)	Working Papers	AeroMACS, L-DACS, SATCOM, and VDL Standards		Note that intra-subnetwork mobility is not part of PT-I responsibility. PT-I may review what is offered by each subnetwork. Otherwise, this is out
	Inter-subnetwork	**ANA**	In-Progress		ICAO	PT-I / MSG	Mobility sub-group to analyze Multi-link mobility options (e.g.,MIPv6, AERO, LISP) and recommend a candidate	Working Papers	LISP - SESAR 15.2.4 AERO - IETF RFC		
		STD	Planned		ICAO	PT-I / MSG	Mobility technical provisions	Doc. 9896		Nov-2020	
	Inter-region	**STD**	Planned		ICAO	PT-I / MSG	Mobility technical provisions	Doc. 9896		Nov-2020	Job Card: CP-DCIWG.006.01
Upper Layers	Transport Options	**ANA**	In-Progress		ICAO	PT-I	Further refinement of transport options, whether UDP/TCP/etc. should both be supported, and including reliability extensions	Working Papers			
		STD	In-Progress		ICAO	PT-I	Document IPS transport provisions	Doc. 9896		Nov-2020	
	Supporting Services Identification	**STD**	In-Progress		ICAO	PT-I PT-I / MSG	Identify additional services necessary to support IPS, e.g. ICMP, local BGP, etc.	Doc. 9896		Nov-2020	
	Profile	**STD**	In-Progress		RTCA	SC-223	IPS profile	DO-TBD		Dec-2017	

APPENDIX D
STANDARDIZATION GAP ANALYSIS DATA

A	B	C	E		F	G	H	I	J	K	L
		IPS-related Standardization Activities									
Work Area	Sub-work Area	Work Type	Work Status	A658 Section where Gap is Addressed	Standards Organization	Working Group / Sub-group	Activity Description / *Gap Description*	Artifact	Dependencies	Planned Completion Date (MMM-YYYY)	Additional Comments
Lower Layer Interfaces	AeroMACS	STD	Complete		ICAO	PT-S	AeroMACS SARPS	Annex 10		Complete	
		STD	Complete		ICAO	PT-S	AeroMACS Technical Manual and Guidance	Doc. 10044		Complete	
		STD	Complete		RTCA	SC-223	AeroMACS Profile	DO-345		Complete	
		STD	Complete		RTCA	SC-223	AeroMACS MOPS	DO-346		Complete	
		STD	Complete		AEEC	AeroMACS	AeroMACS Transceiver and Installation	ARINC 766		Complete	
		STD	*GAP*	5.4.1.2.4	AEEC	AeroMACS	*AeroMACS architecture concepts (for segregation) to support IPS may not be defined adequately for developers*	ARINC 766			If dual connectivity with ACD and AISD is required in the radio.
	LDACS	STD	In-Progress		ICAO	PT-T	LDACS SARPS	Annex 10, Vol III		Dec-2018	Job Card: CP-DCIWG.010.01
		STD	In-Progress		ICAO	PT-T	LDACS Technical Manual	Doc. TBD		Dec-2018	Job Card: CP-DCIWG.010.01
		GM	Planned		ICAO	PT-T	LDACS Guidance Material	Doc. TBD		Dec-2022	Job Card: CP-DCIWG.010.01
		STD	Planned		EUROCAE	WG-82	Development of MOPS/MASPS	Doc. TBD			
		STD	*GAP*	5.4.1.2.5	AEEC	TBD	*LDACS transceiver and interfaces*	ARINC TBD			
	SATCOM (current) - Performance Class B	STD	Planned		ICAO	PT-T	Update SARPs (generic) and Technical Manual, including technology-specific parts (e.g., INMARSAT and Iridium)	Doc. 9925 (new part) Annex 10 Vol3 Ch4		TBD	
		STD	In-Progress		EUROCAE	WG-82	MOPS / MASPS updates for IPS	ED-TBD		Dec-2017	Dates to be confirmed
		STD	In-Progress		RTCA	SC-222	MOPS / MASPS updates for IPS	DO-262x / DO-343x		Dec-2017	Dates to be confirmed
		STD	In-Progress		AEEC	AGCS	MK3 Aviation SATCON Systems Form/Fit/Fn - additional work currently in progress to focus on ACARS (which may support accommodation)	ARINC 771 ARINC 781		TBD	
		STD	*GAP*	5.4.1.2.6	AEEC	AGCS	*Updates (as necessary) and architecture concepts to support IPS*	ARINC 771 ARINC 781			
	SATCOM (future) - Performance Class A	STD	Proposed		ICAO	PT-T	SATCOM Class A Technical Manual and Guidance and SARPS	Doc. TBD		TBD	Proposal presented by Eurocontrol during ICAO CP/2 in October 2016. Draft Job Card presented during ICAO CP/2 in WP02.
		STD	Planned		EUROCAE	WG-82	MOPS / MASPS updates for IPS	ED-TBD		TBD	
		STD	*GAP*	5.4.2	RTCA	SC-222	*Extension of current MOPS/MASPS to accommodate future SATCOM and IPS*	DO-TBD			
		STD	*GAP*	5.4.1.2.6	AEEC	AGCS	*Updates (as necessary) and architecture concepts to support IPS*	ARINC 771 ARINC 781			
	VDLm2	ANA	*GAP*	5.4.1.2.3	AEEC	Joint VDL Group	*Analysis of connectionless VDLm2, including e.g., reliability mechanisms, access network security, etc.*	Working Papers			
		STD	*GAP*	5.4.4	ICAO	PT-M (?)	*Updates for VDLm2 support of IPS, e.g., modifications to VDL Tech Manual to address connectionless VDLm2 exchange, and address IP packets in VDLm2.*	Doc. 9776			
		STD	*GAP*	5.4.2	RTCA	SC-214 / VDLSG	*Updates for VDLm2 support of IPS, e.g., modifications to VDL Tech Manual to address connectionless VDLm2 exchange, and address IP packets in VDLm2.*	DO-224C (MASPS) DO-218B (MOPS)			EUROCAE WG-92 (responsible for ED-92) meets jointly with RTCA SC-214 VDLSG.
		STD	*GAP*	5.4.2	EUROCAE	WG-92	*Updates for VDLm2 support of IPS, e.g., modifications to VDL Tech Manual to address connectionless VDLm2 exchange, and address IP packets in VDLm2.*	ED-92B (MOPS)			
		STD	In-Progress		AEEC	DLK	Updates for VDLm2 support of IPS, e.g., modifications to VDL Tech Manual to address connectionless VDLm2 exchange, and accommodate IP packets in VDLm2.	ARINC 631		Jun-2019	APIM 17-002

APPENDIX D
STANDARDIZATION GAP ANALYSIS DATA

A	B	C	E		F	G	H	I	J	K	L
		IPS-related Standardization Activities									
Work Area	Sub-work Area	Work Type	Work Status	A658 Section where Gap is Addressed	Standards Organization	Working Group / Sub-group	Activity Description / *Gap Description*	Artifact	Dependencies	Planned Completion Date (MMM-YYYY)	Additional Comments
Naming and Addressing	Naming	STD	Planned		ICAO	PT-I	Define naming convention and DNS requirements	Doc. 9896	Coordination with RTCA SC-223	Nov-2020	Job Card: CP-DCIWG.006.01
	Addressing	STD	Planned		ICAO	PT-I	Define addressing	Doc. 9896	Coordination with RTCA SC-224	Nov-2020	Job Card: CP-DCIWG.006.01
	IPv6 Transition Ph1	ANA	In-Progress		AEEC	NIS	Roadmap for IPv6 transition in aviation	ARINC TBD		Oct-2018	APIM 17-001
	IPv6 Transition Ph2	STD	Proposed		AEEC	NIS	Updates to standards for IPv6 transition as identified during the roadmap activity	ARINC 664pX(other parts and/or new part)			APIM 17-001 (proposed Phase 2)
	Administration	OPR	*GAP*	5.4.4	ICAO	PT-I (?)	*Processes for on-going administration of IP names and addresses* *IP database management/translations*				Boeing (Greg): Should ICAO take this, or would this be more of a NIS activity?
		OPR	*GAP*	5.4.5	OTHER	IATA	*Same as above but for AOC*				
Security	Architecture	GM	Planned		ICAO	PT-I & Sec. Panel		Doc. 9896	Doc. 10044	Nov-2020	Job Card: CP-DCIWG.007.01
	End-to-End - Dialogue Service	STD	Complete		ICAO	PT-I / SSG	Secure Dialog Service (SDS), end-to-end Dialogue Service application-layer security applicable to both OSI and IPS	Doc. 9880, Part IV-B		Complete	
		GM	In-Progress		ICAO	PT-I / SSG	Secure Dialog Service (SDS) guidance material			Dec-2017	
		VAL	In-Progress		FAA	WJHTC	SDS validation	Validation Report		Sep-2018	
	End-to-End - non-Dialog Service	STD	Proposed		TBD	TBD	Secure Session Service (SSS), end-to-end non-Dialogue Service application layer security (e.g. FANS, ACARS) using the ATN security protocol	Working Paper for PT-I/SSG	RTCA SC-223	TBD	
		VAL	Proposed		TBD	TBD	SSS validation			TBD	
	PKI	STD	Complete		ICAO	PT-S	AeroMACS PKI Certificate Policy, which includes certificate/CRL profiles. Expected to be reusable for SDS.	Doc. 10044	ATA Spec 42 WMF Certificate Profile & Certificate Policy	Complete	
		VAL	Complete		WMF	AWG	AeroMACS test certificates			Complete	
		STD	*GAP*	5.4.4	ICAO	PT-I / SSG	*Updates to current AeroMACS PKI CP to support IPS at large*	Doc. TBBD			
		GM	*GAP*	5.4.1.2.8	AEEC	NIS	*Key loading and key management necessary for LRU installation and maintenance (e.g., key replacement) -- updates necessary for IPS (all systems)*	ARINC 842			
	Network Layer Security	STD	In-Progress		ICAO	PT-I	*Definition of the security solution for the network level, including for AOC traffic (VPN)*				
	Aircraft Security Reliance on Ground Security	GM	In-Progress		EUROCAE	WG-72 (SC-216)					
		GM	*GAP*	5.2 ?	OTHER	ARAC (?)	*Address this topic and provide recommendations to FAA/EASA*				
		GM	*GAP*	5.2	FAA		*FAA/EASA regulation update or new process??* *Impact on certification if aircraft has reliance on the ground*				
		GM	*GAP*	5.2 ?	EASA		*FAA/EASA regulation update or new process??* *Impact on certification if aircraft has reliance on the ground*				
	Security Management	STD	*GAP*	5.4.2	OTHER	RTCA / EUROCAE	*Overall security processes regarding incident management, logging/analysis, Aviation ISAC, etc.*				
	Security Policy	STD	Planned		ICAO	PT-I / SSG	ICAO Overall Security Policy Requirements	Doc. TBD		TBD	Job Card: CP-DCIWG.007.01

APPENDIX D
STANDARDIZATION GAP ANALYSIS DATA

A	B	C	E		F	G	H	I	J	K	L
		IPS-related Standardization Activities									
Work Area	**Sub-work Area**	**Work Type**	**Work Status**	**A658 Section where Gap is Addressed**	**Standards Organization**	**Working Group / Sub-group**	**Activity Description / *Gap Description***	**Artifact**	**Dependencies**	**Planned Completion Date (MMM-YYYY)**	**Additional Comments**
Performance	QoS	**STD**	Planned		ICAO	PT-I / MSG	Map ATN QoS to IPS DIFFSERV	Doc. 9896	Doc. 9880 Doc. 10044	Nov-2020	RC (Stephane): Should be defined as a end-to-end mechanism by ICAO and/or in RTCA/EUROCAE profiles
		STD	***GAP***	**5.4.1.1**	AEEC	IPS	*Detailed QoS mechanisms for segregating ATS and AOC traffic (part of ATN/IPS router form factor / architecture??)*				
	Compression	**ANA**	***GAP***	**5.4.1.1**	AEEC	IPS	*Compression need analysis;* *Standardization of proposed compression techniques*				
	RCP (B2)	**STD**	**Complete**		RTCA	SC-214 (WG-78)	SPR	DO-350A DO-306			
	RCP (Beyond B2)	**STD**	***GAP***	**5.4.3**	RTCA	SC-214 (WG-78)	*SPR update for beyond-B2 services*				
	Multi-link	**STD**	Planned		ICAO	PT-I / MSG	Multi-link technical provisions	Doc. 9896	SESAR 15.2.4	Nov-2020	Boeing (Greg): AEEC IPS coordination required
		STD	***GAP***	**5.4.1.1**	AEEC	IPS	*Detailed definition of multi-link based on ICAO definition.*		Doc. 9896		RC (Stephane): The CMU standard would need to refer to the IPS router standard for the specification of the multilink functional specification. (I.e., The CMU is one instance of an IPS router.)
	MASPS	**STD**	***GAP***	**5.4.3**	EUROCAE	TBD	*IPS MASPS*	ED-TBD			
	MOPS	**STD**	Planned		RTCA	SC-223	IPS MOPS	DO-TBD		Dec-2019	Concerns raised by IPS participants regarding the need for an IPS MOPS - further discussion required.
Form / Fit / Interfaces	CMU	**STD**	***GAP***	**5.4.1.2.2**	AEEC	DLK	*CMU specification updates to support IPS (e.g., including segregation, new interfaces, data logging, traffic shaping/filtering, etc.)*	ARINC 758			
	IPS Router	**STD**	***GAP***	**5.4.1.1**	AEEC	IPS	*Specification for an IPS-specific router or router function (e.g., including segregation, new interfaces, etc.)*	ARINC TBD			
Ground Systems	OSI/IPS Gateway	**GM**	***GAP***	**5.4.4**	ICAO	PT-I	*Technical definition of what needs to maintained between OSI and IPS in order to maintain application correlation.* *(Ground requirements RTCA/EUROCAE involvement?)*				
	ACARS/IPS Gateway	**STD**	***GAP***	**5.4.1.1**	AEEC	IPS	*Definition of ACARS-IPS gateway function*	ARINC 620			
	IPS NW Topology	**GM**	***GAP***	**5.4.5**	OTHER	Regional CAAs	*Regional implementation of IPS based on the ICAO standard*				