ARINC PROJECT PAPER 858 PART 1
TABLE OF CONTENTS

ARINC PROJECT PAPER 858 PART 1
TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 Purpose

Airlines and other users of the airspace rely on safe, secure, and reliable data communication services to meet their day-to-day operational needs. Air Navigation Service Providers (ANSPs) and Communication Service Providers (CSPs) must deliver these services globally and meet internationally recognized standards for communications performance.

The International Civil Aviation Organization (ICAO) Global Air Navigation Plan (GANP) and the European Union (EU) and United States (US) Air/Ground Data Communications Strategy identify a globally harmonized target aviation communications environment that includes a communication infrastructure based on selected commercial Internet Protocol (IP) standards. ICAO refers to this aviation communication network as the Aeronautical Telecommunication Network using the Internet Protocol Suite (ATN/IPS[1]). The ATN/IPS network will be implemented onboard an aircraft and in ground infrastructure to support safety-related services, including Air Traffic Services (ATS) and Aeronautical Operational Control (AOC). The ATN/IPS network infrastructure is considered the successor to the Airline Communications Addressing and Reporting System (ACARS) and to the ICAO-defined network infrastructure based on the Open Systems Interconnection (OSI) model, referred to as ATN/OSI.

The AEEC developed the ATN/IPS avionics standard in two steps. The first step analyzed and captured high-level user requirements in an ATN/IPS roadmap focusing on the airline user, and where possible, the requirements of ground users such as ANSPs. The roadmap defined the perimeter of the avionics standards for ATN/IPS, and it provided general ATN/IPS standardization work recommendations, which served as valuable input for coordination with other standards development organizations including ICAO, EUROCAE, and RTCA.

This document represents the second step of the process, which is the execution of the recommendations for development of an ARINC Standard for the airborne component of the ATN/IPS. The AEEC coordinated the development of this avionics standard with ICAO, EUROCAE, and RTCA to identify interdependencies and ensure consistency among the ATN/IPS-related industry standards developed by these organizations.

1.2 Scope

This document serves as an ARINC Standard to define the IPS avionics architecture, functions, and interfaces, and to describe implementation options and constraints as well as high level details regarding the accommodation of different applications. The Airborne IPS System described in this standard may be hosted in a Communications Management Unit (CMU) or other equivalent avionics that provides the IPS network stack and air-ground routing functionality. This includes, as necessary, other systems that interface and interoperate with the CMU or equivalent function.

---

[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”.

1.0 INTRODUCTION

This document also describes the end-to-end context of ATN/IPS, as it is recognized that some of the requirements that are levied on the aircraft also impose similar requirements on the peer ground entities. This considers the various aspects of the potential ground entities, including deployment options and architectures, IPS coexistence with other protocol stacks, security, and other aspects. Therefore, ground requirements and considerations are also captured in this document. Figure 1-1 illustrates the ATN/IPS near-term context showing the overlay of IPS Gateways in the current communications environment where IPS-enabled aircraft and existing aircraft co-exist with combinations of existing and IPS-enabled ground systems.

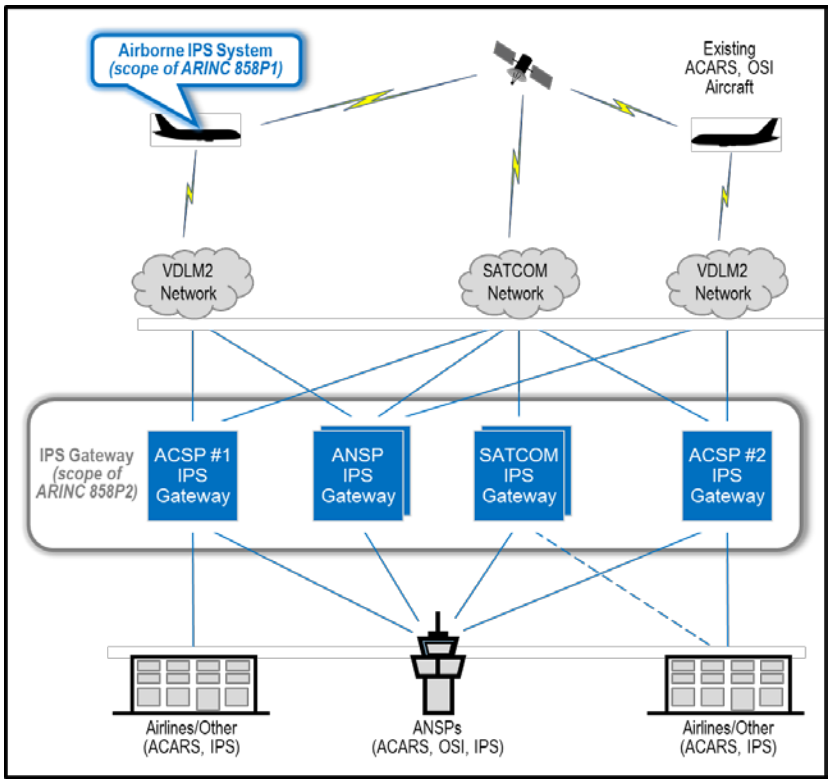

Figure 1-1 – IPS Gateways Overlaid on Current Environment

Note that this figure does not intend to illustrate the various ground administrative domains, but rather it is intended to show flexibility to accommodate various IPS Gateway deployment options, e.g., placement at an Air-Ground Communication Service Provider (ACSP) access network, at an ANSP, etc.

The intent of this document, in coordination with other related industry standards, is to provide implementers of the Airborne IPS System with the level of detail necessary to interface with other aircraft systems and to interoperate securely with Ground IPS Systems.

1.3 Document Overview

1.3.1 Multi-Part Specification Organization

ARINC 858 is published as a multi-part document specification that includes the following documents:

- Part 1 (*this document*) – Airborne IPS System Technical Requirements
- Part 2 – IPS Gateway Air-Ground Interoperability

1.3.2 Part 1 Document Organization

This document is organized as follows:

- Section 1.0 – Introduction

  This section introduces the purpose and scope of this document, identifies related reference documents, and provides guidance for regulatory and export control compliance.
- Section 2.0 – Overall IPS System Architecture

  This section sets the context for specification of the Airborne IPS System by providing an overview of the overall IPS System, including the end-to-end architecture, IPS functions and protocols, deployment and transition considerations, and assumptions and constraints.
- Section 3.0 – Airborne IPS System Architecture

  This section specifies the Airborne IPS System, including Core IPS functions, Application and Datalink Adaptation functions, Non-Core IPS functions, interfaces internal and external to the Airborne IPS System, and performance requirements.
- Section 4.0 – Airborne IPS System Security

  This section specifies the Airborne IPS System security, including security architecture, security mechanisms, security support functions such as key management and security event logging, and security design and implementation guidance.
- Section 5.0 – Airborne IPS System Implementation Options

  This section provides example implementations of the Airborne IPS System in federated and integrated architectures, interface and redundancy considerations, guidance for dual-stack (i.e., ACARS and IPS) implementations, and host versus router considerations.
- Section 6.0 – Airborne Application Data Considerations

  This section presents an overview of accommodation and interoperability considerations for existing and future safety services applications when leveraging IPS networking.
- Attachment 1 – List of Acronyms

  This attachment provides a list of acronyms used in this document.
- Attachment 2 – Glossary

  This attachment explains the precise meaning of terms used in this document to avoid ambiguity and confusion.

- Attachment 3 – ACARS to IPS DS Convergence Function (AICF)

  This attachment specifies the AICF, which adapts ACARS-based applications to the IPS Dialogue Service (IPS DS).
- Attachment 4 – IPS Security Event Log Format

  This attachment specifies the format of security event logs that are generated by the Airborne IPS System.
- Appendix A – ATNPKT Message Format Examples

  This appendix presents examples of the ATNPKT message format specified in ICAO Doc. 9896 for various dialogue service primitives.
- Appendix B – IPS Protocol Build-up

  This appendix provides a top-level overview of the IPS protocol build-up from one stack layer to another.

To assist readers with navigating this document, the following figure is an illustrative guide to the document sections and the relationships among the sections.

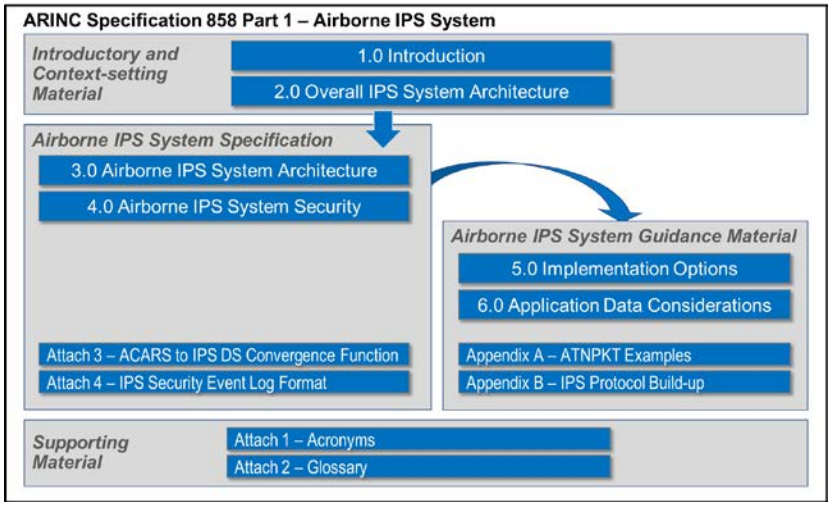

Figure 1-2 – Guide to ARINC Specification 858 Part 1

1.4 Related Documents

ATN/IPS as a whole represents a broad range of functions and components. These necessarily span many different standards development organizations (SDOs). Figure 1-3 illustrates high-level, exemplar relationships between ARINC 858 and ICAO standards, RTCA/EUROCAE standards, and other ARINC Standards produced by the AEEC. At a high level, the top row of standards make use of underlying IPS services, with adaptation provided by IPS as necessary so that existing interfaces are not impacted. The bottom row of standards represents functions to which the IPS service interfaces or uses; note that updates to these existing standards may be required to accommodate IPS-specific functions or interfaces. The ICAO and RTCA/EUROCAE standards on the same level as

1.0 INTRODUCTION

ARINC 858 define the global interoperability requirements necessary for IPS to support aeronautical safety services.

COMMENTARY

The Ku and Ka band Satcom standards are shown with a dashed line since these links do not operate in protected spectrum and are not approved for safety services communications. However, to facilitate commonality, interactions with these standards may still be of interest.

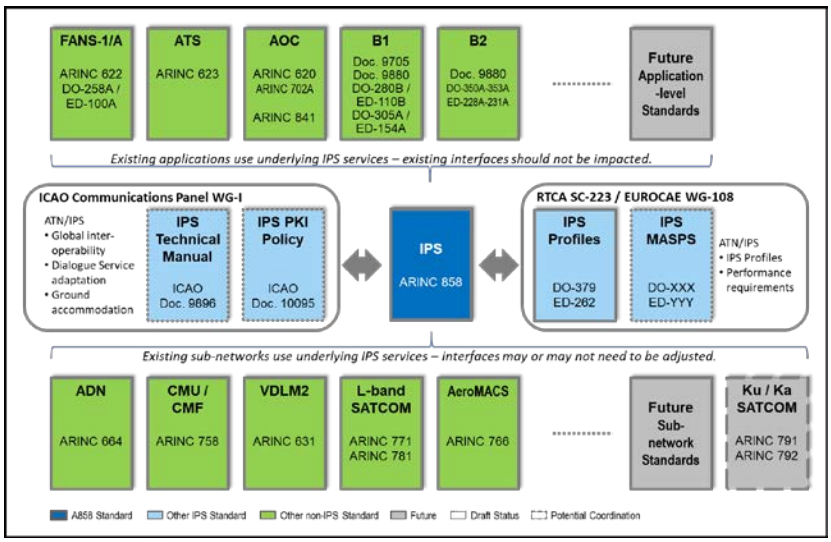

Figure 1-3 – Standards Relationships to ARINC 858

1.4.1 Relationship of this Document to Other ARINC Standards

ARINC Standards related to this specification are listed below. When avionics systems and subsystems are designed to use the capabilities provided by this specification, they should incorporate the provisions of this specification by reference. References to this specification should assume the application of the most recent version.

ARINC Specification 429: *Digital Information Transfer System (DITS)*

ARINC Specification 618: *Air/Ground Character-Oriented Protocol Specification*

ARINC Specification 619: ACARS Protocols for Avionic End Systems

ARINC Specification 620: *Datalink Ground Systems Standard and Interface Design Specification (DGSS/IS)*

ARINC Specification 622: *ATS Data Link Applications over ACARS Air-Ground Network*

ARINC Specification 623: *Character-Oriented Air Traffic Service (ATS) Applications*

ARINC Specification 631: *VHF Digital Link (VDL) Mode 2 Implementation Provisions*

ARINC Specification 653: Avionics Application Software Standard Interface

ARINC Report 658: *Internet Protocol Suite (IPS) for Aeronautical Safety Services Roadmap Document*

ARINC Specification 664: *Aircraft Data Network*

ARINC Report 665: *Loadable Software Standards*

ARINC Characteristic 702A: *Advanced Flight Management Computer System*

ARINC Characteristic 750: *VHF Data Radio*

ARINC Characteristic 758: *Communications Management Unit (CMU) Mark 2*

ARINC Characteristic 766: *Aeronautical Mobile Airport Communication System (AeroMACS) Transceiver and Aircraft Installation Standards*

ARINC Characteristic 771: *Low-Earth orbiting Aviation Satellite Communication System*

ARINC Characteristic 781: *Mark 3 Aviation Satellite Communication System*

ARINC Characteristic 791: *Mark I Aviation Ku-band and Ka-band Satellite Communication System*

ARINC Characteristic 792: *Second-Generation Ku-band and Ka-band Satellite Communication System*

ARINC Report 827: *Electronic Distribution of Software by Craft (EDS Crate)*

ARINC Report 835: *Guidance for Security of Loadable Software Parts Using Digital Signatures*

ARINC Specification 841: *Media Independent Aircraft Messaging (MIAM)*

ARINC Specification 858: *Internet Protocol Suite (IPS) for Aeronautical Safety Services, Part 2, IPS Gateway Air-Ground Interoperability*

1.4.2 Relationship to Other Industry Standards

The following list identifies related industry documentation referenced in this document.

Air Transport Association (ATA)

- **ATA Spec 42:** *Aviation Industry Standards for Digital Information Security, Version 2020.1*

EUROCAE

- **ED-100A:** *Interoperability Requirements Standard for ATS Applications Using ARINC 622 Data Communications.* Also published as RTCA DO-258A.
- **ED-110B:** Interoperability Requirements Standard for Aeronautical Telecommunication Network Baseline 1 (Interop ATN B1). Also published as RTCA DO-280B.

- **ED-120:** *Safety and Performance Requirements Standard for Initial Air Traffic Data Link Services in Continental Airspace.* Also published as RTCA DO-290.
- **ED-122:** *Safety and Performance Standard for Air Traffic Data Link Services in Oceanic and Remote Airspace (Oceanic SPR Standard)*. Also published as RTCA DO-306.
- **ED-154A:** *Future Air Navigation System 1/A – Aeronautical Telecommunication Network Interoperability Standard (FANS 1/A – ATN B1 Interop Standard)*. Also published as RTCA DO-305A.
- **ED-202A:** *Airworthiness Security Process Specification*. Also published as RTCA DO-326A.
- **ED-203A**: Airworthiness Security Methods and Considerations. Also published as RTCA DO-356A.
- **ED-228A:** *Safety and Performance Requirements Standard for Baseline 2 ATS Data Communications (Baseline 2 SPR Standard).* Also published as RTCA DO-350A.
- **ED-229A:** *Interoperability Requirements Standard for Baseline 2 ATS Data Communications (Baseline 2 Interop Standard).* Also published as RTCA DO-351A.
- **ED-231A:** *Interoperability Requirements Standard for Baseline 2 ATS Data Communications, ATN Baseline 1 Accommodation (ATN Baseline 1 - Baseline 2 Interop Standard)*. Also published as RTCA DO-353A.
- **ED-262:** *Aviation Profiles for Internet Protocol Suite.* Also published as RTCA DO-379.

  Note: The following EUROCAE document is in draft status as of the time of this writing. Availability of a mature document and assigned document number are expected coincident with Supplement 1 of this document.

- **ED-YYY:** *Minimum Aviation System Performance Standard (MASPS) for the Internet Protocol Suite used in Aviation Air-Ground Communication Systems*. Also published as RTCA DO-XXX.

International Civil Aviation Organization (ICAO)

- **ICAO Doc. 8585:** *Designators for Aircraft Operating Agencies, Aeronautical Authorities and Services*
- **ICAO Doc. 9705-AN/956:** *Manual of Technical Provisions for the Aeronautical Telecommunications Network*

  Note: ICAO Doc. 9705 has been superseded by ICAO Doc. 9880. Although ICAO Doc. 9880 serves as the primary reference, existing implementations may still reference the predecessor ICAO Doc. 9705 document.

- **ICAO Doc. 9750-AN/963:** The Global Air Navigation Plan
- **ICAO Doc. 9776-AN/970:** *Manual on VHF Digital Link (VDL) Mode 2*
- **ICAO Doc. 9880-AN/466:** *Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using the ISO/OSI Standards and Protocols*

Commented [OML1]: **Ed. Note**: New clarifying note added, driven by a COL comment regarding Figure 1-3.

- **ICAO Doc. 10037-AN/509:** Global Operational Data Link (GOLD) Manual
- **ICAO Doc. 10044**: *Manual on the Aeronautical Mobile Airport Communications System (AeroMACS)*

  Note: The following ICAO documents are in draft status as of the time of this writing. Availability of mature documents is expected coincident with Supplement 1 of this document.
- **ICAO Annex 10, Volume III:** *Aeronautical Telecommunications – Communication Systems*
- **ICAO Doc. 9896:** *Manual for the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocols*
- **ICAO Doc. 10145:** Security Risk Assessment for Aeronautical Communications
- **ICAO Doc. 10095**: *Manual of Public Key Infrastructure (PKI) Policy for Aeronautical Communications*

International Organization for Standardization and International Electro-technical Commission (ISO/IEC)

- **ISO/IEC 7498-1:** *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model – Part 1*. Also published as ITU-T Recommendation X.200.
- **ISO/IEC 8824-1:** *Information Technology – Abstract Syntax Notation One (ASN.1): Specification of Basic Notation*. Also published as ITU-T Recommendation X.680.
- **ISO/IEC 8825-1:** *Information Technology – ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*. Also published as ITU-T Recommendation X.690.
- **ISO/IEC 9594-8:** Information Technology – *Open Systems Interconnection – The Directory: Authentication Framework.* Also published as ITU-T Recommendation X.509.
- **ISO/IEC 19790:2012(E):** *Information Technology – Security Techniques – Security Requirements for Cryptographic Modules*

International Telecommunications Union (ITU)

- **ITU-T Recommendation S.2:** *Telegraphy – Alphabetical Telegraph Terminal Equipment – Coding Scheme using the International Telegraph Alphabet No. 2 (ITA2) to allow the Transmission of Capital and Small Letters*
- **ITU-T Recommendation X.200:** *Information technology – Open Systems Interconnection –Basic Reference Model: The Basic Model*. Also published as ISO/IEC 7498-1.
- **ITU-T Recommendation X.509:** *Information Technology – Open Systems Interconnection – The Directory: Authentication Framework*. Also published as ISO/IEC 9594-8.
- **ITU-T Recommendation X.680:** Information Technology – *Abstract Syntax Notation One (ASN.1): Specification of Basic Notation*. Also published as ISO/IEC 8824-1.

- **ITU-T Recommendation X.690:** *Information Technology – ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*. Also published as ISO/IEC 8825-1.

Internet Engineering Task Force (IETF)

Note: Rather than referencing all IETF Request For Comments (RFCs) directly, this document refers to EUROCAE ED-262 and RTCA DO-379, Internet Protocol Suite Profiles, which reference IETF RFCs relevant to specification of the IPS network stack. This approach minimizes changes to this document as IETF RFCs evolve over time.

- **RFC 2516:** *A Method for Transmitting PPP over Ethernet (PPPoE)*
- **RFC 3339:** *Date and Time on the Internet: Timestamps*
- **RFC 5424:** *The Syslog Protocol*
- **RFC 6012:** *Datagram Transport Layer Security (DTLS) Transport Mapping for Syslog*
- **RFC 7030:** *Enrollment over Secure Transport*
- **RFC 8446:** *The Transport Layer Security (TLS) Protocol Version 1.3*

RTCA

- **DO-258A:** *Interoperability Requirements Standard for ATS Applications Using ARINC 622 Data Communications*. Also published as EUROCAE ED-100A.
- **DO-280B:** *Interoperability Requirements Standard for Aeronautical Telecommunication Network Baseline 1 (Interop ATN B1)*. Also published as EUROCAE ED-110B.
- **DO-290:** *Safety and Performance Requirements Standard for Initial Air Traffic Data Link Services in Continental Airspace*. Also published as EUROCAE ED-120.
- **DO-306:** *Safety and Performance Standard for Air Traffic Data Link Services in Oceanic and Remote Airspace (Oceanic SPR Standard)*. Also published as EUROCAE ED-122.
- **DO-326A:** *Airworthiness Security Process Specification*. Also published as EUROCAE ED-202A.
- **DO-350A:** *Safety and Performance Requirements Standard for Baseline 2 ATS Data Communications (Baseline 2 SPR Standard)*. Also published as EUROCAE ED-228A.
- **DO-351A:** *Interoperability Requirements Standard for Baseline 2 ATS Data Communications (Baseline 2 Interop Standard).* Also published as EUROCAE ED-229A.
- **DO-353A:** *Interoperability Requirements Standard for Baseline 2 ATS Data Communications, ATN Baseline 1 Accommodation (ATN Baseline 1 - Baseline 2 Interop Standard)*. Also published as EUROCAE ED-231A.
- **DO-356A**: Airworthiness Security Methods and Considerations. Also published as EUROCAE ED-203A.

- **DO-379:** *Aviation Profiles for Internet Protocol Suite*. Also published as EUROCAE ED-262.

  Note: The following RTCA document is in draft status as of the time of this writing. Availability of a mature document and assigned document number are expected coincident with Supplement 1 of this document.

- **DO-XXX:** *Minimum Aviation System Performance Standard (MASPS) for the Internet Protocol Suite used in Aviation Air-Ground Communication Systems*. Also published as EUROCAE ED-YYY.

Single European Sky Air Traffic Management Research Joint Undertaking (SESAR JU)

- *European Union and United States Air/Ground Data Communications Strategy, Version 3.00, 7 November 2017*. Published jointly with the US FAA.

US Federal Aviation Administration (FAA)

- *European Union and United States Air/Ground Data Communications Strategy, Version 3.00, 7 November 2017*. Published jointly with the European SESAR Joint Undertaking.

US National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS)

- **FIPS 140-3**: *Information Security – Cryptography – Security Requirements for Cryptographic Modules*

Commented [OML2]: Ed. Note: Changed reference from 140-2 to 140-3 since:
- 9/22/19 – 140-3 effective
- 9/22/20 – 140-3 testing begins
- 9/22/21 – no further 140-2 submissions allowed

Still aligned with ISO/IEC 19790:2012(E).

1.5 Regulatory Approval

This standard, in and of itself, will not ensure regulatory approval. Implementers are urged to obtain all information necessary for regulatory approval and work in close coordination with the appropriate regulatory authorities to gain certification as applicable.

1.6 Export Control Compliance

National and international laws regulate the export of products (e.g., systems, software, and technology) containing cryptography. These laws may require that an export license be obtained for any products containing cryptography, or they may impose restrictions on specific security controls (e.g., encryption) and cryptographic strength. The applicability of these laws depends on many factors including, but not limited to where the product is developed, where and to whom the product will be delivered, and how and by whom the product will be used.

This standard, in and of itself, will not ensure compliance with national and international export control laws. Implementers are urged to obtain all information necessary to comply with applicable export control laws.

COMMENTARY

The Wassenaar Arrangement (*https://www.wassenaar.org/*), which began in September 1996, is a multi-lateral agreement that attempts to harmonize export controls, including controls applicable to encryption technology, among countries participating in the agreement.

2.0 OVERALL IPS SYSTEM ARCHITECTURE

2.1 System Overview

2.1.1 Introduction

The Airborne IPS System described within this document should be designed to provide the airborne element of an end-to-end data communications service between safety services applications on an aircraft and peer applications on the ground. It is delivered over a selection of air-ground access networks with differing characteristics (e.g., bandwidth, delay, security provision, reliability, geographic availability, cost, etc.), but in such a way that the air-ground access network(s) in use at any particular time remain transparent to the applications and the users of the system.

The ATN/IPS system uses the Internet Protocol Suite as the network protocol. This allows aviation data communications to benefit from the ubiquity of IP and years of real network experience that underpins its use in demanding and critical communications environments. Reflecting the evolution of IP that is happening in the commercial Internet, ATN/IPS leverages the IPv6 standard.

While this document defines only the airborne element of the IPS System, this section describes the overall IPS System architecture to provide context for the Airborne IPS System. Detailed specification of the Airborne IPS System is provided in Section 3.0 (architecture), Section 4.0 (security), and the supporting attachments in this document. The other sections and the appendices in this document provide informative guidance material.

2.1.2 Logical End-to-End Architecture

The IPS System comprises an airborne element and a ground-based infrastructure to deliver its functionality. Some functions are self-contained in the Airborne IPS System (e.g., airborne communication management function); others exist solely on the ground (e.g., a ground-based IPS Gateway towards an ATN/OSI or ACARS infrastructure). Additionally, several functions require collaboration between air and ground components of the IPS System, for example end-to-end security, mobility management, and routing.

Figure 2-1 provides a notional illustration of high-level air and ground elements of the overall IPS System within the context of existing and Future Communications Infrastructure (FCI). In this IPS-centric diagram, note that links between the VDLM2 and Satcom access networks and the OSI ground network are not shown since, for the purposes of this illustration, the airborne system is dual-stack (i.e., the aircraft implements the ACARS and IPS stacks but not the OSI stack).

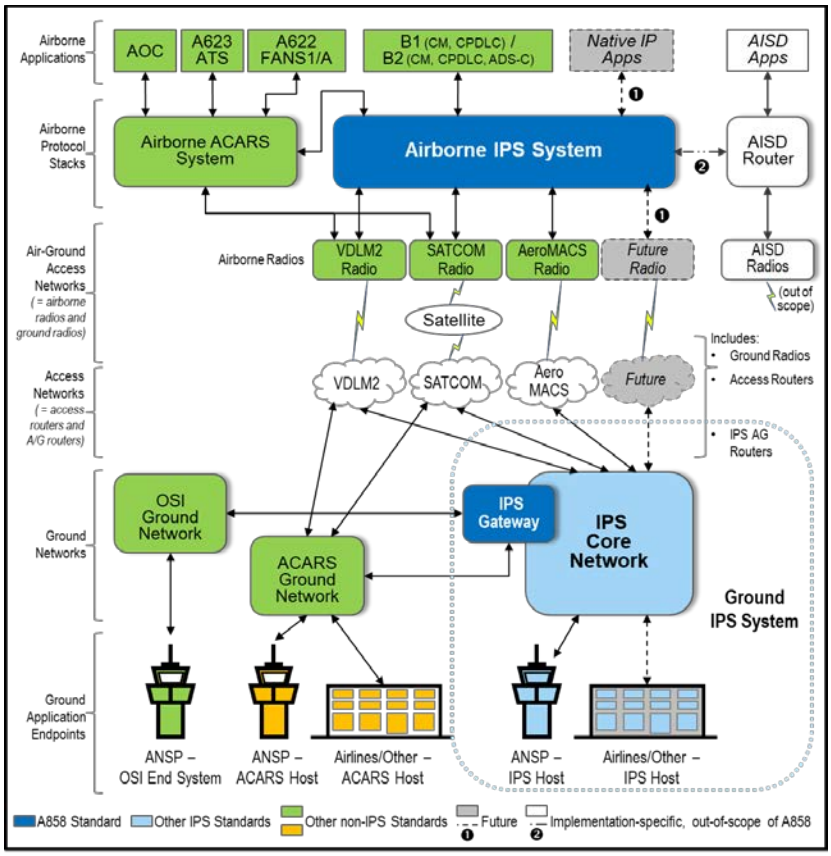

Figure 2-1 – IPS System Context Diagram

The scope of the Airborne IPS System specified in this document is to support ATS and AOC safety services applications as part of the Aircraft Control Domain (ACD).

An aircraft architecture may choose to integrate the Airline Information Services Domain (AISD) with the Airborne IPS System. Different integration approaches are available; for example, an on-aircraft AISD router may be connected directly to the Airborne IPS System. Section 4.0 provides security considerations when interfacing the Airborne IPS System with systems in other aircraft domains, such as AISD; however, the implementation of a cross-domain interface is aircraft architecture-dependent and is outside the scope of this standard.

2.1.3 Airborne IPS System

The Airborne IPS System is designed to provide air-ground connectivity for existing and future safety services applications; therefore, it is specified to connect to the ACD on the aircraft and to serve applications hosted within that domain. As described previously, although not precluded in specific deployments, there is no

specific provision within the standard for connecting to the AIS Domain. To minimize modifications to existing deployed systems, the Airborne IPS System presents an identical interface to the applications, and it provides data flow adaptation towards the radios where needed. Management interfaces (e.g., link and communication management) are as similar as possible. However, internal to the system, features such as end-to-end security and mobility management take advantage of IP technology and are new capabilities.

The Airborne IPS System connects to the existing data capable radios, namely the VHF and L-Band Satcom currently certified for safety communication. It is recognized that the Airborne IPS System should accommodate legacy equipment and its connectivity, as well as newer equipment. The Airborne IPS System will also connect to future planned radios such as AeroMACS, LDACS and Long-term Satcom Evolution as these become available.

To support the transition from ATN/OSI, the Airborne IPS System provides existing applications with a Dialogue Service (DS) interface that is identical to that provided by the ATN/OSI. This approach allows existing ATN applications to use IPS without change. Section 2.4 describes deployment scenarios to accommodate the introduction of aircraft provisioned with IPS, assuming that aircraft may support either OSI or IPS network protocols but not both.

The existing ACARS routing capability does not form part of the IPS System although its wider connectivity to aircraft systems and its need to access the data communications radios necessitates that the coexistence of these two systems be considered within this document. Safety services applications delivered over ACARS infrastructure may be migrated to IPS using accommodation provided by the IPS Dialogue Service (DS), as described in Section 3.2. AOC applications delivered over ACARS infrastructure may also be migrated to IPS using either the DS-based adaptation specified in Attachment 3 in this document or an alternative adaptation approach (refer to Section 3.2).

2.1.4 Ground IPS System Infrastructure

Although not the focus this document, the Ground IPS System infrastructure complements the Airborne IPS System and provides a vital part of the overall capability.

The ground infrastructure provides the connectivity backbone and is assumed to have always-on, reliable, low-cost, and plentiful communication capacity (unlike the air-to-ground links which have none of those properties). As such the system-wide control and management services (e.g., routing and mobility) are mainly orchestrated on the ground where the communications are more cost-effective and reliable. The ground infrastructure is likely to be a complex set of networks and functions among various Air-Ground Communication Service Providers (ACSPs), Communication Service Providers (CSPs), and Datalink Service Providers (DSPs), Air Navigation Service Providers (ANSPs), and Flight Operation Centers (FOCs) cooperating to provide the global infrastructure. This should however be transparent to the Airborne IPS System through well-defined interfaces between the airborne and ground IPS systems (e.g., for mobility signaling).

The accommodation of legacy facilities requires an IPS Gateway, which is a component of the ground infrastructure, to provide protocol conversion as summarized in Section 2.4 in this document and described in detail in Part 2 of this specification.

2.1.5 Applications

While current communications services support ATN applications, the introduction of the IPS System acts as an enabler for the enhancement of aviation data-link services. As shown in Figure 2-2, current services include Baseline1 (B1) and Baseline 2 (B2) carried over the ATN/OSI protocol suite and FANS-1/A, ARINC 623 and AOC applications carried over the ACARS data links.

The links between the aircraft applications and the network services are based on the actual use cases of the data link deployment in Europe and US. Figure 2-2 shows how applications are intended to use the different stacks, particularly IPS, based on the *European Union and United States Air/Ground Data Communications Strategy* document (dated 17 November 2017).

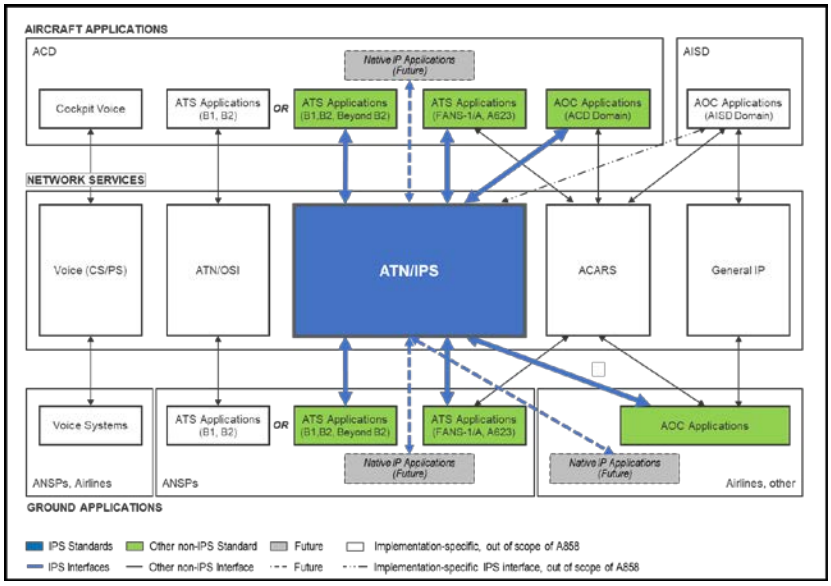

Figure 2-2 – Applications and Networks

As shown in the diagram above, the ATN/IPS service (shown in blue) supports existing FANS-1/A and ARINC 623 applications, but over the IPS protocols. It also supports the introduction of full B2 and Beyond-B2 operations. For clarity, the diagram does not show air-ground and ground-ground networks or the IPS Gateway described previously in Figure 2-1.

AOC applications hosted in the ACD are also supported over IPS. Note that AOC applications in the AIS domain may be able to use the IPS network in certain deployments, but this is not described as a standard use case in this document.

An application may have multiple options for the protocol stack to use (e.g., IPS or ACARS). The mechanism by which the choice is made is implementation-specific and is outside the scope of this standard.

2.1.5.1 Air Traffic Services (ATS) Applications

ATS applications enable interactions between aircraft and ANSPs. The IPS System is intended to support both current and future applications. Specifically, these include the following:

- **Baseline 1 (B1)** – Baseline 1 is a subset of the ICAO ATN application set defined under ICAO Doc. 9705 and ICAO Doc. 9880. It includes Context Management (CM), ADS-C, and CPDLC although currently only CM and CPDLC are implemented in production systems. It is specified to operate over OSI protocols, and its use is mandated within European airspace above Flight Level 285 in accordance with the Data Link Services Implementing Rule (DLS-IR) published as Commission Regulation (EC) 29/2009. The ICAO Doc. 9705 and Doc. 9880 provisions specify a Dialogue Service between the application and the OSI stack. To facilitate the transfer to IPS, ICAO Doc. 9896 specifies a new IPS Dialogue Service that mimics the service interface defined by ICAO Doc. 9705 and Doc. 9880.
- **Baseline 2 (B2)** – The transition from B1 to B2 represents a significant expansion of ATN capability and includes 4D Trajectory (4DT) based operations and airport services. The transition to full B2 functionality will be made using a stepped approach starting with B2A which will be implemented over ATN/OSI within Europe. As with B1, these services will be accommodated on IPS using the IPS Dialogue Service specified in ICAO Doc. 9896.
- **Beyond B2** – The future of ATN beyond B2 is undefined at the time of this writing and may continue to leverage the IPS Dialogue Service used to accommodate B1 and B2, or it may define a new service.
- **ARINC 623** – ARINC Specification 623 covers character-based ATS messages transmitted over ACARS. Although these messages are not directly compatible with the IPS System, accommodation is included in the IPS Dialogue Service specified in ICAO Doc. 9896 and in the ACARS to IPS DS Convergence Function (AICF) specified in this document.
- **FANS-1/A** – FANS-1/A and FANS-1/A+[2] comprise AFN messaging, CPDLC messaging and ADS-C position reporting and operate over the ACARS network. As a bit-oriented protocol, FANS-1/A uses ARINC 622 mechanisms to adapt to the character-oriented protocols of ACARS. As in the case of ARINC 623, accommodation for FANS-1/A is included in the IPS Dialogue Service specified in ICAO Doc. 9896 and the AICF specified in this document.

2.1.5.2 AOC Applications

AOC applications, such as those defined in ARINC 702A and ARINC 620, support services that generally fall into flight planning, weather, dispatching, ground handling, and messaging categories. While current AOC applications operate predominantly over the ACARS network, these messages can be exchanged over

[2] FANS-1/A+ improves upon FANS-1/A by including a message latency detection function. Newer systems support FANS-1/A+; however, some older systems may support only FANS-1/A. In this document the term “FANS-1/A” is used generically to refer to either version, both of which are supported by IPS.

IPS without changes to the existing applications. Attachment 3 in this standard defines an adaptation layer that accommodates the exchange of AOC messages using the IPS Dialogue Service, and alternative adaptation approaches are also possible (refer to Section 3.2). Future AOC applications should be designed to operate over the IPS network natively.

The IPS System is designed to accommodate AOC applications that are hosted on ACD resources (e.g., CMU, FMS, aircraft maintenance computers and condition monitoring systems, cabin terminals, etc.). AOC applications in the AIS domain may be able to use the IPS network in certain deployments; however, this use case is outside the scope of this standard.

2.1.5.3 Native IP Applications

Native IP applications interface directly with the IPS transport layer without the need for an adaptation layer, such as the IPS Dialogue Service interface that is used to accommodate B1, B2, FANS, and ACARS-based applications. The more mature examples at the time of this writing are AOC applications, but ATS applications are not precluded. Examples include:

- **Aeronautical Information Management (AIM)** – The AIM application is being developed at the time of this writing. Most of these services are expected to utilize AISD connectivity and thus fall outside the scope of the ATN/IPS considered here. However, the ATN/IPS accommodates such applications if written to communicate natively over IPS.
- **System Wide Information Management (SWIM)** – At the time of this writing, air-ground SWIM in 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. If air-ground SWIM safety services are deployed in the future, these applications may leverage the native IP application-layer interfaces.

COMMENTARY

While certain aeronautical mobile communication technologies may offer voice services, cockpit voice-over-IP (VoIP) services are outside the scope of this standard. 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 the IPS System can support those requirements.

2.1.6 Communication Links

The IPS System uses multiple air-ground access networks that operate in protected aeronautical spectrum allocated by ITU and ICAO for safety services. The use of a specific air-ground access network is based on media availability, airline or ANSP preference, and the multilink approach for ATN/IPS per ICAO Doc. 9896. Each media employs its own specific encapsulation of the data being transmitted.

2.1.6.1 Satellite Communications (Satcom)

2.1.6.1.1 Existing and Near-Term AMS(R)S Systems

Two Aeronautical Mobile Satellite (Route) Service (AMS(R)S) systems are designed to support oceanic ACARS and voice safety services – Inmarsat and Iridium. Both

systems are being enhanced to enable IPS with performance that supports continental Required Communication Performance (RCP) and Required Surveillance Performance (RSP) requirements (i.e., RCP-130 / RSP-160).

- **Inmarsat SB-Safety** –SwiftBroadband Safety (SB-Safety) is implemented as a set of overlay services on top of the well-established Inmarsat SwiftBroadband (SBB) IPv4 services. SBB is offered through a constellation of geostationary L-band satellites with near global coverage (except polar areas).
- **Iridium Certus** – The Iridium Certus broadband service will support IPS through its polar orbiting Iridium NEXT constellation of low earth orbit satellites with global coverage. The Iridium NEXT constellation and the Certus services use IPv4 as the native network technology.

Because both Inmarsat SB-Safety and Iridium Certus IPS service run on top of IPv4 networks, which are also shared with other non-safety services, adaptation is necessary to enable secure tunneling of the IPv6 packets between the airborne and ground IPS systems. This adaptation is handled within the Satcom system boundaries and as such is not specified in this document. Reference Section 3.4.1 for additional details.

2.1.6.1.2 Long-Term Satcom Evolution

The Satcom IPS services described in the previous section are expected to evolve to support future performance requirements (i.e., more stringent RCP / RSP), such as those required to support full 4D trajectory-based operations and future operational concepts being defined by SESAR and NextGen. These future systems will continue to support both oceanic and continental operations.

Other existing or new Satcom systems may also become available as alternative or complementary enablers for IPS services. Relevant IPS standards will be updated as evolving Satcom solutions become more mature.

2.1.6.2 Terrestrial-based Communications

Terrestrial-based communications support data and/or voice communications, typically in line-of-sight (LOS) scenarios. The following are intended to be supported:

- **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. IPS protocols will also operate over the existing VDLM2, but the service interface used at the time of this writing requires adaptation to carry IPS over the Aviation VHF Link Control (AVLC) protocol.
- **Aeronautical Mobile Airport Communication System (AeroMACS)** – AeroMACS is a radio access network that supports ATC and AOC applications for safety and regularity of flight on the airport surface. It is expected that AeroMACS will operate as an IPS air-ground access network.

In addition to existing air-ground access networks, the following are examples of future communications systems that may operate as an IPS air-ground access network.

- **L-band Digital Aeronautical Communications Systems (LDACS)** – LDACS is a future terrestrial communications system considered to

complement VDLM2 data link operations. LDACS will operate as a native IPS air-ground access network.

- **New Generation HF Radio (HFR)** – The IPS System should remain open to other communication methods and/or means such as new HF links if these links fulfill the performance requirements.

2.2 IPS System Functions

The purpose of the IPS System is to provide air-ground connectivity services between the airborne and ground applications described in Section 2.1.5. As defined in ICAO Doc. 9896, it provides a number of core functions, including: endpoint and service naming and addressing; data transport services including a reliable messaging service; routing, mobility management and QoS; and security services.

2.2.1 Naming and Addressing

All IPS endpoints require addresses which follow a consistent addressing scheme. This allows relevant stakeholders the ability to manage entities in the network based on their addresses.

With the introduction of IP protocols to the aircraft control domain, a ground-based name lookup service is required to resolve long IPv6 addresses to human natural language names.

2.2.2 Mobility

As shown previously in Figure 2-1, the Airborne IPS System connects to one or more radio-based air-ground access networks, which change depending on the current flight phase. Such transitions may occur at the edge of access network coverage or as the result of hand-off due to business or performance policy, for example, when it is more attractive to utilize another link to perform air-to-ground communication instead of the one that is being used. Even within a block of airspace, the available communications channels may change resulting in a change of technology or provider.

It is a requirement of the IPS System that such events are handled with minimum disruption to data flow and that the aircraft is always accessible at an identifiable address. Mobility is the function that enables this to occur.

2.2.3 Security

The introduction of the Internet Protocol (IP) into safety critical systems has security implications. The ubiquity of the Internet Protocol and the interconnected nature of IP networks means that malicious activity directed towards IP hosts is extensive. Furthermore, it cannot be assumed that a network disconnected from the wider internet is immune from such risks. Careful consideration is therefore required when determining how best to secure avionics equipment, software and networks connected to IP networks. The security architecture of the end-to-end IPS System is designed to protect key security attributes including the integrity of safety-critical avionics connected directly and indirectly to the communications system, the integrity of the communications, and the availability of the communications service.

COMMENTARY

The requirement for IPS end-to-end security is specified in Part 1, Chapter 3, Section 3.8 of ICAO Annex 10, Volume 3, which contains

the Standards and Recommended Practices (SARPs) for Aeronautical Telecommunications, Communication Systems.

Refer to Section 4.0 for a detailed description of the IPS system security mechanisms and security support functions including cryptographic key management, security logging, and security configuration.

2.3 IPS Protocol Architecture

A high-level view of the IPS protocol stack is shown in Figure 2-3, mapped onto the 4-layer TCP/IP model.

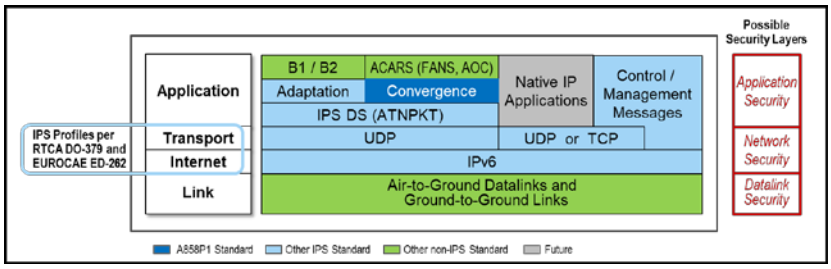

Figure 2-3 – IPS Protocol Stack

2.3.1 Functional Layers

The diagram shows the technologies used at different layers (horizontal) for different types of application (vertical). The air-to-ground radio technologies provide a variety of air-ground access networks which enable the interconnection of the airborne and ground parts of IPS. These have been described in Section 2.1.6 and may provide different types of physical and logical interfaces. On the ground, links within and between access networks form ground-to-ground links that interconnect IPS nodes.

IPv6 is the unifying network layer which inter-connects all IPS airborne and ground hosts, spanning the onboard network, ground networks, and air-ground access networks. Above IPv6, a transport layer protocol inter-connects applications, and the transport protocol may be UDP or TCP, depending on the application. The transport and network layer protocols for IPS have been selected by ICAO and profiled by RTCA/EUROCAE for interoperability and optimization over the diversity of air-to-ground link characteristic (e.g., reliability, delay, etc.).

The application layer may be fragmented due to the requirement for IPS to work with existing applications with minimal modification. Thus:

- B1/B2 applications require adaptation to be interfaced and encapsulated into ATN packets. These are in turn encapsulated into UDP datagrams.
- Similarly, for FANS/AOC applications, a convergence function is required to provide a similar interface to ACARS. The resulting messages are encapsulated into UDP datagrams.
- Native IP applications (see Section 2.1.5.3) interface directly to the transport layer and may use either UDP or TCP depending on their requirements.
- Control and management functions needed for the IPS System (for example security management, routing protocols or mobility signaling) are carried over the most appropriate transport layer for their purposes.

2.3.2 Security Layers

The principle of defense-in-depth suggests independent security barriers ought to exist to maximize the resilience of the overall security solution. The IPS System envisages different layers of security, including:

- **Application Security**: Application layer security provides end-to-end protection of the data exchanged between IPS Nodes, which may be the airborne and ground IPS Hosts on which the applications are run or IPS Gateways, if necessary for protocol conversion. In the context of application security, control and management messages are considered an application. This end-to-end security is further described in Section 4.3.
- **Network Security**: Intra-network security protects communication between ground-based IPS Nodes within an administrative domain, where each IPS Node acts as a security endpoint for segment-by-segment security within the network. Inter-network security protects communications between ground-based IPS Nodes when communications cross administrative domains. Intra-network security mechanisms are selected by network service providers; however, to ensure global interoperability across domains, inter-network security mechanisms are specified in ICAO Doc. 9896.
- **Datalink Security**: Air-ground access network (i.e., datalink) security protects data over the communication link between the airborne avionics and the access network. These security measures, which may vary by access network technology, are defined in the air-ground access network-specific standards. Reference Section 5.3.2.3 for link security implementation guidance, particularly considerations for the implementation of VDLM2 security.

Security must be considered for both the data plane (i.e., application data flows) and the control plane (i.e., management flows), each of which may use different security technologies.

2.4 IPS Deployment

The long-term vision, as described in the *European Union and United States Air/Ground Data Communications Strategy* document, is for IPS to eventually replace existing OSI and ACARS-based networks. The high-level architecture shown in Figure 2-4 reflects the target, harmonized, end-state data link communications deployment environment, where:

- All participating airborne and ground entities are IPS-enabled
- The B2 application is used for ATM operational services
- There's a mix of space-based and terrestrial-based air-ground communication links, access networks operated by Air-Ground Communication Service Providers (ACSPs), and ground-based networks operated by Communication Service Providers (CSPs).

2.0 OVERALL IPS SYSTEM ARCHITECTURE

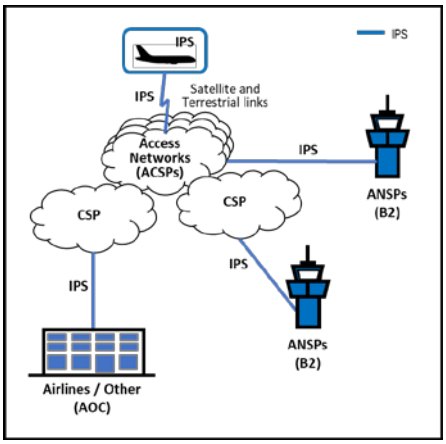

Figure 2-4 – IPS Target Deployment Environment

However, prior to the IPS target end-state, aircraft that are provisioned with OSI and ACARS stacks will operate simultaneously in the same airspace as aircraft that are provisioned with IPS. This may be a significant period of time. Likewise, it is expected that regions will continue to operate existing OSI or ACARS-based ground infrastructure and end systems in parallel with the introduction of IPS-enabled aircraft. During this period of transition, accommodation will be necessary to support the IPS-enabled aircraft while maintaining backward compatibility with existing airborne and ground systems. IPS accommodation may be accomplished with either an airborne-based or a ground-based solution; however, given the large numbers of aircraft relative to the numbers of ground systems, ground-based accommodation is preferred since it minimizes airborne equipage complexity and life cycle cost, particularly for retrofit solutions. Ground-based accommodation can also leverage existing IP network infrastructure.

A ground-based IPS Gateway provides the necessary accommodation, which includes the following functions:

- Application-level gateway between the IPS network and the existing ACARS and OSI networks. It hosts the respective protocol stacks and serves as the IPS ground peer (i.e., terminate IPS DS layer security and re-package application data for delivery to end systems bi-bidirectionally).
- Maintaining an operational association between the Airborne IPS System and the communicating peer OSI or ACARS-based ground system to ensure necessary performance and protocol operation. End system associations and application states are strictly maintained.
- Optionally, connectivity and network management services (e.g., mobility services, access network arbitration, name/address look-up service, key management services, etc.) for Airborne IPS Systems, if those services are not otherwise hosted by another network entity.

COMMENTARY

Unlike existing FANS-1/A and ATN gateways, which handle both network/transport protocol conversion and application level conversion, the IPS Gateway provides only network/transport level protocol conversion. The application data exchanged using IPS is unchanged and maintains its original format including any application-level integrity checks.

2.4.1 IPS Gateways Supporting Existing Ground Endpoint Systems

As shown in Figure 2-5, there are two primary options for placement of the IPS Gateway (annotated as "IPS GW" in the figure) within the ground architecture:

- Endpoint-hosted (Panel A in the figure), and
- Service provider-hosted (Panel B in the figure).

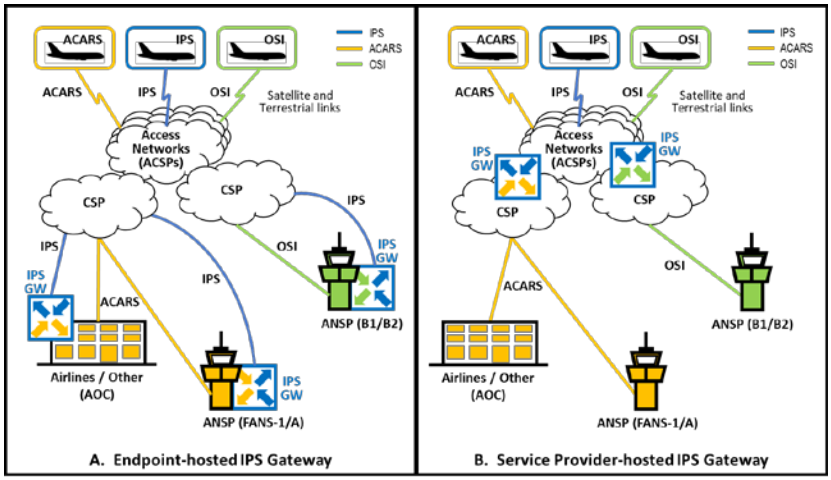

Figure 2-5 – IPS Transition-state Deployment Options

For the endpoint-hosted option, the IPS Gateway is implemented directly at each end user (i.e., ANSPs, airline/flight operations, and other AOC entities) ground end/host system. With this option, the responsibility for providing the application gateway and communicating peer associations resides with the ground end/host system. Additionally, if ACARS-based messages contain optional supplemental addresses, the ground host system is also responsible for forwarding copies of downlink messages to the addressed ground entities, a function that is normally performed by an ACARS service provider.

Alternatively, with the service provider-hosted option, ACSPs or CSPs implement the IPS Gateway and centrally perform all gateway functions on behalf of multiple ground end/host systems (ANSPs and airlines). Likewise, the centralized IPS Gateway also handles delivery of ACARS downlink messages that are addressed to multiple ground entities. Since IPS includes security mechanisms to protect communications at multiple layers, a service-provider based IPS Gateway also serves as the security termination point for network and application layer security.

As such, it acts as a security proxy on behalf of ground end/host systems, which minimizes the impact on the end/host systems themselves, particularly existing systems that do not currently implement application layer security. The message exchanges between the IPS Gateway and the end/host systems are protected using ground-ground security, as is the case today for existing systems.

COMMENTARY

When a service provider hosts the IPS Gateway and serves as the security termination point, the service provider is responsible for end-to-end security/authentication and accountable for safety consequences associated with providing the security proxy functionality.

Both gateway deployment options permit the introduction of IPS aircraft while preserving backward compatibility with OSI and ACARS-based aircraft and ground end/host systems, which continue to operate exactly as they do today as shown in Figure 2-5. It's also important to note that the two gateway deployment options are not mutually exclusive; one region may choose an endpoint-hosted gateway, whereas another region (or airline operators) may prefer the centralized functionality offered by a service provider-hosted gateway.

2.4.2 IPS Gateways Supporting IPS-only Ground Hosts

As illustrated in Figure 2-6, there is a potential deployment scenario in which a next generation ground system is purpose-built to support IPS only. This scenario is more likely when there are greater numbers of IPS-enabled aircraft than OSI and ACARS-based aircraft. In this scenario, aircraft provisioned with IPS communicate directly with a Ground IPS Host; however, a service provider-hosted gateway is necessary to provide accommodation for in-service aircraft that are provisioned with OSI and/or ACARS stacks to communicate with the IPS-only Ground Host.

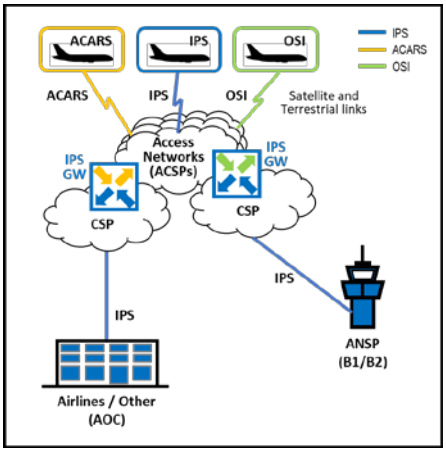

Figure 2-6 – IPS-only Ground Host Deployment

Since the IPS-only Ground Host deployment scenario necessitates a service provider-hosted gateway, this potential future environment may influence decisions

regarding selection of the IPS Gateway options during the intermediate transition state (per Figure 2-5).

Additional IPS deployment scenario considerations are provided in IPS MASPS (RTCA DO-XXX and EUROCAE ED-YYY). While the primary focus of this document is the Airborne IPS System, Part 2 of this specification describes IPS Gateway operation since the IPS Gateway is an important component of the overall IPS deployment.

2.5 Assumptions and Constraints

This section summarizes high-level, system-wide assumptions and design constraints. Further assumptions and constraints may be placed on specific functions or components within the Airborne IPS System, which are captured in the relevant parts of Sections 3.0 and 4.0.

Deployment Assumptions

- As it is not realistic to impose or coordinate an instantaneous switch over from ATN/OSI and ACARS to ATN/IPS for all equipped aircraft and ground infrastructures, it is assumed that the three technologies will co-exist for a potentially long period of time. Moreover, it is assumed that they will also interoperate, such that IPS endpoints (ground and air) can communicate with ATN/OSI or ACARS endpoints (ground and air).
- It is assumed that if an aircraft is equipped with an ATN/OSI stack, it will not also have an ATN/IPS stack, and vice versa. Until IPS is deployed fully, most aircraft will require a dual stack, i.e., ATN/IPS and ACARS. Although not envisioned, a triple stack is not precluded by this specification.

Integration Assumptions

- It is assumed that interoperability between ATN/IPS and ATN/OSI or ACARS endpoints through protocol conversion functionality will take place on the ground. This may be implemented directly at the end user (e.g., ANSP or airline) system. Alternatively, the protocol conversion, along with network management and other services, can be supported by ACSPs or CSPs implementing ground-based IPS Gateways. The deployment approaches are not mutually exclusive.
- If applications can use more than one network protocol stack present on the aircraft, the selection mechanism is implementation-specific and outside the scope of the Airborne IPS System. In addition, this standard assumes that active application dialogues do not transfer from one stack to another, i.e., an application dialogue must be restarted subsequent to a stack switch.
- It is assumed to be commercially unviable to require modifications to applications currently using ATN/OSI and ACARS in order to use ATN/IPS. Since continued use of existing applications is central to the adoption of ATN/IPS, it is essential for the Airborne IPS System to include the same interface to the applications as current stacks.
- It is assumed that Airborne Radios interface with the Airborne IPS System as Layer 2 devices. In other words, the Airborne Radios do not perform any Layer 3 IPS networking functions. Note that this assumption applies to the air-ground communications and not necessarily to any local onboard network between the Airborne IPS System and Airborne Radios.

Commented [OML3]: **Ed. Note**: THA recommendation to capute this point, which was discussed and agreed previously but not included in the document.

2.0 OVERALL IPS SYSTEM ARCHITECTURE

Scope of Use Assumptions

- This document assumes that the supported applications are only those hosted in the ACD. These could be ATS and AOC applications.
- Other aircraft domains (e.g., AISD) may leverage the Airborne IPS System for non-ACD applications; however, the implementation of a cross-domain interface and associated security mechanisms are aircraft architecture-dependent and is outside the scope of this standard.
- Native IP applications may in future use the Airborne IPS System in ways not currently specified (e.g., using other transport layer protocols) and are outside the scope of this standard given the likely deployment schedule.
- This document assumes that streaming applications are out of scope and that the communications are message oriented. Future supplements to this document may address other requirements as Native IP applications mature.

3.0 AIRBORNE IPS SYSTEM ARCHITECTURE

3.1 Introduction

This section describes the Airborne IPS System architecture. It considers the boundary of the system, its relationship to applications and equipment external to the system, and the protocols and interfaces presented by the system to other parts of the aircraft avionics.

This section also considers and specifies the Core IPS functions that define the behavior of the system in relation to existing and future applications. Some of these core functions are standardized by other bodies and are described here in relation to those standards. Other core functions are described and standardized within this document.

Functions that are part of the Airborne IPS System but are not core to its operation are also described here. The realization of these functions may be implementation-specific; however, their behavior is described here and some functionality is standardized within this document.

3.1.1 Airborne IPS System Architecture Overview

A high-level functional representation of the airborne part of the IPS System is shown in Figure 3-1.

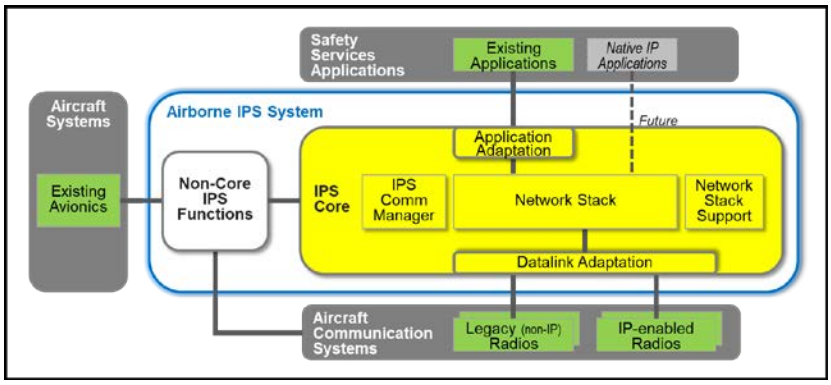

Figure 3-1 – Airborne IPS System Context Diagram

The central rounded box shows the set of Core and Non-Core IPS functions needed to implement the Airborne IPS System. The three, dark grey-shaded boxes represent applications and systems that interface logically with the Airborne IPS System, including:

- **Safety Services Applications** – These applications, which are the users of the Airborne IPS System data services, include existing ATS and AOC applications. These applications are not modified and interface transparently to the Airborne IPS System as they would to legacy OSI or ACARS systems. In the future, new safety services applications may interface directly with the IPS stack without the need for adaptation. This is represented as the Native IP applications.

Commented [OML4]: **Ed. Note**: Per BOE recommendation, all "architecture" diagrams updated to show Application and Datalink Adaptation elements as YELLOW (rather than ORANGE) since those elements are part of the IPS Core.

- **Aircraft Communication Systems** – These systems include the off-board communication systems used by the Airborne IPS System to communicate with peer Ground IPS Systems.
- **Aircraft Systems** – Operation and management of the Airborne IPS System requires interactions with other aircraft systems and functions. This may include avionics data sources required by the Airborne IPS System to manage its behavior (e.g., weight-on-wheels or location information) as well as functions from other communication stacks (e.g., legacy communication managers such as ACARS).

The following section provides a brief overview of the functional blocks within the Airborne IPS System.

3.1.2 Airborne IPS System Functional Overview

The functional decomposition of the Airborne IPS System includes Core IPS functions (large yellow-shaded box in Figure 3-1), Adaptation functions (smaller rounded-yellow boxes within the core), and Non-Core IPS functions (everything else contained within the Airborne IPS System).

The Core IPS functions form the basis for interoperability of airborne and ground IPS deployments, but which are functionally independent of the aircraft architecture, and they include:

- Network Protocol Stack – IPv6 network and transport layer protocols, as well as security mechanisms that protect communications end-to-end and ensure that only legitimate communications are allowed through the onboard system. The network protocol stack is implemented in accordance with the IPS Profiles specified in RTCA DO-379 and EUROCAE ED-262.

COMMENTARY

In Figure 3-1,the logical network stack block could be implemented as a single host or an onboard network including one or more routers and multiple hosts. This is addressed further in Section 5.5.

- Network Stack Support Functions – Protocols and services that aid in the management of the air and ground IPS network as well as the onboard IPS network.
- Communications Manager – Responsible for selecting the air-ground communication path based on user preferences, link availability, and the ability of the link to meet application quality of service requirements.

Future applications and communication systems will be designed to interface natively with the IPS network stack. However, to facilitate the transition from existing legacy networks (e.g., OSI, ACARS) to IPS, the Core IPS Adaptation functions are included as necessary to accommodate existing application and communication interfaces. The adaptation functions include:

- Application Adaptation – Allow existing safety services applications to interface transparently with the Airborne IPS System. Complementary adaptation is performed by the peer ground IPS systems.
- Datalink Adaptation – Accommodate existing off-board communication systems that present a non-IP (e.g., VDLM2) or IPv4-only (e.g., Satcom) interface rather than a native IPv6 interface. The adaptation is specific to the

air-ground communications link, and complementary adaptation must be performed by the Ground IPS System infrastructure.

The Non-Core IPS functions are required for the operation of the Airborne IPS System, and they are dependent on the aircraft architecture and interfaces. Consequently, their functional responsibilities may vary among aircraft types depending on the presence and implementation of other functions that are outside the Airborne IPS System. The Non-Core IPS functions include management functions that support the configuration, operation, and monitoring of the Airborne IPS System, and which may interface with and be dependent upon management functions that exist outside the Airborne IPS System, for example in other systems and protocol stacks available on the aircraft. Although these functions do not interoperate with the Ground IPS System infrastructure, standardization may be required to ensure consistency across a fleet (e.g., security event logging) or among system suppliers (e.g., radio management interfaces).

3.1.3 Airborne IPS System Detailed Architecture

A detailed functional decomposition of the Airborne IPS System is shown in Figure 3-2, which expands upon the high-level system diagram in Figure 3-1.

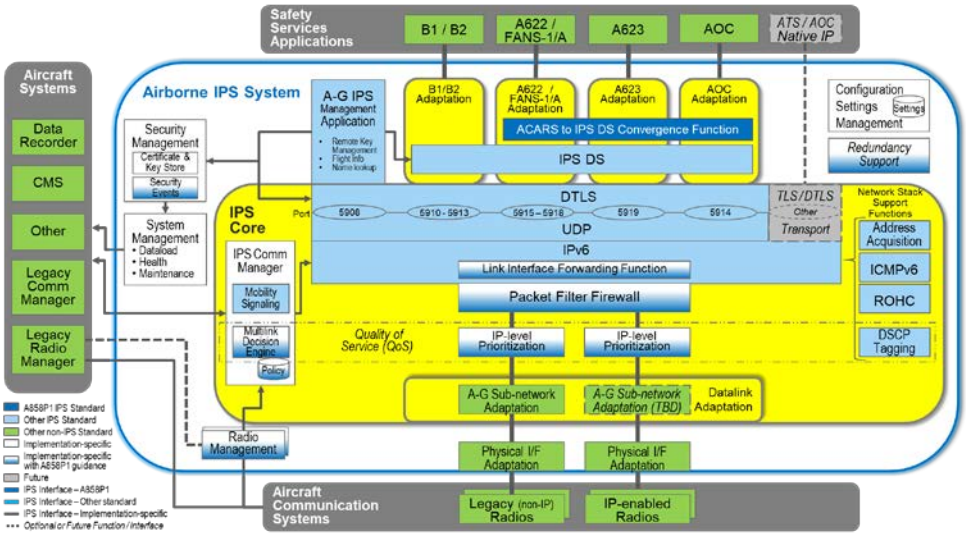

Figure 3-2 – Airborne IPS System Detailed Architecture

This diagram provides the context for detailed descriptions of the functional components of the Airborne IPS System, including:

- Section 3.2 – Core IPS – Application Adaptation
- Section 3.3 – Core IPS Functions
- Section 3.4 – Core IPS – Datalink Adaptation
- Section 3.5 – Non-Core IPS Functions
- Section 3.6 – Air-Ground IPS Management Application

In addition, Section 3.7 describes the interfaces to the Airborne IPS System, both external and internal, and Section 3.8 describes IPS Core performance requirements.

3.2 Core IPS – Application Adaptation

Adaptation of the existing ATN/OSI, FANS-1/A, and AOC applications is accomplished using the IPS Dialogue Service (DS) and the aeronautical telecommunication network packet (ATNPKT) as specified in ICAO Doc. 9896.

COMMENTARY

Alternatively, AOC applications may use a non-DS-based adaptation, which may be specified in another standard document, e.g., Media Independent Aircraft Messaging (MIAM) using the IP Middleware Convergence Function as specified in ARINC 841. Alternative AOC adaptation approaches are outside the scope of ARINC 858.

Section 6.0 provides further details regarding airborne application data considerations.

3.2.1 B1/B2 Application Adaption

The ATN/OSI DS, as specified in ICAO Doc. 9880, Part III (2010 edition), provides the interface between the ATN applications and the ATN/OSI upper layers. The IPS DS replaces the ATN/OSI DS to minimize the impact on the ATN applications. The ATN message flow over the IPS DS is depicted in Figure 3-3.

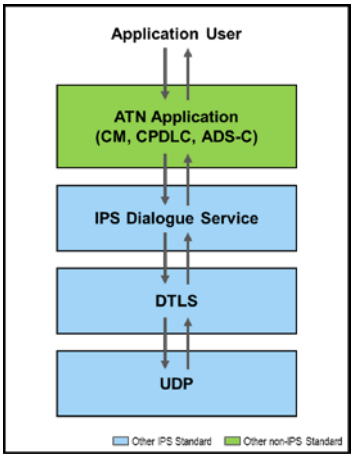

Figure 3-3 – ATN/IPS Upper Layers

3.2.2 ACARS Application Adaption

The IPS DS is also used to support adaptation of ACARS applications. The application (e.g., AOC or FANS-1/A) is indicated in the ATNPKT Application Technology Type field, as specified in ICAO Doc. 9896. The ACARS message flow over the IPS dialogue service via the ACARS to IPS DS Convergence Function (AICF) interface is depicted in Figure 3-4.

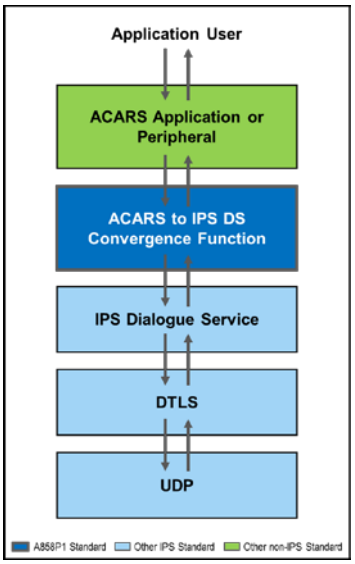

Figure 3-4 – ACARS Upper Layers

Details of the AICF are specified in Attachment 3 in this document.

3.3 Core IPS Functions

3.3.1 Transport

The transport service performs peer-to-peer communication with the remote air or ground transport entity. The data communicated by the transport layer is encapsulated in the transport layer datagram or packet and sent in a network layer IPv6 packet. The air-ground access networks and the network layer nodes (e.g., hosts or routers) transfer the transport packet intact, without decoding or modifying the content of the upper layer data. In this way, only the peer transport entities communicate using the datagrams or packets of the transport protocol. The transport layer relieves the application layer from any concern with providing reliable and/or cost-effective data transfer; however, the application or application adaptation layer is still responsible for fragmentation to meet IPv6 Maximum Transmission Unit (MTU) constraints (refer to Section 3.3.2.1). The transport layer can provide data integrity by adding a message checksum.

Commented [OML5]: Ed. Note: Added per COL recommendation to improve clarity

The transport connection is initiated by either the air or ground application depending on the type of application. For example, in the case of CPDLC, the connection is initiated by the ground system.

3.3.1.1 User Datagram Protocol (UDP)

The User Datagram Protocol (UDP) is the minimum transport layer protocol, providing connectionless datagram services with minimal overhead. The Airborne IPS System implements UDP in accordance with the IPS Profiles (RTCA DO-379 and EUROCAE ED-262).

UDP is specified as mandatory for all dialogue service-based ATS and AOC applications including B1 and B2, as well as for ACARS-based applications, which use the AICF specified in Attachment 3. The UDP payload is the ATNPKT resulting from the application adaptation performed by the IPS DS. Since UDP does not guarantee reliable end-to-end delivery of datagrams, the IPS Profiles (RTCA DO-379 and EUROCAE ED-262) require implementation of the additional UDP reliability mechanisms specified in ICAO Doc. 9896.

In the future, UDP may be used to support additional services (e.g., Native IP applications) that require a connectionless transport service; however, these applications are outside the scope of this standard.

3.3.1.2 Transport Control Protocol (TCP)

The Transport Layer Protocol (TCP) provides reliable, connection-oriented services. Although TCP is supported under ICAO Doc. 9896, its implementation in the Airborne IPS System is optional for non-dialogue service-based and non-ACARS-based applications. When TCP is implemented, air-initiated TCP connections are preferred (i.e., aircraft is the TCP client) since ground-initiated TCP connections may be prohibited due to security considerations (e.g., to limit the attack surface).

In the future, TCP may be required for additional services (e.g., Native IP applications) that require a connection-oriented transport service; however, these applications are outside the scope of this standard.

3.3.1.3 Transport Layer Port Numbers

Transport layer port numbers for IPS services are registered with the Internet Assigned Numbers Authority (IANA) and defined in ICAO Doc. 9896. The IPS Profiles specified in RTCA DO-379 and EUROCAE ED-262 require that the source and destination port numbers be the same for any given application.

COMMENTARY

The assignment and use of ephemeral transport layer port numbers by intermediate IPS systems is not permitted. IPS expects an end-to-end transport layer connection between communicating peer airborne and ground IPS systems using only the IPS-specific port numbers.

The configuration of the port numbers within the Airborne IPS Systems is implementation-dependent and part of the Non-Core IPS functions described in Section 3.5.1.2.

3.3.1.4 Transport Layer Security

IPS uses Transport Layer Security (TLS) and/or Datagram Transport Layer security (DTLS) to provide integrity and authenticity protection mechanisms for all application message traffic. TCP traffic is protected using TLS, and UDP traffic is protected using DTLS in accordance with ICAO Doc. 9896 and further specified by the IPS Profiles (RTCA DO-379 and EUROCAE ED-262).

In addition to integrity and authentication, DTLS/TLS may optionally provide confidentiality via data encryption, where use without encryption is the normative case. Further details and implementation guidance are provided in Section 4.0.

3.3.2 IPv6 Network Layer

The IPv6 function implements the IPv6 protocol and all the features of IPv6 required by ICAO Doc. 9896 and further defined by the IPS Profiles (RTCA DO-379 and EUROCAE ED-262).

COMMENTARY

Network security is out-of-scope of this specification. However, as noted previously in Section 2.3.2, inter-network security mechanisms are specified in ICAO Doc. 9896 for ground-ground communications that cross administrative domains.

Commented [OML6]: Ed. Note: Per COL recommendation, added reference back to Section 2.3.2 to remind reader about ground-ground network layer security.

3.3.2.1 IPv6 Packet

The IPv6 packet consists of header and payload data, as shown in Figure 3-5. The IPv6 header includes information including the source address, destination address and various traffic control fields for determining the quality of service needed by the payload. The IPv6 payload consists of the transport layer header and transport layer payload, which carries the application data. Refer to Appendix B for guidance regarding the protocol build-up for various payload types.

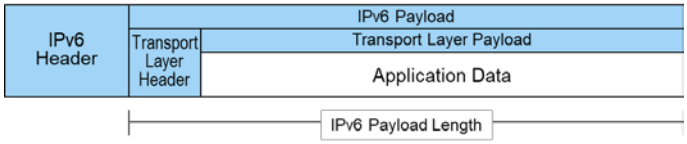

Figure 3-5 – IPv6 Packet

Per the IPS Profiles specified in RTCA DO-379 and EUROCAE ED-262, the minimum MTU size that must be supported by all IPS links is 1280 octets. For existing applications (e.g., B1/B2, FANS-1/A, ACARS-based AOC applications) that use dialogue service-based adaptation (reference Section 3.2), the maximum IPv6 packet is always less than the MTU size since ICAO Doc. 9896 limits the size of the ATNPKT to 1024 bytes and includes provisions for segmentation when the application data exceeds 1024 bytes.

Future Native IP applications, which are outside the scope of this standard, need to consider the MTU size constraints and provide application-level segmentation, as necessary. In addition, as described in Section 3.4.2, lower layer segmentation is necessary for non-IPS radios such as VDLM2 when the air-ground link layer frame size is smaller than the minimum MTU size of 1280 bytes.

3.3.2.2 IPv6 Address

This section describes the various IPv6 addresses that can be assigned to the aircraft's network interfaces that support air-ground communications, how the addresses are derived (i.e., statically or dynamically), and the strategy for their administration on the aircraft.

3.3.2.2.1 Globally Routable IPv6 Address

Every IPS aircraft is assigned a globally unique IPv6 Mobile Network Prefix (MNP) by ICAO or its designee. IPv6 addresses derived from this MNP are used for all air-ground IPS information exchanges. The Airborne IPS System uses one of these IPv6 addresses as the source address for downlink IP packets. Similarly, Ground

IPS Hosts use one of the aircraft's unique, Globally Routable IPv6 address as the destination address for uplink IP packets. Every IPS aircraft shall be assigned at least one globally routable 128-bit IPv6 address derived from the MNP. Refer to Section 3.3.4.1 for a description of how the Airborne IPS System acquires the IPv6 address for Ground IPS Hosts.

Commented [OML7]: Ed. Note: Reworded per FREQ suggestion to improve clarity.

The format of the IPv6 address for IPS is specified in ICAO Doc. 9896. Figure 3-6 provides a summary overview of the three main components of the aircraft's globally routable IPv6 address, including:

- Mobile Network Prefix (MNP) – A 60-bit, globally unique aircraft address prefix
- Subnet ID – A 4-bit field that is configured by the aircraft original equipment manufacturer (OEM) based on the on-board network architecture, avionics connectivity, and application configuration
- Interface ID – A 64-bit field that is also configured by the aircraft OEM and/or system integrator.

	Aircraft Mobile Network Prefix					OEM Configured	
Field Name	**ICAO Prefix**	**Type**	**Operator ID**		**Aircraft ID**	**Subnet ID**	**Interface ID**
Field Description	Assigned by IANA	Type=0001 (Operator Based Aircraft)	MSB is Reserved and set to 0	3 Character Operator Code, each character encoded as 5-bit ASCII per ITA2 with 5 msb selected	24-bit ICAO Aircraft Address	Onboard network identifier (implementation-specific)	Interface ID per the IPv6 Addressing Architecture RFC
Field Length	16 bits	4 bits	16 bits		24 bits	4 bits	64 bits
IPv6 Bit #	1 to 16	17 to 20	21	22 to 36	37 to 60	61 to 64	65 to 128

Commented [OML8]: Ed. Note: BOE recommends "Operator Code" in lieu of "Airline Code" and "24-bit ICAO Aircraft Address" (per ICAO Annex 10) in lieu of "24-but ICAO ID". Associated text updated accordingly.

Coordinated with Aloke, who is concerned that having an ICAO "aircraft address" within the IPv6 "aircraft address" may cause confusion. BUT, Boeing strongly recommends using ICAO Aircraft Address as defined in ICAO Annex 10.

Figure 3-6 – IPS Aircraft IPv6 Address

The following subsections describe the content and administration of the three address components in detail, as well as administration considerations for cases when the Globally Routable IPv6 address changes.

3.3.2.2.1.1 Aircraft Mobile Network Prefix

The MNP includes a 16-bit ICAO address prefix, which is assigned by IANA and/or its Regional Internet Registries (RIRs). The /16 (slash-16) block of IPv6 addresses is dedicated for aviation use and published by IANA in the RIR databases as a reserved block of addresses for ICAO use only. The remaining portion of aircraft's /60 prefix can be auto-configured using information already available on the aircraft. The following bullets describe each field in the MNP:

- ICAO Prefix (bits 1 to 16) – 16-bit value that is permanently assigned to ICAO for aviation; therefore, this constant 16-bit value can be stored in the aircraft's permanent data storage, e.g., an Aircraft Personality Module (APM) or acquired from other aircraft systems. Since the storage location and on-aircraft distribution of this value can vary significantly depending on aircraft architecture, these decisions are implementation-specific and not specified in this document.

- Type (bits 17 to 20) – 4-bit field, immediately following the 16-bit ICAO prefix, that identifies the address class, each of which may use a different format for the remaining address fields. For Operator-based aircraft (i.e., aircraft operated by an airline as well as fleet operators such as air taxis, charters, fractional ownership operators, etc.), the Type value is 0001 binary, and this value can also be stored in the aircraft's permanent data storage along with the ICAO Prefix. Note that all other values for the Type field are reserved, and the remaining address fields in this section are specified for the 0001 Type value.
- Operator ID (bits 21 to 36) – 16-bit field, immediately following the Type field. The Most Significant Bit (MSB, i.e., bit 21) is reserved and shall be set to binary 0. The remaining 15 bits of this field contain the 3-character Operator Code per ICAO Doc. 8585, where each character is encoded as 5-bit ACSII per ITA2 rules (reference ITU-T S.2) by selecting the five (5) most significant bits of each 8-bit ASCII character. Since the Operator Code is configured and available to avionics systems through local means on the aircraft, the content of the Operator ID field can be determined dynamically.

COMMENTARY

It is a common practice for aircraft operators to loan an aircraft to another operator or to the Government for temporary missions for variable durations. Care must be taken that the Operator ID field value is validated, preferably as part of every flight initialization, to ensure that the correct Operator Code is used to derive the aircraft's IPv6 prefix.

- Aircraft ID (bits 37 to 60) – 24-bit field, immediately following the Operator ID field, that contains the aircraft's 24-bit ICAO Aircraft Address as specified in ICAO Annex 10, Volume III, Part I, Chapter 9. Typically, this 24-bit field is configured as the aircraft's transponder code, which is available to avionics systems via aircraft data buses or from the APM. Per regulatory requirement and existing procedures, the 24-bit ICAO Aircraft Address is assigned when the aircraft is registered for entry into service and is globally unique. Therefore, embedding this 24-bit value within the aircraft's IPv6 prefix ensures that the MNP is globally unique within the ICAO /16 address space for Operator-based aircraft (i.e., Type value equal to 0001).

COMMENTARY

For some aircraft operations, the 24-bit aircraft transponder code may change dynamically during flight. For these aircraft, the Airborne IPS System must detect the transponder code change immediately such that IPS communications and IPS security associations are terminated and re-established using the new IPv6 address. Since re-establishing IPS communications and security associations may delay communications, the pilot and controller must be made aware of no-communication conditions so that alternate means, such as voice communications, can be utilized to maintain airspace safety while data communications are re-established.

Changes to the 24-bit ICAO Aircraft Address will also require re-establishment of the B1/B2 context since CM, CPDLC, and ADS-C

services also utilize the 24-bit ICAO Aircraft Address to exchange information with the target aircraft.

3.3.2.2.1.2 Subnet ID

An aircraft OEM or aircraft system integrator may use the 4-bit Subnet ID field to partition aircraft avionics systems into logical groups to meet a variety of IPS communication objectives. For example, and for illustrative purposes only, one subnet may be allocated to the primary avionics for the pilot and a different subnet for the avionics supporting the co-pilot; the IFE systems and cabin management systems can utilize their own subnets, while the engines might be allocated to another. The 4-bit field supports up to sixteen unique subnets. Assignment and configuration of the Subnet ID field are left to system implementers and/or airframe OEMs.

Commented [OML9]: 22-Feb (T.Bauge) - should we be using PIESD examples

Commented [ML10R9]: [Aloke] We want to have the possibility that all aircraft a/g addresses are derived from the same mobile network prefix; even when the subnets might not be connected to the same router on the aircraft. So, the text is fine as is.

3.3.2.2.1.3 Interface ID

When the Airborne IPS System is configured as an Airborne IPS Router connected to one or more Airborne IPS Hosts, the Interface ID field, when combined with the MNP and the Subnet ID fields, uniquely identifies the interface of the Airborne IPS Host(s) beyond the airborne router. When the Airborne IPS Systems is configured as a multi-homed Airborne IPS Host, the Interface ID identifies each interface of the multi-homed IPS host. Refer to Section 5.5 for a description of two possible Airborne IPS System configurations.

The Interface ID field may be configured one of two ways. It can be configured statically for each Airborne IPS Host or for each interface of a multi-homed Airborne IPS Host. Or, it can be auto-configured in accordance with the IPv6 Addressing Architecture RFC specified in the IPS Profiles (RTCA DO-379 and EUROCAE ED-262).

COMMENTARY

If Interface IDs are configured statically on the aircraft, care must be taken to ensure that duplicate Interface IDs do not exist on the same subnet.

3.3.2.2.1.4 Globally Routable IPv6 Address Recovery and Changes

An aircraft's identity and thereby its globally routable IPv6 address may change. These changes could be temporary or permanent.

When an aircraft is sold or transfers ownership to a new ICAO State, the aircraft's current 24-bit ICAO Aircraft Address is deactivated (i.e., recovered) when the aircraft is registered in the new ICAO State and a new ICAO Aircraft Address is issued. There are established procedures for the administration of this ICAO Aircraft Address change, which includes update of the aircraft's transponder code and aircraft configuration data. Once the aircraft 24-bit ICAO Aircraft Address is updated, it should automatically force an IPv6 address refresh. Additional process steps may be also necessary to refresh any IPS digital certificates that are tied to the ICAO Aircraft Address and/or the IPv6 address.

In some operational conditions, an aircraft might be loaned from one operator to another operator. When such a loan is executed, the Operator Code stored on the aircraft must be updated to reflect the correct operator such that the IPv6 address derived using the Operator Code can also be updated. In addition, IPS digital certificates of the lessor must be replaced by the corresponding IPS digital

certificates of the lessee. Similarly, when the aircraft is returned to the original operator, the Operator Code and the IPS digital Certificates must revert.

For special operational use cases, an aircraft's transponder code (i.e., the 24-bit ICAO Aircraft Address) is changed dynamically during flight. As stated previously in Section 3.3.2.2.1.1, changes to the aircraft transponder code and aircraft's globally routable IPv6 address must be synchronized resulting in a change in the IPv6 address mid-flight, and reestablishment of IPS communications. The aircraft administration must ensure that all IPS digital certificates with the appropriate 24-bit ICAO Aircraft Address are available in the aircraft's secure configuration data store to enable all necessary secure IPS session establishments if the aircraft's 24-bit ICAO Aircraft Address changes during flight.

3.3.2.2.2 Link Local IPv6 Addresses

Commented [OML11]: Ed. Note: Revised text provided by Madhu/Michal in response to THA comment.

The Airborne IPS System network-layer interfaces facing the onboard local area network are configured with unique Link Local Addresses (LLAs). Likewise, the Airborne IPS System network-layer interfaces that connect directly with the air-ground access networks are configured with unique LLAs, which are used only for communication with the next-hop ground peers. The LLAs are assigned to each Airborne IPS System network-layer interface in accordance with the IPv6 Addressing Architecture RFC specified in the IPS Profiles (RTCA DO-379 and EUROCAE ED-262). Note that the Airborne IPS System uses the unique, globally routable IPv6 addresses, and not the LLAs, for all air-ground communications with IPS nodes of the directly connected air-ground access network and with IPS nodes beyond the directly connected air-ground access network.

The scheme to assign LLAs, including those assigned to interfaces facing the onboard local area network and those assigned to interfaces with the air-ground access networks, is implementation-specific and left to the aircraft OEMs and Airborne IPS System supplier. In addition, implementers may choose to connect multiple Airborne Radios to the Airborne IPS System using separate network-layer interfaces, or they may use an abstraction of a single virtual network layer interface and assign LLAs accordingly.

3.3.2.2.3 Site Local IPv6 Addresses

Site local IPv6 addresses, as defined in the IPv6 Addressing Architecture RFC specified in the IPS Profiles (RTCA DO-379 and EUROCAE ED-262), have no special meaning and should not be used in the Airborne IPS System. If a site-local format is detected, the address will be treated as a unicast address.

3.3.2.2.4 Anycast, Broadcast, and Multicast IPVv6 Addresses

Use of anycast, broadcast, and multicast addresses over the air-ground access network interfaces are reserved. Use cases are to-be-determined and may be defined in the future.

3.3.2.3 Link Interface Forwarding Function

The Link Interface Forwarding function residing within the IPv6 function is responsible for directing the IPv6 packets of different application data types, which are generated-in or addressed-to the Airborne IPS System or the aircraft network, to/from appropriate Logical Link Interfaces per decisions taken by the Multilink Decision Engine (Section 3.3.6.1). The application data types may be differentiated by DSCP tags, source/destination addresses, transport layer port numbers, etc. The

Commented [ML12]: Ed. Note: Clarification text to address THA comment.

Link Interface Forwarding function shall prevent forwarding IPv6 packets from one Logical Link Interface to another Logical Link Interface (i.e., to prevent bridging from one air-ground access network to another without terminating in the Airborne IPS System).

The Link Interface Forwarding function shall interface with the Airborne Radios via implementation-specific Logical Link Interfaces.

3.3.3 Packet Filter Firewall

The Airborne IPS System shall implement a packet filtering function on all exposed interfaces (i.e., interfaces with off-board air-ground access networks and with the AIS Domain, if interconnected). The main functions of the packet filter firewall are to:

- Validate inbound/outbound traffic from the exposed interfaces to prevent unauthorized communication, and
- Enforce rate limitation of inbound/outbound packets to prevent resource exhaustion and mitigate denial of service (DoS) attacks.

Filtering is applied only to network and transport layer protocols.

While a stateless firewall filtering function would be sufficient for ATS traffic where a defined set of UDP ports is used, stateful filtering also supports AOC applications, which are potentially Native IP applications using dynamic TCP/UDP ports.

The definition of the firewall rules should follow a “whitelist” approach, meaning that the rules should block packets by default and only allow packets that are permitted explicitly. To facilitate context-specific settings and firewall evolutions, the rules shall be configurable and/or customizable via the Configuration Management Settings function (refer to Section 3.5.1).

Detailed packet filter firewall requirements are specified in Section 4.3.2.

COMMENTARY

The Airborne IPS System Architecture diagram (refer to Figure 3-2) shows a packet filter firewall, which is a minimum requirement. The architecture does not preclude additional implementation-specific security mechanisms to monitor network traffic and/or network system activities and block malicious content/behavior.

3.3.4 Network Stack Support Functions

3.3.4.1 Address Acquisition

The Airborne IPS System can use the ICAO-assigned prefix and the Stateless Address Auto Configuration (SLAAC) RFC, as specified in the IPS Profiles (RTCA DO-379 and EUROCAE ED-262), to assign global IPv6 addresses to one or more network-layer interfaces. The ICAO-assigned prefix and the IPS aircraft’s globally routable IPv6 address are known at startup, without external dependencies on the air-ground access network(s).

3.3.4.2 ICMPv6

The ICMPv6 function as defined by the IPS Profiles (RTCA DO-379 and EUROCAE ED-262) provides a network layer error reporting function. Refer to the IPS Profiles (RTCA DO-379 and EUROCAE ED-262) for the functions that are applicable to the Airborne IPS System.

3.3.4.3 Network and Transport Layer Header Compression

To improve communication efficiency particularly over RF links, the network and transport layer headers are compressed together using the Robust Header Compression (ROHC) framework in accordance with ICAO Doc. 9896 and the IPS Profiles (RTCA DO-379 and EUROCAE ED-262). Figure 3-7 identifies the header fields that are compressed using ROHC.

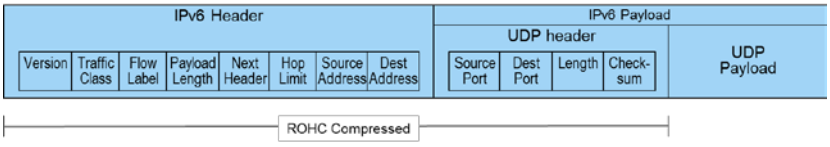

Figure 3-7 – Example of RHOC Compression

3.3.5 Quality of Service

All network traffic handled by the Airborne IPS System is not equal and the Quality of Service (QoS) requirements of each network traffic flow must be considered. Two main functions contribute to the quality of service experienced by a traffic flow:

- The IPS Communication Manager Multilink Decision Engine considers the QoS properties of the available links (statically defined or dynamically measured) as one of the inputs for selecting the air-ground access network with the potential to provide the desired QoS for a given flow. This is described further in Section 3.3.6.
- Independently, the IP-level Prioritization function ensures that, if there is contention for resources within the Airborne IPS System, mechanisms are in place to discriminate between flows and enforce relative service levels in accordance with clear policies. This is described further in Section 3.3.5.2.

COMMENTARY

The Airborne IPS System implementation may include measures to ensure processing prioritization, such that processing of a high-criticality message is finished before processing of low-criticality message in case both are being processed simultaneously by the Airborne IPS System. Alternatively, the Airborne IPS System may be designed such that parallel processing of low- and high-criticality messages does not have unacceptable impact on the performance of the high-criticality messages. Selection of an appropriate approach that meets IPS message performance requirements is left to the Airborne IPS System implementor.

In order to avoid having to support QoS requirements at the granularity of data flows, the data flows are grouped into classes that have similar requirements, following the DiffServ approach. These classes are referred to as Classes of Service (CoS), and the flows within a class are treated uniformly from a QoS perspective. The grouping into Classes of Service is described further in Section 3.3.5.1.

It's important to note that QoS mechanisms themselves do not improve the performance of the communications resources, and air-ground access network capacities represent a constraint for service availability, i.e., if the "high priority"

message load consistently exceeds link capacity, or if no datalink that supports the requires QoS is available, then even high priority messages may be lost.

QoS may be achieved by over-provisioning the communication resources so that data flows never encounter congestion at any layer, even during peak loads, and so that an alternative routing option is always available if a link fails. However, since over-provisioning may not be feasible or cost-effective, a more practical approach is to dimension the communication resources based on typical requirements and then manage peak loads and capacity drops (e.g., link failures) through in-network QoS management mechanisms.

All systems involved in end-to-end communication are responsible for collectively delivering the required end-to-end QoS. Different communication systems contribute to ensuring the QoS in different ways. Using the air-to-ground direction as an example, Figure 3-8 identifies the different IPS system components involved in end-to-end communication for an ATN application, as well as the associated QoS functions and the section in this document where the function is described.

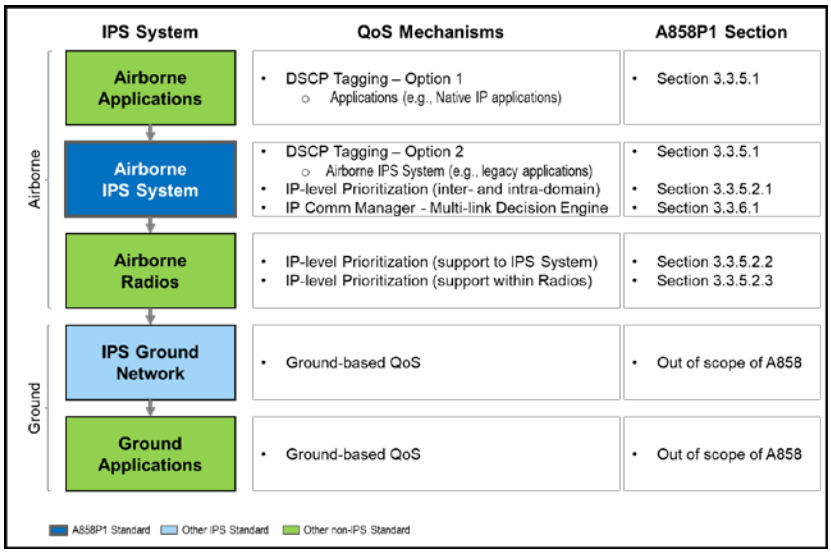

Figure 3-8 – QoS Mechanisms (air-to-ground)

The following sections describe the Class of Service and IP-level prioritization mechanisms supported by the Airborne IPS System to meet the required QoS.

3.3.5.1 DSCP Tagging

Differentiation of network traffic flows into Class of Service (CoS) with similar QoS requirements is critical for the network to discriminate between traffic types. Packet originators (e.g., application hosts, gateways, etc.) in the IPS network signal their QoS requirements for ATS application data (e.g., CM, CPDLC, ADS-C, etc.) and AOC application data using Differentiated Service Code Point (DSCP) tags in the Differentiated Services (DiffServ) field of IPv6 packets. This labelling is carried along the selected route since each hop along the route may prioritize or shape the traffic,

affecting delay, jitter, and loss characteristics. The DSCP tags may be read and used by different functions to perform their tasks (e.g., link selection and prioritization).

COMMENTARY

Each network administrative domain is responsible for implementing per hop behavior mechanisms in its own network and applying them based on the DSCP field of each packet. Therefore, the DSCP field must not be modified by intermediate nodes, in accordance with the IPS Profiles (RTCA DO-379 and EUROCAE ED-262).

The mapping of applications to CoS shall be in accordance with ICAO Doc. 9896. For downlink (i.e., air-to-ground) messages, the value of the DSCP field in IPv6 packets shall be set by either the Airborne IPS System (via the adaptation function for legacy applications) or by Native IP applications such that IPv6 packets leaving the aircraft shall be labeled correctly per their CoS. Note that in the uplink (i.e., ground-to-air) direction, the marking may be done similarly either by the end application or the Ground IPS Network, is outside the scope of ARINC 858.

3.3.5.2 IP-Level Prioritization

Prioritization on an IP packet level relies on labelling Protocol Data Units (PDUs) per their Class of Service. As shown in Figure 3-9, prioritization is typically implemented with a set of queues (e.g., for each CoS), a filter sorting incoming PDUs into the queues, and an algorithm dequeuing PDUs from queues in a specific order, resulting in reordering of the PDUs.

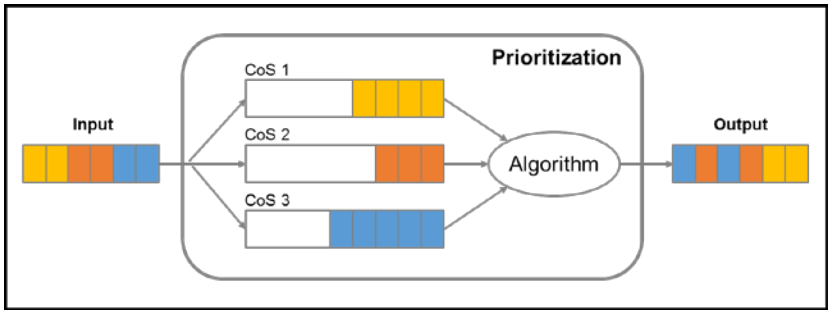

Figure 3-9 – Prioritization Principle

Within the Airborne IPS System, as queues fill they are serviced by allocating data flows among multiple air-ground links, and prioritization decisions can be made across all the data flows. However, as queues fill within an Airborne Radio, the radio only has the options to send or to drop, and prioritization decisions are limited to the subset of data flows allocated to the radio. The following sections describe prioritization mechanisms at various enforcement points within the airborne systems.

Commented [OML13]: **Ed. Note**: Additional clarification per recommendation from THA.

3.3.5.2.1 Prioritization within the Airborne IPS System

The Airborne IPS System shall prioritize traffic at the IPv6 level to ensure that high priority communications do not suffer delay or loss through the presence of lower priority communications. This requires that the Airborne IPS System reorder the

IPv6 packets per their priority. Details of the prioritization mechanism within the Airborne IPS System are a local implementation option as they do not impact interoperability; however, design considerations should include queue depths, queueing disciplines, and the handling of queued packets when a datalink becomes unavailable, since each may have a performance impact. For example, when a datalink becomes unavailable, all queue content may be transferred to another egress queue, or all packets may be re-processed individually through the IPS Communication Manager Multilink Decision Engine.

Requirements for externally observable behavior of the Airborne IPS System are specified as follows:

- The Airborne IPS System shall prioritize ATS application data with respect to AOC application data (i.e., inter-domain prioritization). Since ATS application data are considered more critical than most AOC application data, the ATS application data shall have priority over lower-priority AOC application data, meaning that dispatching ATS application data is not affected by any load on AOC application data.
- The Airborne IPS System shall further prioritize among ATS application data (i.e., intra-domain prioritization) per ICAO Doc. 9896, since some ATS application data are more critical than others (e.g., CPDLC is higher priority than CM). The prioritization among ATS application data should be proportional and not absolute to prevent starvation of less critical ATS application data.
- The Airborne IPS System shall prioritize among AOC application data (i.e., intra-domain prioritization) per airline-defined prioritization policy, since some AOC application data are considered more critical than others. The prioritization among AOC application data should be proportional and not absolute to prevent starvation of less critical AOC application data.

COMMENTARY

In accordance with ICAO Annex 10, Volume III, distress and urgent communications are prioritized over ATS and AOC safety and regularity of flight communications.

Note that this prioritization behavior is applicable to both downlink and uplink processing. However, once an uplink message is received by the Airborne IPS System, prioritization internal to the Airborne IPS System may be less critical since the main performance bottlenecks (i.e., the ground-to-air links) have already been traversed.

3.3.5.2.2 Support for Prioritization from Airborne Radios

Prioritization only has an effect when PDUs are actually waiting in the queues, i.e., when the available output bandwidth is not sufficient to handle incoming traffic immediately. As shown in Figure 3-10, the bottleneck in the airborne part of the IPS communication path is the RF air-ground link, which is shown as BW3. The onboard link, which is shown as BW2, between the Airborne IPS System and an Airborne Radio typically provides much higher bandwidth than the air-ground access network and allows the Airborne IPS System to forward PDUs to Airborne Radios almost immediately. In other words, BW2, which is typically tens to hundreds of megabits/second, is greater than BW3, which is typically tens to hundreds of kilobits/second.

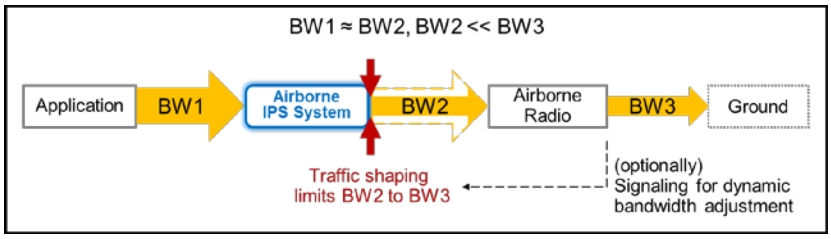

Figure 3-10 – Traffic shaping for prioritization in Airborne IPS System

For prioritization to work efficiently and effectively, the interfaces between the Airborne IPS System and Airborne Radios require traffic shaping. When the packet rates produced by the applications are higher than the interface rate limit, the Airborne IPS System outbound queues for each Airborne Radio interface start filling up with packets. The prioritization mechanisms can then start playing their roles, and there are multiple ways of performing the traffic shaping.

As a baseline, the Airborne IPS System shall implement a rate limiting mechanism with statically configured bandwidth limit that reflects the nominal bandwidth of each of the targeted air-ground access networks (e.g., VDLM2, Satcom, etc.) or its logical channel, if applicable (e.g., Satcom Packet Data Protocol [PDP] context X and PDP context Y). Recommended nominal bandwidth values are specified in the IPS MASPS (RTCA DO-XXX and EUROCAE ED-YYY). The limitation of the static setting is that it is less efficient under sub-nominal link conditions, e.g., when Satcom bandwidth varies based on allocated resources on the channel.

COMMENTARY

The rate-limiting mechanism is implementation-specific as long as the requirement for maximum data rate observed on the interface between the Airborne IPS System and the Airborne Radios is met.

To address this limitation, a dynamic flow control mechanism may be implemented between the Airborne IPS System and the Airborne Radios, reflecting the actual performance of the air-ground link and providing better results over a range of nominal and non-nominal link conditions. However, this technique requires cooperation between the Airborne IPS System and the Airborne Radio, as well as the support for this capability by the Airborne Radio. Specifying a solution for the dynamic flow control mechanism is outside the scope of this document since it depends on the capability of the radio interface.

Note that without some form of traffic shaping, the Airborne IPS System sends both high- and low-priority data to Airborne Radios immediately (i.e., without prioritization) using the data rate of the onboard transport mechanism between the Airborne IPS System and the Airborne Radio. Since bandwidth-constrained Airborne Radios are not able to forward all the data to ground at the same rate, the Airborne Radios will buffer, delay, and eventually drop, the data regardless of CoS, unless prioritized in the Airborne Radio.

3.3.5.2.3 Prioritization within Airborne Radios

IP-level prioritization performed by the Airborne IPS System can be complemented with prioritization performed (possibly on a different protocol layer) by the Airborne Radios, depending on capabilities of each Airborne Radio and its underlying air-

ground access network, as described in the relevant radio standards. If the Airborne Radios perform their own prioritization, it is critical to coordinate this prioritization with the prioritization settings of the Airborne IPS System to optimize the overall impact on performance and avoid conflicting priorities. Otherwise, the result can be sub-optimal performance.

A radio-specific prioritization solution is outside the scope of this document as it depends on the capability of the radios and their interfaces.

COMMENTARY

Each radio-specific standard may specify a different mechanism to identify the packet type transferred over the interface between the Airborne IPS System and the Airborne Radio and its associated priority. Ideally, the packet identification mechanism would be common across all radio interfaces; however, heterogeneous radio-specific solutions would be accommodated by the Airborne IPS System Datalink Adaptation function.

3.3.6 IPS Communications Manager

IPS Communication Manager is an instantiation of the multilink concept within the Airborne IPS System. It consists of a set of functions responsible for taking decisions on which air-ground datalink should be used for which application data and for coordination of the decisions with other communications managers, in the aircraft and on the ground. It consists of a decision function (Multilink Decision Engine as described in Section 3.3.6.1) and a coordination function (Mobility and Multilink Signaling as described in Sections 3.3.6.2).

COMMENTARY

The multilink concept specified in ICAO Doc. 9896 may include mechanisms to improve transmission success rates, e.g., sending the same messages over multiple datalinks simultaneously, retransmission mechanisms among multiple datalinks, etc. The multilink description in this section focuses only on the selection of the most appropriate datalink. Once the multilink concept is fully specified in ICAO Doc. 9896, additional considerations will be included in a future supplement to this document.

Commented [OML14]: Ed. Note: Per THA recommendation, added dependency with ICAO WG-I.

3.3.6.1 Multilink Decision Engine

The Multilink Decision Engine (MDE) function exercises control over selection of the air-ground datalink that is most suitable for the application data. It ensures predictable routing behavior based on configured settings (reference Section 3.5.1.3), but it does not imply use of a routing protocol on the air-ground datalink. The function shall select an air-ground datalink for each known application data type, which is indicated typically by a DSCP field of the IP packet header (reference Section 3.3.5.1), transport layer port number (TCP or UDP) or a combination of source/destination address of the IP packet header. To do this, the MDE function collects the status of air-ground datalinks as reported by the individual Airborne Radio components.

In addition to application data type and air-ground datalink status, the MDE function may take additional parameters into account for air-ground datalink selection, including but not limited to: phase-of-flight; geographic position of the aircraft; ANSP

preferences; airline preferences; or air-ground communications link cost. If the MDE function can also acquire air-ground link quality/performance metrics, which is dependent upon the capability of each Airborne Radio to report this information, then it can make decisions to switch intelligently among communication links in a multilink environment, e.g., selecting a well performing link for high-criticality traffic and a less well performing link for best-effort traffic. The use of these additional criteria by the MDE function are implementation-specific and/or the subject of further standardization in the radio specifications.

COMMENTARY

The Multilink Decision Engine works in concert with the other QoS mechanisms to allocate traffic to available air-ground media to meet QoS for all application classes of service. When that is not feasible, then meeting QoS for higher priority traffic shall be preferred, rather than satisfying the QoS of lower priority traffic. However, as noted previously in Section 3.3.5.2.1, prioritization should be proportional and not absolute so that lower priority traffic is not starved of service for an extended time.

Commented [OML15]: **Ed. Note**: Added per THA recommendation to improve clarity.

The MDE function shall be able to select different air-ground datalinks for different application data types, i.e., multiple air-ground datalinks can be used simultaneously for different applications. However, for any given application data type, the MDE shall select only one air-ground datalink at a time since it is not envisioned currently that duplicate IP packets will be sent over multiple air-ground links simultaneously.

The MDE function shall select only air-ground datalinks that are ready to transfer data at the time of decision. This implies that all air-ground datalinks that are intended to be candidates for the selection shall be up-and-running to be considered for the selection.

As a baseline, the MDE function shall select air-ground links for a given application data type according to a pre-configured static policy, which may be OEM- or operator-configured and stored in a local database or an alternative storage means. The static policy is configured in alignment with QoS needs of the given application data type, nominal QoS capabilities of the air-ground datalinks, and any additional regulatory or business-related aspects. For example, this means that low-criticality, high-volume data will not be configured to be sent over low-bandwidth air-ground datalinks, or that latency-critical data will not be configured to be sent over high-latency air-ground datalink. A dynamic mechanism that reflects actual conditions (QoS capabilities) on the air-ground datalinks may be implemented on top of, or instead of, this static configuration. The choice of static, dynamic, or hybrid approach is implementation-dependent and outside the scope of this standard.

The decision taken by the MDE function shall then be signaled to:

- Link Interface Forwarding function, which executes the decision in the implementation of the IPv6 layer, i.e., it selects the correct link interface for IPv6 packets of a given application data type. The format and content of the signaled information is implementation-dependent, and at a minimum, it should include the following for each application data type:
  - Implementation-specific internal application data type identifier (e.g., DSCP, source/destination addresses, transport layer port number), and

  - Implementation-specific internal link identifier of the selected air-ground datalink.
- Aircraft Systems and Safety Services Applications to indicate whether there is a suitable communication path for given application data type. The format and content of the signaled information is implementation-dependent.

Additionally, the MDE function's decision may be signaled to the Mobility and Multilink Signaling (MMS) function (refer to Section 3.3.6.2), which communicates the decision to the ground infrastructure via the Mobility and Multilink Signaling interface. The ground infrastructure may use this information to select the air-ground link for uplink traffic. The format and content of the data exchanged between the MDE and MMS functions is implementation-specific; however, the MDE function must provide information sufficient for the MMS function to comply with the air-ground signaling interface requirements (refer to Section 3.3.6.2).

3.3.6.2 Mobility and Multilink Signaling

The Mobility and Multilink Signaling (MMS) function coordinates the mobility and multilink-related information between the Airborne IPS System and the ground IPS infrastructure. To facilitate handovers among multiple air-ground datalinks, the MMS function implements the signaling mechanism defined in ICAO Doc. 9896. The signaling mechanism announces the availability of the aircraft Mobile Network Prefix (MNP) in a given access network. Additionally, it coordinates the preferences for using the individual air-ground access networks for various application data types. The ground infrastructure may use this information to select an appropriate air-ground access network for uplink traffic.

COMMENTARY

ICAO Doc. 9896 Edition 3 is in progress, and the final specification of the Mobility and Multilink Signaling interface is not available at the time of writing of this document. Additional information will be included in future supplements to this document.

3.3.7 Coordination with an External Communications Management Function

For dual-stacked avionics implementations that support both ACARS and IPS stacks, an External Communications Management Function (CMF) may be necessary for coordinating parallel operation of IPS and ACARS network protocols. For example, the External CMF provides a means for IPS and ACARS communication managers to negotiate and manage access to shared air-ground access network assets (e.g., VDLM2 radios) that are used for both IPS and ACARS communications. For example, the External CMF ensures that FANS-1/A application traffic being sent via IPS over VDLM2 takes precedence over lower priority AOC traffic being sent via ACARS over a shared VHF data radio. In addition, the External CMF provides the IPS Communications Manager with access to functions that may be provided by an existing ACARS communications manager, including but not limited to:

- Link management for cases where that function is not embedded in the radio itself (e.g., AVLC for VDLM2)
- Radio status for cases where the existing communications manager provides the primary interface to a radio, (e.g., VDR)

- Overall connectivity status (i.e., COMM, NOCOMM) that is reported to end users of the airborne communication systems
- Radio voice/data mode switching (e.g., VDR).

During the transition to IPS, ground systems and access networks covering various regions will transition to IPS according to differing timelines. In this context, IPS will be deployed initially in selected regions, with the IPS coverage area expanding over time. When switching between ACARS and IPS network protocols, the ACARS application session (e.g., FANS-1/A) may also need to be switched, requiring coordination between the aircraft and ground systems. These complex cases should be avoided with the selection of an appropriate transition and deployment approach, e.g., the use of an IPS Gateway to abstract the air-ground networking technology from the ground application systems.

Implementation of the External CMF is highly dependent on the avionics architecture and the implementation of an existing ACARS communications management function. Refer to Section 5.4 for implementation considerations for dual-stack configurations.

3.4 Core IPS – Datalink Adaptation

3.4.1 IPS Accommodation for IP-enabled Radios

Existing satellite communication systems, including Inmarsat SwiftBroadband (ARINC 781) and Iridium NEXT (ARINC 771), implement IPv4 networking with custom air-ground transport protocols and a Virtual Private Network (VPN) to tunnel existing ACARS messages and OSI Protocol Data Units (PDUs) between airborne routers and the next-hop ground router. This tunneling mechanism, which is implemented in the airborne Satellite Data Unit (SDU) and the Satcom ground gateway, hides the IPv4 network and makes the air-ground Satcom link appear like a point-to-point Layer 2 connection between the airborne and ground routers. Since existing SDUs are not IPS Nodes, implementation of a similar tunneling mechanism in the airborne SDU and ground Satcom gateway is necessary to support IPS. Specification of the tunneling mechanisms to support IPS are outside the scope of this standard.

COMMENTARY

At the time of this writing, ARINC Characteristic 766, ARINC Characteristic 771, and ARINC Characteristic 781 do not include technical provisions for encapsulation of IPv6 in IPv4 packets.

Note that the AeroMACS Radio Unit (ARU) should support both IPv4 and IPv6 as specified in ARINC 766 and ICAO Doc. 10044, AeroMACS Technical Manual; however, since the ARU is not an IPS Router, similar encapsulation of IPv6 in IPv4 or IPv6 packets is necessary.

3.4.2 IPS Accommodation for Non-IP-enabled Radios – VHF Digital Link Mode 2

VHF Digital Link Mode 2 (VDLM2) is the primary air-ground communication channel used for the ACARS network worldwide and for the ATN/OSI Network (ATN) in continental Europe. It specifies OSI Layer 1-2 (i.e., physical and datalink) for communication between aircraft and ground stations. VDLM2 uses Carrier Sense Multiple Access (CSMA), which is the “listen before you talk” technique that is also used in IEEE Wi-Fi standards. VDLM2 is half-duplex, which means that only one station transmits at a time and the same frequency is used for all transmissions.

As illustrated in Figure 3-11, VDLM2 uses Aviation VHF Link Control (AVLC) frames to carry ACARS messages, which is known as ACARS-over-AVLC (AOA) and ATN/OSI messages. When VDLM2 is used to transport ATN/IPS messages, the IPv6 packet is also transmitted in an AVLC frame.

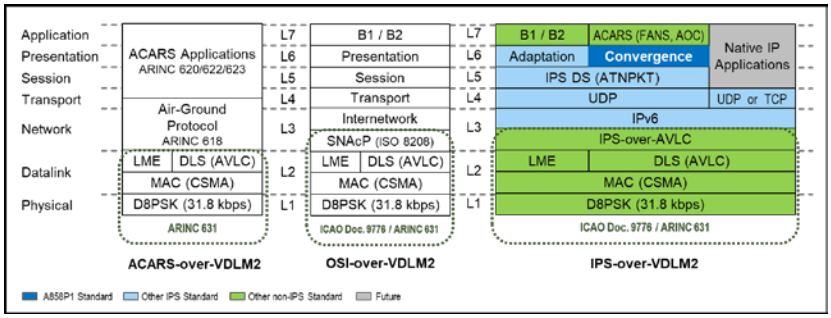

Figure 3-11 – Comparison of Different Payloads over VDLM2 using AVLC

Figure 3-12 shows the AVLC frame detail and the breakdown of the information field inside the AVLC frame with respect to the various networking protocols. Additional information on the AVLC frame is available in ICAO Doc. 9776, 2nd Edition, *Manual on VHF Digital Link (VDL) Mode 2*.

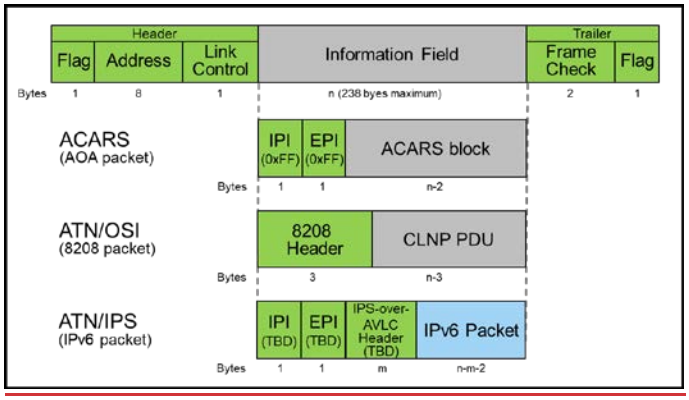

Figure 3-12 – AVLC Frame Format

~~The first two octets in the Information frame are the Initial Protocol Identifier (IPI) and Extended IPI. The combination of the IPI and EPI are used to indicate the type of protocol payload AVLC is carrying. A value of 0xFFFF indicates AOA, a value of 0x1BFF indicates the OSI 8208, and a value of 0x8E specifies the IPv6 protocol, which requires only the IPI value for the payload specification. Refer to ISO 9577 Appendix C for several IPI encoding values for network-level interoperability with internet applications.~~

ARINC Specification 631 (Supplement 9 and later) is expected to include the VDLM2-specific enhancements necessary to support IPS-over-AVLC, including provisions for link layer security and segmentation/reassembly of IPv6 packets that

Commented [OML16]: **Ed. Note**: Revised figure (more detailed and consistent with figure in draft A631s9) per BOE recommendation. Deleted subsequent paragraph which in not correct with respect to updated figure.

Commented [OML17]: **22-Feb (T.Bauge)** – Presumably IPS just uses the IPv6 code and doesn't have a specific code of its own ? Is it possible that "non IPS IPv6 packets" could be transported simultaneously and would it be an issue that they share the same IPI code ?

Commented [OML18R17]: **26-Feb (M.Matyas)** –
An in-process AEEC DLK paper states:
For a VDL IP packet for IPS, precede the IP packet with an IPI of 0x8E but without an EIPI (to indicate that IPv6 is the network layer protocol per ISO 9577:1999(E) Annex C).
With a comment stating: If Orange adds leading bytes and/or is used for more than only IPS, then replace this with an IPI of 0xFF and a new EIPI for Orange (regardless of whether Orange contains an AOA packet, 8208 packet, or IPv6 packet).

Commented [OML19R17]: **Ed. Note**: OBE with changes to figure/text.

are exchanged over VDLM2 using AVLC frames. Segmentation is necessary since the 238-byte maximum size of an AVLC frame information field (i.e., between the header and trailer) is smaller than the minimum Layer 2 MTU size of 1280 bytes per the IPS Profiles (RTCA DO-379 and EUROCAE ED-262).

3.5 Non-Core IPS Functions

The Non-Core IPS functions are required for the operation of the Airborne IPS System. Although these functions are implementation-dependent and driven by specific aircraft architectures and interfaces, this section provides a description of the functions and guidance for implementation.

3.5.1 Configuration Settings Management

The Configuration Settings Management (CSM) function supports setting various preferences and parameters regarding protocol selection, link selection, address selection, routing table management, and firewall configurations. The CSM is implementation-dependent and may include one or a combination of: an external configuration tool that produces a loadable configuration file, a local user interface for settings configuration, or other means defined by the implementer of the Airborne IPS System. Configuration of the Airborne IPS System is intended to be performed as part of maintenance-related actions; avionics configuration settings are not normally modified by flight crews.

3.5.1.1 Network Protocol Preference

The CSM function supports configuration of a default network protocol (i.e., IPS or ACARS) on a per-system basis, permitting application message exchanges to prefer one network protocol stack over another depending on the onboard system from which the application messages originate/terminate. As described in Section 3.3.7, an External CMF may be necessary to facilitate coordination between the IPS communications manager and an existing ACARS communications manager.

The CSM function supports configuration of IPS parameters associated with each network protocol option such as protocol timer values and ICAO Doc. 9896 message reliability parameter values (e.g., number of re-transmission attempts). The final parameter list is identified in the IPS Profiles (RTCA DO-379 and EUROCAE ED-262), which identifies the minimum options necessary for interoperability.

Since IPS and ACARS network protocols may operate simultaneously over the same air-ground link depending on the ground infrastructure and topology, the CSM function allows configuration of a default network protocol by link type, with rules to ensure that conflicting combinations of preferences are not selectable. For example, the Airborne IPS System shall not permit configuration of the IPS network protocol for air-ground access networks (e.g., Classic Aero Satcom) that cannot support IPS. The network protocol preference by link type takes precedence over the network protocol preference by system.

The CSM function allows each of the network protocols to be configured as disabled by default, and the disabled setting may be by system, by geographical location, or by other criteria. The intent is to not provide a protocol choice when it is known beforehand that the protocol is not supported, as well as to prevent configuration of conflicting combinations.

3.5.1.2 Application Transport Preference

Applications are associated with either the TCP or UDP transport layer protocol, described in Section 3.3.1. For legacy applications (e.g., B1, B2, FANS-1/A, and ACARS-based AOC) that utilize IPS DS adaptation, use of UDP transport is mandatory per ICAO Doc. 9896 and is enforced by the Airborne IPS System design and implementation.

Future safety applications (e.g., Native IP applications), may be designed to support multiple transport protocols, and the use of TCP or UDP transport is selected by the application. The CMS function facilitates transport selection by the application with respect to other configuration settings and constraints. Application use of TCP should be considered in concert with the capability of Air-Ground Access Networks to support connection-oriented transport (e.g., TCP may not be appropriate for low-bandwidth air-ground datalinks). As noted previously in Section 3.3.1.2, airborne applications that use TCP should be configured to act as a TCP client such that TCP connections are air-initiated by the Airborne IPS System.

3.5.1.3 Link Preference

The CSM function supports setting the order of air-ground access network preference on a per-protocol, per-application, and/or CoS basis (refer to Section 3.3.6). For example, the system may be configured such that VDLM2 is preferred over Satcom for FANS-1/A operating over IPS. The IPS Communications Manager function uses the pre-configured air-ground access network order preference in concert with real-time information (e.g., link availability, multilink considerations, etc.) to select the most appropriate link.

3.5.1.4 Static Address Lookup for Ground Entities

In lieu of, or in addition to, ground-based address look-up services provided by the IPS Management Application, the CSM function supports configuration of stored static IP addresses for Ground IPS Hosts and/or IPS Gateways. The content and format (e.g., hosts file format) of the address information are locally defined and implementation-specific; however, as a minimum, each static IP address entry must include an IPv6 address and the associated canonical entity name, which may be a 4 to 8-character ICAO facility designator, or a Ground IPS Host domain name or an IPS Gateway domain name in in accordance with host naming requirements specified in the IPS MASPS (RTCA DO-XXX and EUROCAE ED-YYY).

The CSM function allows applications to access the onboard IPv6 address storage to store and retrieve IPv6 addresses. This includes access by the IPS Management Application (e.g., simple name lookup functions), by safety applications such as CM and CPDLC, and by other AOC-related applications that need access to IPv6 addresses for IPS services.

As a minimum, the CSM function should support non-volatile storage of sixteen (16) IPv6 addresses and associated entity name information. The Airborne IPS System should include provisions (e.g., last-in-first-out) to gracefully handle conditions where the addition of new addresses exceeds the storage limit.

3.5.2 IPS System Management

The IPS System Management function serves as an aggregator of events related to the operation of IPS. This includes health and system management input from

security and communications functions and interactions with other aircraft management systems so that a common status picture is possible.

3.5.2.1 IPS Health Management Function

The IPS Health Management function is responsible for the detection, correlation, isolation, and storage of faults from the IPS Core. Faults are reported and/or conveyed as appropriate to other centralized aircraft systems and health management components. This may be integrated with an overall system network management protocol (e.g., SNMP-type) implementation on the aircraft.

3.5.2.2 IPS Maintenance Function

The IPS Maintenance function provides the ability to assist maintenance personnel in troubleshooting issues within the IPS System. This may include software trace data, information on status of individual radios, and other configuration data.

The IPS Maintenance function capabilities should be accessible through existing shared or dedicated displays, and mechanisms should allow offloading of maintenance information to external media for subsequent analysis, including:

- Hardware faults
- Software faults, including exception notifications, core dump-type information
- Information about problems and unusual conditions
- Establishing baselines
- Contributing additional application-specific data for incident investigation, etc.

3.5.2.3 IPS Dataloading Function

The IPS Dataloading function provides the ability to load software parts related to the Airborne IPS System. This is normally handled in accordance with ARINC Report 665, *Loadable Software Standards*.

Supplier-specific dataload requirements that go beyond ARINC 665 or that provide guidance for specific features of the standard or on local implementation are expected to be provided in supplier documentation.

3.5.3 Radio Management Function

The Radio Management function monitors the state of all datalinks (e.g., via status reports from the Airborne Radios) and the health of the Airborne Radios (i.e., it verifies that no reception of status changes of the datalinks is not caused by a non-operative radio). The Radio Management function conveys radio status to the IPS Communications Management and Health Management functions.

For each installed IPS-capable Airborne Radio, the Radio Management function shall monitor the availability of air-ground communication, i.e., “Link Up” and “Link Down” events (or equivalent), and report to the Multilink Decision Engine function (described in Section 3.3.6.1). Additionally, the Radio Management function may monitor other parameters (e.g., RF signal quality) that are made available by the Airborne Radio, and it may also provide control (e.g., radio tuning) for some Airborne Radios (e.g., VDR). Status and control capabilities are specific to each air-ground access network and are defined in the respective radio-specific standards.

3.5.4 Security Management ~~Function~~

As a baseline, the security mechanisms described in the Core IPS functions (e.g., transport layer security, packet filter firewall), and further described in Section 4.0, are considered to be statically configured and do not require dynamic management. Dynamic management capability, as well as additional security functionality (e.g., active intrusion detection) that does not impact interoperability, could be envisaged as a supplier-specific add-on.

The Airborne IPS System should support the provisioning of trust anchor certificates (reference Section 4.4.1.1.4) and the configuration of cryptographic modules including crypto-algorithms and cipher suites, which require replacement once they become deprecated (reference Section 4.5.3). In addition, it is expected that during the lifecycle of the Airborne IPS System, some security parameters may need to be updated or tuned as a result of obsolescence, deficiency, or to account for a security event. The Airborne IPS System should be capable of modifying a subset of security parameters during in-service operation without the need for major operational code revisions. This is necessary to quickly mitigate an emergent issue without imposing the lengthy re-certification process needed for a major change. Examples of parameters that should be capable of modification include items such as access control lists, firewall rules and rate limiting thresholds (reference Section 4.3.2), data flows (reference Section 4.3.3), key management parameters (reference Section 4.4.1), and security event log parameters (reference Section 4.4.2). Existing aviation methods, such as utilizing an Operational Program Configuration (OPC), may be employed to overlay security configuration updates over a baseline security configuration. Note that this does not mean that updates should happen dynamically or in-flight, but rather that configuration updates should leverage existing operations and maintenance processes for re-configuration.

Additional aspects of security management such as key management and security event logging are addressed in Section 4.4.

3.5.5 Redundancy Support

The need for redundancy and the performance requirements that a redundant solution must meet are driven by the performance requirements (e.g., availability, transaction time, integrity, etc.) that are allocated to the Airborne IPS System, as specified the IPS MASPS (RTCA DO-XXX and EUROCAE ED-YYY). Refer to Section 3.8.

Depending on the architecture of the Airborne IPS System and the constituent IPS Core, some aircraft configurations may choose to implement IPS redundancy. For these cases, state information and security associations must be made available to the redundant systems/components in the event of a failover operation.

The redundancy approach is implementation-specific and options include a primary/standby configuration or a parallelized load-share configuration. Regardless of the selected configuration, the following sub-sections describe basic functionality that must be implemented to ensure correct processing and synchronization among redundant components.

Commented [ML20]: 22-Feb (T.Bauge) – This section makes statements about some of the security requirements but doesn't describe a function… everything described in this section could potentially be supported through the Configuration Settings Management (3.5.1) and the Datalaoding (3.52.3).sections… in 3.5.5.1.1 security artifacts are included in "configuration settings" and not broken out into a separate topic.
Recommendation: Either include this under "Configuration Settings Management (e.g. as 3.5.1.5 Security preferences) or describe the requirements for this function (maybe similar to configuration management but with enhanced security ?).

3.5.5.1 Synchronization

3.5.5.1.1 Configuration Settings

The configuration settings described in Section 3.5.1 must be made available to each of the redundant systems. In addition, each redundant system must have access to the security configuration described in Section 3.5.4, which includes cipher suites, security settings (e.g., firewall rules), trust anchor certificates, the aircraft private key, and stored/cached certificates, including the public key certificate associated with the aircraft private key. The redundant implementation must ensure the confidentiality and integrity of the configuration settings and security configuration information that is made available to each system.

3.5.5.1.2 System Management Information

The IPS system management interfaces described in Sections 3.5.2 and 3.5.3 must be made available to each of the redundant systems. Dynamic system information (e.g., system logs) that is stored local to the Airborne IPS System (i.e., not reported to a centralized aircraft system management function) must be synchronized between the redundant systems. At a minimum, the integrity of locally stored system information must be ensured.

3.5.5.1.3 Session-specific Parameters

The parameters associated with the communication sessions established between the Airborne IPS System and communicating peer ground entities, must be made available to a standby system in the event of a switchover. Session-specific parameters include, but are not limited to:

- State data for the individual dialogues and transport-level IPS connections; this can include the current state as per ICAO Doc. 9896 state tables
- Current session information (e.g., source and destination identifiers, called and calling peer identifiers, messages sequence numbers, IPS DS state information, if applicable) for each application context
- Messages that are queued or in-process (e.g., messages that have been sent but not yet acknowledged).
- Security context information (e.g., negotiated cryptographic algorithms, negotiated key lengths, master secret key, air and ground nonces) associated with each application context

COMMENTARY

A redundancy approach should consider the trade-offs between sharing security context information, which has security implications (e.g., potential exposure of secret keys), and re-establishing the security associations, which has performance implications. In addition, the need to share security information may depend on the selected transport, as described in the following paragraph.

Commented [OML21]: Ed. Note: Commentry added per THA recommendation to improve clarity.

For applications using UDP transport, which is connectionless, a switchover may be possible without losing the application-level association and associated secure session; however, applications using TCP transport will need to re-establish transport connectivity and secure sessions. A switchover may be performed independently of existing physical-level radio connections. If switchover and synchronization take too long or if information is lost, it will be necessary for

applications to re-establish transport level connectivity and/or application-level associations. The applications, which are external to the Airborne IPS system, maintain their states independently.

COMMENTARY

A switchover between Airborne IPS Systems must occur within a time that satisfies the performance requirements allocated to the Airborne IPS System.

Messages in transit during a switchover may be lost; however, the communication recovery mechanisms specified in ICAO Doc. 9896 preserve messages by detecting and retransmitting lost messages.

3.5.5.2 Switchover

Logic must be present to determine the conditions that require a switchover. This can be done by status message exchanges between the redundant Airborne IPS Systems. In addition, logic must be present to minimize the number of switchovers and the time between switchovers.

3.6 Air-Ground IPS Management Application

The Air-Ground IPS Management Application exchanges messages with a ground IPS management service located at one or more Ground IPS peers to support proper and efficient operation of IPS air-ground communications. Examples of these services include simple name lookup and remote key management. Unlike legacy ATS and AOC applications, the IPS Management Application does not utilize the ATNPKT format and associated reliability and fragmentation mechanisms. Therefore, these mechanisms must be provided by the IPS Management Application itself. The message format, description of the protocol operation and reliability mechanisms, and detailed specification of the application messages are provided in ICAO Doc. 9896.

3.7 Airborne IPS System Interfaces

This section provides a high-level overview of external and internal Airborne IPS System functional interfaces. Figure 3-13 shows the location of these interfaces with respect to the Airborne IPS System.

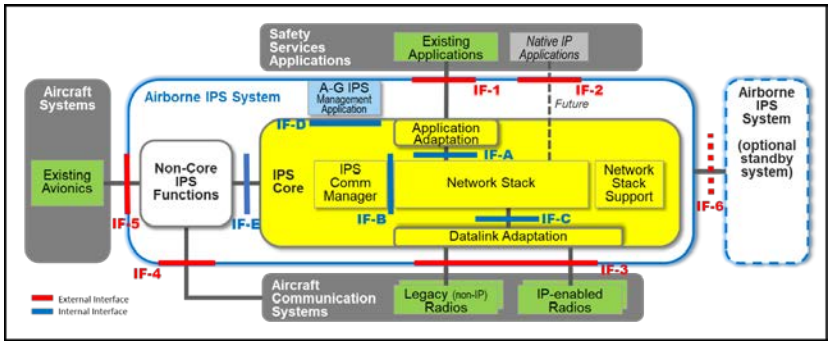

Figure 3-13 – Airborne IPS System and IPS Core External and Internal Interfaces

Interfaces are considered external when they are located between the Airborne IPS System and other airborne systems (e.g., aircraft avionics and communication systems). Interfaces are considered internal when there are located between components within the Airborne IPS System.

The following sections provide an overview of external and internal interfaces and provide pointers to relevant implementation guidance.

3.7.1 External Interfaces

The external interfaces between the Airborne IPS System and other airborne components include the following, where the reference in square brackets refers to the interface designators shown in Figure 3-13:

- Interface with Existing Datalink Applications [IF-1] – located between the Airborne IPS System Application Adaptation function and existing applications (e.g., FANS-1/A, B1/B2).
- Interface with Native IP Applications [IF-2] – located between the Airborne IPS System network stack and future Native IP applications.
- Interface with Airborne Radios-Data [IF-3] – located between the Airborne IPS System Datalink Adaptation functions and Airborne Radios. This interface is used for data flows, and the interface protocols and services shall comply with radio-specific ARINC Standards.
- Interface with Airborne Radios-Control [IF-4] – located between the Airborne IPS System non-Core management functions and Airborne Radios. This interface is used for radio management control flows, and the interface protocols and services shall comply with radio-specific ARINC Standards.
- Interface with Other Avionics Systems [IF-5] – located between the Airborne IPS System non-Core functions and other aircraft avionics systems.
- Interface with Redundant Airborne IPS System [IF-6] – located between two Airborne IPS Systems to support the exchange of status and synchronization information between systems in a redundant configuration.

Since the external interfaces are dependent on the aircraft architecture, further details and implementation guidance are provided in Section 5.3.

3.7.2 Internal Interfaces

The internal interfaces among functional components within the IPS Core include the following, where the reference in square brackets refers to the interface designators shown in Figure 3-13:

- Interface between the Application Adaptation function and the Network Stack [IF-A]
- Interface between the IPS Communications Manager and the Network Stack [IF-B]
- Interface between the Datalink Adaptation function and the Network Stack [IF-C]
- Interface between the Air-Ground IPS Management Application (reference ICAO Doc. 9896) and the Network Stack [IF-D]
- Interface between the IPS Core and Non-Core IPS functions [IF-E].

All internal interfaces are a local, implementation-specific decision that is that is highly dependent on the host platform architecture, which may be driven by the airframe OEM, the Airborne IPS System supplier, or a combination of both. The following are possible options for implementing the interfaces:

- Queueing/sampling ports of a Real-Time Operating System (RTOS), e.g., ARINC 653-based RTOS
- Virtual links in an Integrated Modular Avionics (IMA) architecture
- Application Programming Interface (API) provided by a respective function, e.g., network stack.

3.8 Core IPS Performance Requirements

The Airborne IPS System, especially the IPS Core components, are expected to contribute to the overall performance requirements specified for current and future ATS services.

COMMENTARY

No specific performance requirements are identified yet for AOC services.

Existing specifications including RTCA DO-306/EUROCAE ED-122 (for FANS1-A), RTCA DO-290/EUROCAE ED-120 (for B1), and RTCA DO-350A/EUROCAE ED-228A (for B2) allocate a specific performance to the airborne segment; however, the performance requirements are usually described from an end-to-end perspective only. ATN/IPS routing performance depends on the architecture and implementation, considering the end-to-end constraints. Therefore, a detailed apportionment of performance requirements (e.g., availability, transaction time, etc.) on all components of the IPS network is provided in the IPS MASPS (RTCA DO-XXX and EUROCAE ED-YYY).

Performance requirements allocated to the airborne segment usually apply to the airborne segment in its entirety. Therefore, it is recommended that implementers of the core Airborne IPS System provide sufficient margins that consider other system components (e.g., datalink applications, airborne displays, airborne radios, etc.) and the physical links between these components.

In addition, overall Airborne IPS System performance must consider, as a minimum, the following key parameters and criteria:

- Number of simultaneous transport-layer “connections” and associated security contexts
- Number of IP packets routed per time unit
- Number of application level messages per time unit
- Time duration for establishing/releasing a secured “connection”
- Time duration for establishing a path towards a specific destination (i.e., mobility solution convergence time)
- Time duration for handover between links in a multilink environment (i.e., the time before an application can start sending messages using a new link)
- Time duration for link-level handovers
- Impact of prioritization/QOS management

- Congestion management (particularly when using low speed and bandwidth-constrained links like VDLM2).

4.0 AIRBORNE IPS SYSTEM SECURITY

4.1 Introduction

This section specifies security requirements for the Airborne IPS System. The objective is to provide information for implementers to integrate IPS security into a system security architecture, consistent with the security provisions specified in ICAO Doc. 9896.

COMMENTARY

This document focuses on the security measures for the Airborne IPS System within an aircraft avionics system environment. References to security measures hosted by other avionics or by ground systems are provided for overall context and information only.

The security architecture described in this section considers only Intentional Unauthorized Electronic Interference (IUEI, as defined in RTCA DO-326A and EUROCAE ED-202A). Security mechanisms to mitigate physical security threats are implementation-specific and out of scope of this document.

Commented [OML22]: Ed. Note: Added per THA recommendation to improve clarity

4.2 Security Architecture Overview

This section describes the security scope for the Airborne IPS System by identifying its security perimeter and the security environment.

The Airborne IPS System has logical interfaces with different aircraft-external entities via multiple air-ground access networks. These logical interfaces are implemented via physical interfaces to one or more Airborne Radios, which implement the airborne component of the air-ground access networks. These radio systems connect to the Airborne IPS System either directly (e.g., via ARINC 429 interfaces) or using an airborne local network (e.g., via an ARINC 664 network); both interconnection methods are described in further detail in the implementation guidance in Section 5.0.

The radio systems and ground-based interfaces are considered threat sources for the Airborne IPS System. From these interfaces, an attacker may attempt to spoof, tamper, or disclose information; initiate denial of service (DoS); or elevate privileges. Attacks from the on-board AISD are not considered in this secure environment as the connection with the AISD is related to the specific airframe architecture. Since ATN/IPS can coexist with ACARS and other existing aircraft systems as described in the architecture options in Section 5.0, avionics implementers should consider the security of the context of the overall aircraft systems.

Commented [OML23]: 22-Feb (T.Bauge) – Add "repudiate" after tamper to cover all the elements of STRIDE

To support a defense-in-depth security strategy, the baseline requirement for the overall IPS security architecture is that a minimum of two layers of security shall be incorporated into the design to protect communications from Intentional Unauthorized Electronic Interference (IUEI, as defined in RTCA DO-326A and EUROCAE ED-202A). It is expected that one of these security layers provides end-to-end security.

COMMENTARY

The ICAO WG-I Security Subgroup is developing ICAO Doc. 10145, *Security Risk Assessment for Aeronautical Communications*, which will identify mitigations necessary to reduce security risk to an

acceptable level. Once Doc. 10145 is available, additional security requirement detail and/or cross-references will be included in a future supplement to this document.

As illustrated in Figure 4-1, the overall IPS System security architecture includes both application-level and datalink-level security mechanisms.

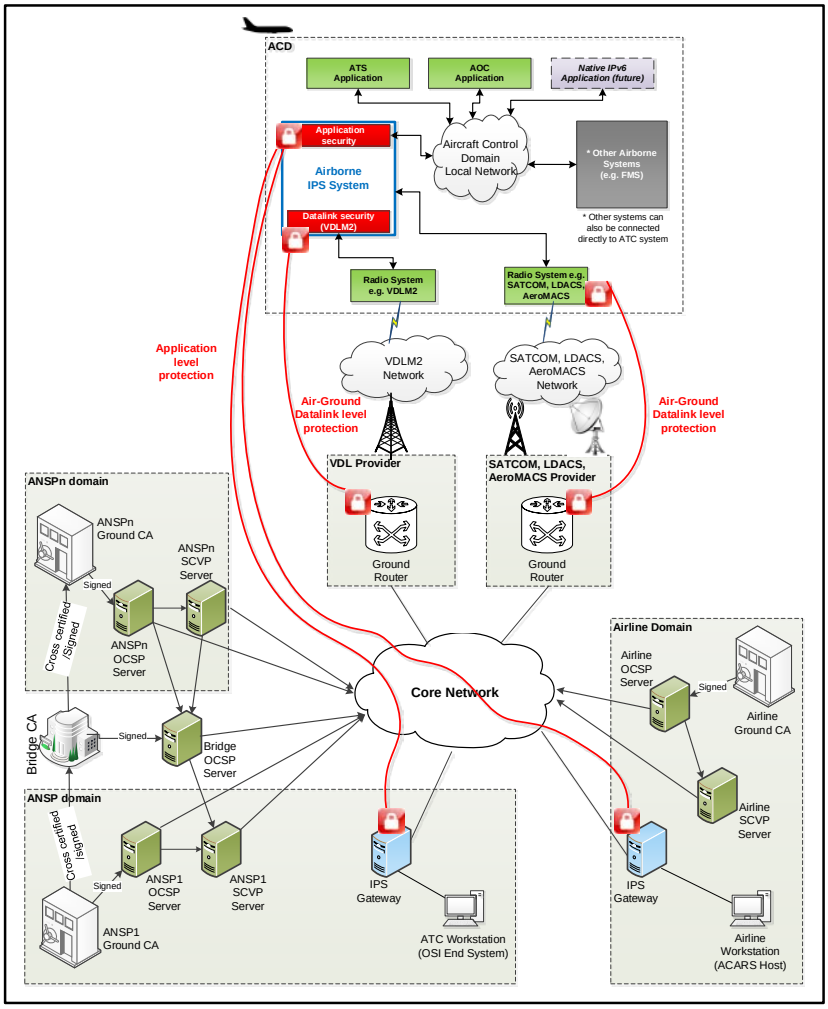

Figure 4-1 – IPS System Security Architecture Overview

Commented [ML24]: Ed. Note: Per a FREQ recommendation, figure updated to clearly show that IPS GW is communicating with an "OSI End System" and "ACARS Host."

Application-level security is intended to meet the requirement for providing end-to-end security between the Airborne IPS System and peer Ground IPS Host. The datalink-level security controls provide security over the air-to-ground access network. As shown in the diagram, the datalink security mechanisms are generally

handled by the radios, with the exception of VDLM2 where the security mechanism is expected to be hosted by the Airborne IPS System (refer to Section 5.3.2.3 for additional detail).

COMMENTARY

Network security is out-of-scope of this specification. However, as noted previously in Section 2.3.2, inter-network security mechanisms are specified in ICAO Doc. 9896 for ground-ground communications that cross administrative domains.

While the IPS System security architecture diagram shows ANSP-hosted and airline-hosted IPS Gateways, a service provider-hosted IPS Gateway can serve as the ground security termination point for application-level security, acting as a security proxy on behalf of the ATC or AOC application hosts.

4.3 System Security Mechanisms

The Airborne IPS System employs multiple layers of security, which are described in the following sections.

4.3.1 Data and Control Plane Security

The Airborne IPS System assumes that the air-ground access networks are protected; however this is outside the scope of this standard (refer to Section 5.3.2.3 for guidance). The IPS network supports application or transport layer security using DTLS to ensure all data and control plane messages are received without modification. Based on TLS, DTLS is a protocol for securing UDP communications. The DTLS standard, any qualifications to the standards, and the required IPS cipher suite(s) are documented in the IPS Profiles (RTCA DO-379 and EUROCAE ED-262).

4.3.1.1 Session Establishment

The DTLS session establishment authentication sequence is described in the IPS Profiles (RTCA DO-379 and EUROCAE ED-262) and the associated RFCs referenced in the IPS Profiles.

4.3.1.2 Numbers of Sessions

The Airborne IPS System must support simultaneous security associations sufficient to accommodate concurrent operation of supported ATS and AOC applications (e.g., B1/B2, FANS-1/A, ARINC 623, AOC) including multiple application connections (e.g., ATS connections to current and next data authority and AOC connections to airline dispatch, airline maintenance, third-party engine provider, etc.). These application-level security associations are in addition to any air-ground access network connections that may be active, which is a concern only when the Airborne IPS System implements datalink-level security (e.g., VDLM2). CPU and memory resources should be sized such that these connections are possible, along with all active links with all available communication air-ground access networks, without degradation of operations.

COMMENTARY

The number of individual security associations between the Airborne IPS System and communicating peer Ground IPS Node is dependent on the IPS deployment, specifically whether security terminates at an IPS Gateway or at a Ground IPS Host. The closer that IPS terminates

Commented [OML25]: Ed. Note: Per THA recommendation, reference back to Section 2.3.2 to remind reader about ground-ground network layer security. (Same as commentary added to 3.3.2 per COL recommendation.)

Commented [ML26]: 28-Feb(B.Haindl) – Although Data and Control Plane Security is in the scope of 4.3.1 the following subsections describes IMHO data plane security only.

Commented [ML27R26]: [Laurent] Traffic outside of DTLS sessions like ICMPV6 traffic (such as Router Solicitation and Router Advertisement) is not taken into account in the DTLS VPN, maybe we have to be more accurate on Control plane definition.

[Timo] I agree with Laurent that there seem to be different views on the understanding of control plane. For example, if the IPS management application is considered control plane, the DTLS considerations apply. For mobility signaling and IPv6 control plane, DTLS, of course, does not apply. So, it may be worth check with Bernhard, whether some clarifications are sufficient to address his comment.

Commented [OML28]: Ed. Note: Text added per THA recommendation.

Commented [OML29]: 22-Feb (T.Bauge) – Highlight the need to consider admission control vs. graceful degradation approaches against operational requirements

to host systems, the more individual connections there may need to be. Refer to guidance in ICAO Doc. 9896.

4.3.1.3 Cryptographic Services

The Airborne IPS System implements confidentiality, mutual authentication, and data integrity cryptographic services to secure various air-ground applications. The Airborne IPS System functions as a DTLS client for both air-initiated and ground-initiated applications; refer to ICAO Doc. 9896 for a description of how ground-initiated applications operate with a client-only Airborne IPS System. The DTLS implementation uses the cipher suites and key exchange mechanisms that are specified in ICAO Doc. 9896 and applicable RTCA and EUROCAE IPS Profiles, and which are summarized in this document for convenience. Where multiple cipher suites are specified, a specific cipher suite is negotiated during DTLS session establishment, during which the DTLS client and server exchange priority-ordered lists and select a preferred cipher suite that is supported by both the Airborne and Ground IPS Systems; refer to ICAO Doc. 9896 for further details.

The following sections describe two operating modes that must be supported by the Airborne IPS System. Note that for both modes, the Airborne IPS System shall support the ECDHE key exchange mechanism with Elliptic Curve Groups secp256r1 and secp384r1 and the DHE key exchange mechanism with Finite Field Group ffdhe4096.

4.3.1.3.1 Authentication, Integrity, and Confidentiality Services

The Airborne IPS Systems shall support a mode of operation that provides authentication, message integrity, and message confidentiality services. The Airborne IPS System shall support the TLS_AES_128_GCM_SHA256, TLS_AES_128_CCM_SHA256, and TLS_AES_256_GCM_SHA384 cipher suites as defined in IETF RFC 8446.

4.3.1.3.2 Authentication and Integrity Only Services

The Airborne IPS System shall support an authentication and integrity only mode of operation where confidentiality services are not provided. This mode is applicable when encryption is restricted by national or international regulations or when messages are not considered sensitive and there is no strong need for confidentiality. To accommodate these cases, the Airborne IPS System shall support the TLS_SHA256_SHA256 and TLS_SHA384_SHA384 cipher suites[3], which do not use encryption but which provide application-level security by enforcing authentication and message integrity.

If a DTLS session is established initially with encryption and there is a subsequent need (e.g., crossing a geographic boundary where encryption is restricted) to downgrade to the authentication and integrity only mode, then the current session shall be terminated and a new session initiated without encryption. If a DTLS client initiates a secure session preferring encryption but encryption is not supported by the DTLS server, then the DTLS server response shall indicate that it supports authentication and integrity only for the current session, and the client shall accept the non-encryption mode.

[3] Reference https://www.iana.org/assignments/tls-parameters/tls-parameters.xml

Commented [OML30]: 22-Feb (T.Bauge) – If it is a *preference" only (i.e. the client offers non-encrypted cipher suites) then the normal outcomes of the negotiation with a server that doesn't support encryption is a non-encrypted session (and I'm not sure why it needs highlighting, it's what happens during negotiation). The more important question to my mind is what happens when there is no overlap, i.e. the client insist on an encrypted session and the server doesn't support it (or vice versa). Is this sentence intended to state that that will never happen, i.e. the client must always advertise non-encrypting suites? ← **Ed.** – As stated, if the client requests encryption but the server declines, then the client must accept a non-encryption mode.

Also is there a reason why the sentence deals only with one scenario when the reverse could also happen (client can't encrypt but server insists on encryption)? ← **Ed.** – Per Section 4.3.1.3, the Airborne IPS System MUST support both modes, so this case is not possible.

4.3.2 Network Filtering and Rate Limitation

The Airborne IPS System shall implement firewall function(s) that employ filtering and rate limitation mechanisms to limit access to only those services that are specified in ICAO Doc. 9896 Technical Manual and the IPS MASPS (RTCA DO-XXX and EUROCAE ED-YYY). These mechanisms protect the aircraft by limiting the attack surface.

COMMENTARY

The network filtering requirements and guidance specified herein for the Airborne IPS System may be applied to IPS Gateways and Ground IPS Hosts as well.

4.3.2.1 Packet Filtering

Packet filtering at Layer 3 is the process of controlling traffic to/from the Airborne IPS System by monitoring all incoming or outgoing packets and allowing only those packets that comply with predefined security policies. The filtering functions described in the following sub-sections may be implemented via one or more firewall applications.

It is recommended that the Airborne IPS System support stateful packet filtering.

4.3.2.1.1 IPv6 Filtering

The Airborne IPS System shall implement stateless IPv6 packet filtering for ingress and egress of all IPS dataflows. The IPv6 filtering implementation should be configurable to filter by the following items, as a minimum:

- Source and destination IPv6 addresses (e.g., allow only specified global-unique or care-of-addresses)
- Payload length (e.g., allow only if the payload length in the IPv6 header matches the actual payload data length)
- Next Header type (e.g., allow only if ICMP, UDP, or TCP (if enabled)),
- ICMPv6 (e.g., allow only supported packets per the IPS Profiles in RTCA DO-379 and EUROCAE ED-262)
- IPv6 Extension Headers (e.g., allow only supported extension headers, per the IPS Profiles in RTCA DO-379 and EUROCAE ED-262)

4.3.2.1.2 UDP Filtering

The Airborne IPS System shall implement a stateless packet firewall for ingress and egress of all UDP packets. The UDP filtering implementation should be configurable to filter by the following items, as a minimum:

- UDP port number (e.g., allow only if UDP destination port number matches the expected application)
- UDP checksum (e.g., allow only if UDP checksum and hash of message match)
- UDP length field (e.g., allow only if UDP Length equals the length of the header plus the data payload)

Note that a UDP checksum value of all zeros should be interpreted as invalid. Unlike IPv4 which uses all zeros to indicate that the UDP checksum field is unused, the IPv6 Pseudo Header can never be all zeros.

Commented [ML31]: 28-Feb(B.Haindl) – Why is required to implement a firewall for egress UDP traffic?

Commented [ML32R31]: [Laurent] It is a request from Boeing to cover filtering not only between ACD domain and Ground but also between AISD and ACD domains.

[Timo] I also remember that this part came from Boeing. Beyond AISD considerations, there may be two further benefits:
• The aircraft contributes to the protection of the CSP / ANSP by not permitting unauthorized traffic to leave the aircraft.
•Violations of corresponding rules may support incident detection and forensic investigations (assuming rule violations are logged).

4.3.2.1.3 TCP Filtering

If TCP transport is disabled, then the Airborne IPS System shall block all TCP traffic.

If TCP transport is enabled, then the Airborne IPS System shall implement a stateful packet firewall for ingress and egress of all TCP packets. The TCP filtering implementation should be configurable to filter by the following items, as a minimum:

- TCP Port number (e.g., allow only if TCP destination port matches the expected application)
- TCP checksum (e.g., allow only if the TCP checksum and the hash of the header, pseudo header and payload match)
- TCP State (e.g., allow only TCP session establishment before data push)
- TCP sequence number (e.g., block if a replay attack is detected)
- TCP Acknowledgement number (e.g., block acknowledgement of a packet that was not sent)

Note that a TCP checksum value of all zeros should be interpreted as invalid. All-zero results are not possible since the IPv6 Pseudo Header can never be all zeros.

4.3.2.2 Payload Inspection and Filtering

Packet filtering at Layer 3 protects only against unauthorized ports and addresses being allowed through the firewall since only the packet header is evaluated. It does not protect against injection of malicious or malformed data via the payload of the packet. To provide enhanced protection against this threat, payload inspection, also known as deep packet inspection (DPI), should be considered. Payload inspection typically happens at the application layer. A combination of application whitelisting and DPI can provide more robustness against this attack vector.

4.3.2.3 Rate Limiting for Security

The Airborne IPS System shall protect itself from denial-of-service attacks originating from the ground. It should be capable of implementing a rate limit function for UDP, TCP, and ICMP flood attacks.

COMMENTARY

The Airborne IPS System implementation assumes that IPS ground systems provide some protection against flooding attacks, which could result in network performance degradation or denial-of-service conditions.

Rate limiting is applied to prevent malicious or errant network traffic from consuming excessive CPU time and filling storage space that would otherwise be available for logs. A suitable rate limiting algorithm (e.g., Token Bucket, Leaky Bucket, Fixed Window, Sliding Window Log, etc.) should be selected and algorithm-specific parameters (e.g., total capacity in the case of a Token Bucket algorithm) should be configurable to support tuning. The individual rate limits on different types of traffic are set to prevent one type of dropped traffic from filling the log and masking other types of dropped traffic. However, these considerations must be balanced against the need to provide enough information in the logs to be useful for incident response and forensics investigations.

For UDP typical rate limiting settings include but are not limited to:

Commented [ML33]: 28-Feb(B.Haindl) – Rate limiting can have negative impact on control plane procedures e.g. convergence time for IPv6 reachability information. For example, if UDP is blocked for a certain time then no control information can be handled during this time. In such a case UDP threshold/blocking has to differentiate between data plane traffic and control traffic or has to be implemented on specific UDP ports.

Commented [ML34R33]: [Laurent] The Rate limiting function is the chicken and egg problem like many security functions. The rate limiting rules configuration will have to be fine-tuned to thwart negative impact on critical safety traffic. We have the same problem with chapter 4.3.2.2 that will be more tricky to manage. Moreover, the end of the comment "UDP threshold/blocking has to differentiate between data plane traffic and control traffic or has to be implemented on specific UDP ports" shows me that I have a misunderstanding of what is control plane.

[Timo] Of course, defining an appropriate rate limitation policy is a challenge. Rules may distinguish ICMP vs. UDP, different UDP ports, and different source IP addresses. Again, it may be worth checking with Bernhard, whether some clarifications are sufficient to address his comment.

Commented [OML35]: 22-Feb (T.Bauge) – This sentence seems to be about log entry rate limiting, not data plane traffic rate limiting.

Commented [ML36R35]: Ed. – My interpretation is that we don't want multiple log entries generated by rate limiting on one type of traffic filling up the logs.

Commented [OML37]: Ed. Note: Per THA comment, existing text reworded to provide flexibility and not appear to impose limits on possible settings. Same change for TCP and ICMP below.

- UDP Threshold (UDP Packets/Second): The average rate of UDP packets-per-second sent to the Airborne IPS System that triggers UDP Flood Protection (i.e., packets exceeding this rate will be dropped). The average can be calculated over a configurable period of time (e.g., when using Sliding Window Log), or it can be represented by an algorithm-specific value (e.g., filling rate when using Token Bucket)
- UDP Blocking Time (Seconds): The duration of time that UDP packets exceed the rate threshold, after which the UDP Flood Protection is activated causing the Airborne IPS System to start dropping UDP packets
- UDP Rate Limited Applications: The set of targeted applications that shall be rate limited to mitigate the consequences of UDP flood

The UDP Threshold should be set globally, per IP address, or per application (e.g., based on UDP port number associated with a specific source IP address).

If TCP transport is enabled, typical rate limiting settings include but are not limited to:

- TCP Threshold (TCP Packets/Second): The average rate of TCP packets-per-second sent to the Airborne IPS System that triggers TCP Flood Protection (i.e., packets exceeding this rate will be dropped). The average can be calculated over a configurable period of time (e.g., when using Sliding Window Log), or it can be represented by an algorithm-specific value (e.g., filling rate when using Token Bucket)
- TCP Rate Limited Applications: The set of targeted applications that shall be rate limited to mitigate consequence of TCP flood.

When TCP is disabled, the TCP Threshold shall be zero.

For ICMP typical rate limiting settings include but are not limited to:

- ICMP Threshold (ICMP Packets/Second): The average rate of ICMP packets-per-second sent to the Airborne IPS System that triggers ICMP Flood Protection (i.e., packets exceeding this rate will be dropped). The average can be calculated over a configurable period of time (e.g., when using Sliding Window Log), or it can be represented by an algorithm-specific value (e.g., filling rate when using Token Bucket)

These settings should be configurable to adapt rate limitation to each aircraft platform; refer to Section 3.5.4.

4.3.3 Data Flow Segregation

The Airborne IPS System shall segregate data flows to prevent interference between data flows, threat propagation, and bypassing of security measures.

Data flows shall be segregated by destination for each type of service. To segregate safety and non-safety traffic, separate security sessions should be established and maintained throughout the communication between communicating air and ground entities. Message integrity, mutual authentication, confidentiality (optional), and non-repudiation (optional) must be handled uniquely for each separate endpoint. For example, B1 application traffic exchanged with a local ANSP is conveyed over one DTLS session, while ACARS AOC messages exchanged with an aircraft operator are conveyed using a different DTLS session. Both sessions can be active at the same time.

Commented [ML38]: 22-Feb (T.Bauge) – Would this example be more compelling if both sessions used the same IPS ground gateway (in which case there is actually scope for security session re-use… as it is currently described, it's not obvious that reuse is possible).
(Relates to a comment in Section 4.4.1.1.3.)

AISD traffic is outside the scope of this document, but not precluded from traversing the IPS network. However, if AISD traffic is expected to traverse the IPS air-to-ground link, it should make use of similar data flow segregation, namely the use of secure sessions between end points facilitated by application, transport, and/or network layer security controls to isolate and protect the data from malicious interference.

For the detailed design of the Airborne IPS System, segregation of data flows between the Airborne IPS System and other connected aircraft systems shall be considered carefully.

COMMENTARY

The Airborne IPS System has interfaces with different aircraft systems such as communication systems, systems hosting safety services applications and other avionics. Depending on aircraft architecture, these interfaces may rely on shared networks. If data flows are not appropriately segregated, the Airborne IPS System may allow for threat propagation among aircraft systems or may allow to bypass the IPS-specific security measures.

Data flows may be segregated by different means depending on how the interfaces between the Airborne IPS System and other aircraft systems are implemented, which is described in Section 5.2. For example, ARINC 429-based architectures may take advantage of the physical segregation provided by point-to-point ARINC 429 links. ARINC 664-based networked architectures may take advantage of logical segregation measures such as virtual links or VLANs if an appropriate level of assurance, commensurate with the protection needs identified by security risk evaluations, is demonstrated. Logical segregation may need to be complemented by physical segregation when logical segregation measures alone do not provide a sufficient level of assurance.

4.3.4 Access Control Lists

In the Airborne IPS System, Access Control Lists (ACLs) may be used for several purposes such as prioritizing traffic for QoS, triggering an alert, restricting remote access, debugging, secure tunnel, etc. Use and implementation of ACLs within the Airborne IPS System is left to the system implementer, and the detailed specification of ACLs is outside the scope of this document.

Commented [ML39]: 28-Feb(B.Haindl) – Although managing ACL is out of scope, I would like to mention its problem: Every change has to be consistently applied (e.g. how you want to handle what IPv6 source addresses of incoming packets are expected if a new ground source is added to the overall IPS system.

An illustrative example of a traffic ACL is described in the following bullets:

- The Airborne IPS System obtains source and destination IPv6 addresses from a packet, and it compares the addresses with respect to expected addresses under a specific condition
- If the packet did not arrive from an expected IPv6 prefix/address or if it is not intended for the Airborne IPS System, then the packet is discarded immediately and the event is logged in the security log
- If both addresses match what is expected, then find an entry for the destination address in a forwarding table.
- If a match is found, then forward the packet. If no match is found, then discard the packet immediately and log the event in the security log.

4.4 Security Support Functions

This section describes the support functions necessary to enforce the protections against malicious electronic interaction and to meet overall security requirements. The support functions include:

- Cryptographic Key Management
- Security Logging.

Security Configuration Management is addressed in Section 3.5.4 as part of the overall Configuration Settings Management function.

4.4.1 Cryptographic Key Management

Since the security mechanisms specified in Section 4.3.1 utilize cryptographic keys to protect communications between the Airborne IPS System and communicating peer entities, a supporting cryptographic key management function is necessary for key/certificate management operations and maintenance. This key management function must address the generation, storage, protection, transfer, usage, and destruction of private keys and their associated X.509 certificates. A guiding principle is to perform key management activities in a secure manner that minimizes airline maintenance activities and ensures safety. For example, it should support over-the-air update capability to remotely manage keys. The key management functions should rely on industry standards, including:

- Manual of Public Key Infrastructure (PKI) Policy for Aeronautical Communications (ICAO Doc. 10095)
- IPS Profiles (RTCA DO-379 and EUROCAE ED-262)

COMMENTARY

The ICAO WG-I Security Subgroup is developing ICAO Doc. 10095, *Manual on PKI Policy for Aeronautical Communications*, which will specify IPS certificate profiles and key/certificate handling requirements. Once ICAO Doc. 10095 is available, additional key management detail and/or cross-references will be included in a future supplement to this document.

The following sub-sections describe the key management life-cycle processes for the management of private keys and associated public key certificates. There are two primary approaches for the key management function. The Airborne IPS System can implement the function locally for its own purposes, or it can leverage a centralized key management function that is made available for use by multiple on-aircraft systems. The local and centralized key management approaches are described in Sections 4.4.1.1 and 4.4.1.2, respectively.

4.4.1.1 Local Key Management Function

If no centralized key management function is available or if it shall not be used, then the Airborne IPS System shall implement the cryptographic key management function locally. The following sub-sections describe the key management life-cycle processes.

4.4.1.1.1 Key Generation

The Airborne IPS System must use securely generated public-private key pairs for protecting the ATN/IPS end-to-end communication. The keys shall be generated securely in accordance with ICAO Doc. 10095.

COMMENTARY

Different designs for the generation of keying material are feasible. The Airborne IPS System may generate public-private key pairs itself or, alternatively, it may rely on a secured LRU (e.g., a smart card) to provide securely generated public-private key pairs.

The Airborne IPS System should create an ITU-T X.509 Certificate Signing Request (CSR) for a public-private key pair that is to be used by the Airborne IPS System. The CSR parameters should be customizable by FLS (Field Loadable Software) to adapt to certificate profiles (e.g., common name, object identifiers, etc.) in accordance with ICAO Doc. 10095 provisions and guidance.

Re-keying, subsequent to initial key generation, is the process by which a new public/private key pair is generated and a new certificate is issued. The Airborne IPS System should rekey when the system does not have appropriate credentials to communicate with the peer entities. The reasons may include, but are not limited to:

- The Airborne IPS System has no private key and/or associated public key certificate
- The current key pair is suspected to be compromised
- The certificate contains the wrong aircraft identifier (e.g., subsequent to maintenance action that includes avionics equipment replacement)
- The certificate is expired or is about to expire.
- Other circumstances for certificate re-keying as specified in ICAO Doc. 10095.

The Airborne IPS System should initiate re-keying automatically when its certificate is about to expire. It should start to perform re-keying within a delta-time before certificate expiration, and the delta-time should be customizable via FLS.

In addition, the ability to inhibit re-keying should be configurable via FLS. For example, it should be possible to inhibit re-keying during flight to prevent re-keying-related operational failures while in-flight.

4.4.1.1.2 Key Information Storage, Access Control, and Export

The Airborne IPS System must store key information securely in accordance with ICAO Doc.10095. This includes protecting the integrity of all key information that is stored locally by the Airborne IPS System, as well as protecting the confidentiality of private keys and secret keys.

COMMENTARY

Private keys are stored in persistent memory (i.e., the key remains intact when power is removed) for the duration of its crypto-period or until the private key is replaced via rekeying. Secret keys, which are generated as a result of DTLS session establishment with a peer communicating entity, are stored in non-volatile memory for the duration of the secure association.

Access to the key management function and associated key information should be subject to access controls within the Airborne IPS System. Access shall be limited to only those functions with a legitimate need to access key information.

The Airborne IPS System shall not permit the export or transfer of private keys or secret keys outside of the system via electronic communication protocols.

COMMENTARY

If the Airborne IPS System is implemented using a redundant configuration, then key information may need to be stored redundantly and synchronized among different parts within the system. A redundant configuration requires security considerations to ensure that the design does not expose private keys or secret keys outside of the system. Refer to Section 3.5.5.1 for considerations.

4.4.1.1.3 Certificate Signing Request Export and Certificate Import

The Airborne IPS System generates a Certificate Signing Request (CSR) whenever a public-private key pair is generated, either initially or in response to a re-key request (e.g., either locally or via a key management request using the Air-Ground IPS Management Application, per ICAO Doc. 9896, or the EST protocol, per RFC 7030 adapted for DTLS/UDP). The CSR, which is a request sent to a CA to obtain a public key certificate, contains the generated public key, key usage information, identifying information for the Airborne IPS System, and a digital signature that provides proof-of-possession of the corresponding private key.

For a generated CSR, the Airborne IPS System should export the CSR and import the issued public key certificate using either of the following options, which are illustrated in Figure 4-2:

- Automated – Sending a CSR over a network connection to a CA and retrieving the public certificate from the CA. While the network connection to send a CSR may need to be secured (e.g., to ensure authenticity of the CSR request), retrieval of the public certificate may not need to be secured since the certificate is signed by the CA and does not contain confidential information. The specific protocols to be used should be customizable via FLS.
- Manual – Using a Local Management Function (LMF) to export the CSR generated by the Airborne IPS System and then import the public certificate.

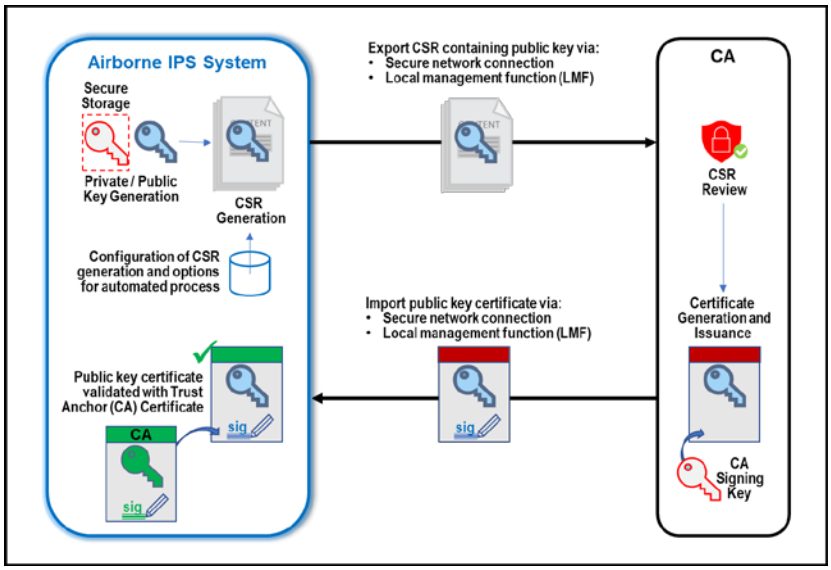

Figure 4-2 – CSR Export and Public Key Certificate Import

The certificate request, issuance, and installation processes should follow the best practices described in ICAO Doc.10095. The issued certificate is in Distinguished Encoding Rules (DER) format per ITU-T X.690.

The Airborne IPS System should implement an option to accommodate cases where a secure communication channel cannot be established with a remote entity supporting certificate management for CSR export and certificate import. These cases include initial key generation (i.e., when the system does not yet have keys/certificates), if the current private key is compromised, or if the associated public key certificate is revoked, e.g., public certificate is rejected by the communicating peer Ground IPS Host or IPS Gateway. Under these conditions, rekeying of the Airborne IPS System may need to be performed manually (e.g., using an LMF to initiate generation of a new key pair, export a CSR, and receive an issued certificate).

If the existing private key is not compromised and the associated public key certificate is not revoked, then the Airborne IPS System can be rekeyed using the automated process for CSR export and certificate import. Depending on customization, this may be accomplished using an operational DTLS session, where one or more operational DTLS sessions established between the Airborne IPS System and a Ground IPS Node supports certificate management services and an interface to a Certificate Management System. This is illustrated in Figure 4-3, and the remote key management messages are specified in ICAO Doc. 9896.

Commented [ML40]: 22-Feb (T.Bauge) – In 4.3.3 we stated that applications should not share DTLS sessions for segregation reasons. Is this contradicting that statement? Do we need a commentary on 4.3.3 to declare an exception and reference this section?

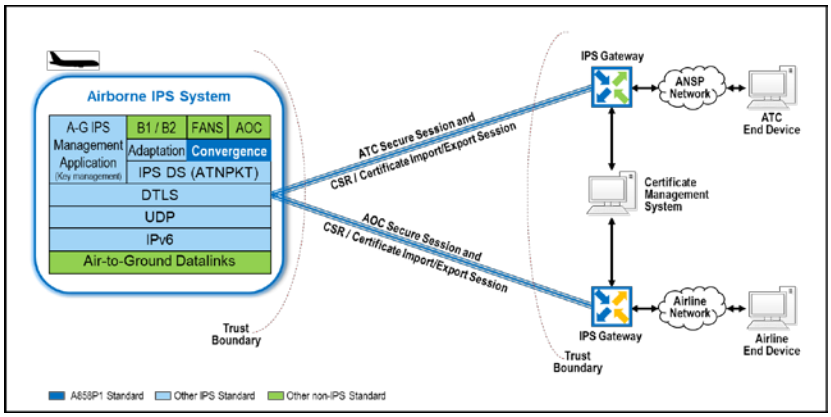

Figure 4-3 – Rekeying Using an Operational DTLS Session

Alternatively, the Airborne IPS System may use a secure session directly with a Certificate Management System, as illustrated in Figure 4-4. This process should use a certificate management protocol to perform the certificate management services. At a minimum, the Airborne IPS System should support the “Enrollment over Secure Transport” protocol (reference RFC 7030), possibly adapted for usage over DTLS. For this protocol, the parameters for accessing the Certificate Management System should be customizable via FLS.

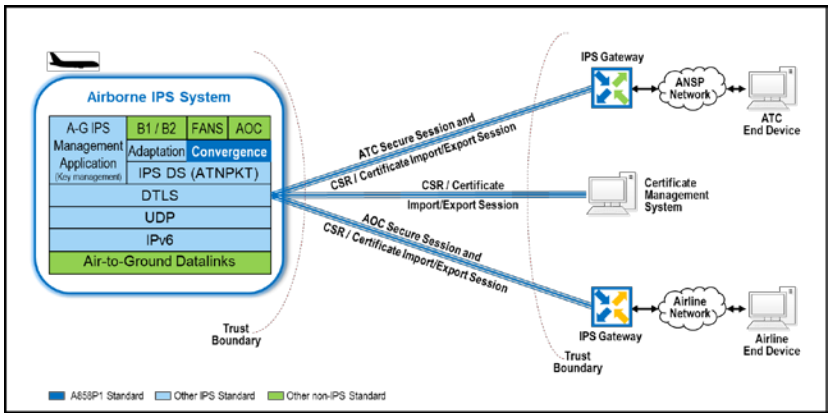

Figure 4-4 – Rekeying using a DTLS Session with a Certificate Management System

4.4.1.1.4 Trust Anchor Certificate Provisioning

For certificate validation, the Airborne IPS System requires trust anchor certificates. The provisioning of trust anchor certificates is implementation-specific, but the process must be considered carefully since the security level of the end-to-end communication depends on secure provisioning.

Prior to initial key generation, the avionics manufacturer may preload trust anchor certificates for all valid IPS-related CAs. Subsequently, the trust anchor certificates

should be data loadable via FLS, which is out-of-band and segregated from the device certificate management process, or they may be loaded remotely over the air.

Chapter 5-13-3 and Appendix A-4, Section 6.1.9 of ATA Spec 42 contains best practice guidance for distribution of trust anchor certificates.

4.4.1.1.5 Certificate Revocation Check

The Airborne IPS System should check the certificate status of a certificate during certificate validation, which requires revocation information. The Airborne IPS System should support checking the revocation of certificates via the Online Certificate Status Protocol (OCSP) Stapling, and it may support Certificate Revocation Lists (CRLs). With OCSP Stapling, the ground peer includes revocation status information in the DTLS handshake to be used by the Airborne IPS System. For CRL-based checks, the Airborne IPS System requires access to CRLs. The transfer of CRLs to the avionics is implementation-specific and not described further in this document.

COMMENTARY

The need for certificate revocation checks may be relaxed if the certificates for IPS ground entities are short-lived. Refer to ICAO Doc. 10095 regarding the use of short-lived certificates.

Depending on ground architecture, CRL Distribution Points may only be accessible via TCP transport. If an Airborne IPS System does not support TCP but requires access to CRLs, then the system must implement an alternative means for retrieving CRLs.

The use of OCSP Stapling may allow the Airborne IPS System to avoid the use of CRLs if the implementation supports multiple Certificate Status Request (i.e., to include the entity certificate and all intermediate CA certificates within the same DTLS handshake).

4.4.1.1.6 Key Usage and Certificate Validation

The Airborne IPS System should use a dedicated private key and associated certificate for the end-to-end communication. This key pair should be used exclusively for this purpose, meaning that the scope of the key shall be limited to end-to-end security.

The Airborne IPS System should validate any certificate it processes. The two main use cases for certificate processing are: importing a certificate for the Airborne IPS System as a response to a Certificate Signing Request and authenticating a ground peer for establishing an end-to-end secure channel.

When importing a certificate for the Airborne IPS System, the Airborne IPS System should check the following properties.

- The certification path is validated in accordance with the IPS Profiles (RTCA DO-379 and EUROCAE ED-262)
- The certification path starts with a certificate (i.e., trust anchor certificate) that is trusted by the Airborne IPS System
- The certificate matches the certificate profile for Airborne IPS Systems as defined by ICAO Doc. 10095

Commented [OML41]: 01-Mar(Madhu): Requires air to ground means as well as ground infrastructure; need to add the details for provision and mechansim to support cert validation related to CRL. Propose some of this requirement to be moved to DOC 9896 and MASPS and develop the needed box level detail in Suppliment 1 of PP858.

Commented [ML42]: 28-Feb(B.Haindl) – Just for my understanding: What happens if OSCP does not work within time? Fail-Safe or Fail-Secure -> meaning still use the last valid public-key (certificate) for ongoing traffic or stop communication?

Commented [ML43R42]: [Laurent] The corner cases should be developed in the WG-108 document.

[Timo] I agree that this is a task for WG-108 (possibly to be covered in the foreseen "fail-secure / degraded modes" section in the MASPS). Personally, I expect that WG-I will move in a direction of short-lived ground certificates. So, we may even be able to remove OCSP considerations in Supplement 1.

- The X.509 notBefore date is before the current date
- The X.509 notAfter date is after the current date
- The certificate does not include an unknown X.509 extension that is marked as critical
- The certificate was issued for the aircraft of the Airborne IPS System
- The certificate was issued for the aircraft operator of the Airborne IPS System.

For authenticating a ground peer, the Airborne IPS System should check the following properties:

- The certification path is validated in accordance with the IPS Profiles (RTCA DO-379 and EUROCAE ED-262)
- The certification path starts with a certificate (i.e., a trust anchor certificate) that is trusted by the Airborne IPS System
- The certificate matches the certificate profile for a Ground IPS Host or for an IPS Gateway as defined by ICAO Doc. 10095
- The X.509 notBefore date is before the current date for each certificate in the certificate path
- The X.509 notAfter date is after the current date for each certificate in the certificate path
- No certificate in the certificate path includes an unknown X.509 extension that is marked as critical
- The leaf certificate was issued for the ground peer with which the Airborne IPS System wants to communicate
- No certificate in the certificate path was revoked.

4.4.1.1.7 Key Destruction

The Airborne IPS System should securely destroy stored secret and private keys upon different events, including but not limited to:

- Dedicated maintenance action
- Moving to a new private key upon successful completion of re-keying
- Detecting mismatches between the aircraft and aircraft information inside the certificate.

The key information should be destroyed securely in accordance with ICAO Doc.10095.

4.4.1.2 Centralized Key Management Function

The Airborne IPS System should use a centralized key management function when available on the aircraft. The centralized key management function may provide functions for generation, storage, protection, transfer, usage, and destruction of private keys and their associated certificates. The centralized key management function may use the Airborne IPS System as a Native IP application for its communication needs.

COMMENTARY

The centralized key management function may be closely integrated in the DTLS session establishment. For example, it may provide functionality to respond to challenges within challenge-response protocols. It may also provide functionality for validating certificates provided during the DTLS handshake.

The Airborne IPS System should use a protected interface between the Airborne IPS System and the centralized key management function. For example, the interface may rely on a segregated physical link. The scope of the centralized key management function and the definition of the interface is implementation-specific and not addressed further in this document.

4.4.2 Security Logging

The Airborne IPS System should implement security logging to support the detection of and the response to security incidents. Security logs should support the assessment of expected security events, the detection and dispositioning of abnormal behaviors, and the quantification of the impacts of detected security incidents. This section provides guidance for the Airborne IPS System by establishing a set of security related data elements and format(s) that are produced by the system and suitable for use by airline IT and/or avionics supplier analytical ground tools. The purpose of this section is to:

- Provide designers of the Airborne IPS System with a set of security logging guidelines
- Establish a baseline for security related data that should be logged
- Define the security and integrity of logs
- Consider log file formats that facilitate interoperability

Note that this section focusses on the generation, storage, transfer, and export of security logs, but it does not consider the analysis of security logs, which generally is performed by ground-based systems and tools.

4.4.2.1 Generation of Security Event Log Entries

The security related data to be logged is dependent on the aircraft architecture, system function, the aircraft security risk analysis, and the resulting security design solutions. Hence, this document can only give a baseline for security log entries, but it cannot be considered exhaustive.

When defining the detailed content of security log entries, the sensitivity of the information written to the log files should be considered. For example, secrets such as cryptographic key material should not be included in the log entries. In addition, Personally Identifiable Information (PII) should not be included unless the information is protected according to applicable standards, regulations, and laws.

4.4.2.2 Format of Security Event Log Entries

The format of security log messages is specified in Attachment 4 in this document.

4.4.2.3 Types of Security Event Log Entries

4.4.2.3.1 System and Service Lifecycle Events

The Airborne IPS System should record information on the lifecycle of the system and its services, including, but not limited to:

- Start-up and shutdown of the system and its services
- Results of self-tests performed at start-up
- Abnormal service failures (e.g., software crashes during runtime)
- System failures that affect the ability to perform security functions
- Information on the current configuration (e.g., aircraft identifier, hardware and software part numbers of the system, and unsigned hash or similar data of persistent files)
- Any change to its configuration (e.g., due to dataloading actions)
- Any change to the system time that is not caused by the system clock itself (e.g., time synchronization events)

4.4.2.3.2 Secure Channel

The Airborne IPS System implements secure channels to protect the data and control plane messages exchanged over the IPS network. It should record the following events, but not limited to:

- Successful and failed authentication attempts
- Closure information and errors related to the secure channels, including additional information on the reasons for the closure or error
- Resources used per secure session (e.g., the amount of data sent/received within a secure session).

4.4.2.3.3 Cryptographic Key Management

When starting, the Airborne IPS System should log the status of artifacts related to cryptographic key management. For example, it should log metadata on locally stored certificates (e.g., serial number, issuer name, expiration date, subject name, and subject alt name fields) and revocation data.

The Airborne IPS System should log any change to the status of artifacts related to cryptographic key management such as the creation of CSRs, the reception of CSR responses, and metadata on newly received revocation information (e.g., on an updated CRL or received OCSP response). This also includes, for example, renewals of cryptographic keys as part of session re-keying.

In aircraft implementations that use a centralized key management system, the Airborne IPS System logging design should consider logging performed by a centralized key management system so as to facilitate integrated log analysis across all relevant systems.

Commented [OML44]: Ed. Note: Text added per THA recommendation.

4.4.2.3.4 Network Communication

The Airborne IPS System shall record any change to the status of its network interfaces. For example, the starting and stopping of network interfaces should be logged as well as changes to IP addresses and routing information.

The Airborne IPS System shall record the identity (e.g., MAC and IP addresses) of network entities with which it communicates.

The Airborne IPS System shall log changes and failures of network connections. The logging of network communication events should be rate limited to prevent excessive logging that may result in resource exhaustion (i.e., a denial-of-service).

4.4.2.3.5 Filtering and Rate Limitation

The Airborne IPS System should record basic characteristics of traffic that is blocked due to filtering or rate limitation (e.g., network-level as well as on application level). For example, for dropped IPv6 packets, the Airborne IPS System should record IP addresses, protocols, packet sizes, a sampling of packet information and the reason for dropping the packet.

Rate limiting can also be used to preserve log storage. When used in this way, at least one complete log entry shall be logged for each burst. Subsequent instances of the same type of events may be logged using a simple counter function.

4.4.2.3.6 Performance Metrics

The Airborne IPS System should periodically record system performance metrics (e.g., processor, memory, and network utilization), which may allow identification of threats that affect the system performance (e.g., denial-of-service).

4.4.2.4 Storage of Security Event Log Entries

The Airborne IPS System should store the security log entries locally when not transferring the log entries to an on-board centralized log collector.

If the Airborne IPS System stores the security log entries locally, then it should:

- Ensure the integrity of the security logs at rest (e.g., cryptographically protect the log entries)
- Control the access to logs to prevent unauthorized access
- Store the log entries, and not schedule them for deletion, until the transfer to a ground system has been determined to be complete or the time-to-live of the log has expired
- Raise a maintenance message when the storage capacities for security logs are about to be exhausted and before time-to-live of the log is reached
- Record any commanded or routine deletion of stored security log entries.

4.4.2.5 Transfer and Export of Security Event Log Entries

Successful utilization of the Airborne IPS System security logs by, or on behalf of, an operator requires export of the logs from the aircraft on a regular and routine basis for ingestion into ground analytical tools. If the Airborne IPS System transfers the security log entries to an on-board centralized log collector, then the transfer should use a communication channel that is protected against threats.

If the Airborne IPS System stores the security log entries locally, it should allow automatic export of security logs from the aircraft via a secure method, without maintenance action, when ground connectivity is available. The transfer should use a secure channel that protects the integrity and confidentiality of the communication. The Airborne IPS System should also allow manual downloading of the security logs via a local maintenance device on-board.

Security logs may be sent in real-time to a ground-based server if the aircraft has an agreement with a ground entity, e.g., airline operations or Air-Ground Communications Service Provider (ACSP) that supports real-time logging. For cases where on-board centralized log collection is used, real-time log transmission is a function of the centralized system and is outside the scope of this document. When the Airborne IPS System sends logs to the ground directly, then RFC 6012, *DTLS Transport Mapping for Syslog*, may be used to transfer the logs securely via IPS air-ground access networks. If alternative air-ground access networks (e.g., non-safety communications) are employed, then the choice of a secure transport protocol is left to the implementer.

COMMENTARY

Even if logs are sent to the ground, there may be regulatory requirements to also maintain a local copy of the logs in the centralized system or in the Airborne IPS System. In addition, implementers should consider constraints associated with air-ground access networks to support real-time logging.

4.5 Security Design and Implementation Guidance

4.5.1 Security Assurance

The overall security level of a system depends on the quality of its design and implementation. Security assurance activities ensure that a system operates at the right level of security and help to prevent successful attacks on the system.

The Airborne IPS System should be developed according to (architecture-specific) security assurance requirements. While the precise security assurance requirements are specific to the aircraft architecture, RTCA DO-356A and EUROCAE ED-203A provide further guidance on security assurance and methods for determining the security assurance level (SAL).

COMMENTARY

NIST FIPS 140-3 and ISO/IEC 19790:2012(E) specify requirements for the secure design and implementation of cryptographic modules utilized within a security system, such as the Airborne IPS System. These documents identify key requirement areas, including: module boundary, algorithms, and policy; ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/compatibility; self-tests; design assurance; and mitigation of other attacks. The applicability of these security standards to achieve security design assurance of the Airborne IPS System is driven by an aircraft OEM, system integrator, and/or system implementer.

4.5.2 Data Loading Security

The Loadable Software Parts (LSPs) of the Airborne IPS System should be secured in accordance with ARINC Specification 835.

In particular, to counter threats related to tampering with a Loadable Software Part:

- Any LSP associated with the Airborne IPS System should be digitally signed

- The signature of an LSP should be verified before the part is installed on the Airborne IPS System.

The Airborne IPS System may receive verified Loadable Software Parts from an external data loader (e.g., airborne or portable data loader). It is not required for the Airborne IPS System to verify the authenticity and integrity of an LSP itself. The Airborne IPS System should use secured communication channels for receiving and internally distributing LSPs.

The ability of the Airborne IPS System to enter a data load state should be controlled strictly to ensure that only software from trusted sources can be loaded (see Section 4.5.5). This should include provisions for incorporating interlocks such as discrete logic (e.g., WoW, aircraft door open), mechanical Interlocks (e.g., Dataload Enable Switch), and/or ARINC 429 Input (e.g., ground speed).

4.5.3 Design for Cryptographic Agility

The Airborne IPS System should be designed for cryptographic agility in order to evolve and adopt alternatives to the cryptographic primitives without the need for Operating System patching, re-installation, or physical replacement of the Airborne IPS System. To facilitate this agility, cryptographic algorithms should be manageable separately from the IPS application. Conditions that may necessitate updates to the cryptography include, but are not limited to:

- A cryptographic algorithm is compromised
- The implementation of a cryptographic algorithm or supporting function (e.g., random number generator) creates a vulnerability
- New cryptographic algorithms that provide greater strength are introduced
- Existing cryptographic algorithms are deprecated.

Note that changes to crypto-algorithms and cipher suites must be coordinated between IPS air and ground entities to ensure continued interoperability.

4.5.4 Design for Geo-restriction Accommodation

The Airborne IPS System should be designed with flexibility to accommodate the different domestic encryption regulations of States around the world.

4.5.5 Resistance to Unauthorized Change

The Airborne IPS System equipment should be resistant to unauthorized change to maintain the integrity of its function, to protect its private key material from unauthorized disclosure, and to prevent alternation of security event logs. ARINC 827 and ARINC 835 provide applicable guidance.

To further enhance resistance to unauthorized change, the following three layers of aircraft software protection apply:

- Authenticity of software parts: ensuring that airplane software is tamper protected
- Access control to software parts: ensuring that airplane software cannot be improperly obtained
- Confidentiality of software parts: ensuring that airplane software is unusable, except for intended use.

5.0 AIRBORNE IPS SYSTEM IMPLEMENTATION OPTIONS

5.1 Overview and Assumptions

Since IPS is designed for safety services, the security, performance, and safety requirements have an impact on its implementation within a given avionics communications architecture. The continuing evolution of these architectures may necessitate different approaches for introducing IPS on different generations of aircraft.

Segregation between functions is a key feature that impacts Airborne IPS System architecture options. And, based on operational availability needs (i.e., to satisfy minimum equipment list (MEL) requirements) and/or the required Design Assurance Level (DAL) level, redundancy of the Airborne IPS System may need to be considered.

This section describes Airborne IPS System implementation options for federated and integrated avionics architectures based on the Core IPS function requirements described in Sections 3.0 and the IPS Security requirements described in Section 4.0. The intent is not to impose stringent avionics architectures on airframers and suppliers, but rather to highlight important considerations for defining acceptable IPS solutions.

5.2 Implementation Examples

This section presents two primary examples that are foreseen for the Airborne IPS System implementation, including:

- Federated Avionics Architecture
- Integrated Modular Avionics (IMA) Architecture

Note that these examples do not preclude airframers or suppliers from implementing a different approach.

5.2.1 Federated Avionics Architecture

Since IPS is a new network stack that is similar to the legacy ACARS and OSI network stacks, the existing ARINC 758-based Communications Management Unit (CMU), which hosts the ACARS and OSI communication stacks, is a candidate for hosting IPS as well. This approach minimizes the impact on existing aircraft avionics architectures since the CMU is updated to support IPS, but the interfaces with the applications, the radios, and the peripheral aircraft systems are reused. Since IPS is expected to replace the OSI protocol stack, this approach is advantageous for retrofit of OSI with IPS on legacy platforms that employ federated avionics. Dual-stack considerations and the role of the External Comm Manager are discussed further in Section 5.4.

The notional architectures in the following figures illustrate how the Core IPS functions may be integrated in an ARINC 758 CMU architecture, replacing the OSI stack, providing necessary security mechanisms, and co-existing in parallel with the ACARS stack. Note that ARINC 758 (Supplement 4 and later) supports both the ARINC 429 data bus and the ARINC 664 Ethernet interface. The use of Ethernet interfaces (i.e., ARINC 664 Part 2) may ease the integration in legacy architectures where switched Ethernet data networks (i.e., ARINC 664 Part 7) are less prevalent; however, additional security considerations may be applicable.

Commented [OML45]: 28-Feb (M.Niraula) – Figures (5-1, 5-2, 5-2, 5-10) assume that all communication between the AICF and legacy application has to be managed via "External Comm Manager", this give just one implementation depiction. It is quite possible to route message from AICF directly to legacy applications or peripherals without going through the external manager.

Commented [OML46R45]: Ed. – I think the existing text includes lots of cues for the reader to understand that diagrams are notional and just one possible approach. Showing overlays of multiple approaches within one diagram may get messy and potentially cause more confusion.

[Stephane P.] You are describing well the approach we have taken, assuming that we cannot cover all the avionics architectures, including the fact that the airframers/airframes may not want to share their detailed architecture in the standard. I think that, with the text provided in section 5, this should be enough for the standard.

COMMENTARY

AOC applications may be accommodated using the AICF, as shown in these figures, or an alternative approach. Refer to Section 3.2.

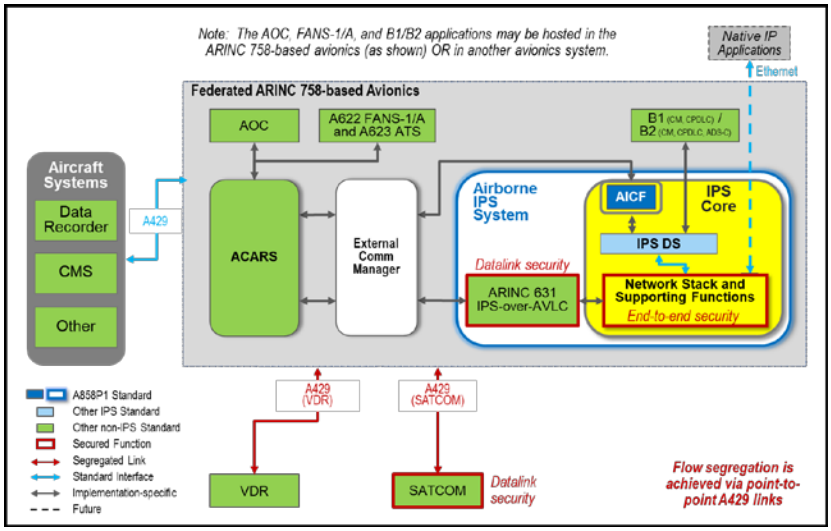

Figure 5-1 – Integration Example: IPS Integrated in Federated Avionics with ARINC 429 Interfaces to Communication Radios

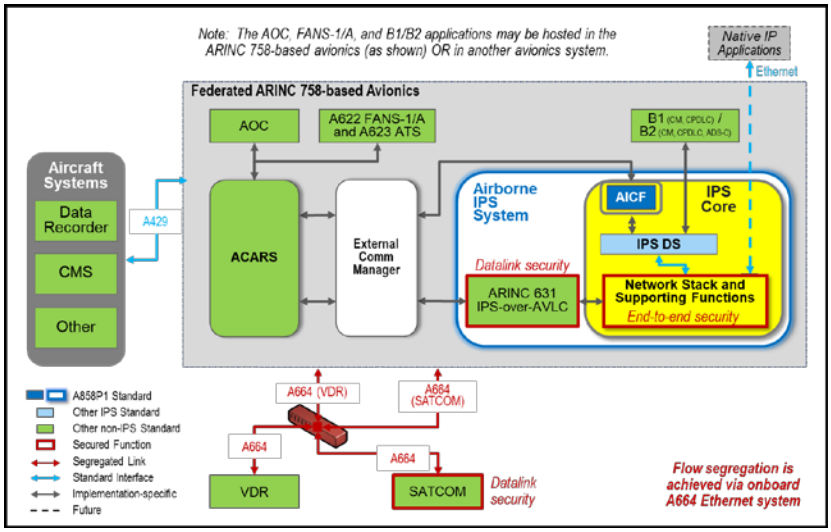

Figure 5-2 – Integration Example: IPS Integrated in Federated Avionics with ARINC 664 Ethernet Interfaces to Communication Radios

These examples also illustrate the integration of link-level security measures to protect the air-ground communications. These security measures are defined in the radio-specific standards. For example, ARINC Specification 631, VDLM2, describes the features necessary to support IPS including link security, which may be implemented in the federated avionics hosting ACARS and the Airborne IPS System (as shown in figures above) rather than in the VDR. Refer to Section 5.3.2.3 for additional security integration considerations.

COMMENTARY

ARINC Specification 631 (Supplement 9 and later) is expected to include the IPS-specific enhancements to existing VDLM2 functionality (e.g., AVLC) necessary to support ATN/IPS.

5.2.2 Integrated Modular Avionics (IMA) Architecture

The Airborne IPS System may be viewed as a function that can be hosted on various hardware modules such as shared computing resources. As illustrated in the figure below, the Airborne IPS System interfaces with other avionics systems using the ARINC 664 Part 7 Ethernet data network. Alternatively, but not shown, legacy radios may be connected to the Airborne IPS System using ARINC 429 data buses.

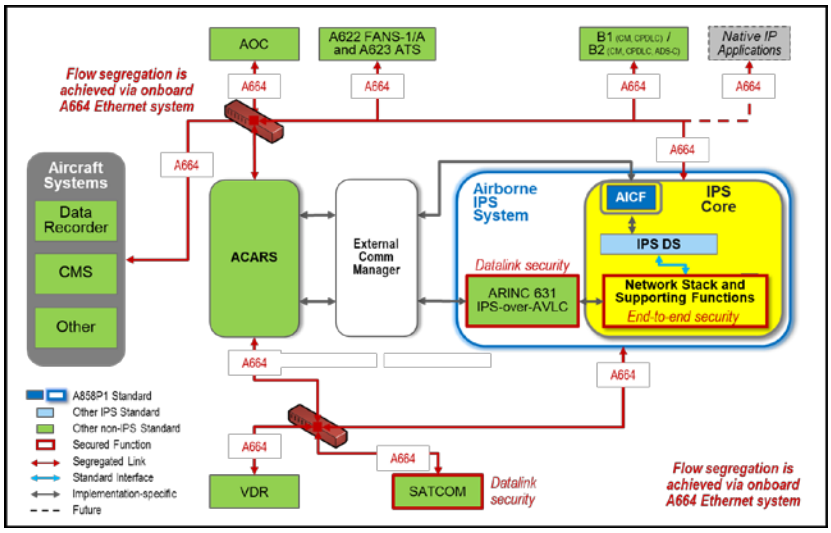

Figure 5-3 – Integration Example: IPS Integrated in an IMA Architecture

The figure illustrates the case where the ARINC 664 Ethernet data network is split in two to reinforce the segregation between the radios and the other avionics systems. Note that segregated networks may necessitate additional security measures to allow radio systems attached to one network to access shared or centralized functions (e.g., centralized dataloading, CMS, FWS, etc.) provided by avionics systems attached to the other network. Since the figure is intended to be notional, an alternative is to combine the separate switches into one switch, as long as the flow segregation among systems is managed properly.

5.0 AIRBORNE IPS SYSTEM IMPLEMENTATION OPTIONS

In an IMA architecture, the Airborne IPS system can be connected to applications and avionics systems via an ARINC 664 Ethernet data network. Switches supplemented with Virtual Local Area Networks (VLANs) provides segregation among flows, which reduces the risk of having a specific system interfering with ATS applications, for example.

Alternatively, applications may be hosted on the same hardware as the Airborne IPS System. In this case, the interface between applications and the Airborne IPS System is implementaion-specific and does not require standardization.

The figure below illustrates a representative deployment of the Airborne IPS System functions in an IMA architecture on existing hardware. In this example, the IPS functions are hosted in a Common Processing and Input/Output Module (CPIOM) environment and uses an ARINC 664 Ethernet data network to interface with radios and other systems. This example deployment also illustrates that some functions, such as existing applications, can be hosted on other systems (e.g., FMC, as shown) or hosted on the same platform as the Airborne IPS System.

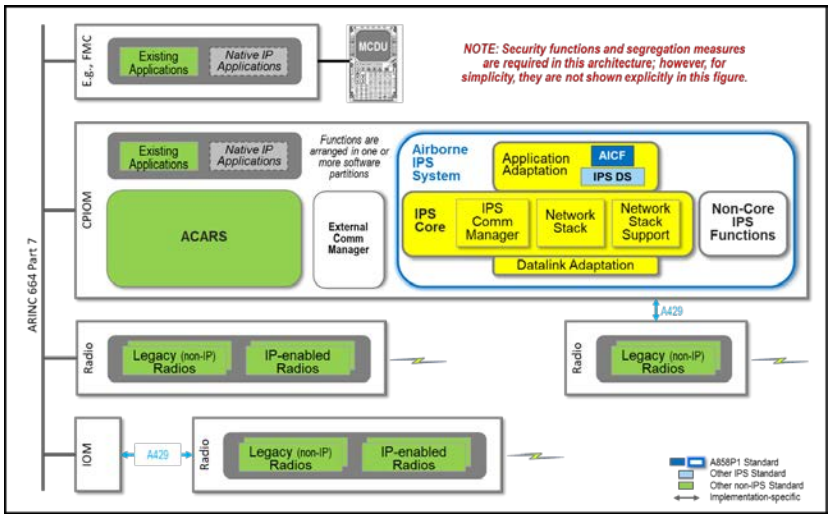

Figure 5-4 – Integration Example: Representative Allocation of IPS Functions in an IMA Architecture

5.3 Interface Considerations

This section provides implementation guidance and considerations for the various external interfaces between the Airborne IPS System and other avionics systems. Options are presented for leveraging existing ARINC Standards; however, some interfaces may be implementation-specific and aircraft architecture-dependent. In addition, based on the Airborne IPS System Architecture requirements in Section 3.0 and the IPS Security requirements in Sections 4.0, guidance is provided for some interfaces to facilitate the implementation.

The following subsections reference the Airborne IPS System external interfaces that are denoted IF-1 through IF-6 in the following figure.

5.0 AIRBORNE IPS SYSTEM IMPLEMENTATION OPTIONS

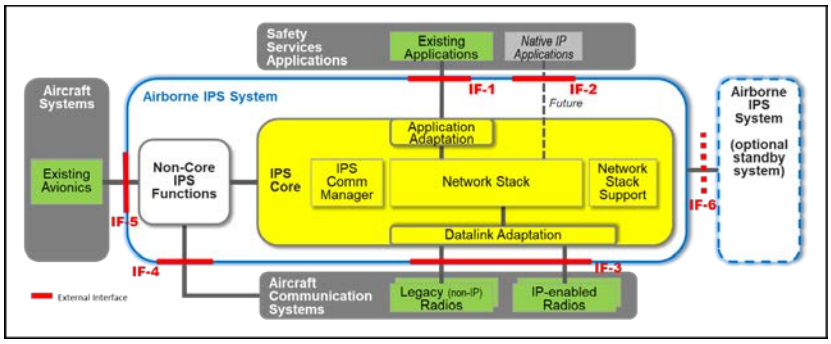

Figure 5-5 – Airborne IPS System External Interfaces

5.3.1 Application Interface Considerations

5.3.1.1 Interface with Existing Applications [IF-1]

This interface is located between the Airborne IPS System Application Adaptation function and existing applications.

The Airborne IPS System implements the IPS Dialogue Service (DS), which provides adaptation of existing applications to the IPS network stack, as specified in ICAO Doc. 9896. The IPS DS appears as an instance of the dialogue service specified in ICAO Doc. 9880, Part III. The B1/B2 applications interface directly with the IPS DS since they present a DS interface. ACARS-based ATS and AOC applications use the ACARS-to-IPSDS Convergence Function (AICF) specified in Attachment 3 of this document to adapt ACARS applications to the IPS DS.

COMMENTARY

AOC applications may be accommodated using the AICF, as described in this section, or an alternative adaption approach. Refer to Section 3.2.

This interface should offer the following services:

- D-REGISTER and D-UNREGISTER Services, parameters to include AE Qualifier, Version number, number of dialogues, etc.
- D-DATA Service
- D-START Service
- D-END Service
- D-ABORT Service (both user and provider)
- Get Destination IP Address Service, parameters to include ATN/OSI Network Entity Title, IP ground destination address
- Get Router Available, parameters to include Destination IP Address

Although existing applications use the IPS DS to interface with the network stack, the detailed implementation of the service interface between the applications and IPS DS is not standardized. The following examples illustrate possible implementation of the application interface in federated and IMA architectures.

Figure 5-6 illustrates a federated ARINC 758-based CMU architecture, as descried in Section 5.2.1. As shown, existing applications can be hosted in the same Line Replaceable Unit (LRU) as the Airborne IPS System (e.g., B1 hosted in a CMU) or in a peripheral (e.g., FANS-1/A hosted in an FMS).

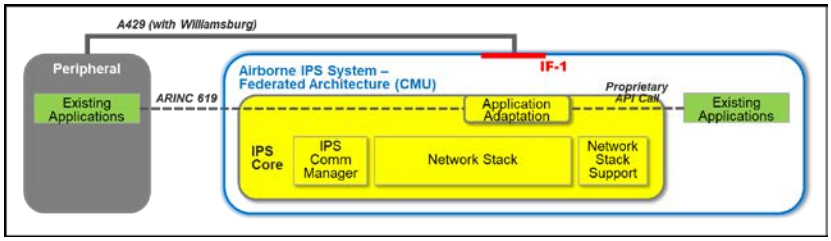

Figure 5-6 – Existing Application Interface in a Federated Architecture

When existing applications are hosted within the same LRU, no physical interface is required, and the functional interface is implementation-specific (e.g., proprietary API call) and defined by the avionics supplier. When the application is hosted in a peripheral, then the physical interface may be ARINC 429 (shown) or ARINC 664, and the transport mechanism may be one of several options, including ARINC 619 (shown), ARINC 702A, ARINC 834, or an implementation-specific interface.

Figure 5-7 illustrates an IMA architecture, as described in Section 5.2.2. Like the federated architecture, existing applications may be hosted on the same IMA platform as the Airborne IPS System or on a different system.

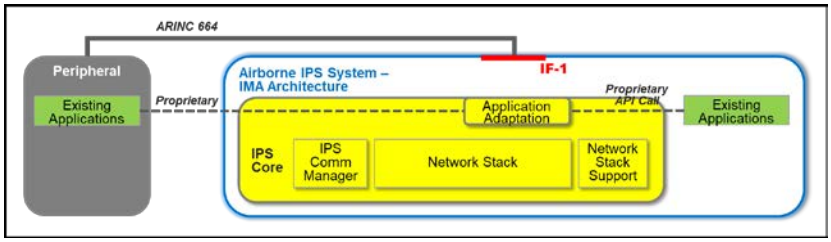

Figure 5-7 – Existing Application Interface in an IMA Architecture

When the existing application are hosted on the same IMA platform, no physical interface is required, and the functional interface is implementation-specific. When the application is hosted on hardware other than the platform that hosts the Airborne IPS System, then the physical interface may be ARINC 664 (shown) or ARINC 429, but the transport protocol is implementation-specific. Platform-specific operating systems and Application Programming Interface (API) should comply with ARINC Specification 653.

5.3.1.2 Interface with Native IP Applications [IF-2]

This interface is located between the Airborne IPS System and future Native IP applications.

Unlike existing applications, future Native IP applications can be designed to interface directly with the network stack without requiring use of the IPS DS. The Native IP applications may use socket interfaces or an implementation-specific API.

These future applications are outside the scope of this standard; however, they may be addressed in a future supplement to this standard.

5.3.2 Radio Interface Considerations

5.3.2.1 Interface with Airborne Radios-Data [IF-3]

This interface, which is between the Airborne IPS System Datalink Adaptation function and an Airborne Radio or Satellite Data Unit (SDU), is used for data transfer.

The interface protocol and services shall comply with applicable ARINC Standards (e.g., ARINC Characteristic 750 for the VHF Digital Radio); no IPS-specific functional services are identified for this interface.

5.3.2.2 Interface with Airborne Radios-Control [IF-4]

This interface, which is located between the Airborne IPS System Radio Management function and Airborne Radios or SDUs, is used to configure and manage communication radios, as well as to receive link status information (e.g., link-up, link-down).

The radio management interface protocol and services shall comply with applicable ARINC Standards (e.g., ARINC Characteristic 750 for the VHF Digital Radio). At the time of this writing, no IPS-specific functional services are specified for the radio-specific interface; however, some radio specifications may evolve over time to provide additional status information, for example, real-time link quality to enhance the performance of multilink operations.

5.3.2.3 Physical Radio Interface Options

The following figure illustrates the radio interfaces for both legacy radios and IPS-aware radios. Note that the data interface and radio management interface may share the same physical connection (i.e., IF-3 and IF-4 use the same physical connection), or they may use dedicated physical connections.

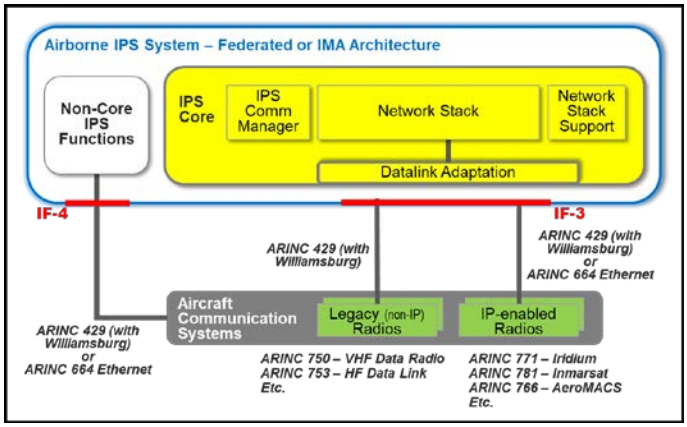

Figure 5-8 – Radio Interfaces in Federated or IMA Architecture

For legacy radios, such as the ARINC 750 VDR, the physical interface to the Airborne IPS System is via existing ARINC 429 data buses. Other radios, such as

ARINC 771 and ARINC 781 Satellite Data Units (SDU), may interface using either ARINC 429 data bus or ARINC 664 Ethernet interface.

For federated architectures, ARINC Characteristic 758 (Supplement 4 and later) specifies both ARINC 429 data bus and ARINC 664 Ethernet interfaces. An IMA architecture may support both ARINC 429 and ARINC 664 interfaces; however, interconnection via ARINC 429 may require an Input/Output Module (IOM), as shown previously in Figure 5-4.

5.3.2.3.1 ARINC 429

Commented [OML47]: Ed. Note: Revised text from COL for A429 and Ethernet

When the interface is ARINC 429, the Airborne Radio or SDU uses the Williamsburg Protocol Version 3 to exchange IPv6 data. The General Format Identifier (GFI), which indicates the payload type exchanged with the Airborne IPS System, is set to a value of decimal 6 to indicate IPv6 over Williamsburg Protocol Version 3. The Airborne Radio or SDU may perform segmentation if the air-ground link layer frame size is smaller than the minimum MTU size of 1280 bytes.

The Airborne Radio or SDU indicates network operational status and Link Up/Down events via the ARINC 429 broadcast status labels such as Label 270 and Label 271.

5.3.2.3.2 Ethernet

When the interface is Ethernet, the Airborne Radio or SDU may utilize Point-to-Point Protocol over Ethernet (PPPoE) per RFC 2516. When using PPPoE, the two-byte ETHER_TYPE field in the Ethernet frame is set to the value 0x86DD to indicate that IPv6 data packets are contained in the payload of the frames exchanged with the Airborne IPS System.

The Airborne Radio or SDU provides Link Up/Down event status, and supported MTU size if available, using Discovery Ethernet frames with the ETHER_TYPE field set to the value 0x8863.

5.3.2.4 Air-Ground Link Security Implementation Considerations

Since the communication radios connect to local airborne networks in the aircraft control domain, the security architecture presented in Section 4.0 shows that the Airborne Radio systems represent the first point of entry for an external threat to the aircraft. Consequently, a secure channel between the Airborne Radio systems and the peer radio access endpoints on the ground is necessary to ensure authentication and integrity of air-ground message exchanges in support of an overall defense-in-depth security strategy.

Two approaches to protecting the air-ground communications can be envisaged:

- Secure the radio system itself,
- Ensure that all radio traffic is protected by security measures hosted by the Airborne IPS System.

The first approach is applicable to radios, such as Satcom and AeroMACS, with an integrated security function that provides a first layer of security. In this case, the traffic received by the Airborne IPS System from the radio is considered as coming from a trusted source.

The second approach is applicable to existing non-secure radios where modifications to the radio itself may be complex and/or cost prohibitive. An example is existing VDRs, where it is practical to consider a link security mechanism hosted

by the Airborne IPS System to minimize the impact to installed radio systems. The figures in Sections 5.2.1 and 5.2.2 illustrate this approach, which is shown in the diagrams as the secured function “ARINC 631 IPS-over-AVLC.”

The feasibility of this approach should be based on a security risk assessment, and the complexity of the security implementation may depend on the interface between the radio and the Airborne IPS System. If an ARINC 429 point-to-point bus architecture is used, then a level of segregation is provided since the radio is connected directly to one single endpoint. Whereas, if the radio is one of many devices connected via a local area network using an ARINC 664 Ethernet data network, then additional on-aircraft security measures may be necessary to protect other systems from threats that originate from the radio system.

5.3.3 Interface with Other Avionics Systems [IF-5]

This interface is located between the Airborne IPS System interface and other aircraft systems such as a Centralized Maintenance System (CMS), flight warning system (FWS), data recorder, and an external security management system. Since these systems are specific to the airframe manufacturers’ avionics platforms and architectures, the interfaces are implementation-specific and are not defined in this standard.

5.3.4 Interface with Redundant Airborne IPS Systems [IF-6]

This interface is located between two Airborne IPS Systems to support the exchange of status and synchronization information between systems in a redundant configuration. While the notional diagram in Figure 5-5 depicts a single interface between the redundant systems, multiple physical interfaces may be necessary to achieve redundancy that meets the overall performance requirements for the Airborne IPS System. This interface is implementation-specific and is not defined in this standard.

5.4 Dual-Stack Considerations

Per the deployment assumptions in Section 2.4, aircraft will be equipped with an OSI stack or an IPS stack, but not both. However, as shown in the implementation examples in Section 5.2, IPS-equipped aircraft may be dual-stacked to include both the IPS stack and the ACARS stack.

In a dual-stack configuration, ACARS and IPS should co-exist and operate in a complementary manner, and the External Communications Manager function described in Section 3.3.7 provides the necessary coordination. The External Communications Manager function and the dual-stack approach are aircraft architecture-dependent and implementation-specific. Figure 5-9 illustrates a notional dual-stack configuration; note that this logical diagram is not intended to imply a physical implementation, but rather it shows the collection of functional elements, which may be distributed or integrated in a number of ways. Example configurations include:

- All functions may be integrated in one federated LRU (e.g., a CMU), as shown previously in Section 5.2.1
- The functions may be allocated to multiple federated LRUs (e.g., an existing CMU and a new Airborne IPS System, either of which may also host the External Communications Manager function)

- The functions may be allocated to one or more processing components in an IMA architecture, as shown previously in Section 5.2.2

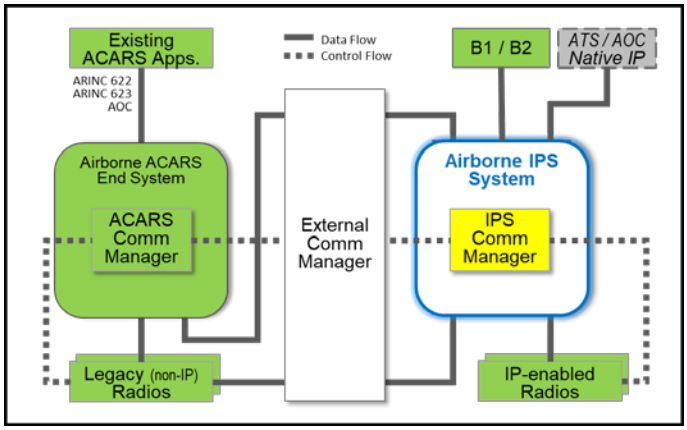

Figure 5-9 – Notional Dual-Stack Configuration

As shown in the diagram, the External Communications Manager function receives link decision information (i.e., dotted-line control flows from the ACARS and IPS Communication Managers) that is based on radio management information (i.e., dotted-line control flows from the radios indicating JOIN and LEAVE events). This information allows the External Communications Manager function to direct the flow of application data to either the ACARS End System or the Airborne IPS System.

Some Airborne Radios (e.g., SDU) may provide multiple interfaces, in which case the ACARS End System and the Airborne IPS System may be connected via separate physical connections. However, when an Airborne Radio is shared (e.g., an existing VDR connected to an existing CMU), then the External Communications Manager function facilitates the coordination between the ACARS and IPS communication managers. The priority among the messages must be managed properly when ACARS and IPS message flows are inter-mixed. In the case of VDLM2, the AVLC layer provides logical data separation via the IPI value associated with the message.

5.5 Airborne IPS Router versus Multi-homed Airborne IPS Host Considerations

The IPS interoperability provisions in ICAO Doc. 9896 and the IPS Profiles (RTCA DO-379 and EUROCAE ED-262) support a variety of avionics implementations. As illustrated in Figure 5-10, the Airborne IPS System may be implemented either as one or more Airborne IPS Hosts plus an Airborne IPS Router or as a multi-homed Airborne IPS Host. The choice is implementation-specific, taking into consideration how the Airborne IPS System integrates into the overall aircraft system and communications architectures. Both options must conform to the functional architecture described in Section 3.0.

COMMENTARY

The functional architecture described in Section 3.0 maps most simply to the multi-homed Airborne IPS Host implementation.

Whereas, additional effort is necessary to map individual elements of the functional architecture to both the Airborne IPS Host(s) and the Airborne IPS Router.

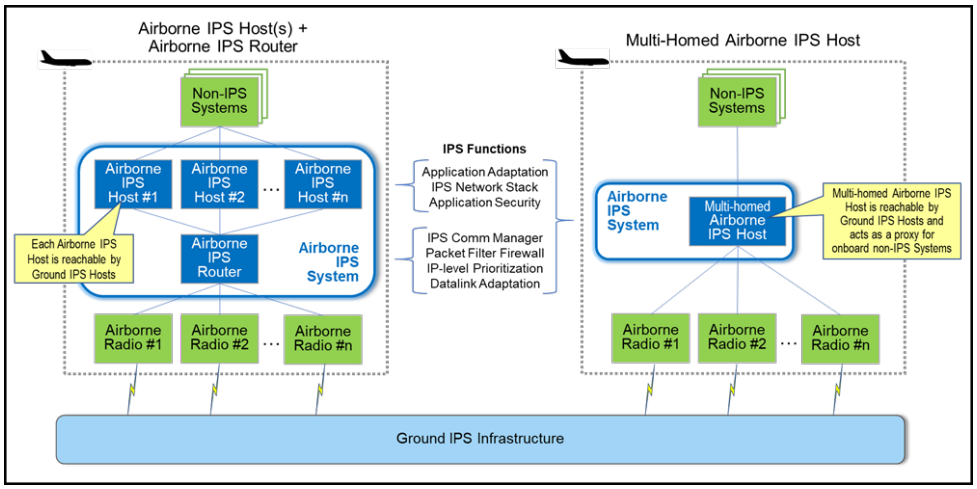

Figure 5-10 – Airborne IPS Router versus Multi-homed Airborne IPS Host

The following sub-sections describe each approach and associated considerations.

5.5.1 Airborne IPS Router

The Airborne IPS System may be implemented as a collection of one or more Airborne IPS Hosts and an Airborne IPS Router that routes IPv6 packets to/from each IPS Host via an onboard network. For example, this implementation approach supports an aircraft architecture where multiple IPS Hosts are associated with different application types (e.g., one host for ATC, one for AOC, one for SWIM services, etc.).

The Airborne IPS System functions in this standard are allocated to each constituent Airborne IPS Host and Airborne IPS Router element. As shown in the left-hand side of Figure 5-10, each Airborne IPS Host is responsible for implementing application adaptation, as necessary, and the full IPS stack from network layer to application layer, including the application-level security functions that protect exchanges end-to-end between communicating peer airborne and ground IPS Hosts. The Airborne IPS Router is responsible for selecting the air-ground access network with the potential to provide the desired QoS requested by each Airborne IPS Host application. The Airborne IPS Router directs the IPv6 packets generated by the IPS Hosts towards appropriate Airborne Radios, and it provides the packet filter firewall, IP-level prioritization, datalink adaptation as necessary, and the IPS Communication Management functions (e.g., mobility, multilink) described in Section 3.3.6.

COMMENTARY

The Airborne IPS Router forwards traffic only between Airborne IPS Hosts and Airborne Radios. All IPS exchanges with an aircraft originate or terminate at an Airborne IPS Host, and the Airborne IPS

Router is configured such that it: (1) does not route IPv6 traffic received from one access network directly to another access network; (2) does not run dynamic routing protocols; and (3) does not share neighbor discovery information across air-ground access networks to prevent bridging from one access network to another without terminating at the Airborne IPS System.

Each Airborne IPS Host is assigned one or more globally routable IPv6 addresses that are reachable from Ground IPS Hosts and which are derived from a unique fixed mobile network prefix assigned to the aircraft, as described in Section 3.3.2.2. Any access network-specific requirements imposed on the Airborne IPS System (e.g., air-ground signaling between the Airborne IPS System and ground Access Router, as described in Section 3.3.6.2) are handled by the Airborne IPS Router and not by the Airborne IPS Hosts.

5.5.2 Multi-homed Airborne IPS Host

When implemented as a multi-homed Airborne IPS Host, the Airborne IPS System acts as an IPS Host that can attach to multiple access networks simultaneously or one at a time. With this implementation approach, the Airborne IPS System acts as a proxy for other non-IPS-enabled onboard systems and applications (e.g., ATS application hosted in an FMC) that are not reachable directly from Ground IPS Hosts (i.e., these systems cannot exchange IPv6 packets with Ground IPS Hosts).

As shown in the righthand side of Figure 5-10, the multi-homed Airborne IPS Host integrates all IPS functionality in accordance with the Airborne IPS System requirements specified in this standard. This includes application adaptation as necessary, the full network stack, application-level security, packet filter firewall, prioritization, communications management, datalink adaptation as necessary, etc.

The multi-homed Airborne IPS Host is assigned one or more globally routable IPv6 addresses that are reachable from Ground IPS Systems, derived from a unique fixed mobile network prefix assigned to the aircraft, as described in Section 3.3.2.2. Any access network-specific requirements imposed on the Airborne IPS System (e.g., air-ground signaling between the Airborne IPS System and ground Access Router, as described in Section 3.3.6.2) are handled by the multi-homed Airborne IPS host itself.

6.0 AIRBORNE APPLICATION DATA CONSIDERATIONS

The IPS System 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. One of the basic goals of the application interface is to support the use of existing applications over IPS without requiring changes to those applications. This offers the benefit of not changing systems on the aircraft, and it facilitates commonality and reuse of existing procedures. However, achieving this goal is made more difficult by legacy interfaces that tightly couple network and application technologies.

To use the IPS System effectively, applications need a compatible interface definition. Legacy applications including FANS-1/A, B1/B2, and ACARS-based applications all have some intermixing of application and network layer data. That is, there are messaging aspects that need to be known at the application level. This makes it difficult to change network technologies, since doing so also causes changes to the applications themselves, which is very expensive. Therefore, for legacy applications that are non-native-IP, a specialized interface is needed to communicate with peers and preserve maximum application compatibility. Native IP applications (i.e., those designed to take advantage of IP via TCP or UDP directly) may need a different type of interface to communicate via IPS.

For legacy applications, ICAO Doc. 9896 specifies an IPS Dialogue Service (DS), which includes an accommodation layer for applications that use OSI and ACARS protocols. The data encapsulation element, which is called the ATN Packet (ATNPKT) format, is used to convey state, connection, application, and other details between peer end/host systems. Note that while ICAO Doc. 9896 specifies both TCP and UDP transport options, legacy applications use only the UDP transport protocol to provide commonality.

The choice of UDP for ATS applications offers some advantages when compared to TCP. Those familiar with TCP, UDP and TP4 may find this odd since TCP is closer in operation to TP4 and would seem a more natural fit for IPS, especially when compared to OSI. However, TCP also has a higher connection overhead, including multiple transactions to establish and maintain a connection. For applications like CM, more transactions are needed to manage the connection than to actually exchange data, making a connection-oriented protocol like TCP less efficient. For applications like CPDLC or ADS-C, where there are multiple transactions per connection, it might make more sense to use a connection-oriented transport. However, due to the nature of ATS transactions and the generally smaller data size of legacy applications (i.e., they are not streaming megabytes of data, but only sporadically sending small messages, e.g., 2-6 message exchanges of 0.006 – 1.5kb per 30 minutes of flight time per aircraft, based on analysis of current continental operations). This again makes a connectionless transport that has some reliability more attractive, which is why UDP was chosen for ATS applications. However, note that future services may have requirements to transfer or stream more data than legacy applications; therefore, TCP could be considered in the future when a use case for connection-oriented transport is identified.

As mentioned, not all applications necessarily need the IPS DS per ICAO Doc. 9896, and may adapt more readily to the communication stack, making use of existing transport layer services. These differing needs must be considered based on the specific application.

The actual interface definition is a local matter, depending on specific hardware and software choices by airframers and suppliers. Interoperability with peer applications is achievable if the interfaces conform to the definitions and protocols specified in ICAO Doc. 9896.

6.1 B1/B2

The original intent of ICAO Doc. 9896 was to allow a replacement of the upper layer communication service (ULCS), as specified in the original ICAO Doc. 9705, with something that could be mapped to TCP and UDP. The mapping was specified with the intent of not requiring any changes to the applications themselves. From the application point of view, communication with peers would act the same as if the applications were using OSI protocols.

This was achieved by the combination of defining the IPS DS and the ATNPKT format. The IPS DS provides the Dialogue 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. ATNPKT is carried in the payload part of the transport protocol (UDP), and it is used to convey parameters of the service primitives that cannot be mapped to existing IP or transport header fields. The ATNPKT also conveys information to indicate the Dialogue Service protocol function (e.g., the type of DS primitive).

To ensure interoperability between peer OSI-based implementations when using IPS networking, accommodation of the OSI-based ATN applications must adhere to the provisions specified in the “Legacy ATN Applications” section of ICAO Doc. 9896, Part II.

6.2 FANS-1/A

IPS is also intended to support legacy, ACARS-based FANS-1/A applications (note that other ACARS-based safety applications are discussed in Section 6.3). The FANS-1/A structure contains a message payload (CPDLC, ADS-C, and AFN messages) that is put into a communication envelope in accordance with ARINC Specification 622. For IPS, this envelope is mapped to the contents of an ATNPKT. Since ACARS-based applications have different communications parameters than OSI-based applications, the elements of the ATNPKT are used differently for FANS-1/A messages. This includes the ATNPKT parameters as well as the primitive types, which are used to reflect the connectionless nature of the ACARS protocol while also providing the necessary reliability. The mapping to ATNPKT is defined to allow maximum compatibility with existing end/host systems on the aircraft and ground while also providing benefits of moving towards the IPS infrastructure.

To ensure interoperability between peer FANS-1/A-based implementations when using IPS networking, accommodation of the FANS-1/A applications must adhere to the provisions specified in ICAO Doc. 9896, Part II and the ACARS to IPS DS Convergence Function specified in Attachment 3 of this document.

6.3 Other ACARS Messages

AOC and non-FANS-1/A ATS applications supporting safety and regularity of flight currently supported over ACARS can also make use of the IPS infrastructure. This can be accomplished using the IPS Dialogue Service, an adaptation layer, or IP-based messaging solution, e.g., Media Independent Aircraft Messaging (MIAM) using the IP Middleware Convergence Function as specified in ARINC 841.

The AOC and non-FANS-1/A ATS structure has a message payload (e.g., as defined in ARINC 702A, or ARINC 623 messages) that is put into a communication envelope. For IPS, these payloads may be mapped to the contents of an ATNPKT. As described previously in Section 6.2, since ACARS-based applications have different communications parameters than OSI-based applications, the elements of the ATNPKT are used differently for ACARS messages. This includes the ATNPKT parameters as well as the primitive types, which are used to reflect the connectionless nature of the ACARS protocol while also providing the necessary reliability. The mapping to ATNPKT is defined to allow maximum compatibility with existing end/host systems on the aircraft and ground while also providing benefits of moving towards the IPS infrastructure.

To ensure interoperability between ACARS-based implementations when using IPS networking, accommodation of AOC and non-FANS-1/A ATS applications must adhere to the provisions specified in ICAO Doc. 9896, Part II. and the ACARS to IPS DS Convergence Function specified in Attachment 3 of this document.

6.4 AOC Applications (non-ACARS)

Non-ACARS AOC applications serving airline operations and supported by general, non-safety IP services to the aircraft are assumed to be outside the scope of ATN/IPS. These applications may base their provisions on IPS to take advantage of commonalities and unified architectures; however, additional requirements (e.g., software partitioning, design assurance level of some components, etc.) may require further considerations.

Non-ACARS applications may use the IPS Dialogue Service interface, which may require further definition of the ATNPKT format, or they may use a different interface. If a new interface is used with UDP transport, then an error detection and correction scheme should be implemented to guard against lost packets. Likewise, if a new interface is used with TCP transport, then the performance of TCP needs to be considered, and parameters tailored as necessary, when using a bandwidth constrained-link.

6.5 Future Safety Services Applications

New ATS (e.g., Beyond-B2), AOC, and air-ground SWIM applications to support future safety services may be developed as Native IP applications using IPS. Standard profiles and interfaces may 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 settings. While it is impossible to predict future applications' requirements, the IPS provisions for current and near-term applications provide adequate capabilities for usage. Currently, Aeronautical Information Service and Weather/Meteorological data services are expected to utilize IPS.

ATTACHMENT 1 LIST OF ACRONYMS

4DT	Four-Dimensional Trajectory
A-G or A/G	Air-to-Ground
AAC	Aeronautical Administrative Communication
ACARS	Aircraft Communications Addressing and Reporting System
AC	Aircraft Control
ACD	Aircraft Control Domain
ACK	Acknowledgement
ACL	Access Control List
ACMS	Aircraft Condition Monitoring System
ACSP	Air-Ground Communications Service Provider
ADN	Aircraft Data Network
ADS	Automatic Dependent Surveillance
ADS-C	Automatic Dependent Surveillance-Contract
AE	Application Entity
AEEC	Airlines Electronic Engineering Committee
AES	Advanced Encryption Standard
AeroMACS	Aeronautical Mobile Airport Communications System
AFN	ATS Facilities Notification
AICF	ACARS to IPS DS Convergence Function
AIM	Aeronautical Information Management
AIS	Aircraft Information Services
AISD	Aircraft Information Services Domain
AMS(R)S	Aeronautical Mobile Satellite (Route) Service
ANSP	Air Navigation Service Provider
AOA	ACARS Over AVLC
AOC	Airline or Aeronautical Operational Control
API	Application Programming Interface
APM	Aircraft Personality Module
App	Application
AppID	Application Identifier
ARU	AeroMACS Radio Unit
ASCII	American Standard Code for Information Interchange
ASN	Abstract Syntax Notation
ASN.1	Abstract Syntax Notation One
ATA	Air Transport Association
ATC	Air Traffic Control
ATM	Air Traffic Management
ATN	Aeronautical Telecommunication Network
ATNPKT	ATN Packet

ATTACHMENT 1
LIST OF ACRONYMS

ATS	Air Traffic Services
AVLC	Aviation VHF Link Control
B1 / B2	Baseline 1 / Baseline 2
BER	Basic Encoding Rules
BLOS	Beyond Line Of Sight
BOM	Byte Order Mask
BU	Binding Update
BW	Bandwidth
CA	Certificate Authority
CCM	Counter mode with Cipher block chaining Message authentication code
CDA	Current Data Authority
CER	Canonical Encoding Rules
CM	Context Management
CMF	Communications Management Function
CMU	Communications Management Unit
CMS	Centralized Maintenance System
CNS/ATM	Communications Navigation Surveillance/Air Traffic Management
CoA	Care-of Address
COMM	COMMunications
CoS	Class of Service
CPDLC	Controller Pilot Data Link Communications
CPIOM	Common Processing and Input/Output Module
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CS	Circuit Switched
CSM	Configuration Settings Manager
CSMA	Carrier Sense Multiple Access
CSP	Communication Service Provider
CSR	Certificate Signing Request
D8PSK	Differential 8-Phase Shift Keying
DAL	Design Assurance Level
DDoS	Distributed Denial of Service
DER	Distinguished Encoding Rules
DGSS/IS	Datalink Ground Systems Standard and Interface Design Specification
DHCP	Dynamic Host Control Protocol
DHE	Diffie-Hellman Ephemeral
DITS	Digital Information Transfer System
DL	Downlink
DLS	Data Link Service
DLS-IR	Data Link Services Implementing Rule

ATTACHMENT 1
LIST OF ACRONYMS

DNS	Domain Name Service
DoD	Department of Defense
DoS	Denial of Service
DPI	Deep Packet Inspection
DS	Dialogue Service
DSCP	Differentiated Services Code Point
DSI	Dialogue Service Interface
DSP	Data Link Service Provider
DTE	Data Terminal Equipment
DTLS	Datagram Transport Layer Security
EC	European Commission
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral
ECN	Explicit Congestion Notification
EDS	Electronic Distribution of Software
EIPI	Extended Initial Protocol Identifier
ES	End System
EST	Enrollment over Secure Transport
EU	European Union
FAA	Federal Aviation Administration
FANS	Future Air Navigation System
FCI	Future Communications Infrastructure
FCS	Frame Check Sequence
FIPS	Federal Information Processing Standard
FIR	Flight Information Region
FL	Flight Level
FLS	Field Loadable Software
FlightID	Flight Identifier
FMC	Flight Management Computer
FMF	Flight Management Function
FMS	Flight Management System
FOC	Flight Operations Center
FWS	Flight Warning System
G-G or G/G	Ground-to-Ground
G-LISP	Ground-based Locator/Identifier Separation Protocol
GANP	Global Air Navigation Plan
GCM	Galois Counter Mode
GFI	General Format Identifier
GOLD	Global Operational Data Link
GW	Gateway

ATTACHMENT 1
LIST OF ACRONYMS

HA	Home Agent
HF	High Frequency
HFDL	High Frequency Data Link
HFN	High Frequency Next
HFR	High Frequency Radio
IANA	Internet Assigned Numbers Authority
ICAO	International Civil Aviation Organization
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol Version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IF	Interface
IMA	Integrated Modular Avionics
IMI	Imbedded Message Identifier
IOM	Input/Output Module
IP	Internet Protocol
IPI	Initial Protocol Identifier
IPS	Internet Protocol Suite
IPS DS	Internet Protocol Suite Dialogue Service
IPS GW	Internet Protocol Suite Gateway
IPv4 / IPv6	Internet Protocol Version 4 or Version 6
ISO	International Standards Organization
ITA2	International Telegraph Alphabet Number 2
ITU	International Telecommunication Union
IUEI	Intentional Unauthorized Electronic Interference
LDACS	L Band Digital Aeronautical Communication System
LISP	Locator/Identifier Separation Protocol
LLA	Link Local Address
LME	Link Management Entity
LMF	Local Management Function
LOS	Line of Sight
LRU	Line Replaceable Unit
LSP	Loadable Software Part
MAC	Media Access Control
MASPS	Minimum Aviation System Performance Standards
MCDU	Multi-purpose Control and Display Unit
MDE	Multilink Decision Engine
MEL	Minimum Equipment List
MFI	Message Function Identifier

ATTACHMENT 1
LIST OF ACRONYMS

MIAM	Media Independent Aircraft Messaging
MMS	Multilink and Mobility Signaling
MNP	Mobile Network Prefix
MOPS	Minimum Operational Performance Standards
msb/MSB	Most Significant Bit
MSG	Message
MSGID	Message Identifier
MSN	Message Sequence Number
MTI	Message Type Identifier
MTU	Maximum Transmission Unit
MU	Message Unit
NAK	Negative Acknowledgement
NDA	Next Data Authority
NDP	Neighbor Discovery Protocol
NextGen	Next Generation Air Transportation System
NIST	National Institute of Standards and Technology
NOCOMM	NO COMMunications
NVRAM	Non-Volatile Random-Access Memory
OCSP	Online Certificate Status Protocol
OEM	Original Equipment Manufacturer
OPC	Operational Program Configuration
OSI	Open System Interconnection
PDP	Packet Data Protocol
PDU	Protocol Data Unit
PIESD	Passenger Information Services Domain
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
POA	Plain Old ACARS
PPP	Point to Point Protocol
PPPoE	Point to Point Protocol over Ethernet
PRF	Pseudo Random Function
PRI	Priority Value
PS	Packet Switched
QoS	Quality of Service
RA	Router Advertisement
RCP	Required Communication Performance
RCTP	Required Communication Technical Performance
RF	Radio Frequency
RFC	Request for Comment
RIR	Regional Internet Registry
RNAV	aRea NAVigation

ATTACHMENT 1
LIST OF ACRONYMS

ROHC	RObust Header Compression
RS	Router Solicitation
RSP	Required Surveillance Performance
RTOS	Real-Time Operating System
SAL	Security Assurance Level
SARPS	Standards and Recommended Practices
Satcom	Satellite Communications
SB-Safety	Swift Broadband-Safety
SBB	Swift Broadband
SCVP	Server-based Certificate Validation Protocol
SD	Structured Data
SDO	Standards Development Organization
SDP	Satellite Data Protocol
SDU	Satellite Data Unit
SESAR	Single European Sky Air Traffic Management (ATM) Research
SESAR JU	SESAR Joint Undertaking
SHA	Secure Hash Algorithm
SLAAC	Stateless Address Auto Configuration
SNMP	Simple Network Management Protocol
SP	Special Publication
SPR	Safety and Performance Requirement
SWIM	System Wide Information Management
TBC	To Be Confirmed
TBD	To Be Determined
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TTL	Time To Live
TP4	Transport Protocol 4
UDP	User Datagram Protocol
UI	Unnumbered Information
UL	Uplink
ULCS	Upper Layer Communication Services
US	United States
UTC	Universal Time Coordinated
UTF	Unicode Transformation Format
VDL	VHF Digital Link
VDLM2	VHF Digital Link Mode 2
VDR	VHF Data Radio
VHF	Very High Frequency
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol

ATTACHMENT 1
LIST OF ACRONYMS

VPN	Virtual Private Network
WG	Working Group
WoW	Weight on Wheels

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. [Source: ICAO Doc. 9705]

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).

Access Network

A network that is characterized by a specific access technology. [Source: ICAO Doc. 9896]

ACD – Aircraft Control Domain

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.

ACSP – Air-Ground Communication Service Provider

Service provider that provides air-ground communication services via an access network.

Administrative Domain

An administrative entity in the ATN/IPS. An administrative domain can be an individual State, a group of States, an aeronautical industry organization (e.g. an air-ground service provider), or an air navigation service provider (ANSP) that manages ATN/IPS network resources and services. From a routing perspective, an administrative domain includes one or more autonomous systems. [Source: ICAO Doc. 9896]

ADS-C – Automatic Dependent Surveillance-Contract

A means by which the terms of an ADS-C agreement will be exchanged between the ground system and the aircraft, via a data link, specifying under what conditions ADS-C reports would be initiated, and what data would be contained in the reports. [Source: ICAO Annex 10, Volume III]

Air-Ground Access Network

Access network that provides air-ground communication services.

Air-Ground Datalink

Refer to the definition for Air-Ground Access Network.

Airborne IPS Host

Airborne instantiation of an IPS Host.

ATTACHMENT 2
GLOSSARY

Airborne IPS Router

An airborne device that is used to support ATN/IPS packet forwarding between one or more Airborne IPS Hosts and Airborne Radios.

Airborne IPS System

The collection of airborne components and functions that provide IPS services.

Airborne Radio

Physical airborne radio that provides the communication over-the-air using the specific air-ground access network specification and the Layer 2 interface to the Airborne IPS System.

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

AMS(R)S – Aeronautical Mobile-Satellite Route Service

An aeronautical mobile-satellite service reserved for communications related to safety and regularity of flights, primarily along national or international civil air routes. [Source: ICAO Annex 10, Volume II]

AOA – ACARS Over Aviation VHF Link Control

Protocol that enables ACARS messages to be encapsulated within the AVLC frame of the VDL Mode 2 datalink layer protocol to deliver an ACARS message.

AOC – Aeronautical Operational Control

Communication required for the exercise of authority over the initiation, continuation, diversion or termination of flight for safety, regularity and efficiency reasons. [Source: ICAO Annex 10, Part III]

AOC – Airline 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.

Application

The ultimate use of an information system, as distinguished from the system itself. [Source: ICAO Doc. 9880].

ATC – Air Traffic Control

A service operated by an appropriate authority to promote the safe, orderly, and expeditious flow of air traffic. [Source: FAA Pilot-Controller Glossary]

ATTACHMENT 2
GLOSSARY

ATC – Air Traffic Control Service

A service provided for the purpose of: a) preventing collisions between aircraft and on the maneuvering area between aircraft and obstructions; and b) expediting and maintaining an orderly flow of traffic. [Source: ICAO Doc. 10037]

ATM – Air Traffic Management

The dynamic, integrated management of air traffic and airspace (including air traffic services, airspace management and air traffic flow management) — safely, economically and efficiently — through the provision of facilities and seamless services in collaboration with all parties and involving airborne and ground-based functions. [Source: ICAO Doc. 10037]

ATN – Aeronautical Telecommunications Network

A global internetwork architecture that allows ground, air-ground, and avionic data subnetworks to exchange digital data for the safety of air navigation and for the regular, efficient and economic operation of air traffic services. [Source: ICAO Annex 10, Part III]

ATN/IPS

The set of technical provisions and standards that define the architecture and operation of Internet Protocol-based networking services. Also referred to as IPS.

ATN/IPS Network / 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 (area control service, approach control service or aerodrome control service) and aerodrome flight information service. [Source: ICAO Annex 11]

CM – Communication Manager

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

- IPS Communication Manager, which manages in the IPS System the selection of the air-ground access network 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.

CM Application – Context Management Application

An ATN application that provides a logon service allowing initial aircraft introduction into the ATN and a directory of all other data link applications on the aircraft. It also includes functionality to forward between ATS units. [Source: ICAO Doc. 9880]

ATTACHMENT 2
GLOSSARY

CMU – Communication Management Unit

The CMU performs two important functions: it manages access to the various air-ground access 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 seamless global Air Traffic Management. Modern CNS systems will eliminate or reduce a variety of constraints imposed on ATM operations today.

Control Plane

Data exchanged to manage communication sessions between users. The control plane includes protocols providing information needed to move traffic from one device to another through the network. Routing protocols and DNS belong to the control plane.

CoS – Class of Service

Represents a set of traffic that require specific delay, loss, and jitter characteristics from the network. Conceptually, a Class of Service pertains to applications with similar characteristics and performance requirements. Service classes are used consistently within the IPS System. [Source: RFC 4594 (wording adapted for IPS)]

CPDLC – Controller-Pilot Data Link Communications

A means of communication between controller and pilot, using data link for ATC communications. [Source: ICAO Doc. 10037]

CPDLC Application – Controller-Pilot Data Link Communications Application

An ATN application that provides a means of data communication between controlling, receiving or downstream ATS units and the aircraft, using air-ground and ground-ground subnetworks, and which is consistent with the ICAO phraseology for the current ATC voice communication. [Source: ICAO Doc. 9880]

CSP – Communication Service Provider

Any public or private entity providing communication services for general air traffic.

Data Plane

The collection of resources across all network devices responsible for forwarding traffic to the next hop along the path to the selected destination network according to the control plane logic.

Downlink

A data packet sent from an aircraft to a ground-based system.

DS – Dialogue Service

An interface between the ATN applications and the ATN/OSI or ATN/IPS upper layer protocols via the control function.

ATTACHMENT 2
GLOSSARY

End System

A system that contains the OSI seven layers and contains one or more end-user application processes. [Source: ICAO Doc. 9880]

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 ensure 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 IPS Host

Ground instantiation of an IPS Host.

Ground IPS Node

Ground instantiation of an IPS Node.

Ground IPS Router

A ground device that is used to support ATN/IPS packet forwarding in both air-ground and ground-ground environments. [Source: RTCA DO-379 and EUROCAE ED-262]

Ground IPS System

The collection of ground components and functions that provide IPS services.

Handover

A process where an aircraft moving across heterogeneous air-ground access networks, including the ANSP ground networks, is able to switch between the different air-ground datalinks and access the air-ground access networks with minimum impact for transactions in transit (e.g. delayed or even loss of transaction).

Infrastructure

This is a general term corresponding to the communication systems that support the application sets. It consists of the network and subnetwork functions.

ATTACHMENT 2
GLOSSARY

Integrity

Safety usage – Qualitative or quantitative attribute of a system or an item indicating that it can be relied upon to work correctly. It is sometimes expressed in terms of the probability of not meeting the work correctly criteria.

Security usage – Property whereby data or an asset has not been modified in an unauthorized manner since it was created, transmitted, or stored.

IPS (aka IPS for Safety Services)

Refer to the definition for ATN/IPS.

IPS Air-Ground Router

A ground IPS Router that interfaces directly with an adjacent airborne host/router over RF media. In other words, the air-ground router is the first-hop ground router for the airborne host/router. [Source: RTCA DO-379 and EUROCAE ED-262]

IPS Gateway

A system that establishes and maintains an operational association between two heterogeneous peer communicating systems, where one system is an IPS Node and the other is a different communication system, such as an OSI End System or an ACARS Host. Note: An IPS Gateway exchanges IPv6 packets with the IPS Node, which may be an Airborne IPS System or a Ground IPS Host.

IPS Host

The originator or terminator of IP packets in the IPS System. IPS Hosts do not route IP packets that are not addressed to it. [Source: RTCA DO-379 and EUROCAE ED-262]

IPS Node

A device that implements IPv6. There are two types of IPS nodes: an IPS Host and an IPS Router. Note: An IPS Gateway could be considered an IPS Node.

IPS Router

A node that forwards Internet protocol (IP) packets not explicitly addressed to itself. A router manages the relaying and routing of data while in transit from an originating IPS Host to a destination IPS Host. [Source: ICAO Doc. 9896]

IPS System

The IPS System is the all-encompassing aviation internet that provides data transport, networking, routing, addressing, naming, mobility, multilink and information security functions to the aviation services. The IPS System includes the Layer 3 and Layer 4 functions of the ISO/IEC 7498-1 OSI 7-layer Reference Model. The IPS System does not include the underlying subnetwork functions that provide connectivity or the applications. [Source: RTCA DO-379 and EUROCAE ED-262]

Join Event

An event generated by a mobile subnetwork when it is recognized that a system has attached to the subnetwork and is available for communication using the subnetwork.

ATTACHMENT 2
GLOSSARY

Leave Event

An event generated by a mobile subnetwork when it is recognized that a system has disconnected from the subnetwork and is no longer available for communication using the subnetwork.

Link Local Address

Link-Local addresses are for use on a single link. Link-Local addresses are designed to be used for addressing on a single link for purposes such as automatic address configuration, neighbor discovery, or when no routers are present.

MASPS – Minimum Aviation System Performance Standards

Specifies characteristics of systems intended for operational use within a defined airspace. Where the systems are global in nature, the system may have international applications that are taken into consideration. The MASPS describes the system (subsystems / functions) and provides information needed to understand the rationale for system characteristics, operational goals, requirements and typical applications. Definitions and assumptions essential to proper understanding of the MASPS are provided as well as minimum system test procedures to verify system performance compliance (e.g., end-to-end performance verification). [Source: RTCA]

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

Ability to use all available air-ground access networks in order to provide the specified performance.

Native IP Application

An application that interfaces directly with the IPS transport layer without the need for an adaptation layer, such as the IPS Dialogue Service interface that is used to accommodate B1, B2, FANS, and ACARS-based applications.

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.

Physical and Link Layers

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

ATTACHMENT 2
GLOSSARY

SARPS – Standards and Recommended Practices

International Standards and Recommended Practices adopted by the Council of ICAO in accordance with Article 37 of the Convention on International Civil Aviation for "securing the highest practicable degree of uniformity in regulations, standards, procedures and organization in relation to aircraft, personnel, airways and auxiliary services in all matters in which such uniformity will facilitate and improve air navigation."

Standard: Any specification for physical characteristics, configuration, materiel, performance, personnel or procedure, the uniform application of which is recognized as necessary for the safety or regularity of international air navigation and to which Contracting States will conform in accordance with the Convention; in the event of impossibility of compliance, notification to the Council is compulsory under Article 38.

Recommended Practice: Any specification for physical characteristics, configuration, matériel, performance, personnel or procedure, the uniform application of which is recognized as desirable in the interest of safety, regularity or efficiency of international air navigation, and to which Contracting States will endeavor to conform in accordance with the Convention.

[Source: *ICAO Website* and ICAO Annex 10, Volume III]

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.

Subnetwork

An actual implementation of a data network that employs a homogeneous protocol and addressing plan and is under control of a single authority. [ICAO Doc. 9705]

Transport Layer

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

Uplink

A data packet sent from a ground-based system to an aircraft.

VDL – VHF Digital Link

A constituent mobile subnetwork of the aeronautical telecommunication network (ATN), operating in the aeronautical mobile VHF frequency band. In addition, the VDL may provide non-ATN functions such as, for instance, digitized voice. [Source; ICAO Annex 10, Volume I]

ATTACHMENT 2
GLOSSARY

VDLM2 – VHF Digital 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.

ATTACHMENT 3
ACARS TO IPS DIALOGUE SERVICE CONVERGENCE FUNCTION

ATTACHMENT 3 ACARS TO IPS DIALOGUE SERVICE CONVERGENCE FUNCTION

3.0 INTRODUCTION

This attachment specifies the ACARS to IPS Dialogue Service Convergence Function (AICF), including its interfaces and functional elements. The AICF adapts ACARS applications to the IPS Dialogue Service (IPS DS), which provides a mechanism for exchanging application messages over the IPS communications infrastructure.

3.1 AICF Overview

Figure 3-1 illustrates the ACARS message flow over the IPS dialogue service via the AICF, as well as the placement of the AICF within the upper layers between the ACARS application or peripheral and the IPS DS. The DTLS and UDP layers are shown for completeness.

COMMENTARY

In this attachment, any detail regarding the IPS DS, DTLS, and UDP layers is provided for illustrative purposes only. Normative information is available in the respective standards for those layers.

The ACARS application, or a peripheral (e.g., FMS), represents existing aircraft applications or systems that exchange messages with ground systems using the ACARS protocol stack. The application messages and protocols are specified in existing standards such as ARINC 620, ARINC 622, ARINC 623, etc. The ACARS application messages are accommodated by the AICF without any changes to the existing ACARS applications, systems, or specifications.

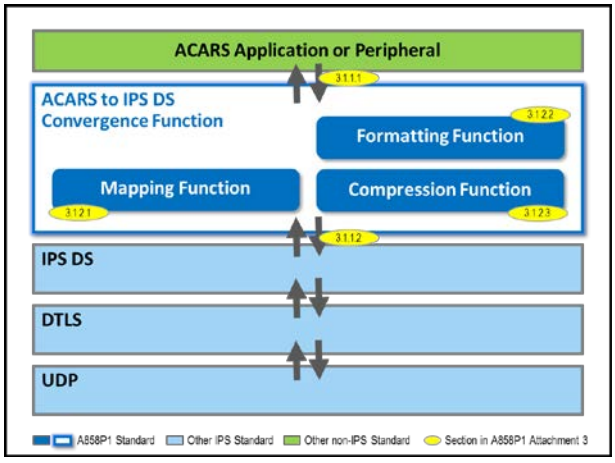

Figure 3-1 – AICF Placement within the Upper Layers

Each AICF function and interface is introduced in the following sub-sections, which are referenced in the figure by yellow ovals. Detailed specifications of downlink and uplink message processing are described in Sections 3.2 and 3.3, respectively, in this attachment.

ATTACHMENT 3
ACARS TO IPS DIALOGUE SERVICE CONVERGENCE FUNCTION

3.1.1 AICF Interfaces

3.1.1.1 ACARS Message Interface

The detailed interface between the ACARS application/peripheral and the AICF is local and implementation-dependent. At a minimum, the interface must support a transport mechanism for exchanging the following ACARS message fields:

- ACARS message Label consisting of two characters.
- Optional ACARS Sub-label consisting of two characters preceded by a "#" character. The Sub-label is present when the ACARS application is hosted in a peripheral, e.g., ARINC 622 hosted in an FMS, and it uniquely identifies the peripheral.
- Optional Supplementary Address field which begins with the "/" character and terminates with a "." character and which may contain:
  - Optional Message Function Identifier (MFI) consisting of two characters immediately following the "/" character and followed by a space character. This field, which identifies flow types from an ACARS peripheral, is mandatory for ARINC 622 messages, and may be present for other ACARS applications as well.
  - One or more supplementary addresses containing three, four, or seven alpha-numeric characters, each of which is separated by a space character. This field is mandatory for ARINC 622 messages and contains either a four-character ATC Facility designator or a seven-character ATC Facility address.
- Application Text field, which contains the bit-oriented (e.g., ARINC 622) or character-oriented (e.g., ARINC 623) data generated/consumed by the ACARS application. If the application text includes a Cyclic Redundancy Check (CRC) to ensure end-to-end integrity, the CRC is preserved during the AICF processing.
- Flight Identifier (FlightID), which is six alpha-numeric characters consisting of a two-character airline identifier and a four-character flight number, and the Message Sequence Number (MSN), which consists of four alpha-numeric characters. Note that the FlightID and MSN are conveyed via this interface only for downlink messages; for uplink messages, the MSN is not included and the FlightID terminates in the AICF and is not presented to the ACARS application or peripheral.

3.1.1.2 IPS Dialogue Service Interface

The interface between the AICF and the IPS DS is the Dialogue Service (DS) interface per ICAO Doc. 9880, Part III. As specified in ICAO Doc. 9896, the IPS Dialogue Service appears as an instance of the dialogue service; therefore, reusing the same interface for the AICF facilitates commonality between B1/B2 application adaptation and ACARS application adaptation. The detailed implementation of the service interface is local and implementation-dependent.

For ACARS application adaptation, the AICF uses the following dialogue service primitives, which represent a subset of primitives supported by the IPS DS:

- D-START – a confirmed service used to establish the binding between communicating peer IPS DS entities

- D-DATA – an unconfirmed service used to exchange messages between peer IPS DS entities
- D-ABORT – an unconfirmed service used to terminate the binding between communicating peer IPS DS entities

In addition to the DS primitives and associated parameters, this interface also conveys control parameters used to identify the ACARS application type as well as the specific ACARS application.

3.1.2 AICF Functions

The AICF consists of three primary functions that operate on ACARS application messages: a Mapping Function, a Formatting Function, and a Compression Function.

3.1.2.1 Mapping Function

The AICF Mapping Function provides the mapping between ACARS application messages and IPS DS primitives and associated parameters. It also maintains the status of the dialogue (i.e., “open” or “closed”) for each application and end entity for which a binding is established using the D-START primitive; the specific mechanism for maintaining the dialogue status is local and implementation-dependent.

Section 3.4 in this attachment specifies the application-specific criteria for mapping to a dialogue service primitive and for setting the dialogue status.

3.1.2.2 Formatting Function

The AICF Formatting Function receives ACARS downlink messages via the ACARS Message Interface and assembles the relevant ACARS application message fields into Uncompressed Application Data, which serves as the input to the Compression Function. Conversely, in the uplink direction, this function parses the Uncompressed Application Data, which is the result of de-compression, into the ACARS application message fields.

Figure 3-2 illustrates the Uncompressed Application Data format, which is the concatenation of the ACARS message label, sub-label (if present), supplementary address field (if present), and the application text.

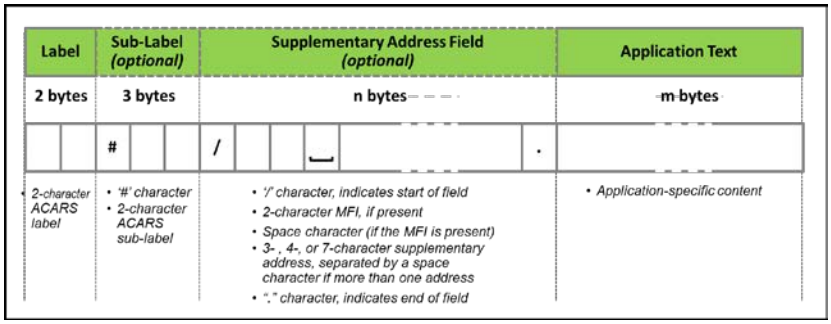

Figure 3-2 – Uncompressed Application Data Format

Note that this function assembles and parses the ACARS application message fields, but it does not in any way change or manipulate the content of the fields

themselves. In addition, since ACARS application messages exchanged using IPS are not encapsulated in the ARINC 618 air-ground protocol, downlink and uplink ACARS messages are not segmented into ARINC 618 ACARS blocks.

3.1.2.3 Compression Function

The AICF includes a Compression Function that applies a data compression algorithm to reduce the size of ACARS application messages exchanged over IPS. The input to the Compression Function (or output resulting from de-compression) is the Uncompressed Application Data. As shown in Figure 3-3, the output of the Compression Function (or input to de-compression) is a 1-byte Compression Parameter concatenated with the Compressed ACARS Message.

COMMENTARY

Some messages (e.g., small or encoded messages) may increase in size when compressed. The compression parameter allows the sending entity to determine compressibility and indicate the most efficient method of conveying the data, which may be with no compression.

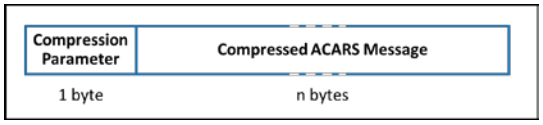

Figure 3-3 – Compressed Application Data Format

The format and field values of the Compression Parameter are shown in Table 3-1.

Table 3-1 – Compression Parameter Format and Field Values

Compression Parameter – 8 bits							
Reserved Field				Compression Algorithm Field			
(MSB) **8**	**7**	**6**	**5**	**4**	**3**	**2**	(LSB) **1**
0x0 thru 0xF: Reserved (future) By default, this field is set to 0x0				0x0: No compression 0x1: DEFLATE compression 0x2 thru 0xF: Reserved (future)			

In addition to “no compression,” Airborne IPS Systems, IPS Gateways, and Ground IPS Hosts that handle ACARS application messages shall support the DEFLATE algorithm, as a minimum. Reserved values in the compression parameter support the addition of other compression algorithms in the future.

3.1.3 IPS Dialogue Service Accommodation of the AICF

To facilitate commonality between B1/B2 application adaptation and ACARS application adaptation, the IPS Dialogue Service (IPS DS) per ICAO Doc. 9896 is used to convey ACARS application messages using the ATNPKT format; refer to Appendix A in this document for ATNPKT examples. The ATNPKT consists of a fixed part, which is always present, and a variable part, which contains optional fields depending on the dialogue service primitive and application data. The inclusion of optional fields in ATNPKT complies with the IPS DS mapping in Table II-1-6 in ICAO Doc. 9896, with the following exceptions:

- The Called Peer ID, Calling Peer ID, and User Data fields are mandatory in any ATNPKT containing a D-START, D-STARTCNF, D-DATA, or D-ABORT primitive.
- The optional Content Version field, which specifies an ASN.1 syntax version associated with B1/B2 application messages, is not used for ACARS-based messages.
- The optional QoS parameter is not used for ACARS-based messages. The network layer utilizes the port number associated with specific ACARS ATS and AOC applications, as described in Section 3.2.2.1 and Table 3-3, to assign message priority. This information is then used to set the differentiated service field in IP packets.

3.2 AICF Downlink Message Processing

Figure 3-4 illustrates the processing of downlink messages from an ACARS application or peripheral.

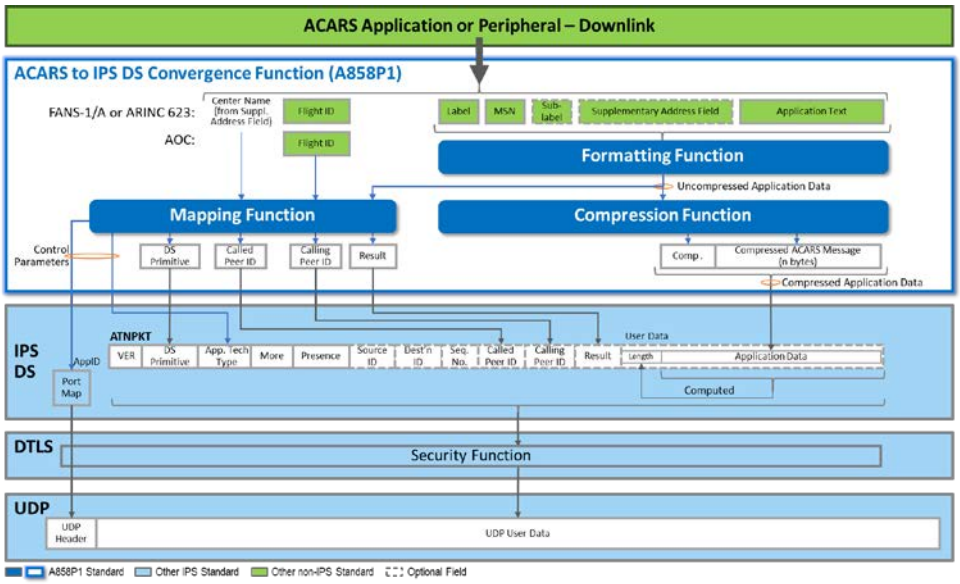

Figure 3-4 – AICF Downlink Processing

For downlink messages, the AICF Mapping Function uses information contained in the Uncompressed Application Data to determine values for the Application Technology Type, Dialogue Service primitive, Called Peer, Calling Peer, and Result parameters.

Other fixed and optional ATNPKT fields (e.g., Source ID and Destination ID) shown in the IPS DS block in Figure 3-4 are generated by the IPS DS for downlink messages, and they are not provided by the AICF via the IPS DS interface.

3.2.1 User Data

As specified in Section 3.1.2.2, the AICF Formatting Function assembles the ACARS application message fields to create Uncompressed Application Data, which serves as an input to both the AICF Mapping Function and Compression Function.

Compressed Application Data, which is the output of the AICF Compression Function specified in Section 3.1.2.3, is the User Data that is conveyed to the IPS DS.

3.2.2 Control Parameters

3.2.2.1 Application Technology Type

The Application Technology Type field indicates the type of application information carried in the IPS DS messages. The AICF communicates the Application Technology Type parameter to the IPS DS via a local, implementation-dependent interface.

For ACARS-based applications, this parameter indicates one of two types: “ACARS ATS / IPS DS” for ARINC 622 (FANS-1/A) or ARINC 623 (character-based ATS) messages; and “ACARS AOC / IPS DS” for all other non-ATS ACARS messages. As shown in Table 3-2, the AICF Mapping Function assigns the Application Technology Type based on the value of the ACARS message Label or the MFI (in the case of an ACARS peripheral) contained in the Uncompressed Application Data, as follows:

ACARS MU/CMU-hosted Application:

`Label/Address(es).Application_text`

ACARS Peripheral-hosted Application:

`Label#Sub-label/MFI<sp>Address(es).Application_text`

Table 3-2 – Application Technology Type

Value of ACARS MFI or Label	Application Technology Type	Application Technology Type Field Value (per ICAO Doc. 9896, Part II, Section 2.1)
Ax, Bx (i.e., the first character is ‘A’ or ‘B’)	“ACARS ATS / IPS DS”	b011
All other MFI / labels (i.e., the first character is not ‘A’ or ‘B’)	“ACARS AOC / IPS DS”	b101

3.2.2.2 Application Identifier

The AICF Mapping Function also provides the IPS DS with an Application Identifier (AppID). The IPS DS uses the AppID to select the appropriate transport layer port number from the application-specific port numbers that are registered with the Internet Assigned Numbers Authority (IANA) and specified in ICAO Doc. 9896.

COMMENTARY

The use of AppID to communicate port information is an optional implementation construct; alternatively, the AICF mapping function

could identify the port directly. However, for the purposes of specifying the AICF, the AppID serves as a convenient abstract representation in lieu of referencing detailed port numbers.

As shown in Table 3-3, the Mapping Function determines the specific application based on the value of the ACARS message Label or the MFI (in the case of an ACARS peripheral) contained in the Uncompressed Application Data.

Table 3-3 – Application Identifier

Value of ACARS MFI or Label	Application Identifier (AppID)	Associated Port Assignment (per ICAO Doc. 9896, Part II, Section 2.2)
A0 (uplink) B0 (downlink)	"ARINC 622 AFN"	5915
A6 (uplink) B6 (downlink)	"ARINC 622 ADS-C"	5917
AA (uplink) BA (downlink)	"ARINC 622 CPDLC"	5916
AW (uplink) BW (downlink)	"ARINC 622 ATS WIND"	5918
Ax (uplink) Bx (downlink) (i.e., MFI / Labels starting with 'A' or 'B', except: A0, B0, A6, B6, AA, BA, AW, BW)	"ARINC 623"	5919
All other MFI / Labels (i.e., the first character is not 'A' or 'B')	"AOC"	5914

The AICF may communicate the AppID to the IPS DS via the same local, implementation-dependent interface used to communicate the Application Technology Type.

3.2.3 Dialogue Service Parameters

3.2.3.1 Dialogue Service Primitive

For downlink messages, the dialogue service primitive is selected based on parameters and values contained in the Uncompressed Application Data, as well as the current state of the dialogue, in accordance with the application-specific criteria specified in Section 3.4 in this attachment.

3.2.3.2 Called and Calling Peer ID Parameters

For downlink messages, the Called Peer ID parameter identifies the intended ground IPS DS peer recipient, and the Calling Peer ID parameter identifies the airborne IPS DS peer originator that is sending the downlink.

For all ACARS ATS application downlink messages (ARINC 622 and ARINC 623), the Called Peer ID parameter contains the ATC Facility designator or address, which is the single 4- or 7-character supplementary address contained in the Uncompressed Application Data. The ATC Facility designator or address is located

between the "/" character and "." character excluding any optional MFI and space <sp> character, as follows:

ACARS MU/CMU-hosted Application:

`Label/`**`ATC_Facility`**`.Application_text`

ACARS Peripheral-hosted Application:

`Label#Sub-label/MFI<sp>`**`ATC_Facility`**`.Application_text`

For all ACARS AOC application downlink messages, the Called Peer ID parameter is not included since the FlightID also contains the airline identifier. For all ACARS ATS and AOC downlink messages, the Calling Peer ID parameter contains the FlightID that is obtained via the ACARS Message Interface, as described in Section 3.1.1.1. The content and length of the Called and Calling Peer ID parameters for downlink messages are summarized in the following table.

Table 3-4 – Called and Calling Peer ID Parameter Content: Downlink

Application Technology Type	Called Peer ID		Calling Peer ID	
	Value	Length (bytes)	Value	Length (bytes)
"ACARS ATS/IPS DS"	ATC Facility designator or address	4 or 7	FlightID	6
"ACARS AOC/IPS DS"	Not included	--	FlightID	6

The Called Peer ID and Calling Peer ID parameters are mandatory when the dialogue service primitive is a D-START, D-STARTCNF, D-DATA, or D-ABORT.

3.2.3.3 Result Parameter

For downlink messages, the Result parameter indicates the airborne acceptance or rejection of a ground-initiated request to establish a dialogue for an application. The value of the Result parameter is per ICAO Doc. 9896, and the application-specific criteria for setting the parameter value is specified in Section 3.4 in this attachment. The AICF Mapping Function uses the Result value to set the status of the dialogue (i.e., "open" when Result is accepted or "closed" when Result is rejected).

The Result parameter is a mandatory parameter when the dialogue service primitive is a D-STARTCNF; otherwise, the parameter is not present for other primitives.

3.3 AICF Uplink Message Processing

Figure 3-5 illustrates the processing of uplink messages to an ACARS application or peripheral.

ATTACHMENT 3
ACARS TO IPS DIALOGUE SERVICE CONVERGENCE FUNCTION

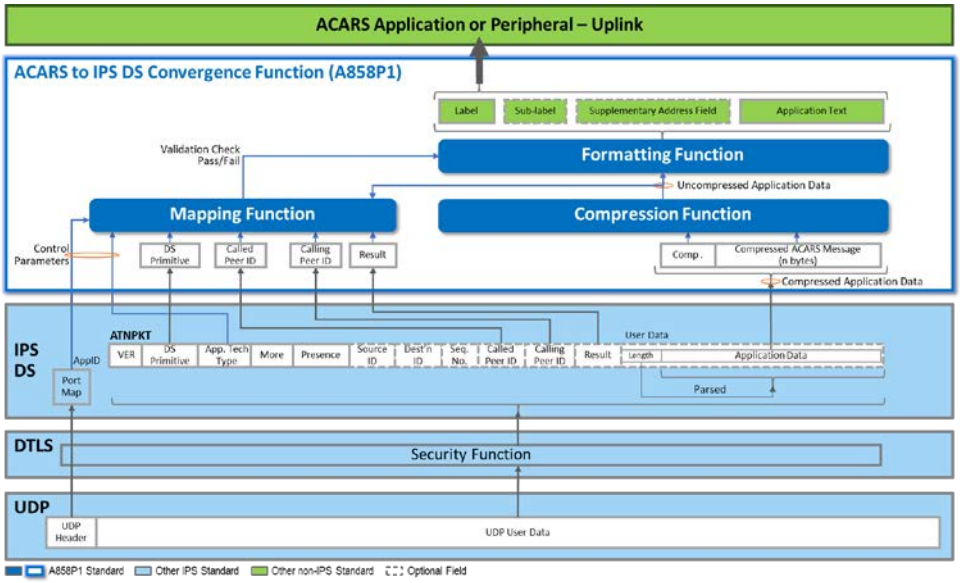

Figure 3-5 – AICF Uplink Processing

For uplink messages, the AICF Mapping Function uses received values for the Application Technology Type, Dialogue Service primitive, Called Peer ID, Calling Peer ID, and Result fields to associate uplink responses with downlink requests and to perform consistency checks (e.g., detect a malformed message).

Other fixed and optional ATNPKT fields (e.g., Source ID and Destination ID), as shown in the IPS DS block in Figure 3-5 are consumed by the IPS DS for uplink messages, and they are not presented to the AICF via the dialogue service interface.

3.3.1 User Data

The User Data received via the IPS DS interface is the Compressed Application Data, which is the input to the Compression Function. As specified in Section 3.1.2.3, the Compression Function applies the appropriate data decompression algorithm to recover the Uncompressed Application Data.

If received parameters in the Uncompressed Application Data are validated by the AICF Mapping Function, as described in the following sections, the Formatting Function parses and conveys the received ACARS application message fields to the ACARS application or peripheral as specified in Section 3.1.2.2.

3.3.2 Control Parameters

3.3.2.1 Application Technology Type and Application Identifier

Upon receipt of an uplink message, the IPS DS communicates the Application Technology Type and AppID information to the AICF via a local, implementation-dependent interface. Once the Uncompressed Application Data is recovered, the

AICF Mapping Function validates that the ACARS message Label or the MFI (in the case of an ACARS peripheral) in the received message is consistent with the Application Technology Type and AppID, based on the values in Table 3-2 and Table 3-3. If the consistency check is successful, then the AICF Mapping Function indicates success to the Formatting Function. If the consistency check fails, then the received message is considered malformed and the AICF discards it; recovery is relegated to the application layer, which detects when an expected response is not received before expiration of a message timer.

3.3.3 Dialogue Service Parameters

3.3.3.1 Dialogue Service Primitive

Upon receipt on an uplink message, the AICF Mapping Function validates the dialogue service primitive based on received parameters and the current state of the dialogue associated with the end entity sending the message.

Section 3.4 in this attachment specifies the application-specific criteria for identifying the expected uplink dialogue service primitive and for setting the dialogue status.

3.3.3.2 Called and Calling Peer ID

For uplink messages, the Called Peer ID parameter identifies the intended airborne IPS DS peer recipient, and the Calling Peer ID parameter identifies the ground IPS DS peer originator that is sending the uplink.

For all ACARS ATS and AOC uplink messages, the Called Peer ID parameter contains the aircraft FlightID. For all ACARS ATS application uplink messages (ARINC 622 and ARINC 623), the Calling Peer ID parameter contains the ATC Facility designator or address. For all ACARS AOC application uplink messages, the Calling Peer ID parameter is not included since the FlightID also contains the airline identifier. The following table summarizes the content and length of the Called and Calling Peer ID parameters for uplink messages.

Table 3-5 – Called and Calling Peer ID Parameter Content: Uplink

Application Technology Type	Called Peer ID		Calling Peer ID	
	Value	Length (bytes)	Value	Length (bytes)
"ACARS ATS/IPS DS"	FlightID	6	ATC Facility designator or address	4 or 7
"ACARS AOC/IPS DS"	FlightID	6	No included	--

The Called Peer ID and Calling Peer ID parameters are mandatory when the dialogue service primitive is a D-START, D-STARTCNF, D-DATA, or D-ABORT. Both fields are consumed by the AICF and are not transferred to the ACARS application or peripheral. The AICF uses the information contained in the fields to perform the following consistency checks:

- For all uplink messages, verify that the length and format of the received parameter values are consistent with expected values (e.g., the value of the received FlightID matches the aircraft-local flight identifier value)

- For ATS uplink messages, verify that the received ATC Facility designator or address corresponds to the ATC Facility designator or address associated with an open dialogue

If the consistency check is successful, then the AICF Mapping Function indicates success to the Formatting Function. If the consistency check fails, then the received message is considered malformed and the AICF discards it; recovery is relegated to the application layer, which detects when an expected response is not received before expiration of a message timer.

3.3.3.3 Result Parameter

For uplink messages, the Result parameter indicates the ground acceptance or rejection of an air-initiated request to establish a dialogue for an application. The value of the Result parameter is per ICAO Doc. 9896, and the application-specific criteria for setting the parameter value is specified in Section 3.4 in this attachment. The AICF Mapping Function within the AICF uses the Result value to set the status of the dialogue (i.e., “open” when Result is accepted or “closed” when Result is rejected).

The Result parameter is a mandatory parameter when the dialogue service primitive is a D-STARTCNF; otherwise, the parameter is not present for other primitives.

3.4 Application-specific DS Primitive Mapping

This section specifies the parameters and values contained in ACARS-based messages that are used to select the dialogue service primitive. Two tables are included for each ACARS-based application: one for primitive mapping when the entity initiating the request does not have an existing dialogue, and one for primitive mapping once a dialogue is established. Each table includes the following information:

- **Procedure** – application-specific procedure (e.g., connection request)
- **Request** – Application message sent by an initiating entity
  - **Message** – Values that specify a specific application message
  - **UL/DL** – Indication of whether the message is an uplink (to aircraft) or downlink (from aircraft)
  - **DS Primitive** – dialogue service primitive for the specific application message
- **Response** – Application message sent by a responding entity
  - The sub-columns are defined the same as for Request
- **Dialogue Status** – status of the application-specific dialogue between the aircraft and a ground entity at the completion of the request-response sequence

The ACARS-based applications addressed in this section include:

- Section 3.4.1 – ARINC 622 – ATS Data Link Applications, including AFN, CPDLC, ADS-C, and ATS WIND
- Section 3.4.2 – ARINC 623 – Character-oriented ATS
- Section 3.4.3 – AOC

Each of these sections also describes the application-specific criteria for determining and setting the open/closed status of the dialogue.

3.4.1 ARINC 622 – ATS Data Link Applications

3.4.1.1 AFN Application

The Uncompressed Application Data is an AFN application message when AppID equals “ARINC 622 AFN” per the criteria in Table 3-3 in this attachment.

In each of the following tables, the columns labeled “A622 Message” specify the three-character Imbedded Message Identified (IMI) and Message Type Identifier (MTI) values that are contained in the application text and which identify a specific AFN application message, including:

- FN_CON (MTI = FPO) – AFN Contact message
- FN_AK (MTI = FAK) – AFN Acknowledge message
- FN_CAD (MTI = FCA) – AFN Contact Advisory message
- FN_RESP (MTI = FRP) – AFN Response message
- FN_COMP (MTI = FCP) – AFN Complete message

The IMI and MTI values are used to select the dialogue service primitive in concert with the current state of the dialogue, which is associated with a specific ground center (i.e., the ATC Facility designator or address included in the Called or Calling Peer ID parameter). Some AFN messages include a one-byte reason code after the MTI, and the value of this code is used to determine the dialogue status upon completion of the request-response sequence.

The following table specifies the primitive mapping when a dialogue does not exist, meaning that the dialogue status is “AFN-CLOSED” for the entity initiating the request. “AFN-CLOSED” is the initial state when the AICF is initialized.

Table 3-6 – DS Primitive Mapping for AFN Application: No Existing Dialogue

Procedure	Request			Response			Dialogue Status	Notes
	A622 Message	UL/ DL	DS Primitive	A622 Message	UL/ DL	DS Primitive		
Contact (Logon)	IMI = AFN MTI = FPO	DL	**D-START**	IMI = AFN MTI = FAK Reason = 0	UL	**D-STARTCNF** Result = Accepted	AFN-OPEN	1, 2
				IMI = AFN MTI = FAK Reason ≠ 0	UL	**D-STARTCNF** Result = Rejected	AFN-CLOSED	

Note 1: Initial AFN logon to a center when no dialogue with that center exists.
Note 2: When a ground center has an existing (i.e., residual) AFN dialogue with the aircraft that is initiating a new AFN dialogue using D-START, then the ground center supplants the existing dialogue with the new dialogue.

The following table specifies the primitive mapping when a dialogue exists, meaning that the dialogue status is “AFN-OPEN” for the entity initiating the request.

ATTACHMENT 3
ACARS TO IPS DIALOGUE SERVICE CONVERGENCE FUNCTION

Table 3-7 – DS Primitive Mapping for AFN Application: Existing Dialogue

Procedure	Request			Response			Dialogue Status	Notes
	A622 Message	UL/ DL	DS Primitive	A622 Message	UL/ DL	DS Primitive		
Contact (Logon)	IMI = AFN MTI = FPO	DL	**D-DATA**	IMI = AFN MTI = FAK Reason = 0	UL	**D-DATA**	AFN-OPEN	1
				IMI = AFN MTI = FAK Reason ≠ 0	UL	**D-DATA**	AFN-CLOSED	
Address Forwarding	IMI = AFN MTI = FCA	UL	**D-DATA**	IMI = AFN MTI = FRP	DL	**D-DATA**	(no change)	
	IMI = AFN MTI = FCP Reason = 0	DL	**D-DATA**	None	--	**--**	AFN-CLOSED	
	IMI = AFN MTI = FCP Reason ≠ 0	DL	**D-DATA**	None	--	**--**	(no change)	2

Note 1: AFN logon to a center when there is an existing dialogue with that center, e.g., when the pilot enters a new flight number for a multi-leg flight.
Note 2: If the result of the procedure not successful, then the AFN dialogue remains open.

Once a dialogue for AFN messages is opened between an aircraft and a specific ground center, the dialogue remains open until one of the request-response sequences results in "AFN-CLOSED" dialogue status. In addition, the dialogue may be closed silently[4] and the dialogue status set to "AFN-CLOSED" upon the termination of a flight (e.g., weight-on-wheels and forward door open). The discrete inputs used to determine end-of-flight is implementation-dependent.

3.4.1.2 CPDLC Application

The Uncompressed Application Data is a CPDLC application message when AppID equals "ARINC 622 CPDLC" per the criteria in Table 3-3 in this attachment.

In each of the following tables, the column labeled "A622 Message" specifies the three-character IMI value that is contained in the application text and which identifies a specific CPDLC application message. The IMI value is used to select the dialogue service primitive in concert with the current state of the dialogue, which is associated with a specific ground center (i.e., the ATC Facility designator or address included in the Called or Calling Peer ID parameter). The connection confirmation (CCx) and disconnect request (DRx) messages are used to set the dialogue status upon completion of the request-response sequences for connection initiation and termination, respectively.

The following table specifies the primitive mapping when a dialogue does not exist, meaning that the dialogue status is "CPDLC-CLOSED" for the entity initiating the request. "CPDLC-CLOSED" is the initial state when the AICF is initialized.

[4] Silently means that a dialogue is closed locally by the aircraft.

ATTACHMENT 3
ACARS TO IPS DIALOGUE SERVICE CONVERGENCE FUNCTION

Table 3-8 – DS Primitive Mapping for CPDLC Application: No Existing Dialogue

Procedure	Request			Response			Dialogue Status	Notes
	A622 Message	UL/ DL	DS Primitive	A622 Message	UL/ DL	DS Primitive		
Connection Request	IMI = CRx	UL	**D-START**	IMI = CCx	DL	**D-STARTCNF** Result = Accepted	CPDLC-OPEN	1, 2, 3
				IMI = DRx	DL	**D-STARTCNF** Result = Rejected	CPDLC-CLOSED	
Note 1: In the IMI, the value of the third character 'x' is the version number of the message, e.g., CR1. Note 2: A successful AFN logon is required prior to an initial CPDLC connection request. After a successful AFN login, the aircraft will accept a CPDLC connection request from other centers within the same administrative domain, which is the recommended implementation per RTCA DO-258A/ EUROCAE ED-100A. Note 3: When the aircraft has an existing CPDLC dialogue with a specific center, a subsequent connection request (using D-START) from the same center is treated as a new CPDLC dialogue that supplants the existing dialogue.								

The following table specifies the primitive mapping when a dialogue exists, meaning that the dialogue status is "CPDLC-OPEN" for the entity initiating the request.

Table 3-9 – DS Primitive Mapping for CPDLC Application: Existing Dialogue

Procedure	Request			Response			Dialogue Status	Notes
	A622 Message	UL/ DL	DS Primitive	A622 Message	UL/ DL	DS Primitive		
Connection Request	IMI = CRx	UL	**D-START**	IMI = CCx	DL	**D-STARTCNF** Result = Accepted	CPDLC-OPEN	1, 2
				IMI = DRx	DL	**D-STARTCNF** Result = Rejected	CPDLC-CLOSED	
Uplink Message (UMxxx)	IMI = ATx	UL	**D-DATA**	Depends upon the uplink message	DL	**D-DATA**	(no change)	1
Downlink Message (DMxxx)	IMI = ATx	DL	**D-DATA**	Depends upon the downlink message	UL	**D-DATA**	(no change)	1
Connection Termination	IMI = ATx (UM161 end service)	UL	**D-DATA**	IMI = DRx	DL	**D-ABORT**	CPDLC-CLOSED	1, 3
	IMI = DRx (ground initiated)	UL	**D-ABORT**	None	--	**--**	CPDLC-CLOSED AFN-CLOSED	1, 4
	IMI = DRx (aircraft initiated)	DL	**D-ABORT**	None	--	--	CPDLC-CLOSED AFN-CLOSED	1, 5

ATTACHMENT 3
ACARS TO IPS DIALOGUE SERVICE CONVERGENCE FUNCTION

Note 1: In the IMI, the value of the third character 'x' is the version number of the message, e.g., CR1.
Note 2: When the aircraft has an existing CPDLC dialogue with a specific center, a subsequent connection request (using D-START) from the same center is treated as a new CPDLC dialogue that supplants the existing dialogue.
Note 3: Ground-initiated end service uplink message UM161, which occurs after transfer from the current data authority (CDA) to next data authority (NDA), closes the CPDLC dialogue for the CDA when the disconnect request (DRx) message is sent.
Note 4: Ground-initiated disconnect request closes both the CPDLC and associated AFN dialogues when the disconnect request (DRx) message is sent. No impact on any open ADS-C dialogues. Since some avionics implementations do not support DRx uplinks, ICAO Doc. 10037 specifies using an ATx uplink containing a UM161 End Service message to terminate a CPDLC connection (refer to the prior row in this table).
Note 5: Aircraft-initiated (e.g., by pilot) disconnect request closes both the CPDLC and associated AFN dialogues when the disconnect request (DRx) message is sent. No impact on open ADS-C dialogues.

Once a dialogue for CPDLC messages is opened between an aircraft and a specific ground center, the dialogue remains open until one of the request-response sequences results in "CPDLC-CLOSED" dialogue status. In addition, the dialogue may be closed silently and the dialogue status set to "CPDLC-CLOSED" upon the termination of a flight (e.g., weight-on-wheels and forward door open). The discrete inputs used to determine end-of-flight is implementation-dependent.

3.4.1.3 ADS-C Application

The Uncompressed Application Data is an ADS-C application message when AppID equals "ARINC 622 ADS-C" per the criteria in Table 3-3 in this attachment.

In each of the following tables, the column labeled "A622 Message" specifies the three-character IMI value that is contained in the application text and which identifies ADS-C application messages. The IMI value is used to select the dialogue service primitive in concert with the current state of the dialogue, which is associated with a specific ground center (i.e., the ATC Facility designator or address included in the Called or Calling Peer ID parameter). The disconnect (DIS) message is used to set the dialogue status upon completion of the request-response sequence for connection termination.

The following table specifies the primitive mapping when a dialogue does not exist, meaning that the dialogue status is "ADS-CLOSED" for the entity initiating the request. "ADS-CLOSED" is the initial state when the AICF is initialized.

Table 3-10 – DS Primitive Mapping for ADS-C: No Existing Dialogue

Procedure	Request			Response			Dialogue Status	Notes
	A622 Message	UL/ DL	DS Primitive	A622 Message	UL/ DL	DS Primitive		
Initial Contract Establishment	IMI = ADS (any contract request)	UL	**D-START**	IMI = ADS (ACK or NAK tag)	DL	**D-STARTCNF** Result = Accepted	ADS-OPEN	1, 2
				IMI = DIS	DL	**D-STARTCNF** Result = Rejected	ADS-CLOSED	3
Note 1: Establish an ADS-C dialogue, which is independent of AFN and CPDLC dialogues. Note 2: When an aircraft has an existing (i.e., residual) ADS-C dialogue with the center that is initiating a new ADS-C dialogue using D-START, then the aircraft supplants the existing dialogue with the new dialogue.								

Note 3: When the ground attempts to establish an ADS-C contract but the aircraft ADS-C function is disabled, the aircraft response is a downlink disconnect request.

The following table specifies the primitive mapping when a dialogue exists, meaning that the dialogue status is "ADS-OPEN" for the entity initiating the request.

Table 3-11 – DS Primitive Mapping for ADS-C Application: Existing Dialogue

Procedure	Request			Response			Dialogue Status	Notes
	A622 Message	UL/ DL	DS Primitive	A622 Message	UL/ DL	DS Primitive		
Contract Establishment	IMI = ADS (any contract request)	UL	**D-DATA**	IMI = ADS (ACK or NAK tag)	DL	**D-DATA**	(no change)	1
ADS-C Report	IMI = ADS (report tag + data)	DL	**D-DATA**	None	--	**--**	(no change)	
Cancel Contract(s) (Ground-initiated)	IMI = ADS (cancel contract)	UL	**D-DATA**	IMI = ADS (ACK or NAK tag)	DL	**D-DATA**	(no change)	2
	IMI = ADS (cancel all contracts and terminate connection)	UL	**D-DATA**	IMI = DIS	DL	**D-ABORT**	ADS-CLOSED	3
Disconnect (Aircraft-initiated)	IMI = DIS	DL	**D-ABORT**	None	--	**--**	ADS-CLOSED	4

Note 1: Establish an additional ADS-C contract(s) when there is an existing dialogue with the center requesting the contract.
Note 2: Cancelling a specific contract does not close the dialogue, which allows other existing ADS-C contracts to be maintained and new ADS-C contracts to be established.
Note 3: Cancelling all contracts terminates the connection, which closes the ADS-C dialogue.
Note 4: An aircraft initiated disconnect may be the result of pilot action, three consecutive ADS-C negative acknowledgements (NAKs), or expiration of the ADS-C application inactivity timer.

Once a dialogue for ADS-C messages is opened between an aircraft and a specific ground center, the dialogue remains open until one of the request-response sequences results in "ADS-CLOSED" dialogue status.

3.4.1.4 ATS WIND Application

The Uncompressed Application Data is an ATS WIND application message when AppID equals "ARINC 622 ATS WIND" per the criteria in Table 3-3 in this attachment.

In each of the following tables, the column labeled "A622 Message" specifies the three-character IMI value that is contained in the application text and which identifies a specific ATS WIND message. The IMI value is used to select the dialogue service primitive in concert with the current state of the dialogue, which is associated with a specific ground center (i.e., the ATC Facility designator or address included in the Called or Calling Peer ID parameter).

ATTACHMENT 3
ACARS TO IPS DIALOGUE SERVICE CONVERGENCE FUNCTION

The following table specifies the primitive mapping when a dialogue does not exist, meaning that the dialogue status is "WIND-CLOSED" for the entity initiating the request. "WIND-CLOSED" is the initial state when the AICF is initialized.

Table 3-12 – DS Primitive Mapping for ATS WIND Application: No Existing Dialogue

Procedure	Request			Response			Dialogue Status	Notes
	A622 Message	UL/ DL	DS Primitive	A622 Message	UL/ DL	DS Primitive		
Uplink Wind	IMI = PWF or PWI	UL	**D-START**	IMI = RES	DL	**D-STARTCNF** Result = Accepted	WIND-OPEN	1
				IMI = REJ	DL	**D-STARTCNF** Result = Rejected	WIND-CLOSED	
Note 1: When the aircraft has an existing (i.e., residual) ATS WIND dialogue with the center that is initiating a new ATS WIND dialogue, then the aircraft supplants the existing dialogue with the new dialogue.								

The following table specifies the primitive mapping when a dialogue exists, meaning that the dialogue status is "WIND-OPEN" for the entity initiating the request.

Table 3-13 – DS Primitive Mapping for ATS WIND Application: Existing Dialogue

Procedure	Request			Response			Dialogue Status	Notes
	A622 Message	UL/ DL	DS Primitive	A622 Message	UL/ DL	DS Primitive		
Uplink Wind	IMI = PWF or PWI	UL	**D-DATA**	IMI = RES	DL	**D-DATA**	(no change)	
				IMI = REJ	DL	**D-ABORT**	WIND-CLOSED	1
Note 1: A rejection (REJ) downlink is sent when one or more errors is detected in the uplink, which closes the ATS WIND dialogue.								

Once a dialogue for ATS WIND messages is opened between an aircraft and a specific ground center, the dialogue remains open until one of the request-response sequences results in "WIND-CLOSED" dialogue status. In addition, the dialogue may be closed silently and the dialogue status set to "WIND-CLOSED" upon the termination of a flight (e.g., weight-on-wheels and forward door open). The discrete inputs used to determine end-of-flight is implementation-dependent.

3.4.2 ARINC 623 – Character-oriented ATS

The Uncompressed Application Data is an ARINC 623 application message when AppID equals "ARINC 623" per the criteria in Table 3-3 in this attachment.

In each of the following tables, the column labeled "A623 Message" specifies the three-character IMI value that is contained in the application text and which identifies a specific ARINC 623 message. The IMI value is used to select the dialogue service primitive in concert with the current state of the dialogue, which is associated with a specific ground center (i.e., the ATC Facility designator or address included in the Called or Calling Peer ID parameter).

ATTACHMENT 3
ACARS TO IPS DIALOGUE SERVICE CONVERGENCE FUNCTION

The following table specifies the primitive mapping when a dialogue does not exist, meaning that the dialogue status is "623-CLOSED" for the entity initiating the request. "623-CLOSED" is the initial state when the AICF is initialized.

Table 3-14 – DS Primitive Mapping for ARINC 623 Messages: No Existing Dialogue

Procedure	Request			Response			Dialogue Status	Notes
	A623 Message	UL/ DL	DS Primitive	A623 Message	UL/ DL	DS Primitive		
Pushback Clearance	IMI = PCx	DL	**D-START**	IMI = PCx or FSx	UL	**D-STARTCNF** Result = Accepted	623-OPEN	1, 2, 3
Taxi Clearance	IMI = ETx	DL	**D-START**	IMI = ETx or FSx	UL	**D-STARTCNF** Result = Accepted	623-OPEN	1, 2, 3
Departure Clearance	IMI = DCx	DL	**D-START**	IMI = DCx or FSx	UL	**D-STARTCNF** Result = Accepted	623-OPEN	1, 2, 3
Oceanic Clearance	IMI = OCx	DL	**D-START**	IMI = OCx or FSx	UL	**D-STARTCNF** Result = Accepted	623-OPEN	1, 2, 3
Automatic Terminal Information Service	IMI = TIx	DL	**D-START**	IMI = TIx	UL	**D-STARTCNF** Result = Accepted	623-OPEN	1, 2
Terminal Weather	IMI = TWx	DL	**D-START**	IMI = TWx	UL	**D-STARTCNF** Result = Accepted	623-OPEN	1, 2

Note 1: In the IMI, the value of the third character 'x' is the version number of the message.
Note 2: When a ground center has an existing (i.e., residual) ARINC 623 dialogue with the aircraft that is initiating a hew ARINC 623 dialogue, then the ground center supplants the existing dialogue with the new dialogue.
Note 3: The uplink response may be a Flight Service message (IMI = FSx), which the ground ATC may use to indicate: the status of the request; the need to standby while processing is completed; or the need to revert to voice in the event of an error with the request.

The following table specifies the primitive mapping when a dialogue exists, meaning that the dialogue status is "623-OPEN" for the entity initiating the request.

Table 3-15 – DS Primitive Mapping for ARINC 623 Messages: Existing Dialogue

Procedure	Request			Response			Dialogue Status	Notes
	A623 Message	UL/ DL	DS Primitive	A623 Message	UL/ DL	DS Primitive		
Pushback Clearance	IMI = PCx	DL	**D-DATA**	IMI = PCx or FSx	UL	**D-DATA**	(no change)	1, 2
Taxi Clearance	IMI = ETx	DL	**D-DATA**	IMI = ETx or FSx	UL	**D-DATA**	(no change)	1, 2
Departure Clearance	IMI = DCx	DL	**D-DATA**	IMI = DCx or FSx	UL	**D-DATA**	(no change)	1, 2

ATTACHMENT 3
ACARS TO IPS DIALOGUE SERVICE CONVERGENCE FUNCTION

Oceanic Clearance	IMI = OCx	DL	**D-DATA**	IMI = OCx or FSx	UL	**D-DATA**	(no change)	1, 2
Automatic Terminal Information Service	IMI = TIx	DL	**D-DATA**	IMI = TIx	UL	**D-DATA**	(no change)	1
Terminal Weather	IMI = TWx	DL	**D-DATA**	IMI = TWx	UL	**D-DATA**	(no change)	1
Note 1: In the IMI, the value of the third character 'x' is the version number of the message. Note 2: The uplink response may be a Flight Service message (IMI = FSx), which the ground ATC may use to indicate: the status of the request; the need to standby while processing is completed; or the need to revert to voice in the event of an error with the request.								

Once a dialogue for ARINC 623 messages is opened between an aircraft and a specific ground center, the dialogue remains open until a subsequent D-START sequence restarts the dialogue. In addition, the dialogue may be closed silently and the dialogue status set to "623-CLOSED" upon the termination of a flight (e.g., weight-on-wheels and forward door open). The discrete inputs used to determine end-of-flight is implementation-dependent.

In addition, to minimize the number of open dialogues, the Airborne IPS System may be designed to maintain a single ARINC 623 dialogue such that a dialogue with each new ground center silently closes a prior dialogue with a previous ground center. For example, a dialogue may be opened initially at a departure airport when the flight crew requests weather information and/or pushback/taxi clearance. During flight, an open ARINC 623 dialogue is closed silently each time the flight crew requests weather information from a different airport. Upon arrival, an open ARINC 623 dialogue is closed silently when the flight crew requests weather information and/or taxi clearance from the arrival airport.

3.4.3 AOC

The Uncompressed Application Data is an AOC message when AppID equals "AOC" per the criteria in Table 3-3 in this attachment. In each of the following tables, the presence of an AOC Label or MFI is used to select the dialogue service primitive in concert with the current state of the dialogue.

The following table specifies the primitive mapping when a dialogue does not exist, meaning that the dialogue status is "AOC-CLOSED" for the entity initiating the request. "AOC-CLOSED" is the initial state when the AICF is initialized.

Table 3-16 – DS Primitive Mapping for AOC Messages: No Existing Dialogue

Procedure	Request			Response			Dialogue Status	Notes
	AOC Message	UL/ DL	DS Primitive	AOC Message	UL/ DL	DS Primitive		
Any AOC UL or DL message	Any	Any	**D-START**	Any	Any	**D-STARTCNF** Result = Accepted	AOC-OPEN	1
Note 1: The first AOC message is sent in a D-START to initiate the dialogue. This occurs upon AICF initialization or whenever the aircraft FlightID changes.								

ATTACHMENT 3
ACARS TO IPS DIALOGUE SERVICE CONVERGENCE FUNCTION

The following table specifies the primitive mapping when a dialogue exists, meaning that the dialogue status is "AOC-OPEN" for the entity initiating the request.

Table 3-17 – DS Primitive Mapping for AOC Messages: Existing Dialogue

Procedure	Request			Response			Dialogue Status	Notes
	AOC Message	UL/ DL	DS Primitive	AOC Message	UL/ DL	DS Primitive		
Any AOC UL or DL message	Any	Any	**D-DATA**	Any	Any	**D-DATA**	(no change)	

Once a dialogue for AOC messages is opened, the dialogue remains open until the FlightID changes and a subsequent D-START sequence restarts the dialogue. In addition, the dialogue may be closed silently and the dialogue status set to "AOC-CLOSED" upon expiration of an application inactivity timer or upon the termination of a flight (e.g., weight-on-wheels and forward door open), whichever occurs first. The discrete inputs used to determine end-of-flight is implementation-dependent.

ATTACHMENT 4 IPS SECURITY EVENT LOG FORMAT

4.0 GENERAL FORMAT

The format of IPS security event log messages is based on the standardized logging format specified in RFC 5424, *The Syslog Protocol*. RFC 5424 defines a message log format consisting of three general elements:

- HEADER element
- Structured Data (SD) elements – Optional information using IANA-registered identifiers.
- Message (MSG) element – Free-form field that provides detail about the log event.

For IPS log entries, the composition and formatting of the HEADER element complies with RFC 5424 and contains the following sub-elements:

- PRI – Priority Value that represents both the facility (e.g., kernel) and the severity (e.g., Critical)
- VERSION – Version of the Syslog protocol specification
- TIMESTAMP – date/time of the log event in accordance with RFC 3339
- HOSTNAME – the system originating the syslog message
- APP-NAME – the device or application originating the syslog message
- PROCID – if applicable, the name or identifier of the process originating the syslog message
- MSGID – an optional message identifier that may be included to help with filtering types of messages

To minimize implementation complexity and log size, the Structured Data (SD) elements shall not be used in implementations of the Airborne IPS System.

The Message (MSG) element content is defined specifically for the Airborne IPS System in order to log necessary security event information while minimizing the log size. Note that the specification of the IPS-specific Message element includes a version number, with a value ranging from “1” to “9” and “A” to “Z”, to support evolution of the log content over time as Airborne IPS Systems are fielded and enhancements to log information (e.g., additional fields) are identified.

COMMENTARY

This document specifies an initial version, identified as Version 1. As necessary, additional versions will be included in future supplements to this document.

The following sections in this attachment define the IPS-specific content of the Message (MSG) element.

COMMENTARY

While the log format specified in this attachment is applicable to logs generated by the Airborne IPS System, the same format may be adopted by Ground IPS Systems (i.e., Ground IPS Hosts and IPS Gateways). However, ground system logs are outside the scope of this document.

ATTACHMENT 4
IPS SECURITY EVENT LOG FORMAT

4.1 IPS-specific Message (MSG) Element – Version 1

4.1.1 Encoding

For Version 1, the text in the MSG element should use 8-bit Unicode Transformation Format (UTF-8) encoding.

4.1.2 Content

For Version 1, the content of the MSG element includes the IPS-specific fields specified in the following table.

Table 5-1 – IPS-specific Message Element Content

MSG Element Field	Description	Details
BOM	Byte Order Mask	Per RFC 5424, fixed 3-byte value of 0xEF 0xBB 0xBF, which signals the start of the MSG element and indicates UTF-8 encoding.
Version Number	Version of the IPS-specific Message Element	1 = Initial version, as specified herein
System ID	Airborne IPS System identification and version information	Vendor-specific (e.g., model number, part number, etc.)
Event Type	Type of log entry for the Airborne IPS System	Logged using the numerical value or the associated ASCII string. NOTE: Numbers in parentheses reference event descriptions in the main body of this document. 0 = Debug 1 = System (Section 4.4.2.3.1) 2 = ConfigChg (Section 4.4.2.3.1) 3 = SecChannel (Section 4.4.2.3.2) 4 = KeyMgmt (Section 4.4.2.3.3) 5 = NetInterface (Section 4.4.2.3.4) 6 = Firewall (Section 4.4.2.3.5) 7 = RateLimit (Section 4.4.2.3.5) 8 = Perf (Section 4.4.2.3.6)
Interface Type	Type of interface to/from which data was sent/received	Logged if applicable using the values: 0 = Other 1 = Satcom-INMARSAT 2 = VDR 3 = AeroMACS 4 = HF 5 = Satcom-Iridium
IP Addresses/ Ports	Destination addresses and port number associated with the log event	Logged if applicable using the format: `[IPv6 address]:port` where the IPv6 address is inside square brackets to distinguish address colons from the colon preceding the port number.
Pattern (Code Rule Set)	Identify what rule set violation caused the logging event	1 = Unauthorized config change 2 = Buffer/Queue Limit rule 3 = Interface Input Data rule

ATTACHMENT 4
IPS SECURITY EVENT LOG FORMAT

MSG Element Field	Description	Details
		4 = Network layer rule 5 = Transport layer rule 6 = Application signature failure 7 = Service Access Control List (ACL) Exception/configuration rule 8 = Receive Data Rate limit rule 9 = Cipher Modes rule 10 = Configuration change rule 12 = System Exceptions 11-255 = Reserved for future use
Traffic Direction	Direction of the data flow associated with the event	1 = Aircraft to Ground 2 = Ground to Aircraft 3 = Ground to Ground (Note: This value may be used by Ground IPS Systems; however, it is not applicable to log entries generated by the Airborne IPS System.) 4 = Aircraft-internal
Data Signature	Data signature that triggered the log	Logged if applicable. Data signature of the application payload that triggered the event and can be co-aligned with the ground log, e.g., the first 32 octets of application data
Service/ Application Details	Information regarding the service/application that triggered the log, if multiple levels of logging are performed	Application type as defined in ARINC 620 and ICAO Doc. 9896 for the ATNPKT (and other documents, when future Native IP applications are defined)
User Information/ Access Control Data	User information and access control information	Logged if applicable. System services/functions or user system access information, including but not limited to: Username, Application / System partition or system service name, and Access Control Data • User and System access control data if system configuration is modified • Traffic access control data (e.g., for a forwarding function if IPS System is configured as router – refer to Section 4.3.4).
Payload	User data payload associated with the log entry	Logged if applicable. First 64 bytes of user data payload

4.1.3 Field Delimiter

With the exception of the initial Byte Order Mask (BOM), each subsequent field in the MSG element terminates with the comma (“,”) character, which serves as a field delimiter. The comma delimiter shall not be present after the last field. This syntax is

illustrated in the following example, which shows that there is no comma after the BOM, there is a comma after the version field ("1"), and then there is no comma after the last field, which is the payload:

`BOM1,…,Payload`

Note that in the example above, the unprintable Unicode BOM field is represented simply as "BOM".

If the content of a field is null, then the field must include just the comma delimiter character. In the following example, FieldN is null but the preceding and subsequent fields include content:

`…,FieldN-1,,FieldN+1,…`

If the content of a field contains a comma character, then the content of the field shall be enclosed in double quotes, as shown in the following example:

`…,FieldN-1,"When in Rome, do as the Romans do",FieldN+1,…`

4.1.4 Examples

The following are examples of the Message (MSG) element of a security event log. Note that the RFC 5424-compliant HEADER element is not shown.

Example Log 1:

```
BOM1,,5,2,[20010db80a0b12f0000000000000000a:171a],2,2,H1
210ACV053A#T2B/ILNGE7X.CLB102.TRXVCKCV3CLX53A
191001235257TJBQEHAM+00007
8F959112670000E00022124M70P03C090C09004060D092401M43P04,1,3,00
42000004200000004I900002290000911:::::::00002G010000C1002001K
```

Message Content Description:

MSG Element Field	Details
BOM	Byte Order Mask per Table 5-1
Version Number	1
System ID	Null
Event Type	5 = NetInterface (Section 4.4.2.3.4)
Interface Type	2 = VDR
IP Addresses/ Ports	`[20010db80a0b12f0000000000000000a:171a]`
Pattern (Code Rule Set)	2 = Buffer/Queue Limit rule
Traffic Direction	2 = Ground to Aircraft
Data Signature	`H1  210ACV ... 2401M43P04`
Service/ Application Details	1 = ACARS
User Information/ Access Control Data	3 = Traffic Access Violation
Payload (initial 64 bytes)	`0042000004 ... 0C1002001K`

ATTACHMENT 4
IPS SECURITY EVENT LOG FORMAT

Example Log 2:

```
BOM1,,2,0,[:00],10,4,"Chain FORWARD (policy DENY) Port(*):
TCP(0),UDP(1), ALL
Chain FORWARD (policy ACCEPT) port 5908
Chain FORWARD (policy ACCEPT) port 5909
Chain FORWARD (policy ACCEPT) port 5910
Chain FORWARD (policy ACCEPT) port 5913
Chain FORWARD (policy ACCEPT) port 5914
Chain FORWARD (policy ACCEPT) port 5915
Chain FORWARD (policy ACCEPT) port 5916
Chain FORWARD (policy ACCEPT) port 5917
target prot opt source destination LOG UDP – ::00/0 ::00/FFFF
REJECT UDP – ::00/0 ::00/FFFF UDP
reject-with icmp”
,52,4,00420000042000000004I900002290000911
```

Message Content Description:

MSG Element Field	Details
BOM	Byte Order Mask per Table 5-1
Version Number	1
System ID	Null
Event Type	2 = ConfigChg (Section 4.4.2.3.1)
Interface Type	0 = Other
IP Addresses/ Ports	[:00] = Localhost
Pattern (Code Rule Set)	10 = Configuration change rule
Traffic Direction	4 = Aircraft-internal
Data Signature	“Chain Forward ... with icmp”
Service/ Application Details	52 = service application - packet processing rule set
User Information/ Access Control Data	4 = Traffic access control data
Payload	0042000004 ... 2290000911

Example Log 3:

```
BOM1,,4,{1,2},[::00],12,4,MIIDqDCCAy+gAwIBAgIDAZouMAoGCCqGSM49
BAMDMIGQMQswCQYDVQQGEwJVUzEL,6,8,
```

Message Content Description:

MSG Element Field	Details
BOM	Byte Order Mask per Table 5-1
Version Number	1
System ID	Null
Event Type	4 = KeyMgmt (Section 4.4.2.3.3)

ATTACHMENT 4
IPS SECURITY EVENT LOG FORMAT

MSG Element Field	Details
Interface Type	1 = Satcom-INMARSAT OR 2 = VDR
IP Addresses/ Ports	[:00] = Localhost
Pattern (Code Rule Set)	12 = System Exceptions
Traffic Direction	4 = Aircraft-internal
Data Signature	MIIDqDCCAy ... QGEwJVUzEL
Service/ Application Details	6 = service application – X.509 certificate
User Information/ Access Control Data	8 = incorrect trust anchor certificate signature
Payload	Null

APPENDIX A
ATNPKT MESSAGE FORMAT EXAMPLES

APPENDIX A ATNKPKT MESSAGE FORMAT EXAMPLES

A-1 ATNPKT Overview

As specified in ICAO Doc. 9896, the IPS Dialogue Service (IPS DS) uses the ATNPKT message format to convey information between peer airborne and ground IPS DS entities. The airborne entity is the Airborne IPS System specified in this document. The ground entity may be a Ground IPS Host or an IPS Gateway, which is described in Part 2 of this specification.

As illustrated in Figure A-1, the information may be either B1/B2 application data or ACARS application data that has been mapped to the ATNPKT format using the ACARS to IPS DS Convergence Function (AICF) specified in Attachment 3 in this document.

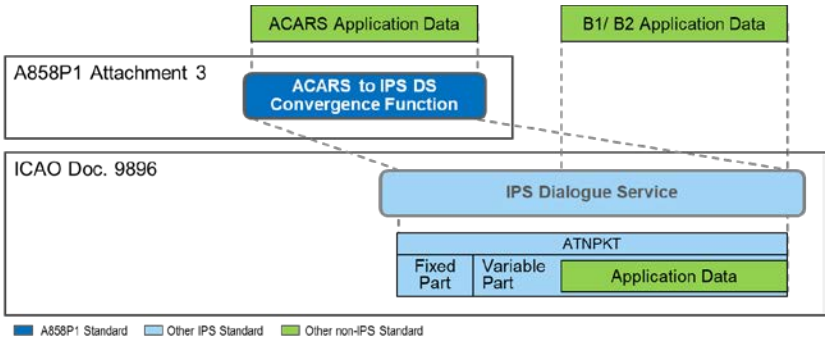

Figure A-1 – ATNPKT Overview

As shown in the figure, the ATNPKT consists of a fixed part, which is always present, and a variable part, which contains optional fields that depend on the DS primitive and application data type. The following sections provide ATNPKT examples for various DS primitives. The descriptions assume familiarity with the ATNPKT specification in ICAO Doc. 9896.

A-2 D-START and D-STARTCNF Primitives

The D-START and D-STARTCNF primitives provide a confirmed service that is used to establish the binding between communicating peer IPS DS entities. The following figure shows an example ATNPKT with D-START primitive.

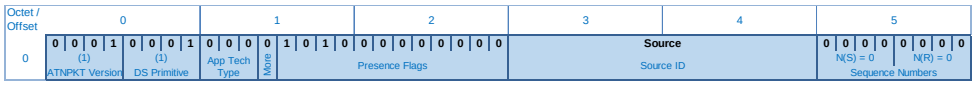

Figure A-2 – Example ATNPKT with D-START Primitive

In this example:

- ATNPKT Version is set to 1, which identifies the current version
- DS Primitive is set to 1, which defines the message as a D-START
- App Tech Type is set to b000, which indicates ATN/IPS DS
- More bit is set to 0, which indicates a single-segment message

APPENDIX A
ATNPKT MESSAGE FORMAT EXAMPLES

- The first and third Presence Flags are set to 1, which indicates that the following fields are present:
  - Source ID, which is a unique identifier (e.g., a random integer generated locally by the initiator) that identifies the system initiating the dialogue
  - Sequence Numbers, which indicate the sequence number for the packet being sent (e.g., 0) and the sequence number of next expected packet to be received (e.g., 0).

A D-STARTCNF message is generated in response to a D-START message. The following figure shows an example ATNPKT with D-STARTCNF primitive.

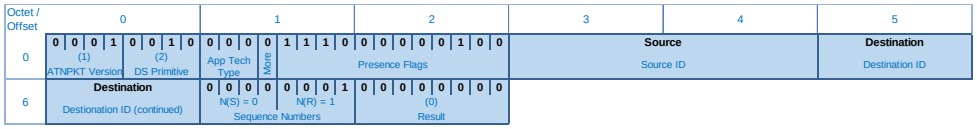

Figure A-3 – Example ATNPKT with D-STARTCNF Primitive

In this example:

- ATNPKT Version is set to 1, which identifies the current version
- DS Primitive is set to 2, which defines the message as a D-STARTCNF
- App Tech Type is set to b000, which indicates ATN/IPS DS
- More bit is set to 0, which indicates a single-segment message
- The first, second, third, and tenth Presence Flags are set to 1, which indicates that following fields are present:
  - Source ID, which is a unique identifier (e.g., a random integer generated locally by the responder) that identifies the system responding to the dialogue initiation
  - Destination ID, which is set to the value of the Source ID received in the D-START
  - Sequence Numbers, which indicate the sequence number for the packet being sent (e.g., 0) and the sequence number of next expected packet to be received (e.g., 1)
  - Result is set to 0, which indicates acceptance of the D-START; non-zero values reject the D-START.

Note that an ATNPKT with either a D-START or a D-STARTCNF primitive can optionally carry user data, which may require multiple segments. Refer to the D-DATA examples in Section A-3, which illustrate multi-segment user data.

A-3 D-DATA Primitive

The D-DATA primitive is an unconfirmed service used to exchange application data (e.g., B1/B2, FANS-1/A, ARINC 620 AOC, etc.) messages between IPS DS entities. When the D-DATA service is used with a reliable, connection-oriented transport (e.g., TCP), no acknowledgement is required. However, when used with a connectionless transport (e.g., UDP), an explicit acknowledgement using a D-ACK (refer to Section A-4) is required.

APPENDIX A
ATNPKT MESSAGE FORMAT EXAMPLES

The content of the ATNPKT fields depends on the type of data and whether it's the first or subsequent segment in a fragmented message, as indicated by the More bit.

A-3.1 D-DATA Example with B1/B2 Payload

In the following example, Figures A-4 and A-5 illustrate segment one and segment two of a two-segment D-DATA message with an ATN/IPS DS payload (e.g., B1/B2 application data). In the first segment, the More bit is set to 1, and in the second segment, the More bit is set to 0 indicating that it is the last segment in the fragmented message. In each segment, the first two bytes of the User Data field indicate the total length of the data carried in that segment. In this example, the total data length is 1,214 bytes, and the first segment contains the maximum size of 1,024 bytes, and the second segment contains the remaining 190 bytes.

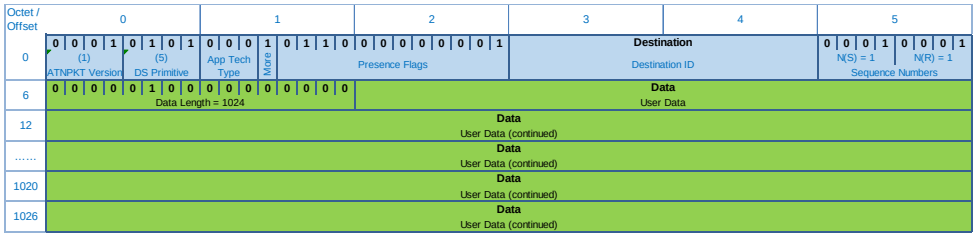

Figure A-4 – Example ATNPKT with D-DATA Primitive: B1/B2 Payload – 1st of 2 Segments

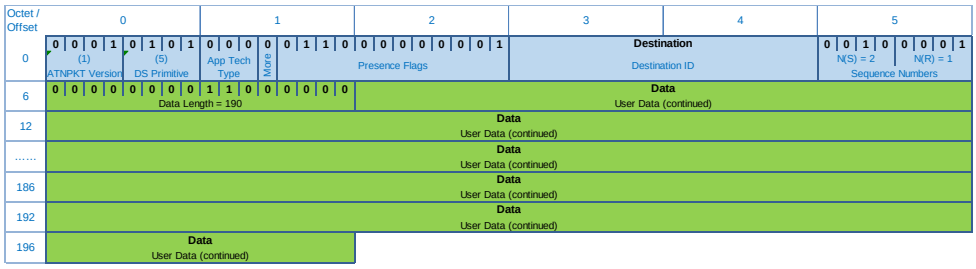

Figure A-5 – Example ATNPKT with D-DATA Primitive: B1/B2 Payload – 2nd of 2 Segments

In this example:

- ATNPKT Version is set to 1, which identifies the current version
- DS Primitive is set to 5, which defines the message as a D-DATA
- App Tech Type is set to b000, which indicates ATN/IPS DS
- More bit is set to 1 in the first segment and 0 in the second segment
- In every segment, the second, third, and twelfth Presence Flags are set to 1, which indicates that the following fields are present:
  - Destination ID, which is set to the value of the Source ID received in the D-START
  - Sequence Numbers, which indicate the sequence number for the packet being sent (e.g., 1 for the first segment, 2 for the second segment) and

APPENDIX A
ATNPKT MESSAGE FORMAT EXAMPLES

the sequence number of the next expected packed to be received (e.g., 1)

- o User Data, where the first two bytes in each segment indicate the length of the data carried in that segment.

A-3.2 D-DATA Example with FANS-1/A Payload

In the following example, Figures A-6 and A-7 illustrate segment one and segment two of a two-segment D-DATA downlink message with a FANS-1/A payload. As shown for the first segment, the More bit is set to 1 and the Called Peer ID and Calling Peer ID fields are included. In the second segment, the More bit is set to 0 indicating that it is the last segment in the fragmented message, and the Called and Calling Peer ID fields are not repeated. In each segment, the first two bytes of the User Data field indicate the total length of the data carried in that segment. In this example, the total data length is 1,190 bytes, and the first segment contains the maximum size of 1,024 bytes, and the second segment contains the maximum size of 1,024 bytes, and the second segment contains the remaining 166 bytes.

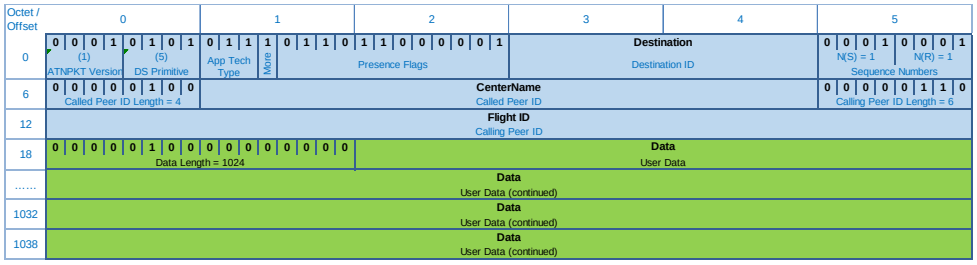

Figure A-6 – Example ATNPKT with D-DATA Primitive: FANS-1/A Payload – 1st of 2 Segments

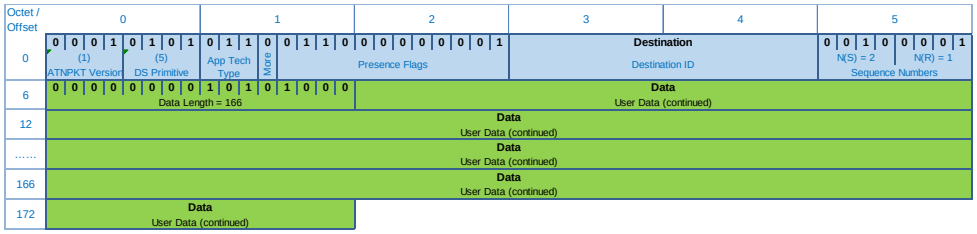

Figure A-7 – Example ATNPKT with D-DATA Primitive: FANS-1/A Payload – 2nd of 2 Segments

In this example:

- ATNPKT Version is set to 1, which identifies the current version
- DS Primitive is set to 5, which defines the message as a D-DATA
- App Tech Type is set to b011, which indicates ACARS ATS/IPS DS
- More bit is set to 1 in the first segment and 0 in the second segment
- In the first segment, the second, third, fifth, sixth, and twelfth Presence Flags are set to 1, which indicates that the following fields are present:

APPENDIX A
ATNPKT MESSAGE FORMAT EXAMPLES

- Destination ID, which is set to the value of the Source ID received in the D-START
- Sequence Numbers, which indicate the sequence number for the packet being sent (e.g., 1 for the first segment, 2 for the second segment) and the sequence number of the next expected packed to be received (e.g., 1)
- Called Peer ID, which contains the ATC Facility designator or address of the ground destination
- Calling Peer ID, which contains the aircraft FlightID
- User Data, where the first two bytes in each segment indicate the length of the data carried in that segment. Note that for ACARS-based messages such as FANS, the first byte of data following the length field is a one-byte Compression Parameter, per the AICF specified in Attachment 3 in this document.

- In the second segment, the second, third, and twelfth Presence Flags are set since the Destination ID, Sequence Numbers, and User Data are included in every segment of a multi-segment FANS-1/A message; whereas, Called Peer ID an Calling Peer ID are included only in the first segment of a multi-segment FANS-1/A message.

For a FANS-1/A uplink message (not shown), note that the contents of the Called and Calling Peer ID fields are reversed, i.e., the Called Peer ID is the aircraft FlightID, and the Calling Peer ID is the ground ATC Facility designator or address.

A-3.3 D-DATA Example with ACARS AOC Payload

In the following example, Figures A-8 and A-9 illustrate segment one and segment two of a two-segment D-DATA downlink message with an ACARS AOC payload. As shown for the first segment, the More bit is set to 1 and only the Calling Peer ID is included. In the second segment, the More bit is set to 0 indicating that it is the last segment in the fragmented message, and the Calling Peer ID field is not repeated. In each segment, the first two bytes of the User Data field indicate the total length of the data carried in that segment. In this example, the total data length is 2,020 bytes, and the first segment contains the maximum size of 1,024 bytes, and the second segment contains the remaining 996 bytes.

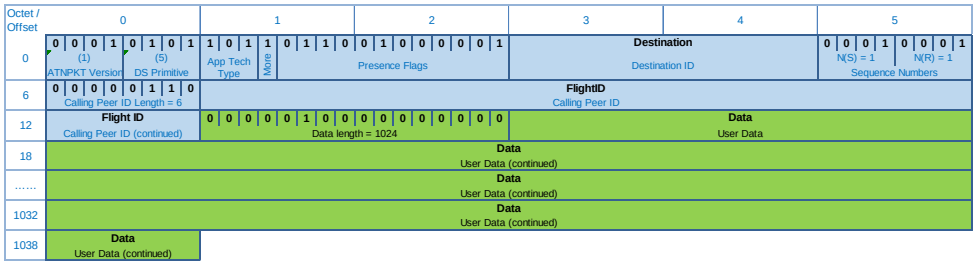

Figure A-8 – Example ATNPKT with D-DATA Primitive: ACARS AOC Payload – 1st of 2 Segments

APPENDIX A
ATNPKT MESSAGE FORMAT EXAMPLES

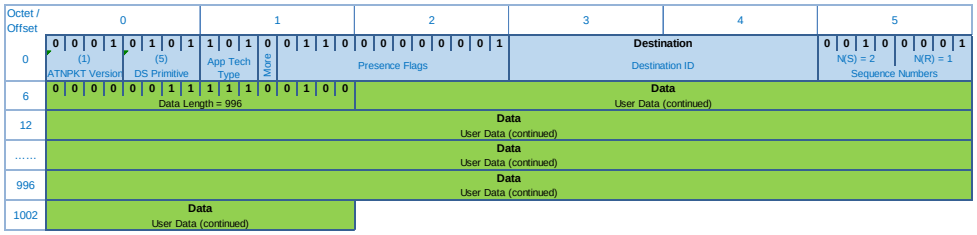

Figure A-9 – Example ATNPKT with D-DATA Primitive: ACARS AOC Payload – 2nd of 2 Segments

In this example:

- ATNPKT Version is set to 1, which identifies the current version
- DS Primitive is set to 5, which defines the message as a D-DATA
- App Tech Type is set to b101, which indicates ACARS AOC/IPS DS
- More bit is set to 1 in the first segment and 0 in the second segment
- In the first segment, the second, third, sixth, and twelfth Presence Flags are set to 1, which indicates that the following fields are present:
  - Destination ID, which is set to the value of the Source ID received in the D-START
  - Sequence Numbers, which indicate the sequence number for the packet being sent (e.g., 1 for the first segment, 2 for the second segment) and the sequence number of the next expected packed to be received (e.g., 1)
  - Calling Peer ID, which contains the aircraft FlightID
  - User Data, where the first two bytes in each segment indicate the length of the data carried in that segment. Note that for ACARS-based messages such as AOC, the first byte of data following the length field is a one-byte Compression Parameter, per the AICF specified in Attachment 3 in this document.
- In the second segment, the second, third, and twelfth Presence Flags are set since the Destination ID, Sequence Numbers, and User Data are included in every segment of a multi-segment ACARS AOC message; whereas, Called Peer ID an Calling Peer ID are included only in the first segment of a multi-segment ACARS AOC message.

In accordance with the AICF in Attachment 3, note that only the Calling Peer ID, which contains the aircraft FlightID, is included in an ACARS AOC downlink message and the Called Peer ID is not used. Conversely, for an ACARS AOC uplink message (not shown), only the Called Peer ID, which contains the aircraft FlightID, is included and the Calling Peer ID is not used.

A-4 D-ACK Primitive

The D-ACK primitive provides explicit acknowledgement of ATNPKT primitives received via a connectionless transport. The following figure shows an example ATNPKT with D-ACK primitive.

APPENDIX A
ATNPKT MESSAGE FORMAT EXAMPLES

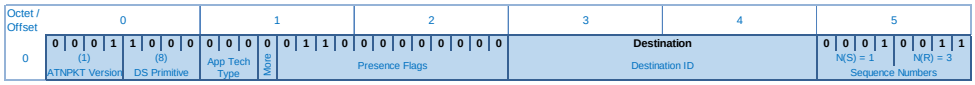

Figure A-10 – Example ATNPKT with D-ACK Primitive

In this example:

- ATNPKT Version is set to 1, which identifies the current version
- DS Primitive is set to 8, which defines the message as a D-ACK
- App Tech Type is set to b000, which indicates ATN/IPS DS
- More bit is set to 0, which indicates a single-segment message
- The second and third Presence Flags are set to 1, which indicates that the following fields are present:
  - Destination ID, which is set to the value of the Source ID received in the D-START
  - Sequence Numbers, which indicate the number for the last packet sent (e.g., 1 for the last D-DATA message) and the number of the next expected packed to be received (e.g., 3). Note that D-ACK, as well as D-KEEPALIVE, are the only primitives where the send sequence number is not incremented; so, the value repeats the number for the last non-D-ACK or non-D-KEEPALIVE packet that was sent.

A-5 D-END and D-ENDCNF Primitives

The D-END and D-ENDCNF primitives provide a confirmed service used to unbind the dialogue between communicating peer IPS DS entities in an orderly manner such that any data-in-transit is delivered before the unbinding is completed. Note that the D-END service is not used for ACARS-based applications. The following figure shows an example ATNPKT with D-END primitive.

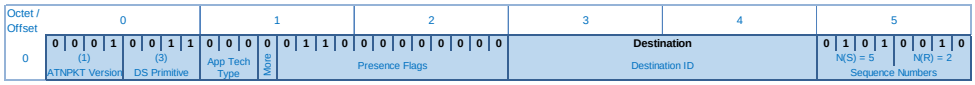

Figure A-11 – Example ATNPKT with D-END Primitive

In this example:

- ATNPKT Version is set to 1, which identifies the current version
- DS Primitive is set to 3, which defines the message as a D-END
- App Tech Type is set to b000, which indicates ATN/IPS DS
- More bit is set to 0, which indicates a single-segment message
- The second and third Presence Flags are set to 1, which indicates that the following fields are present:
  - Destination ID, which is set to the value of the Source ID received in the D-START
  - Sequence Numbers, which indicate the sequence number for the packet being sent (e.g., 5) and the sequence number of next expected packet to be received (e.g., 2).

APPENDIX A
ATNPKT MESSAGE FORMAT EXAMPLES

A D-ENDCNF message is generated in response to a D-END message, and it contains a positive or negative response regarding the completion of the dialogue termination. The following figure shows an example ATNPKT with D-ENDCNF primitive.

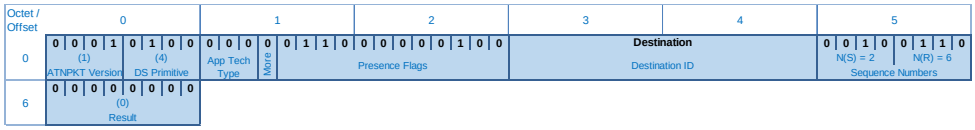

Figure A-12 – Example ATNPKT with D-ENDCNF Primitive

In this example:

- ATNPKT Version is set to 1, which identifies the current version
- DS Primitive is set to 4, which defines the message as a D-ENDCNF
- App Tech Type is set to b000, which indicates ATN/IPS DS
- More bit is set to 0, which indicates a single-segment message
- The second, third, and tenth Presence Flags are set to 1, which indicates that following fields are present:
  - Destination ID, which is set to the value of the Source ID received in the D-START
  - Sequence Numbers, which indicate the sequence number for the packet being sent (e.g., 2) and the sequence number of next expected packet to be received (e.g., 6)
  - Result is set to 0, which indicates acceptance of the D-END; non-zero values reject the D-END (e.g., if the responding entity has additional data to send before the dialogue is terminated).

Note that an ATNPKT with either a D-END or a D-ENDCNF primitive can optionally carry user data, which may require multiple segments. Refer to the D-DATA examples in Section A-3, which illustrate multi-segment user data.

A-6 D-ABORT Primitive

The D-ABORT primitive is an unconfirmed service used to abort the dialogue between communicating IPS DS entities. Unlike the D-END service, which provides orderly dialogue termination, any data in transit may be lost when the D-ABORT is invoked. The following figure shows an example ATNPKT with D-ABORT primitive.

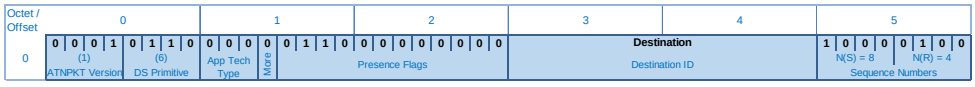

Figure A-13 – Example ATNPKT with D-ABORT Primitive

In this example:

- ATNPKT Version is set to 1, which identifies the current version
- DS Primitive is set to 6, which defines the message as a D-ABORT
- App Tech Type is set to b000, which indicates ATN/IPS DS
- More bit is set to 0, which indicates a single-segment message

APPENDIX A
ATNPKT MESSAGE FORMAT EXAMPLES

- The second and third Presence Flags are set to 1, which indicates that the following fields are present:
  - Destination ID, which is set to the value of the Source ID received in the D-START
  - Sequence Numbers, which indicate the sequence number for the packet being sent (e.g., 8) and the sequence number of next expected packet to be received (e.g., 4).

Note that an ATNPKT with the D-ABORT primitive can optionally carry user data; however, unlike D-START and D-END, the data cannot be segmented and is limited to a single segment.

APPENDIX B IPS PROTOCOL BUILD-UP

B-1 Introduction

This appendix provides a top-level overview of the IPS protocol build-up from one stack layer to another. This material is provided as general guidance for implementers of both airborne and ground IPS systems.

COMMENTARY

This section provides an information-only summary overview of the IPS protocol layers. Refer to ICAO Doc. 9896, the IPS Profiles (RTCA DO-379 and EUROCAE ED-262), and relevant IETF RFCs, which are the normative source references for detailed technical specifications of the protocol layers.

The IPS stack is illustrated in Figure B-1.

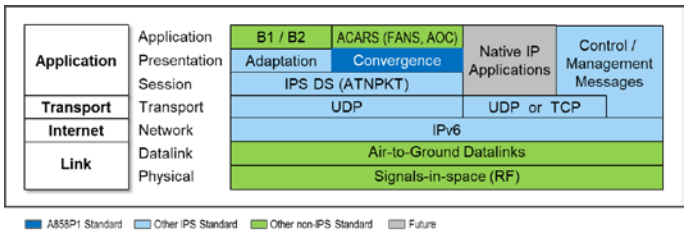

Figure B-1 – IPS Protocol Stack Overview

This appendix provides detail for three classes of messages:

- Session Establishment Messages (Section B-2)
- Air-Ground IPS Management Application Messages (Section B-3)
- Application Messages (Section B-4)

In addition, Section B-5 provides additional background regarding the transport and network layers.

B-2 Session Establishment Messages

The protocol build-up for session establishment is shown in Figure B-2. Session establishment utilizes UDP port 5908, which is reserved for authentication and Air-Ground IPS Management Application messages. Prior to authentication, UDP port 5908 is the only port that is open and listening.

APPENDIX B
IPS PROTOCOL BUILD-UP

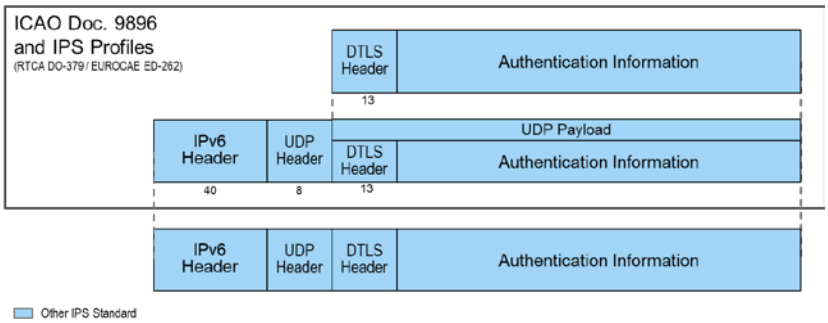

Figure B-2 – Protocol Build-up for Session Establishment Messages

B-3 Air-Ground IPS Management Application Messages

Air-Ground IPS Management Application exchanges DTLS encapsulated messages over UDP port 5908. The messages are specified in ICAO Doc. 9896. As shown in Figure B-3, the protocol build-up includes the DTLS header and the DTLS Encrypted Record.

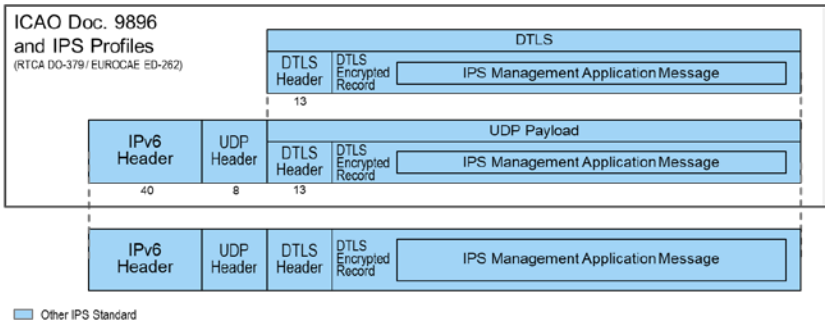

Figure B-3 – Protocol Build-up for Air-Ground IPS Management Application Messages

All Air-Ground IPS Management Application messages exchanged via UDP port 5908 use the DTLS header. For exchanges on UDP port 5908, all IPS management messages (e.g., information message, simple name lookup, etc.) are encrypted.

Air-Ground IPS Management Application messages may be sent by either an IPS network management entity or by the end applications.

B-4 Application Messages

B-4.1 Dialogue Service-based Applications

Dialogue Service-based applications are those that use the IPS DS and ATNPKT format specified in ICAO Doc. 9896. These applications include:

- B1 and B2 applications, which are accommodated by the IPS DS in accordance with ICAO Doc. 9896

APPENDIX B
IPS PROTOCOL BUILD-UP

- ACARS-based applications (e.g., FANS-1/A, AOC), which are adapted to the IPS DS using the ACARS to IPS DS Convergence Function specified in Attachment 3 of this document.

COMMENTARY

AOC applications may be accommodated using the AICF, as shown in this section, or an alternative adaptation approach. Refer to Section 3.2.

As shown in Figure B-4, the ATNPKT consists of a 3-byte fixed part and a variable part, which consists of supplementary ATNPKT header information including the application data itself. The application data is not modified when encapsulated using the ATNPKT.

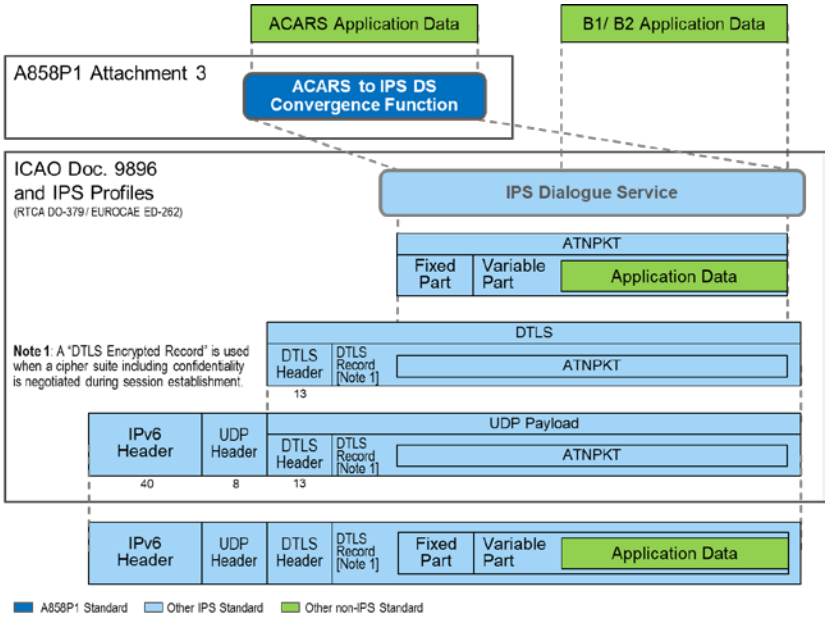

Figure B-4 – Protocol Build-up for DS-based Application Messages

Dialogue service-based application messages are exchanged via UDP using application-specific port numbers, which are defined in ICAO Doc. 9896 and used to identify the type of application data carried in the payload.

The UDP payload includes the ATNPKT, which is wrapped in a DTLS Record to ensure authenticity and message integrity while in transit. If a cipher suite that supports confidentiality is negotiated during session establishment, then the ATNPKT is wrapped in a DTLS Encrypted Record.

APPENDIX B
IPS PROTOCOL BUILD-UP

B-4.2 Native IP Applications

IPS supports Native IP applications, which are encapsulated directly in the transport layer payload without the need for adaptation or conversion as shown in Figure B-5. Native IP applications, which are future and not yet defined, may elect to use either TCP or UDP transport protocols (as shown), or any other transport protocol that may be supported by IPS. As shown previously in Figure 3-2 in the main body of this document, Native IP applications are secured using a security protocol (e.g., TLS or DTLS) that is appropriate for the selected transport protocol; in the following diagram, note that security overhead is not shown explicitly but is an implied part of the Native IP Application Data field.

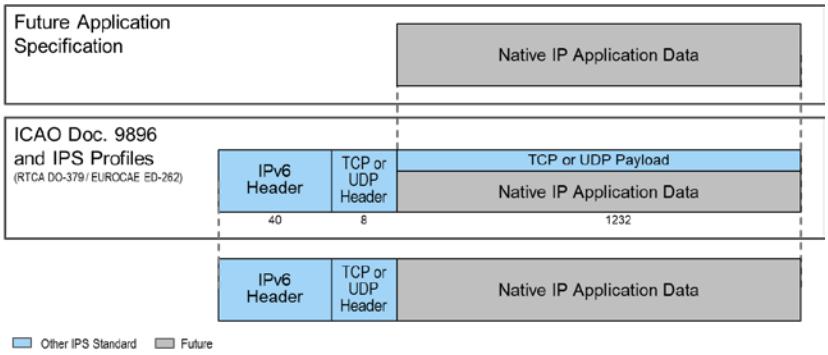

Figure B-5 – Protocol Build-up for Native IP Application Messages

Further protocol build-up detail will be contained in respective Native IP application specifications, when developed.

B-5 Transport and Network Layer Background

This appendix addresses only UDP transport, which is specified for the session establishment, Air-Ground IPS Management Application messages, and dialogue service-based applications. IPS may support other transports in the future.

B-5.1 UDP Transport Layer

The UDP packet consists of an 8-byte header and a variable size data payload. The UDP packet content and layout are shown in in the following figure.

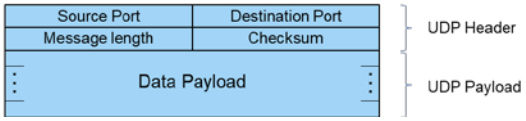

Figure B-6 – UDP Packet Content

B-5.1.1 Source and Destination Port

The port number defines the service access point. IPS port numbers are registered with IANA and defined in ICAO Doc. 9896.

APPENDIX B
IPS PROTOCOL BUILD-UP

As noted previously, only port 5908 is open and listening prior to authentication. Subsequent to authentication, port 5908 is used to exchange Air-Ground IPS Management Application messages, and application-specific ports are used to exchange associated application messages.

B-5.1.2 Message Length

The message length field specifies the length in bytes of the entire UDP packet, including the header fields and data payload. The minimum length is the 8 bytes, which is the length of the UDP header.

B-5.1.3 Checksum

The checksum field is mandatory for UDP running over IPv6. The UDP checksum is computed by taking the one's complement of the one's complement sum of all 16-bit words in the header (a pseudo header of information from the IP header, the UDP header, and the data payload, padded at the end with zero-filled octets, as necessary, to make a multiple of two octets). In other words, all 16-bit words are summed using one's complement arithmetic, and the sum is then one's complemented to yield the value of the UDP checksum field. If the checksum calculation results in the value zero (all 16 bits equal 0), then the checksum is set to the one's complement (all 16 bits set to 1).

The layout of this IPv6 pseudo header is shown in the following figure.

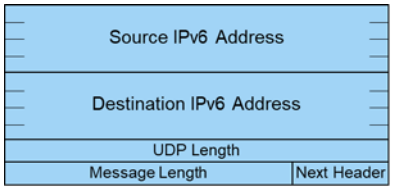

Figure B-7 – IPv6 Pseudo Header

B-5.1.4 Data Payload

The data payload is dependent on the application data and the port numbers, as described in Sections B-2 thru B-4 in this appendix.

B-5.2 IPv6 Packet

The IPv6 packet sits directly on top of datalink and physical layers of the overall protocol stack. The IPv6 packet consists of a 40-byte header and a variable size data payload, which consists of the transport layer packet (e.g., UDP header and UDP data payload). The maximum size of the IPv6 packet is 1280 bytes.

The IPv6 packet content and layout are shown in the following figure.

APPENDIX B
IPS PROTOCOL BUILD-UP

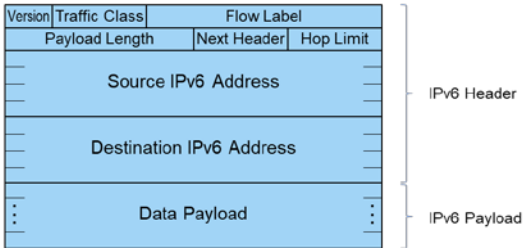

Figure B-8 – IPv6 Packet Content

B-5.2.1 IPv6 Header

Nominally, the header is the first 40 bytes of the IPv6 packet. As specified in Section 3.3.4.3 of this document, robust header compression (ROHC) is used to compress the network and transport layer headers, allowing smaller packet sizes over the RF spectrum.

The IPv6 header includes the following information:

- Version (4 bits) – the constant 6, as binary “0110”.
- Traffic Class (8 bits) – The most significant 6 bits indicate the Type of Service to let the router know what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN). Default is all bits set to “0”.
- Flow Label (20 bits) – Used to maintain sequential flow of packets. Default is all bits set to “0”.
- Payload Length (16 bits) – Specified the length in octets of the data payload field following the IPv6 header.
- Next Header (8 bits) – Identifies the type of header immediately following the IPv6 header and located at the beginning of the data field (payload) of the IPv6 packet. The value 0x11 in this field identifies the UDP transport protocol as the data payload.
- Hop Limit (8 bits) – Used to prevent packets from looping infinitely in the network, similar to time-to-live (TTL) in IPv4. The value of the Hop Limit field is decremented by 1 as it passes a link (router/hop). The packet is discarded if the Hop limit reaches 0 at any point in the intermediate ground network.
- Source and Destinations Addresses (128 bits each) – The aircraft and ground IP addresses using to route packets across the IPS network.

B-5.2.2 IPv6 Payload

The IPv6 payload consists of the transport layer packet. In the case of UDP transport, it contains the UDP packet, which carries session establishment messages, Air-Ground IPS Management Application messages, and dialogue service-based applications messages encapsulated using ATNPKT. As introduced in Section B-4.2in this appendix, Native IP applications may use UDP, TCP or other transport layer protocols supported by IPS.