[**1.0** **Introduction (ALL)** 4](#_Toc461120237)

[2.0 IPS OVERVIEW 4](#_Toc461120238)

[3.0 IPS Architectures 5](#_Toc461120239)

[3.1 High level requirements & assumptions 7](#_Toc461120240)

[3.1.1 Safety requirements 9](#_Toc461120241)

[3.1.2 Security Requirements 12](#_Toc461120242)

[3.1.2.1 Introduction 12](#_Toc461120243)

[3.1.2.2 Objectives & Design Principles for Secure Airborne Architectures 13](#_Toc461120244)

[3.1.2.2.1 Objectives 13](#_Toc461120245)

[3.1.2.2.2 Design Principles 13](#_Toc461120246)

[3.1.2.3 Assumptions & Operational Requirements 15](#_Toc461120247)

[3.1.2.4 Security Scope Definition 15](#_Toc461120248)

[3.1.2.5 Interfaces 16](#_Toc461120249)

[3.1.2.6 Assets 17](#_Toc461120250)

[3.1.2.7 External Dependencies 17](#_Toc461120251)

[3.1.2.8 Security Requirements 17](#_Toc461120252)

[3.1.3 Performance requirements 19](#_Toc461120253)

[3.2 Current architectures ) 20](#_Toc461120254)

[3.2.1 Avionics architectures – 2000’S 21](#_Toc461120255)

[3.2.2 Avionics architectures – 2010’S 23](#_Toc461120256)

[3.3 Integration of IPS in ARINC 429 Avionics Architectures 24](#_Toc461120257)

[3.3.1 Risk assessment 25](#_Toc461120258)

[3.3.2 Implementation considerations 27](#_Toc461120259)

[3.4 Integration of IPS in ARINC 664 Avionics architectures 29](#_Toc461120260)

[3.4.1 Risk assessment 30](#_Toc461120261)

[3.4.2 Implementation considerations 31](#_Toc461120262)

[3.5 Considerations for future avionics architectures 33](#_Toc461120263)

[3.6 Ground segment considerations (ROCKWELL IMS, SITA?) 34](#_Toc461120264)

[3.7 Information security requirements (AIRBUS, ROCKWELL COLLINS & IMS, THALES for review) 34](#_Toc461120265)

[4.0 IPS Work Scope Considerations 36](#_Toc461120266)

[5.0 IPS Standardization ROADMAPS 36](#_Toc461120267)

[6.0 IPS Validation Activities 36](#_Toc461120268)

[7.0 SUMMARY AND CONCLUSIONS 36](#_Toc461120269)

[**List of Acronyms** 37](#_Toc461120270)

[**GLOSSARY** 41](#_Toc461120271)

1. **Introduction (*ALL*)**

# IPS OVERVIEW

# IPS Architectures

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

The scope of the on-board IPS router is presented in the following Context Diagram. This figure depicts the main functions of the system of interest and the interfaces to the most important external systems.

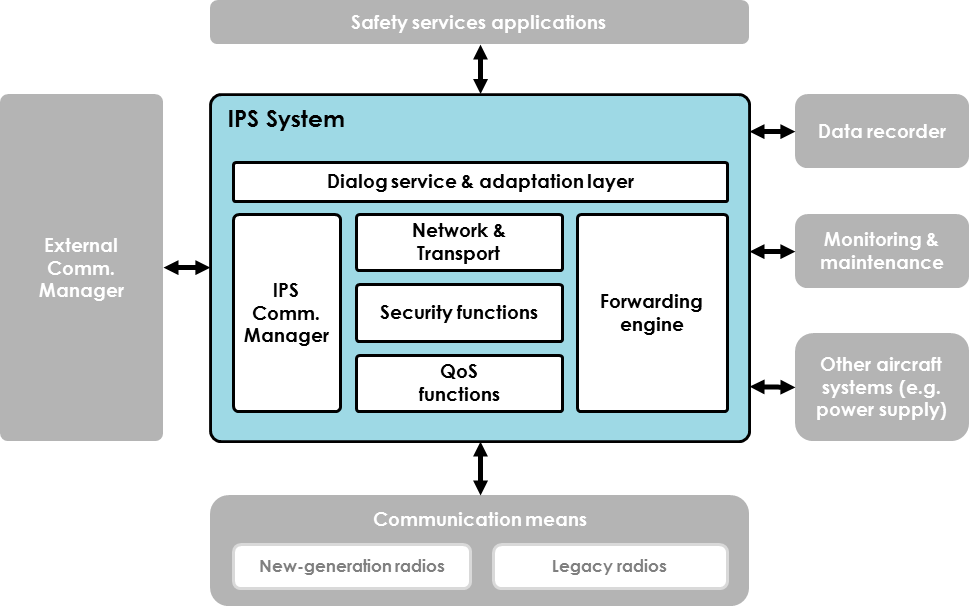


Figure 2-1 IPS System Context Diagram (avionics perspective)

The IPS System consists of the following main functions:

* **Dialog service & adaptation layer**: Applications may require an adaptation (service) layer over the Transport (e.g., using the IPS Dialog Service described in ICAO Doc. 9896 or MIAM over IP for AOC)
* **Forwarding engine**: The function of the forwarding engine is to transfer incoming traffic flow to an outgoing interface directed towards the next-hop interface.
* **Network & Transport protocols:** It consists of IP and associated Transport protocols (UDP, TCP). This function includes in particular the routing engine that determines the best path through the network.
* **Security functions**: Such entity implements all security functions that will be required to secure the traffic (e.g. firewall, admission control).
* **QoS functions:** Methods used to optimize and guarantee the performances of high-priority traffic.
* **IPS Communication Manager:** This function manages the selection of the radio bearer for a dedicated traffic flow and the associated mode of communication. This function works in correlation with the routing module of the Network & Transport protocols as the routing paths may also depend on the radio bearer.

The IPS System interfaces with multiple external systems in the aircraft, including:

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

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

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

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

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

As shown in Figure TBD, the IPS is an avionics specific general purpose internet protocol suite (IPS) based communication management function that is utilized by safety services avionics systems. IPS provides similar functionality currently offered by ACARS and ATN OSI protocols based communication management system. Even though current deployed provision only supports ARINC 429 interfaces to air to ground media link radios, the IPS will interface with various radios using ARINC 429 as well as Ethernet interfaces. The IPS networks may support all existing applications which are being deployed using ACARS and ATN OSI protocol. The IPS also supports future capabilities such as ATN B2 applications and beyond.

Hosting hardware platform may vary based on specific implementation and aircraft type. The scope for the IPS system should be bounded by the system boundary in the diagram in figure TBD. The larger system architecture impacts should not propagate beyond the scope of the IPS message router system. The IPS roadmap (this document), should define the perimeter where impacts are constrained within IPS network.

## High level requirements & assumptions

As described in section XX, IPS network infrastructure aims at supporting a wide set of applications, from AOC to ATC (ATN B2 and beyond, identified as “ATN B3” in SESAR 15.2.4 documents referred in this document or as ATN B2B in other documents). IPS also needs to be ready for future ATM applications not defined yet, and therefore also already encompass growing capabilities.

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

Note: In this section, the IPS system refers to set of equipment that will host the airborne part of the IPS function.

Main requirements:

Requirement 1: The IPS system shall provide connectivity to ATC applications via an ATN/IPS air-ground network infrastructure.

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

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

Note: Any AOC application considered as Safety (ICAO definition) should have access to ATN/IPS. These applications will be connected to ground AOC applications hosted at Airline premises or by third parties.

Note: The IPS system may provide connectivity to AOC applications hosted in AISD domain (in particular EFB) via an ATN/IPS air-ground network infrastructure. This capability may not be possible on each type of architecture (e.g. due to data security considerations).

Requirement 4: The IPS system shall be able to utilize multiple communication means.

Note: Several communication means are candidate to support ATN/IPS: Future SATCOM, AeroMACS, LDACS, others...

Requirement 5: The IPS system shall support multi-links concept as described in XX.

Requirement 6: IPS mobility should be managed mainly on ground

Rationale: The IPS mobility solution should allow minimizing the complexity of the airborne ATN/IPS network

Requirement 7: IPS mobility solution shall minimize the volume of routing/connectivity information exchanged on the air-ground segment

Rationale: In order to reduce costs and optimize air-ground links performance

Requirement 8: The IPS system shall support QoS and Airline policy driven media selection (in addition the multi-links concept)

Main assumptions:

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

Note: Triple stack (ATN/OSI, ATN/IPS and ACARS) is not envisaged.

Note2: ACARS/IPS system may replace the existing ACARS/OSI router for retrofit.

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

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

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

Assumption 3: IPS system will be IPv6 only

Note: IPV6 communication stack offers all the necessary addressing, mobility and security mechanisms.

### Safety requirements

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

Nevertheless, as IPS aims at supporting ATN B1, B2 and beyond B2 applications, its specification needs to consider all the relevant requirements and the feasibility of the most stringent should be at least assessed.

When supporting ATN B1 or B2 applications, IPS replaces or provides the alternative network and transport layers communication protocols. Failure condition does not change or remains the same as existing communication management Software /System. Safety and design assurance level is same as the ATN OSI per RTCA DO-178C, DO-278 or EUROCAE ED-12C DAL D.

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

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

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

The table below provides a summary of expected performances:

|  |  |  |  |
| --- | --- | --- | --- |
| **Hazard (Ref ED228)** | | **ATN-B2** | **ATN-B3/IP** |
| **OH-CPDLC-1** | Detected loss of CPDLC capability [single aircraft] | SC4 (Minor) | SC3 (Major) |
| **OH-CPDLC-2** | Detected loss of CPDLC capability [multiple aircraft] | SC4 (Minor) | SC3 (Major) |
| **OH-CPDLC-4** | Detected reception of corrupted CPDLC messages [multiple aircraft] | SC4 (Minor) | SC3 (Major) |
| **OH-CPDLC-6** | Detected reception of a unintended CPDLC message [multiple aircraft] | SC4 (Minor) | SC3 (Major) |
| **OH-CPDLC-8** | Detected unexpected interruption of CPDLC transactions [multiple aircraft] | SC4 (Minor) | SC3 (Major) |
| Undetected unexpected interruption of CPDLC transactions [multiple aircraft] | SC4 (Minor) | SC3 (Major) |

Table 1: Qualitative Safety Requirements anticipated for future ATM services (extract from SESAR 15.2.4-D4)

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

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

• A detected loss of the Aircraft ATC applications

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

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

Other causes linked to the detected and non-detected loss of the communication means can also be identified (not described in this document as the focus is on the ATN/IPS system).

Note: Underlying communications bearers themselves would contribute to all detected hazards identified in table 1, not just loss of capability.

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

|  |
| --- |
| The likelihood of a detected loss of ATN/IPS communication due to a **failure of the Aircraft ATN/IPS routing system shall be less than 1.0 10-6/FH** |
| The detected loss of ATN/IPS communications, due to a failure of the Aircraft ATN/IPS routing system, and which leads to a situation where it can be determined that CPDLC should not be used anymore, shall be considered **MAJOR**. |
| Loss of the ATN/IPS Routing system shall be considered **MAJOR** |

Table 2: Safety objectives for the ATN/IPS network

The quantitative safety objective onto the IPS routing system implies that the likelihood of a failure of the Aircraft IPS routing system shall be less than 1.0 10-6/FH. Such an objective would be very difficult to achieve with one single Airborne ATN/IPS router equipment, because, with current technology, availability of complex avionics equipment items is generally known to be lower than 1.0 10-5/FH.

It can be therefore inferred that Aircraft will need to be equipped with two redundant IPS routers to meet the safety requirements. This will have an impact on the IPS system design and all its interfaces.

The loss of ATN/IPS Routing capability is to be considered as a Major failure condition. This will translate, by following ARP4754 guidelines, into a choice between 2 options regarding the Development Assurance Level of the ATN/IPS router equipment:

1. Option 1: Two dissimilar, redundant IPS routers, which can be DAL D
2. Option 2: Two identical IPS routers, which will have to be DAL C

It is assumed that Airframers will generally prefer option 2, as it will generally be cheaper and simpler to go along with.

In a global safety analysis including the communication means (Future SATCOM, LDACS…), multi-link concept may also need to be considered.

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

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

Assumption 4: For beyond ATN B2 applications support, IPS router will be developed at DAL C

### Security Requirements

#### Introduction

This section contains data security considerations that are intended for the ARINC 658 system designers involved in the development of an Internet Protocol Suite (IPS) for Aeronautical Safety Services, both Air Traffic Services (ATS) and Aeronautical Operational Communications (AOC).

It provides guidance and constraints that will assist in development of IPS airborne architectural designs (see §3.0 IPS High Level Architectures and §3.3.3/§3.4.3 IPS Implementation Considerations) that is intended to satisfy regulatory requirements by providing adequate risk mitigation against threats.

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

From a security perspective, the aircraft network systems are divided into three domains (cf. ARINC 811 Commercial Aircraft Information Security Concepts of Operation and Process Framework) being: Aircraft Control Domain (ACD), Airline Information Services Domain (AISD) and Passenger Information and Entertainment Services Domain (PIESD).

The IPS system should satisfy security requirements and this is particularly the case when it is providing service to the ACD domain and at a lower level to the AISD domain. FANS services (e.g. ADS-C and CPDLC) and AOC safety are viewed as ACD domain while EFB and non-safety AOC are viewed as AISD domain.

The security requirements are to demonstrate, by an appropriate security process, that the functions (shared or independent) contained within the IPS airborne system can provide adequate segregation between domains and withstand potential threats that are introduced by its use in an open air-ground network environment.

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

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

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

Summary of the airborne risk assessment analysis with identification of security risk factors and consequent security objectives, are provided in §3.3.1 for ARINC 429 avionics architectures and in §3.4.1 for ARINC 664 avionics architectures.

#### Objectives & Design Principles for Secure Airborne Architectures

##### Objectives

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

These objectives are typically based on the experience of the system designer and security experts, and guided by an understanding of the functional role of the system, the threat environment in which it will operate and its criticality level. These general objectives are intended to be further refined and augmented during the security analysis phase.

The following high-level objectives have been identified for the ARINC 658 IPS airborne system supporting ATN/IPS for Aeronautical Safety Services. They are not in ranked order and should all be taken into consideration for a system design:

* IPS system design should ensure that security threats targeting the IPS system or using the IPS system as an attack vector cannot cause any safety impact to the aircraft;
* Security controls should not unduly complicate maintenance and operations activities;
* Data loading functions should be designed to preclude the creation of new vulnerabilities that could be exploited by an attacker or malware directed at the system software or that of any connected system;
* Data loading operations should be performed only when explicitly enabled by authorized maintenance personnel;
* Means should be provided to prevent spoofing of safety-related communications;
* Security measures should be designed to prevent attacks that would result in the decreased or loss of availability of services (e.g. via resource exhaustion);
* IPS system should act as a transparent on-board ATN/IPS router and should not interpret the content of data;
* … *(Non-exhaustive list – To be further reviewed through panel comments & discussions)*

##### Design Principles

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

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

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

* Airbus Model A350-900 Airplane; Electronic System-Security Protection from Unauthorized External Access [Docket No. FAA-2013-0909; Special Conditions No. 25-533-SC]:

– Extract: The applicant must ensure airplane electronic system-security protection from access by unauthorized sources external to the airplane, including those possibly caused by maintenance activity.

* Airbus Model A350-900 Airplanes; Isolation or Protection of the Aircraft Electronic System Security from Unauthorized Internal Access [Docket No. FAA-2013-0910; Special Conditions No. 25-534-SC]:

– Extract: The applicant must ensure that the design provides isolation from, or airplane electronic system security protection against, access by unauthorized sources internal to the airplane. The design must prevent inadvertent and malicious changes to, and all adverse impacts upon, airplane equipment, systems, networks, or other assets required for safe flight and operations.

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

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

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

As a consequence the following key architecture drivers should be considered:

* + Aircraft security architecture shall be based upon layered protection capabilities;
  + At least one on-board security boundary shall be implemented between threat sources and assets.

*Note: Security boundary number is defined by aircraft safety impact of protected asset.*

Strong and Very strong safety impact requires two barriers protection between threat agents and impacted assets, or an equivalent simple device (either based on simple hardware or very small code source and exhaustive security evaluation done).

The avionics IPS network has to rely on existing security standards and practices.

Guidance materials shall provide the minimum set of acceptable common security guidance framework for airworthiness certification based on the existing standards:

1. Airworthiness Security Process Specification, RTCA DO-326() / EUROCAE ED-202()
2. Airworthiness Security Methods and considerations, RTCA DO-356() when harmonized version of “Airworthiness Security Methods and considerations, EUROCAE ED-203()” document will be produced.
3. ARINC 811 Commercial Aircraft Information Security Concepts of Operation and Process Framework

#### Assumptions & Operational Requirements

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

* IPS system software are assumed to be RTCA DO-178 / EUROCAE ED-12 Level C or Level D design assurance levels (see §3.1.1 Safety Requirements);
* Maintenance personnel will follow approved procedures (including MRO personnel):

The system designer, operator, and regulator should agree on a characterization of the likelihood and severity of maintenance personnel errors, including the possibility that malware may be unknowingly carried to the airplane on a maintenance terminal or any mass storage device;

* Flight crews will follow approved procedures:

The system designer, operator, and regulator should agree on a characterization of the likelihood and severity of flight crew errors, including the possibility that malware may be unknowingly carried to the airplane on a portable crew device (e.g. EFB laptop, tablet, USB sticks…);

* Physical access to the IPS system items will be controlled to the same degree as physical access to other installed on-board electronic systems in general (i.e. avionics e-bay). That is, there are no special access physical control requirements, nor is access control requirements relaxed;
* IPS router should not be logically mixed with AISD router or PIESD router;
* The security requirements of the ground infrastructure and satellite network, while outside the scope of this document, are an important part of overall security and will be further described in section 3.1.2.7;
* Interfaced systems at higher assurance levels will not serve as a launching point for attacks on the IPS system:

1. Higher-assurance systems will not be corrupted by attackers;
2. Such systems may not provide any protection to the IPS system if attacks are simply passed through them to the IPS system, thus enabling the attack vector;

Any such dependencies should be evaluated for each installation.

* … *(Non-exhaustive list – To be further reviewed through panel comments & discussions)*

#### Security Scope Definition

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



***Fig. General Definition of the Security Scope***

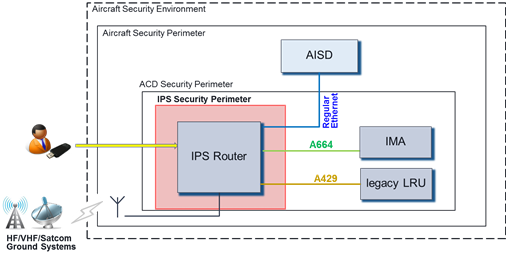
The assets are the logical and physical items that characterize the system well enough to identify all the potential targets of attack. It includes functions, data and resources that, if attacked, will cause an adverse effect on aircraft safety.

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

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

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

This section aims at being focused on the system level as shown on the figure hereafter:



***Fig. IPS System Security Scope***

#### Interfaces

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

Possible network interfaces on IPS system are:

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

***Tab. IPS System Security Scope***

#### Assets

* *To be completed*

#### External Dependencies

* *To be completed*

#### Security Requirements

**Security Requirement 1:** Assumption was that based on current ICAO provisions, aircraft shall not be denied of service by the ground, but ground could be denied of service by the aircraft. This indicates that air-ground authentication needs to be optionally asymmetric:

* IPS network shall request authentication from ground systems (i.e. ATC center and Airline Operations Centers) to aircraft entity.
* IPS network may request authentication from aircraft entity to ground systems (i.e. ATC center and Airline Operations Centers).

*Note: Access network (i.e. Data Link Service Providers) problematic is not treated here but will have to be treated elsewhere.*

**Security Requirement 2:** IPS network shall provide integrity protection against unauthorized modification and corruption of messages.

*Note: Authentication without integrity protection is useless.*

**Security Requirement 3:** The standard shall propose something globally acceptable for all countries rules and regulations, or shall propose an acceptable fall back.

**Security Recommendation 1:** IPS network may propose optionally to protect confidentiality of data exchanged.

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

**Security Requirement 4:** The IPS system shall be developed with requirements coming from Security Assurance Level (SAL) (level which will be defined later).

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

TO BE MOVED ELSEWHERE (end-to-end security considerations)

This needs to provide the uniform security policy between air-to-ground and ground-to-ground. Air and ground need to support security policy and process, which provide the entity authentication, integrity and safety against various. Security provision should provide the level of service and type of separation between different flows between ground entities and air entities.

### Performance requirements

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

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Performance**  **Parameter** | **ATN B1**  **ED120 SPR**  **Standard published**  **Based on Eurocontrol Generic ACSP Requirements doc.** | **ATN B2**  **ED228 SPR**  **Standard published**  **Based on most stringent**  **RCP130/RSP160** | **ATN B3**  **SESAR 15.2.4 predicted (no standards started)**  **Based on most stringent**  **RCP60/RSP60** |
| Transaction Time  One way (sec) | 4 - 95% of messages  12 – 99.9% of messages | 5 - 95% of messages  12– 99.9% of messages | 2 - 95% of messages  5 – 99.9% of messages |
| Transaction Time  Two way (sec) |  | 10 - 95% of messages  18– 99.9% of messages | 4 - 95% of messages  8 – 99.9% of messages |
| Availability -CSP | 0.999 | 0.9995 | 0.999995  (maybe reduced by multi-link) |
| Availability - Aircraft |  | 0.99 | 0.999 |
| Integrity | 1-10-5 | Not specified  Must be good enough to meet RCP/RSP | Not specified  Must be good enough to meet RCP/RSP |
| Security | Physical protection  Unauthorised access | Not specified  but Unauthorised access protection needed, ICAO requirements | Technical security requirement likely |

Table 3: Performances requirements of future ATM services (extract from SESAR 15.2.4-D04)

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

Assumption 1: QoS functions will be required to meet the timing performance with acceptable operating costs (i.e. without over dimensioning the network).

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

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

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

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

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

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

Assumption 4: The A/G data-link capacities represent a hard constraint for service availability, i.e. if the “high priority” offered load consistently exceeds link capacity there will be loss.

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

## Current architectures )

### Avionics architectures – 2000’S

ARINC 429 defines the Air Transport Industry’s standard for the transfer of digital data between avionics systems and is formally known as the MARK 33 Digital Information Transfer System (DITS) specification.

The legacy architecture uses ARINC 429 interfaces between on-board functions involved in datalink.

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

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

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

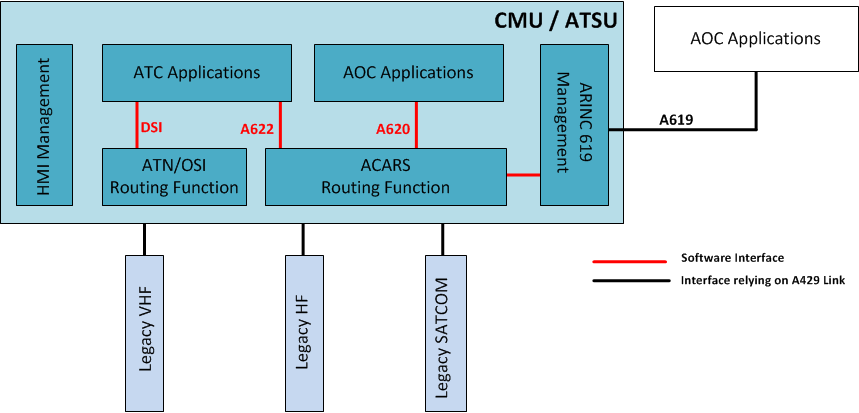


Figure 1: Current Architecture based on ARINC 429

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

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

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

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

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

Moreover, dual configurations are possible.

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

### Avionics architectures – 2010’S

ARINC Specification 664 **Erreur ! Source du renvoi introuvable.** is primarily a guidance document that establishes the architecture framework for IP-based aircraft. It contains a detailed implementation specification for the Ethernet physical layer. ARINC 664 also provides aeronautical profiles for IPv4 and an IP address allocation scheme using private IP address space.

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

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

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

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

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

A sample of such architecture is represented below.



Figure 2: Current Architecture Based on ARINC 664

The ACARS & ATN/OSI routing function (ACR) is a software element hosted on an IMA module. The VDR and SatCom systems are ARINC 600 units defined with a standardized inter-wiring (several ARINC standards may apply).

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



Figure 3: Example of ARINC 664 based architecture

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

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

* Access network functions (e.g., VDR, SatCom, Gatelink) may be implemented in federated equipment connected via ARINC 429.
* The ACR (ATN, ACARS routing function) is implemented as a software function hosted on an IMA module.
* The ATC applications are implemented as software functions hosted on an IMA module

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

## Integration of IPS in ARINC 429 Avionics Architectures

### Risk assessment

Note: This section will provide a summary of the airborne risk assessment analysis conducted by Airbus (based on current Airbus architectures), and consequent security objectives; including identification of security risk factors

Results are expected by mid-2016

Threats may originate from devices connected (via wired and wirelessly) to the IPS network.The attacks may originate in portable devices that are temporarily connected to the IPS network (by the ground crew and various RF links). AC/AMJ25.1309 defines a 5-level scheme of hazard classifications and probability requirements. This task requires the identification and classifications of threats and mapped to the 5-level classification scheme.

Table below contains some of the threat conditions to be considered for the IPS network. <<This needs to be worked through>>

Table 3‑4: Threat Conditions

|  |  |  |
| --- | --- | --- |
| Threat ID | Threat Condition | Severity |
| 1 | Loss of IPS network stored data integrity | minor |
| 2 | Miss-delivery of message | Minor |
| 3 | Corruption / Misleading representation of message | Minor |
| 4 | Unauthorized IPS network access | Minor |
| 5 | Loss of aircraft IPS router function | Minor |
| 6 | Loss of print function | No Effect |
| 7 | Misleading display of IPS ARINC 661 / ARINC 739 pages | Minor |

Threat conditions related to denial of service (DOS) exists for IPS, therefore further analysis of DOS conditions needs to be performed.

Risk analysis needs to focus on: consistent risk analysis by different assessors, efficacy of risk assessment measurements to support risk management decisions and identifying common cause vulnerabilities. This should provide built-in protection for availability, means protection against denial-of-service and interference/flooding.Pilot-in-the-loop - pilot Awareness, monitoring of air to ground links / radio, flight plans, able to land even if all ATC and all non-essential equipment are shut down, Fail-Operational - Essential systems must not have a single point of failure andmobility. Configuration Compliance, aircraft not authorized to operate unless critical SW/HW is up-to-date

### Implementation considerations

First thoughts on ATN/IPS implementations are listed below:

Note: These considerations mainly aim at clarifying the detailed scope of AEEC standardization needs.

General and security considerations:

* IPS system architecture shall provide means for guaranteeing a not to exceed delay for messages processing. It shall be deterministic in order to demonstrate the required performances (transaction time).
* IPS system could be hosted either in the ATSU/CMU or in dedicated/standalone equipment, taking into account that segregation is likely required for providing a layered security solution.

It should be preferable to have a multi-program approach for the IPS system. Even if integrated in a different way depending on the aircraft type, it is suitable that the ATN/IPS router is common to all aircraft types.

* In this architecture a first security barrier would be the trusted channel (e.g. VPN) implemented between the airborne and ground gateways (assumed that the ground infrastructure is trusted and the ground gateway is certified), and a second barrier (if necessary) could be a simple security device between the ATN/IPS router and the CMU/ATSU. Other options could be envisaged for this second barrier.



Figure 4: Possible ATN/IPS high level architecture in ARINC 429 legacy environment

* IPS system could interface with the AOC applications through a new simple and dedicated messaging service (e.g. MIAM over IP)
* Selection between ACARS and IPS should remain implementation dependent (no need for standardisation)
* The IPS system architecture and security design will take the assumption that communication means are secured (e.g. by a VPN). Current definition of SBB safety “Light Cockpit SATCOM” ARINC 781-8 can be considered for a first layer of defense if the ground gateway is certified. Other medias (AeroMACS, LDACS…) would have to implement similar mechanisms and also be certified.
* End-to-end security (e.g. between Airborne and ground ATC systems) should be implemented in the ATN/IPS router (rather than on the applications).
* The IPS system has to segregate the flows between ATC and AOC, that for security (ATC communications should not be compromised by AOC traffic).

Physical interface considerations:

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

Note: ARINC 429 could also be used on legacy aircraft (as for Iris PRECURSOR SATCOM & new types of L-BAND SATCOM services).

* Interfaces with the ARINC 619 peripherals (FMS, FWS, Clock…) should be based on ARINC 429
* Interfaces with the AOC applications (through MIAM protocol)could be based on ARINC 429 or Ethernet.
* If implemented in a different equipment, interface with the ATC applications (hosted on ATC) should be based on ARINC 429 or Ethernet

Logical interfaces considerations:

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

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

* For IHM purpose, the Avionics IPS system should use A739 to interface with the CDU
* The Avionics IPS system can use VDL Mode 2 via ARINC 429 for IP communication, using a dedicated IPI value to multiplex IP data and AOA and ISO8208.

## Integration of IPS in ARINC 664 Avionics architectures

### Risk assessment

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

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

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

Spoofing - Modifying data that otherwise appears to be from a legitimate source, Flooding/Denial of service - using an air to ground connection to disrupt service, Corruption, Missed Delivery

Note: This section will provide a summary of the airborne risk assessment analysis conducted by Airbus (based on current Airbus architectures), and consequent security objectives; including identification of security risk factors

Results are expected by mid-2016

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

### Implementation considerations

First thoughts on IPS implementations are listed below:

General and security considerations:

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



Figure 5: Possible ATN/IPS high level architecture in ARINC 664 environment

* Systems on the ACD network shall be reachable from the ground, but security mechanisms need to be in place to control flow of traffic from the ground to systems on the ACD network.
* ATN/IPS network could interface with the AOC applications through a new simple and dedicated messaging service (MIAM over IP)
* Selection between ACARS and ATN/IPS should remain implementation dependent (no need for standardisation)
* The ATN/IPS network architecture and security design will take the assumption that communication means are secured (e.g. by a VPN). Current definition of SBB safety “Light Cockpit SATCOM” ARINC 781-8 can be considered for a first layer of defense if the ground gateway is certified. Other medias (AeroMACS, LDACS…) will have to implement similar mechanisms and be certified.

In order to protect the ACD (Aircraft Control Domain) from any malicious IP traffic, ATN/IPS solution shall allow:

* Preventing at the earliest possible moment any unauthorized IP traffic to enter the Aircraft Control Domain internal Local Area Network
* Preventing any unauthorized IP traffic to reach any Aircraft systems directly interfaced with the Aircraft radios and with the Aircraft ATN/IPS router,
* Offering at least two independent security barriers

Note: There is a risk that the Secured Dialogue Service solution might be incompatible with the presence of such other security solutions. A as a consequence:

* End-to-end security (e.g. between Airborne and ground ATC systems) should be implemented in the ATN/IPS router (rather than on the applications).
* The ATN/IPS network has to segregate the flows between ATC and AOC, that for security (ATC communications should not be threatened by AOC traffic).

Physical interfaces considerations:

* Interfaces with the communication means (radios) should be based on Ethernet and standard protocols (e.g. PPPoE)
* Interface with the ATC applications (hosted on ATC) should be based on ARINC 664 network or point-to-point (because protected by two barriers)
* Interface with the AOC applications (hosted TBC) should be based on Ethernet

Logical interfaces considerations :

* Logical interface between ATC and the ATN/IPS network could be at Dialogue Service level

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

## Considerations for future avionics architectures

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

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

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

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

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

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

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

## Ground segment considerations (ROCKWELL IMS, SITA?)

This section will in particular address the following topics:

High-level descriptions of ground gateways - accommodation considerations

## Information security requirements (AIRBUS, ROCKWELL COLLINS & IMS, THALES for review)

This section will in particular address the following topics:

* Ground security environment (security measures, ground certification...) with the objective to identify if airborne security demonstration can rely on ground components (e.g. what is envisaged for SBB 200 Cockpit SATCOM)
* Focus on End-to-end security
* Description how end-to-end security or ground components can be considered for A/C protection demonstration
* Differences (or impact) between AOC and ATC traffic (ATC centers versus Airline Ops centers connexion)
* Confidentiality – do we need it?
* Confidentiality is optional.
* Authentication/data integrity
* L2 authentication is optional (based on ICAO provisions). Application level authentication is required
* Availability
* End to end security policy
* Implement same seamless security policy between service provider, ANSPs, Operators and airlines
* Quality of service and traffic separation
* Implementation and certification guidance

1. IPS Work Scope Considerations
2. IPS Standardization ROADMAPS

.

1. IPS Validation Activities
2. SUMMARY AND CONCLUSIONS

**List of Acronyms**

4DT Four Dimensional Trajectory

4DTRAD Four Dimensional Trajectory Downlink

AAtS Aircraft Access to SWIM

ACARS Aircraft Communications Addressing and Reporting System

ACD Aircraft Control Domain

ACL ATS Clearance

ACM ATS Communications Management

ADS-C EPP ADS-C Extended Projected Profile

ADTRAD Automatic Downlink of Trajectory

AEEC Airlines Electronic Engineering Committee

AFN ATS Facilities Notification

AFTN Aeronautical Fixed Telecommunication Network

AIM Aeronautical Information Management

AIS/MET Aeronautical Information Services/Meteorological

ANSP Air Navigation Service Provider

AOA ACARS Over AVLC

AOC Airline Operational Control

AOR Atlantic Ocean Region

ASBU Aviation System Block Upgrade

ATC Air Traffic Control

ATM Air Traffic Management

ATN Aeronautical Telecommunication Network

ATS Air Traffic Services

ATSU Air Traffic Services Unit

AVLC Aviation VHF Link Control

BLOS Beyond Line Of Sight

CADS Centralized ADS-C System

CARATS Collaborative Actions for Renovation of Air Traffic Systems (Japan)

CDU Control Display Unit

CDM Collaborative Decision Making

CDS Cockpit Display System

CFR Certified Federal Regulation

CFRS Centralized Flight Management Computer Waypoint Reporting System

CIWS Corridor Integrated Weather System

CM Context Management

CMF Communications Management Function

CMU Communications Management Unit

CNS/ATM Communications Navigation Surveillance/Air Traffic Management

COCR Communications Operating Concept and Requirements

COI Communities of Interest

COTS Commercial Off The Shelf

CPDLC Controller Pilot Data Link Communications

CRT Cathode Ray Tube

CSMA Carrier Sense Multiple Access

CSP Communication Service Provider

CSPR Closely Spaced Parallel Runway

CSS-Wx Common Support Services-Weather

CTA Constrained (or controlled) Time of Arrival

D8PSK Differential 8-Phase Shift Keying

D-ATIS Digital Automatic Terminal Information Service

D-HZWX Datalink Hazardous Weather

D-OTIS Datalink Operational Terminal Information Service

D-TAXI Digital TAXI

DCL Departure Clearance

DLIC Data Link Initiation Capability

DLS-IR Data Link Services Implementing Rule

DM Downlink Message

DoD Department of Defense

DSB Double Side Band

DSC Downstream Clearance

DSP Data Link Service Provider

EASA European Aviation Safety Agency

EATM European Air Traffic Management

EFB Electronic Flight Bag

FAA Federal Aviation Administration

FANS Future Air Navigation System

FDMA Frequency-Division Multiple-Access

FIM Flight deck Interval Management

FIR Flight Information Region

FISDL Flight Information Service Data Link

FLIPCY Flight Plan Consistency

FM Flight Management

FMC Flight Management Computer

FMF Flight Management Function

FMS Flight Management System

FPL Flight Plan

GEO Geostationary orbit

GOLD Global Operational Data Link Document

HFDL High Frequency Data Link

I4D Initial Four Dimension

ICAO International Civil Aviation Organization

IFR Instrument Flight Rules

IMS Information Management Services

IP Internet Protocol

IPS Internet Protocol Suite

IS Information Services

ITWS Integrated Terminal Weather System

L DACS L Band Digital Aviation Communication System

LOS Line of Sight

MASPS Minimum Aviation System Performance Standards

MCDU Multi-purpose Control and Display Unit

MEO Medium Earth Orbit

MET Meteorological

MMR Multi-Mode Receiver

MOPS Minimum Operational Performance Standards

MSS Mobile Satellite System

MUAC Maastricht Upper Air Center

NAS National Airspace System

NAS EA NAS Enterprise Architecture

NATS North Atlantic Track System

NESG NAS Enterprise Security Gateway

NextGen Next Generation Air Transportation System

NOP Network Operations Plan

NOAA National Oceanic and Atmospheric Administration

NSS Network Server System

OCL Oceanic Clearance

ODC Oceanic Departure Clearance

OI Operational Improvements

PDC Pre-Departure Clearance

PIREP Pilot Report

POA Plain Old ACARS

RCP Required Communication Performance

RNP Required Navigation Performance

SARPS Standards and Recommended Practices

Satcom Satellite Communications

SBAS Space Based Augmentation System

SBD Short Burst Data

SESAR Single European Sky Air Traffic Management (ATM) Research

SoL Safety of Life Service

SOA Service Oriented Architecture

SPR Safety and Performance Requirement

STC Supplemental Type Certificate

SUA Special Use Airspace

SWIM System Wide Information Management

TBO Trajectory Based Operations

TDMA Time Division Multiple Access

TMR Trajectory Management Requirement

UM Uplink Message

VDL VHF Data Link

VHF Very High Frequency

WPR Waypoint Position Reporting

**GLOSSARY**

**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, etc.).

**ADS-C – Automatic Dependent Surveillance-Contract:**

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

**AOA – ACARS Over Aviation VHF Link Control:**

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

**AOC – Airline Operational Control (Aeronautical Operational Control):**

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

**ATN – Aeronautical Telecommunications Network:**

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

**ATSU – Air Traffic Services Unit:**

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

**CMU – Communication Management Unit:**

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

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

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

**CPDLC – Controller-Pilot Data Link Communications:**

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

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

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

**FMF – Flight Management Function:**

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

**FMS – Flight Management System:**

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

**LINK 2000+ – The EUROCONTROL LINK 2000+ Program:**

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

**MASPS – Minimum Aviation System Performance Standards:**

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

**MOPS – Minimum Operational Performance Standards:**

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

**NAS – National Airspace System:**

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

**SARPS – Standards and Recommended Practices:**

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

**Satcom – Satellite Communications:**

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

**SESAR – Single European Sky ATM Research:**

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

**VDL – VHF Data Link:**

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

**VDLM2 – VHF Data Link Mode 2:**

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