atf CYBER®

Foundational Network Requirements and Concept of Operations to Enable and Support Interoperability of Air Navigation Services

Prepared by: atfCYBER
Version 0.1
May 13, 2018

Disclaimer

Any of the following descriptions that appear to be stating a policy are simply examples to provide a practical context for understanding the scope of the proposal and highlight issues to be considered. To avoid the distraction of inserting "one possible policy" before every instance of something that looks like a policy, an example is stated to show how a set of policies might enable functional deployment of the concepts. Actual policy decisions are out of scope for this document.

Table of Contents

1 Executive Summary ... 1
2 Overview ... 2
3 Introduction ... 5
3.1 Purpose ... 5
3.2 Problem Statement ... 5
3.3 Risks ... 6
3.4 Scope ... 7
3.5 Guiding Principles ... 8
3.6 Organization of this Document ... 8
3.7 Relationship to Other Documents ... 8
4 Concept of Operations ... 9
4.1 New Air Traffic Control Communications and Management Services ... 11
4.2 Ecosystem ... 13
5 Ecosystem Components ... 14
5.1 Digital Identity ... 14
5.2 Services Message Authentication ... 15
5.2.1 ATA Spec 42 ... 15
5.2.2 Augmentation of Basic Authentication Services ... 15
5.3 Naming ... 16
5.3.1 Resolution Services ... 17
5.4 Network Architecture ... 18
5.4.1 Locations ... 18
5.4.2 Topology ... 18
5.4.3 Time ... 20
5.5 Network Addressing ... 21
5.6 Cyber Security and Resilience ... 22
5.7 Services Based Application and Message Systems ... 24
6 Migration to the New Network Infrastructure and Communications Services ... 26
7 Governance and Operational Considerations ... 27
8 Benefits and Summary ... 28
Appendix ... 30
A) Terminology ... 30

B) Use Cases 32
Scenario 1 Passenger Flight International Handoff 33
Pre-flight 33
Weather 35
Aircraft Pre-flight Weight & Balance 36
Aircraft Handoff Sequence 37
Scenario 2 Air-Ambulance Flight International Handoff 38
Scenario 3 Autonomous Cargo Flight International Handoff 39

Table of Figures

Figure 1 International Civil Aviation Airspace Users includes the flight operations centers (FOC) and the entity responsible for the execution of a flight. 11
Figure 2 Infrastructure functions called for in both FF-ICE & SWIM are further detailed in this document 14
Figure 3 Standard structure for DNS labels within ICAO's governance 17
Figure 4 Network Architecture showing overlay model with protected paths between Service Guards. 20
Figure 5 IPv6 address block options for the members-only private overlay network 22
Figure 6 Cyber Resilience perspective of the members-only architecture, including isolated realms (for detail on the ATC components, please see Figure 7). 24
Figure 7 Timeline of information provision relative to events pertaining to a single flight, referenced sections detail FF-ICE activities in more detail 33
Figure 8 Preflight data exchange between Service Guards via protected paths established between LSR functions 34
Figure 9 Weather acquisition sequence 35
Figure 10 Message Service interactions to acquire weight & balance, and manifest before negotiating spacing 36
Figure 11 Aircraft handoff sequence between ANSPs 37
Figure 12 Air ambulance sharing air-to-ground link between FF-ICE realm, and Medical Information Realm 38
Figure 13 Autonomous cargo flight sharing air-to-ground link between FF-ICE realm, and Cargo Management realm 39

1 Executive Summary

To enable “Advanced Air Traffic Management” (AATM) and “Advanced Air Traffic Control Communications” (AATCC) systems, the aviation community has identified collaborative information exchange as a process that needs to occur between all stakeholders to ensure participants make and share timely and consistent decisions among all participants using common methods and technology. Accomplishing this will require the entire international civil aviation community to evolve from the current national or regional labyrinth of disparate technologies to a consistent global framework of policies, infrastructure and operations. This document provides a concept of operations (ConOps) that delivers on this need.

The scope and scale of this ConOps encompasses currently deployed Commercial, General Aviation, and emerging categories such as remotely piloted vehicles.

The aviation industry has relied on humans to analyze information and take appropriate action to ensure the safety of air operations. However, as the aviation industry evolves, increasing complexity is pushing the bounds for human analysis of critical data and information, thereby impacting the decision-making processes. Continued process improvement, automation, and consolidation of various infrastructures must occur to safeguard flight operations. These improvements involve airspace user training; situational and weather awareness; and air traffic management, including ground-to-ground, air-to-ground and ground-to-air systems.

The AATM/AATCC environment is a network of networks: air carrier ground networks, multiple ATM/ATC networks in multiple Member States, aerodromes, airframers, air network service providers (ANSPs), and so on. Moreover, stakeholders need to be able to make procurement and deployment decisions that are appropriate for their particular needs, situation, and circumstance. The proven model for enabling such a diverse set of networks, needs, and requirements is the public Internet. However, some of the unique requirements of the Global Aviation Ecosystem will require regulations to be developed that are globally applicable across all ICAO Member States.

Aviation Week, in their first 2018 issue, identifies 8 new satellite data services in development. Experience shows that without the architecture described in this ConOps to enable and support Interoperability in Global Aviation Ecosystem, these developing communications systems are not likely to be interoperable, nor are they likely to provide global reachability between aircraft in flight using different ANSPs or aircraft operators.

This ConOps suggests that the aviation industry develop a set of design and implementation policies to ensure standard uniform global infrastructure-based technologies used in private enterprise and the Internet. Uniformity is required to ensure that air vehicles can utilize new AATCC services globally, and new entrants can properly interact without customization for individual Member States. Customizations, or other deviations from routine practice, often lead to reductions in data handling resiliency due to increased latent defects found after deployment. The net effect of implementing these suggestions is to create a members-only aviation internet.

2 Overview

This ConOps will use technologies developed for the public Internet to accomplish its goals of providing collaborative information exchange in the Global Aviation Ecosystem. However, the unique needs of the Global Aviation Ecosystem result in some special requirements. To accomplish the vision of collaborative information exchange, the aviation industry will need to facilitate the creation of a new global aviation communications infrastructure for AATM and AATCC. This will require acquisition of address space for the new infrastructure, as well as registration of an appropriate segment of the name space so that stakeholders also connected to the public Internet can avoid conflicts. Coordinating the name space will help to insulate the system when an actor, either maliciously or inadvertently, connects the aviation network to the Internet. Assuming the address space resources are in hand, this document lays out a plan for deployment that builds on the knowledge and experience the industry has gained through the global Aircraft Communications Addressing and Reporting System (ACARS) and Aeronautical Telecommunication Network (ATN) communication systems. Deploying the network infrastructure discussed here will result in an operating environment based on Internet technologies that have been developed by the aviation industry to address its specific requirements. By leveraging widely deployed technologies, the aviation community gains from existing extensive reliability testing, as well as reduced costs both from the availability of existing products and the availability of staff trained in its deployment and operations.

The environment presented herein is an ecosystem supporting continuous technology evolution that allows policy updates without major impact to deployed infrastructure or aircraft currently in service. To be clear, this ConOps allows AATCC service to be deployed with zero impact to existing aircraft or ground infrastructures that are not participating. Simultaneous fleet-wide upgrades are also avoided due to the focus on continuous technology evolution. As business and policy requirements evolve, AATCC services can be added to new aircraft or retrofitted in accordance with regulators, airframers, and airlines negotiated timeframes.

While consistency of Service Names across ANSPs assures global interoperation, by introducing new message types, airframe manufacturers will have the ability to differentiate services to meet their customer’s specific requirements. At the same time, through this architecture, legacy aircraft with existing Internet service links can easily improve resiliency around ACARS and ATN services. While existing mechanisms continue to operate as usual, through the addition of an interface module to the aircraft’s Communications Management Unit (CMU), a parallel data path over a secured IPv6 infrastructure would start the migration and immediately improve data integrity. This interface would be similar to small hand sized systems used in other industries to interface with legacy industrial or grid control systems.

Unfortunately, cyber hazards have become a global threat to all industries; aviation is no less threatened. As this new infrastructure develops, the industry must consider the increased threat from cyber disruptions on safety and resilience. Digitization has revolutionized business models for entire industries and transformed daily lives. In the aviation industry it has contributed to numerous efficiencies in scheduling, ground handling, and flight planning. However, expansion to include more sensitive Flight and Flow navigation operations must be carefully planned and implemented to mitigate and minimize the inherent vulnerability to cyber threats.

While not directly addressed here, the concepts discussed are compatible with the work done by the industry to create ATA Spec 42, which includes a framework for PKI assurances and also to establish a global trust framework. Similar models are used in other industries sensitive to cyber risks. These frameworks incorporate international standards, global governance, and a federated hub. In the present case, such a hub would limit membership to aviation stakeholders and provide secure collaboration within the community.

This ConOps provides guidelines about policy targeting consistent implementation of standard names and network addresses for global interoperability. The industry will need to establish global naming and network addressing policies for this infrastructure before deployment begins. Once these policies are in place, the industry will be able to use the policies and projected network scale as the basis to apply for the name(s) and Internet addresses that will be deployed. Initially, the industry will need to register a Second Level Domain (SLD) under the .INT generic top-level domain (gTLD) until such time as ICAO is able to obtain its own gTLD from the Internet Corporation for Assigned Names and Numbers (ICANN).

The ConOps retains familiar ICAO naming standards for identities across the aviation infrastructure. For commercial aviation use it proposes name structures consistent with the Internet that use ICAO's existing country-airline, airport codes, and aircraft tail numbers. Entities in the AATCC are addressed with names, or a Digital Identity, that have a form similar to “flight#”, “airline”, “group-class”, “country-code”, “icao-SLD.int”. Once ICAO has its own gTLD, the final two (2) parts “icao-SLD.int” will be replaced by the new gTLD.

The Internet Domain Name System (DNS) protocols will provide basic resolution services, linking existing ATM systems and services to the new infrastructure. Additional resolution services may be needed to functionally bridge the physical and operational worlds of air traffic control and management to this new cyber world.

This ConOps envisions that the industry will obtain and manage a global allocation of IP addresses for the industry in a manner similar to the existing ACARS address process. The address space will be from the IPv6 address pool, as it has superior scaling capabilities. By contrast, the IPv4 address pool is exhausted: no globally routable IPv4 Internet address blocks are available in sufficient quantity to support even a single State's deployment of new Advanced Air Navigation Services. Finally, current alternatives to IPv6 are being deprecated in operational use globally.

The ConOps presented in this document will enable Member States to define messaging structures and protocols for applications that will meet the reliability requirements of advanced air traffic control communication. These developments should be validated on scaled cyber test labs and network ranges. These concepts will dramatically reduce the financial and operational risks associated with AATCC deployment and aircraft equipage. Most existing digital air-to-ground links with capacities over 100 kilobits per second and certified for “safety of flight” communication can be readily upgraded to support the addition of an IPv6 overlay for AATCC. This decreases AATCC equipage costs by using an aircraft's existing air-to-ground link, thus requiring minimal supporting hardware for equipage.

The overall model of Continuous Technology Evolution does not preclude any of the recommended initial deployment technologies from being replaced by a successor. In fact, the ability to replace technology over time, coupled with the need to minimize complexity to assure operational resilience, drives a separation of function and compartmentation approach.

Finally, this ConOps show a clean separation of existing in-service legacy aircraft and communications, leaving them untouched for an initial AATCC implementation. Considering the rapidly growing aviation ecosystem with its increasing need to connect and exchange data, the industry will continue to improve safety of flight through the expeditious implementation of consistent global policies and infrastructure.

In conclusion, the industry faces a number of major risks if they do not advance the standards for the foundation of this new IPv6 communications infrastructure for advanced ATM/ATC communications and services. These are some of the key risks items:

- Internet Name Space – lead time could adversely affect 2021 roll out plans.
  - Coordination work with appropriate Internet agencies to secure ICAO global aviation namespace may require more than one year.
  - Development of policies for implementation and maintenance of namespace will take two or more years to develop and implement. This may require ICAO to work with the UN to acquire Global Critical Infrastructure IP address block.
- Address Block Allocation - lead time could adversely affect 2021 roll out plans.
  - Coordinate with appropriate Internet agencies to secure a global aviation IP address block.
  - Once acquired, develop a standardized Global Critical Infrastructure address schema for allocation to members.
- Risk of inaction or delay in implementing the ATM/ATC ConOps could:
  - Limit introduction of business process improvement (e.g. limiting optimization of airspace capacity optimization, exposure compromised information security which could lead to aviation disruption…)
  - Limit introduction of new technologies that could improve and enhance Safety/Resilience, and business process improvements.
  - Result in fractured regional/state actions which are not interoperable.
  - Create further congestion of national air space due to:
    - Ignoring new entrants
    - Increasing demand

Delaying this work may prevent meeting the industry anticipated rollout dates for the global infrastructure necessary to support advanced ATM/ATC services. The ripple effects of failure to meet the planned rollout dates cannot be understated in either the financial cost to global commercial aviation or the inability to maintain the safety record improvements of the last fifty years. These concerns become particularly acute as increasing airspace demands from existing commercial aviation and new entrants press the currently deployed ANSP technologies. Cyber security for network infrastructure used by the aviation community must be robust.

3 Introduction

3.1 Purpose

This project proposes to leverage ICAO's unique position as an independent standards organization to facilitate the deployment of a global interoperable airspace digital communications infrastructure for air-to-ground, ground-to-ground, and air-to-air operations, plus the associated network based on Internet technologies to support them. A common architecture for these services is required to ensure that all stakeholders can deploy local environments that are interoperable with the members-only global system.

NOTE: Any of the following descriptions that appear to be stating a policy are simply examples to provide a practical context for understanding the scope of the proposal and highlight issues to be considered. To avoid the distraction of inserting "one possible policy" before every instance of something that looks like a policy, an example is stated to show how a set of policies might enable functional deployment of the concepts. Actual policy decisions are out of scope for this document.

3.2 Problem Statement

At the top of the list of key issues to focus on is that the existing processes and procedures used for air traffic management were clearly never designed to deal with the threat of someone actively trying to subvert or interfere with the system. Air Traffic Management is currently conducted over open radio channels with unauthenticated voice used to transmit critical flight safety information. While some attempts at digitization of information passing between the air and ground have been deployed, those too have no authentication mechanism to validate the messages. Moving the ATM system from unauthenticated voice over open radio channels to a digitized environment that can be authenticated and secured is required for dependable and resilient management of the airspace. This is necessary for efficiency and safety.

Among the key issues in improving airspace safety and efficiency is the need to improve the aviation industry's ability to manage operations, both for clarity of information being distributed and for the increased situational awareness resulting from information availability. Globally, the airspace environment is set to radically change over the next few decades. Just a few of the major changes envisioned include:

- Rapid expansion of the number of air vehicles in use as Remotely Piloted Vehicles and air sport usage soars.
- Autonomy of air vehicles will continue to improve.
- Crews are re-trained for updated avionics, as well as regulatory changes by Airspace Navigation Service Providers (ANSP).
- Training and average certification level of operators will dramatically decrease, even as training programs improve, due to a massive influx of untrained users operating Remotely Piloted Vehicles.
- Spacecraft begin routinely operating in the national airspaces.
- In most cases, AATCC will have to share an air-to-ground data link with other aircraft operations.
- Data exchange to/from the aircraft for Flight and Flow as well as other operations will dramatically expand while air-to-ground communications capacity will only expand moderately.

Sharing of the air-to-ground resources with a priority for Safety of Flight is the critical issue addressed here, meaning some Flight and Flow messages will require prioritization over all other air-to-ground link uses. Data exchange to/from the aircraft will need a standard framework that allows interleaving messages at a more granular level than simple Information Realm prioritization. For example, an air ambulance would have life-safety messages related to patient data in an Information Realm that is not AIS or Flight and Flow but would share the same data links. This means policy needs to be established for the system to classify and prioritize messages and Service Classes rather than focus on interfaces. Complexity of operations with new Airspace Users (AU) and types of aircraft will require a robust and safe ground-to-ground communication network in support of a global information management system.

While that is taking place, industrial use of low-cost short-range aircraft is already happening with no integration into situational awareness for Flight and Flow. Compounding that problem, we are already at a point where it is technically feasible for someone to send a Personal Autonomous Aircraft (PAA) to the local deli to retrieve lunch. Development of the policies and infrastructure necessary to support these emerging use cases needs to happen before the costs are reduced to the point where the global mass market can afford it. Failure to act promptly will result in chaos that undermines all other traffic congestion management efforts.

The primary repercussion of a unified architecture is that historical modes of independent operation need to stop sooner rather than later. The sooner the industry can establish a governance framework for the aviation environment, the better the outcome will be for all stakeholders including cost reduction and overall system security and resilience. This governance framework needs a broad scope to deal with everything from standard names for services to address allocation policies. This framework will also need to establish policies for notification between Network Operation Center / Security Operation Center environments and procedures for delegating services for stakeholders lacking the resources to properly deploy and operate some of the more complex technologies like PKI that are necessary for a trusted and resilient environment.

3.3 Risks

It is recognized that the transition to the Advanced Air Navigation Services (AANS) will involve significant operational and financial considerations. At the same time, there are substantial consequences associated with inaction or delay. The expected growth and dynamism in air transportation, together with the need for improved situational awareness of the new AUs and missions, makes it necessary to begin implementation of the AANS concept as soon as pragmatic realities allow. Substantial delay in aligning the existing digitization efforts increases the risk that fragmented partial implementations will require significant reinvestment of both time and capital to transition to the globally consistent approach.

One significant risk to deviating from a common architecture is the lack of interoperability, leaving some stakeholders behind. The costs for implementing multiple partial schemes impacts both equipment and staffing beyond simple redundancy of effort. Confusion in operational practice or device configurations due to inconsistent implementation choices will lead to misaligned security assumptions. Misaligned security assumptions are a leading cause of reduced resilience, thereby exposing the entire system to intrusion or tampering.

A risk of not deploying an architecture capable of continuous technology evolution is that new technologies that could improve airspace safety, traffic management resilience, or business processes, will be difficult and expensive to integrate. Complexity or high cost reduces the number of stakeholders able to stay current. Wide divergence in operational capability or practice further increase overall system complexity and reduces resilience.

System Block upgrade plans for 2021 and beyond might be at significant risk of delay unless prompt action is taken to secure both name space and an address block from the appropriate Internet coordinating bodies.

3.4 Scope

The scope of this Concept of Operations (ConOps) is to describe the global network and service infrastructure necessary to support Advanced Air Traffic Control Communications (AATCC). This includes messages that are critical to safety of flight and ground-to-ground air traffic management between Member States. As the global air space evolves, this architecture is readily able to incorporate any class of piloted, remotely piloted, or autonomous air vehicles that are defined by ICAO for regulation. This includes flight safety communications ground-to-ground, air-to-ground, as well as air-to-air when defined at some future date.

The scope does not cover internal operations of any data link providers, aircraft operators, or third-party support or service providers. However, the network architecture and Internet naming concepts of this document could be readily used to support air-to-ground communications within the Airline Information Systems (AIS) domain, Passenger Internet and Entertainment System Domain (PIES), and the Passenger Electronics Domain (PED).

The concept is a platform that will provide Member States and the Industry with a set of tools and regulatory provisions to enable a globally interoperable information management environment. Being connection type agnostic, including the ability to leverage the public Internet, the resulting infrastructure will interconnect existing State and Regional Systems. This information management infrastructure and supporting services will provide equal access to all aviation stakeholders, regardless of means or ability, ensuring no country is left behind.

Deployment of the infrastructure can be achieved by coordinating:

- Extension of existing service-oriented architectures (SOA) from ground-to-ground to include air-to-ground, and air-to-air.
- Definition of the requirements for standard services including communication data link capacity, resiliency, security, etc.
- IPv6 addressing
- A naming structure that is consistent with public Internet use.
- Some or all services of a global Public Key Infrastructure (PKI).
- Standards development with recommended practices for IP based communication.

The defining characteristic of the architecture is that it uses technologies widely available and deployed in the public Internet where appropriate but implements them in a parallel members-only configuration. Use of existing commercial technology reduces deployment costs while ensuring that trained staff, who truly understand the technology and how to deploy and operate it for maximum resilience, are readily available.

This approach ultimately allows for the development of globally interoperable AATCC services. The resulting loosely coupled system allows policy to evolve as needed without major impact to deployed infrastructure. New or updated services can be developed with a focus to be 'secure by design' in a manner that integrates with the System Wide Information Management (SWIM) concepts.

3.5 Guiding Principles

Principles forming the foundation of this document include:

- Evolution to the SWIM model of operations must be inclusive and incremental, allowing AUs, States, and other stakeholders to participate at their own pace.
- Interoperability between all stakeholders is assured through a common architecture for seamless and efficient messaging services on a global scale.
- Resiliency of the communications is maximized by utilizing design concepts that limit the cyberattack surfaces. This includes compartmentalization of the network and the applications, as well as layering of protections in the infrastructure and limiting the number of systems participating.
- Strong identification, authentication, authorization, integrity, and confidentiality services allow network resources to be shared between Information Realms while maintaining appropriate isolation.
- Service Names that are consistently defined system-wide simplifies operations and improves efficiency and safety of flight.
- Aircraft should be reachable for AATM and AATCC over any available data link whether Gatelink, WiMAX, Satcom, 3/4/5G, or other future data links.

3.6 Organization of this Document

The document is organized as follows:

Section 3 provides an overview of the ConOps.

Section 4 discusses the architecture and ecosystem components.

Section 5 considers migration issues.

Section 6 identifies issues related to governance and operations.

Section 7 summarizes the benefits.

3.7 Relationship to Other Documents

The Global Air Traffic Management Operational Concept (Doc 9854) presents the ICAO vision of an integrated, harmonized, and globally interoperable ATM system. The Manual on Flight and Flow – Information for a Collaborative Environment (FF-ICE Doc 9965) describes the information environment in support of that vision. The key aspects include support for a Performance-Based Approach (PBA), Collaborative Decision-Making (CDM), and System-Wide Information Management (SWIM) by trajectory. The Manual on System Wide Information Management (SWIM Doc 10039) describes compartmentalization of the information, both to ensure that all required recipients have what they need and to limit distribution to only those recipients. The AANS concept described in this document identifies the network infrastructure components necessary to deliver the information. It also defines the interface characteristics, between the information environments and the network that facilitate interoperability between regions, as well as enables sharing of resources while maintaining isolation for the independent environments. Specifically, this document focuses on FF-ICE figure 4-3, communications network, and SWIM figure 8, network connectivity functions.

4 Concept of Operations

As the processes for digitization of the Air Traffic Management system continues to expand, the need for a globally consistent infrastructure is urgent. The FF-ICE messaging approach uses a Service Oriented Architecture (SOA) with standardized Message formats to distribute Flight and Flow information system-wide. The SOA model allows individual Information Realms to be partitioned with different technology and service implementations in each, as long as the standardized service interface is used when interacting between participants. This use of a standardized interface also allows multiple Information Realms to share resources while remaining independent. The set of functions that deliver identification, authentication, authorization, integrity, and confidentiality is the infrastructure that ties together the partitions, or independent Information Realms, into a system-wide coherent service IC. Achieving these core functions relies on a strong Digital Identity, plus globally consistent conventions for naming and addressing, tied to a resolution, authentication, and integrity infrastructure.[1]

The ConOps presented here not only delivers the services necessary to facilitate the FF-ICE vision of system-wide information consistently, but it will also accommodate emerging Information Realms of interest to the AU community. The technologies used in this approach apply equally well for the ground-to-ground needs for Flight planning and coordination, as they do for the air-to-ground needs of Controller-Pilot data.

The concept of operations proposed in this document rests on these items:

- All new ATM/ATC Communications Services, whether ground-to-ground, air-to-ground, or air-to-air, are defined as message passing "services" whether the message is a short digital instruction or a file like maps, NOTAMS, or weather. They can be considered to be a "smart ACARS" in that in their definition is information on the type of message and its intended recipient group. A "service" can define aircraft equipage requirements to receive the service, and may include, aircraft models, required security, priority, etc.
- The ability to define new or updated ATM/ATC Communications Services at any time without impacting in-service aircraft.
- An architecture delivering security and fine-grained prioritization for the FF-ICE message services which will enable peak efficiency and safety in the airspace.
- A globally common network architecture based on existing Internet technology, ensuring that air vehicles can establish communications service with any ANSP when needed.
- A naming and addressing policy that minimizes the operational complexity of managing, securing, and resiliency of these global communication services.
- Establish a common format secure Digital Identity for all AUs (including air sports through passenger aircraft) which uniquely identifies them to assure communications are with the intended party.
- An aircraft operating anywhere on the globe can locate and utilize flight management services and ATC services appropriate to its equipage.
- Advanced ATM/ATC service communications can utilize any "approved" IPv6 link to contact the aircraft whether 3/4/5g, Satcom, WiMAX, or others.

[1] ICAO Doc 9965 Manual on Flight and Flow – Information for a Collaborative Environment

- “Approved” IPv6 links to an aircraft ensure that key interoperability functions like naming, addressing, and message prioritization are implemented such that the aircraft is reachable by that link for advanced ATM/ATC services.

The overall goal is to provide a framework for AUs and other stakeholders to establish standards for operational procedures and policy which enhance both ‘safety of flight’ and efficiency. Using stress tested technologies common in private enterprise networks, coupled with appropriate policies and best-practice operations, the resulting network-of-networks will provide improved situational awareness with manageable risk. At the same time the current system is evolving, the concepts presented here allow the environment to expand the number of participants both for new entrants and new missions. Development of the policies and infrastructure necessary to support new entrants (RPAS, air sports, space vehicles, etc.) needs to happen soon. Urgency is called for as unit costs are being reduced to the point where shear production volumes mean they will soon be the overwhelming majority of aircraft in operation. Manufacturers achieve their low production costs by limiting configurability of the control systems, meaning these aircraft will be impossible to retrofit and airspace management will suffer until entire generations of product are retired.

Figure 1 International Civil Aviation Airspace Users includes the flight operations centers (FOC) and the entity responsible for the execution of a flight.[2]

International Civil Aviation encompasses a wide array of participants making use of the shared airspace. From a ConOps perspective, awareness of these participants, their scale, capacity constraints, and relationships are required to ensure the information source is authentic and that data gets delivered to where it is needed in a secure and timely manner. Policies will need to be developed to establish which AUs are required to interact with AATM/AATCC and which will be exempt. Additional policies will be needed to establish methods of integrating new entrants, as well as frequency of interactions to align with airspace management requirements.

4.1 New Air Traffic Control Communications and Management Services

Integrating the diverse systems involved in FF-ICE and safely delivering its message services requires focusing the network architecture on resiliency, capacity, and security. The communications network identified in FF-ICE is described in slightly more detail under network services in the SWIM manual. The AANS architecture delivering AATCC services discussed by this ConOps will present a structured relationship between the network components identified in

[2] 9965 FF-ICE 3.3.2

those documents and the necessary infrastructure to deliver the expected services, including definitions for:

- Service Class - identifies technical performance requirements, policy groupings, and minimum-security expectations.
- Digest Exchange - handles transformation between verbose SOA constructs and a concise form used for transport over the constrained air-to-ground links.
- Legacy Exchange - handles transformation between legacy bus or IPv4 network systems and constructs.
- Service Exchange - identifier for the collection of processes and infrastructure that provide services between the Message Publishers in an Information Realm and the data-link providers connecting locations or between realms. This includes at least the Service Guard, the Network Interchange, and the Link Security Router.
- Service Guards -– Flexible, individually defined security protection points. They can be defined by the location in the infrastructure and/or the service class definition. They enforce content policies at the messaging or application level. The policies are defined in the definition of the “service” and its associated “service class”. The “service class” defines the carrying layer 3 IP network, authentication requirements, confidentially, and required cyber security protections (i.e. poison packet detection, malware inspection of messaged “files”, message blocking, etc.).
- Link Security Router (LSR)- establishes the virtual infrastructure as an overlay network.
- Link Management Router (LMR) - enforces the Service Classes a given data link is authorized to carry and manages prioritization consistent with policy. The LMR transports opaque packets between Link Security Routers.
- Network Interchange (NI) –enforces access controls at the network level (layer 3 firewall). The NI handles all processes and services that are necessary between the LSR’s overlay abstraction, and the Service Guard’s message passing abstraction. These include at least DNS, DHCP, NTP, Certificate-Server caching, and network routing within the virtual infrastructure

Aviation digital air traffic control communications and management services will be defined by Service Names and Service Classes. A service will be named like CPDLC and assigned a Service Class by ICAO or the states. The Service Name will have an associated short descriptive like “controller pilot data link communications” with the Service Name itself being a short Internet name like “CPDLC” or “CPD” for data or “CPVLC or CPV” for voice.

A service will then be assigned to a Service Class. The Service Class will then define the data link requirements like capacity, reliability, resiliency, etc. Service Class can also define data link isolation requirements such the ARINC and RTCA utilize to maintain separation of the aircraft onboard communication domains. Today these aircraft domains are divided into:

- Aircraft Control Domain (ACD) isolates systems and functions necessary to the aircraft’s flight safety, which includes Air Traffic Control (ATC) communications.
- Airline Information Systems (AIS) domain isolates systems involved with aircraft management for the operator like ACARS communications.
- Passenger Internet and Entertainment (PIES) and Passenger Electronic Devices (PED) support in cabin passenger entertainment, Internet, and voice communications.

For the purposes of this document, these air-to-ground communications Service Classes are ACD, AIS, and PIES. It is envisioned that these Service Class definitions will be refined and likely expanded as they develop. An example of this is that the aircraft weight and balance messages in ACARS could be redefined into an ACD service that allowed them to be securely fed directly into the flight management computer.

Air traffic information management systems services can be defined for ground-to-ground communications between the Member States and ICAO regions. These definitions will include appropriate definition in the Class of Service and protections in the Service Guard.

Legacy Exchanges can be defined to accept flight management or control input from legacy non-IP and IPv4 systems that can interact with an ACD service. For example, a Legacy Exchange could receive existing ATN FANs and CPDLC traffic, encapsulating them into an IPv6 IPSec message that could be received on the aircraft via an IP data link, where the encapsulated data is “unwrapped” and forwarded directly into the CMU. Migrating to the layered security architecture of the AANS would offer improved resilience for ATN communications to the aircraft.

These concepts could be used to allow dual use systems or appliances like an EFB, to have one AIS service for receiving new flight management and information via an operator infrastructure and another service for presenting in-flight updates and aerodrome moving maps to ACD systems.

Further they allow services to be created for items like meteorological data, sensor data, and aerodrome information that can publish to or subscribe to any Service Class allowed by policy. This facilitates sharing items like weather data, cabin statistics, aircraft cameras, etc. between aircraft domains or Information Realms as required.

It should be emphasized that services discussed in this document are data exchange services that may or may not carry message authentication depending on their Service Class. To minimize associated cyber security risks, these message services should not be envisioned or designed as end-to-end Internet Protocol connections, but as application data exchanges where the message receiver is responsible for screening before final delivery to any air or ground systems.

4.2 Ecosystem

This document discusses the infrastructure support components identified in Doc 9965 FF-ICE section 4.6. The resulting ecosystem facilitates collaborative interactions between AUs and regions, as well as between regions to assure data consistency, reliability, and resilience. By establishing a pluggable framework that decouples message services from the underlying transport infrastructure, the resulting loosely coupled system enables continuous technology evolution.

This is not just another link standard. It is an architecture encompassing the facilities and procedures necessary to enable a distributed collaborative messaging system through a standard interface. This standard interface is designed to enable multiple Information Realms to share limited resources, like the air-to-ground link, while isolating these Information Realms from each other. The uses of this architectural approach of a standard message passing interface with structured content include; common interchange for different implementations of FF-ICE by different regions; transitional inclusion of legacy information and formats by wrapping them in a structured container; and sharing of the underlying network services by compartmentalizing each Information Realm behind its own message passing interface known as a Service Exchange.

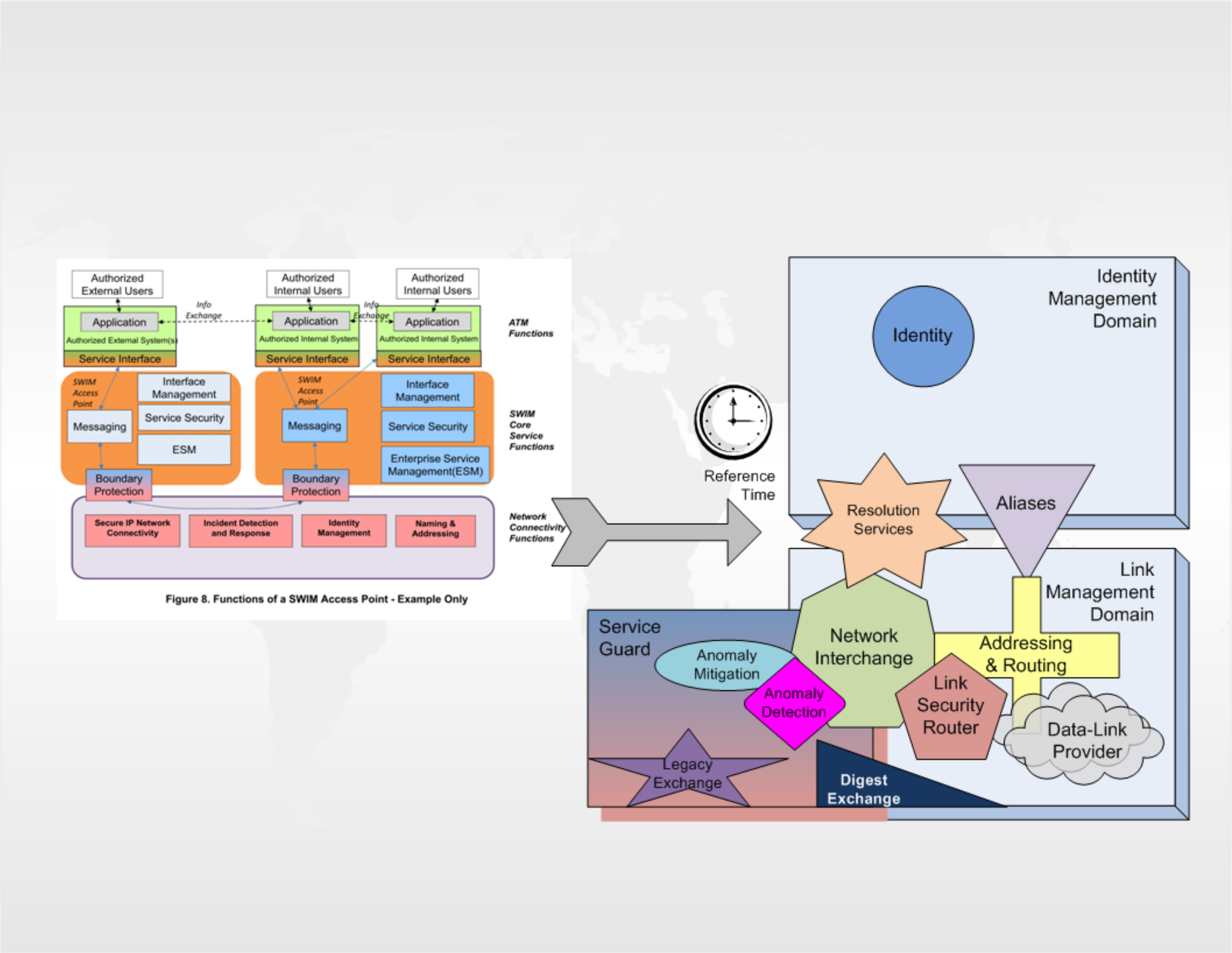


Figure 2 Infrastructure functions called for in both FF-ICE & SWIM are further detailed in this document

The SWIM framework describes a set of Network Connectivity Functions[3] along with a Boundary Protection function that spans between Core Services and Network Connectivity.[4] This document provides an architectural description for the functions in the Network Connectivity block and interfaces to the block. The standard interface between the message service and the infrastructure includes a Service Guard policing agent to handle bounds checking on messages that have passed the authentication and authorization hurdles.

5 Ecosystem Components

5.1 Digital Identity

For future airspace management, a common secure Digital Identity mechanism encompassing all AUs and equipment from air sports through passenger aircraft must be developed. For continued safety of flight, this invariant Digital Identity must uniquely identify not only the aircraft itself, but also many of its major components. Just as an aircraft can be simultaneously known as its flight number for passenger operations and its tail number for fleet management or maintenance purposes, the vast array of objects related to management of the airspace may have an alias that

[3] ICAO Document 10039 SWIM Manual Table 3
[4] ICAO Document 10039 SWIM Manual Figure 8

is specific to the context of the interacting parties. Having a common Digital Identity will enable electronic tracking of aircraft as they move between operators, as well as components like engines as they move between aircraft, in a manner similar to traditional processes using mechanically affixed serial numbers. This Digital Identity of each entity needs to be unique, persistent, and invariant.

5.2 Services Message Authentication

Authentication is not specifically covered in this document but will require policy definition before new AATCC services can be implemented. Ongoing work in the industry on development of a global trust anchor may provide true authentication for safety of flight communications. The technologies involved have been around for an extended period, but the political relationships and operational practice necessary to make them practical have proven to be a challenge in other environments.

Message Service Exchanges may or may not require authentication depending on the importance of their related Service Class. For example, authentication may not be required, except at the link layer, for PIES Services as this is truly just an extension of the Internet for passenger use, thus leaving authentication to the passenger. AIS message exchanges are likely to utilize airline specific authentication services like a private root PKI or other proprietary authentications. However, messages destined for the ACD relating to safety of flight will require authentication using a globally recognized ICAO certified service that operates on a global scale.

5.2.1 ATA Spec 42

This standard has been developed over the last 15 years for global message assurance. It utilizes the PKI bridge developed for industry by CertaPath. This type of message assurance is adequate for some messages but questions remain within industry as to its full suitability for the authenticating safety of flight communications.

5.2.2 Augmentation of Basic Authentication Services

The overall architecture and the design of message-oriented services readily enable each service to utilize independent authentication types at the application level. Message authentication can be handled by either the ANSP or the aircraft operator as appropriate for the service. In any case, the aircraft will need mechanisms to validate that information it receives from the ground is authentic, and the ground needs to validate that information about the aircraft could only have originated there. Validation lifetimes need to balance between the conflicting impacts from available bandwidth and mobility changes to addresses that may have been considered in the validation process.

The robust nature of integrity related to PKI systems comes at the price of responsiveness and transaction rate scaling. A variety of one-time-password and session key techniques are often used in conjunction with PKI systems to improve responsiveness and transaction rates.

While legacy password type authentication is not excluded, its susceptibility to unauthorized disclosure is the primary reason to discourage its use. The included network layer path protections using IPsec will help limit exposure for password authentication, but care must be exercised with respect to routine password updates as well as prompt password changes when compromise is suspected.

In any case, the type of authentication used must be adequate for the information it is related to. While password type authentication is generally inadequate for weight-and-balance information, a full-scale PKI is excessive and impractical for passenger access to Internet services.

5.3 Naming

The name space is structured to align with the natural administrative relationships between AUs. This is both for the practical realities of managing data sets, as well as the protocol necessities of signature authority for approaches like DNS Security Extensions (DNSSEC). Generally, the proposed DNS structure aligns with ICAO recognized stakeholders, ICAO responsibility, state responsibility and airline responsibility. It proposes the use of the existing ICAO three letter codes for states, aircraft operators, and aerodromes to minimize operational confusion as new services are added. ICAO policy will be required to ensure naming is globally consistent, allowing all aircraft to locate ATC services for the airspace in which each is operating.

In Internet terms, this is the Domain Name System (DNS) but operated in a members-only configuration. This naming structure could also easily be extended to cover other aircraft types and air space users as required.

For the AIS and PIES domain, no recommendation is made although both could readily be named along the same lines to minimize airline operational complexity. Policy and Implementation for each largely rests with the aircraft operators as these domains are outside of ICAO’s purview.

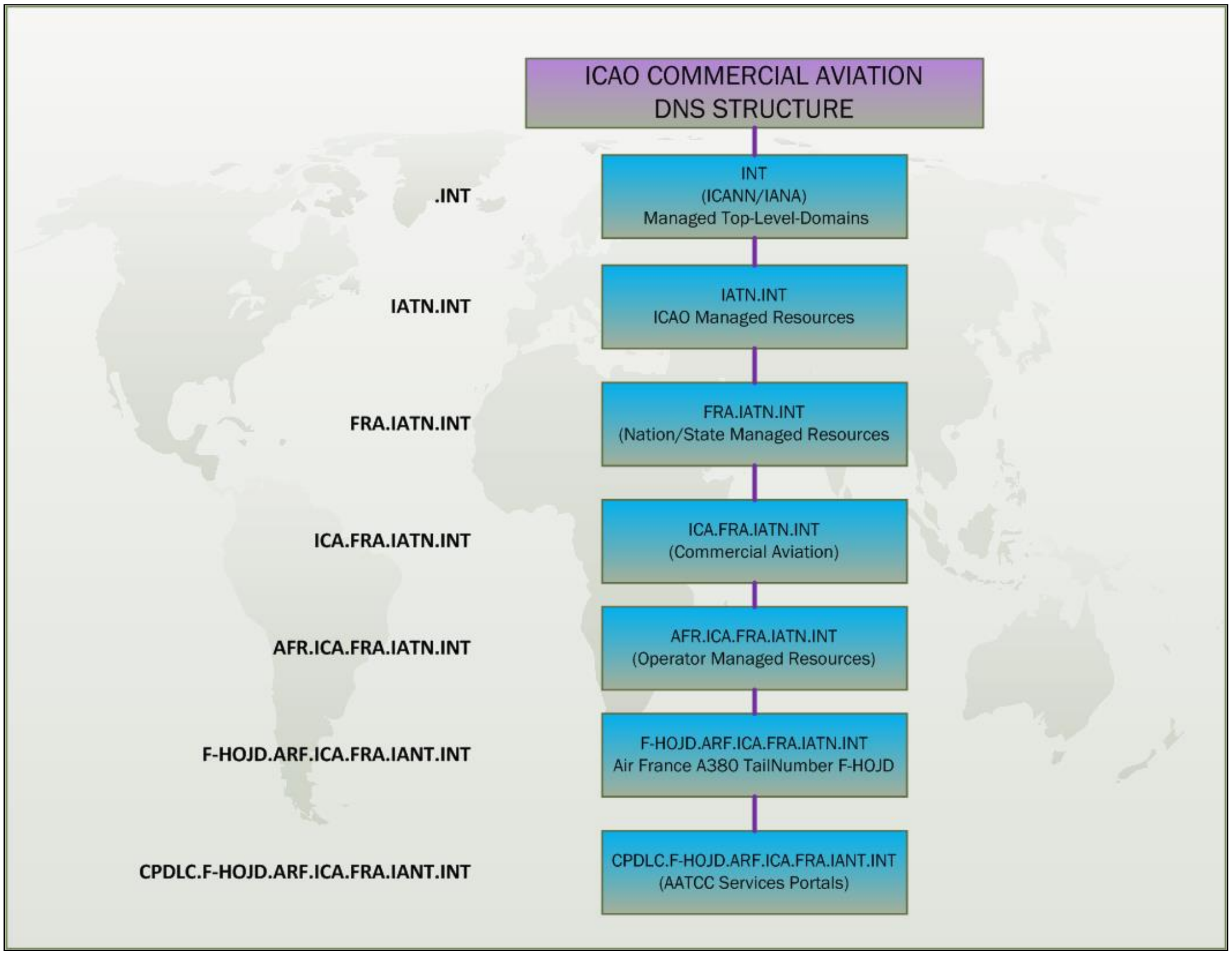

ICAO COMMERCIAL AVIATION DNS STRUCTURE
.INT
INT (ICANN/IANA) Managed Top-Level-Domains
IATN.INT
IATN.INT ICAO Managed Resources
FRA.IATN.INT
FRA.IATN.INT (Nation/State Managed Resources
ICA.FRA.IATN.INT
ICA.FRA.IATN.INT (Commercial Aviation)
AFR.ICA.FRA.IATN.INT
AFR.ICA.FRA.IATN.INT (Operator Managed Resources)
F-HOJD.ARF.ICA.FRA.IANT.INT
F-HOJD.ARF.ICA.FRA.IATN.INT Air France A380 TailNumber F-HOJD
CPDLC.F-HOJD.ARF.ICA.FRA.IANT.INT
CPDLC.F-HOJD.ARF.ICA.FRA.IANT.INT (AATCC Services Portals)

Figure 3 Standard structure for DNS labels within ICAO's governance

As a fundamental principle, DNS content is Information Realm specific, therefore not useful outside the domain. As such Service Guards should make sure DNS queries and/or responses between domains are dropped.

5.3.1 Resolution Services

Resolution Services may take several forms as any given alias is mapped through the Digital Identity to find the target alias. Technology evolution over time will produce a variety of approaches to resolution. The architecture presented here considers database lookups, on-the-fly calculations, and third-party resolvers to be equally capable of providing the function. The decision about any given implementation or instance needs to be based on the type of alias to be resolved coupled with current best-practice deployments that meet the engineering constraints. For the sake of simplicity, the remainder of this document will focus on DNS as it aligns well with the distributed nature of the authority structure in the Civil Aviation environment.

One instance of a resolution service is the DNS and supporting protocols. A private members-only deployment of these will be used to map between various aliases, in particular name strings and network address strings. It may also provide mappings between services and name strings. Mirroring many other entities that operate a closed network on a global scale, the AANS DNS infrastructure will operate in a members-only private enterprise context with different regional or national authorities being comparable to semi-independent divisions in an enterprise. This DNS infrastructure will operate in isolation from the public Internet DNS but using a common name space. The common name space is required to avoid any confusion or overlap as many of the contractors and facilities are also connected to the public Internet. While the definition of root is shared, labels may overlap, meaning the mapping for a label internal to the closed environment may be different than any public mapping.

5.4 Network Architecture

The network architecture is a members-only private virtual network comparable to deployments used by global private enterprises. The infrastructure gains from technologies that are based on open standards are extensively deployed in similar production environments. Use of existing technologies also increases global availability of staff trained in its deployment and operation.

The foundation of the overall AANS environment starts with a strong unique Digital Identity, and a responsive mapping system that allows dynamic aliases to be managed by the point of authority for each alias type. The environment supports the concepts of independent Information Realms and enforces their isolation or managed interactions including onboard the aircraft. The topology interconnecting different locations (an aircraft is just a location) within and between Information Realms is recognized to be explicitly outside the scope of the content realms, therefore in its own Information Realm, identified here as the Link Management Domain. From a policy perspective, the content realms consider the Link Management Domain to be equivalent to the open public Internet even for private services. This perspective is necessary as it is often impossible to tell from the service interface if any part of a data link service traverses as an overlay or is integrated with the public Internet. Unless otherwise noted, path protection technologies are assumed to be available and deployed between locations (including any aircraft) and might be deployed between Information Realms even at the same location.

5.4.1 Locations

Locations on the network include both flight operations centers and aircraft. While some of these locations are fixed and some move, the fundamental network architecture does not differentiate between locations based on that. In fact, since the most constrained network resource in this system is the air-to-ground link, the architecture is defined with that as the basis. Fixed locations like, flight operations centers, may be viewed as stationary aircraft where communications resources are more flexible and abundant.

5.4.2 Topology

The network architecture discussed here is an overlay that abstracts random link types and addressing models into the appearance of a coherent whole. Security is layered by having different components of the network responsible for very specific tasks. This focus improves overall performance and resilience by removing obviously errant traffic before it reaches the more complex processes for application integrity checks. An analogy will be used to relate the physical world to the concepts of compartmentalization and decision points in the abstract data network environment.

Suppose that someone at location 1 wants to send a handwritten message to someone at location 2 without anyone else knowing its contents. To accomplish that, they might put the message in a locked attaché and only the sender and recipient hold the keys. To move the attaché from location 1 to location 2, the sender hires a courier and a car service to provide transport. The courier provides the destination to the driver in a widely recognized form and the driver then chooses the appropriate roads to reach the destination.

In this scenario, the locked attaché carries the content, the courier carries the attaché, the car carries the courier, and the road carries the car. This collection is a simple form of layering with focused roles to securely move the paper message from location 1 to location 2. The locked attaché precludes all but the authorized recipient from being aware of the contents.

The security of that sequence can be improved by having the courier require identification from the recipient to assure proper delivery. The recipient in turn could require identification from the courier, prior to even attempting to unlock the attaché. This removes the time-wasting effort to try the key on whatever random attachés might show up. Since the courier might end up at multiple destinations, they might need to carry several forms of identification and would need some hints as to which form is appropriate at any given location.

Further improving on that situation, the car service could be instructed to only transport specific couriers or be given a prioritization if multiple couriers are carried at once. The driver selects specific roads based on availability and efficient delivery of any couriers based on priority order. Complicating matters, the selected roads might have restrictions where only certain vehicle types may use specific lanes, exits, or destinations, and unexpected closures may force detours.

While this sequence is lengthy to describe, it happens every day in the physical world outside data networking. Despite the complications, messages get delivered. While not an exact match, the functions of the AANS infrastructure can be independently described and layered to provide focused services similar to the attaché analogy above.

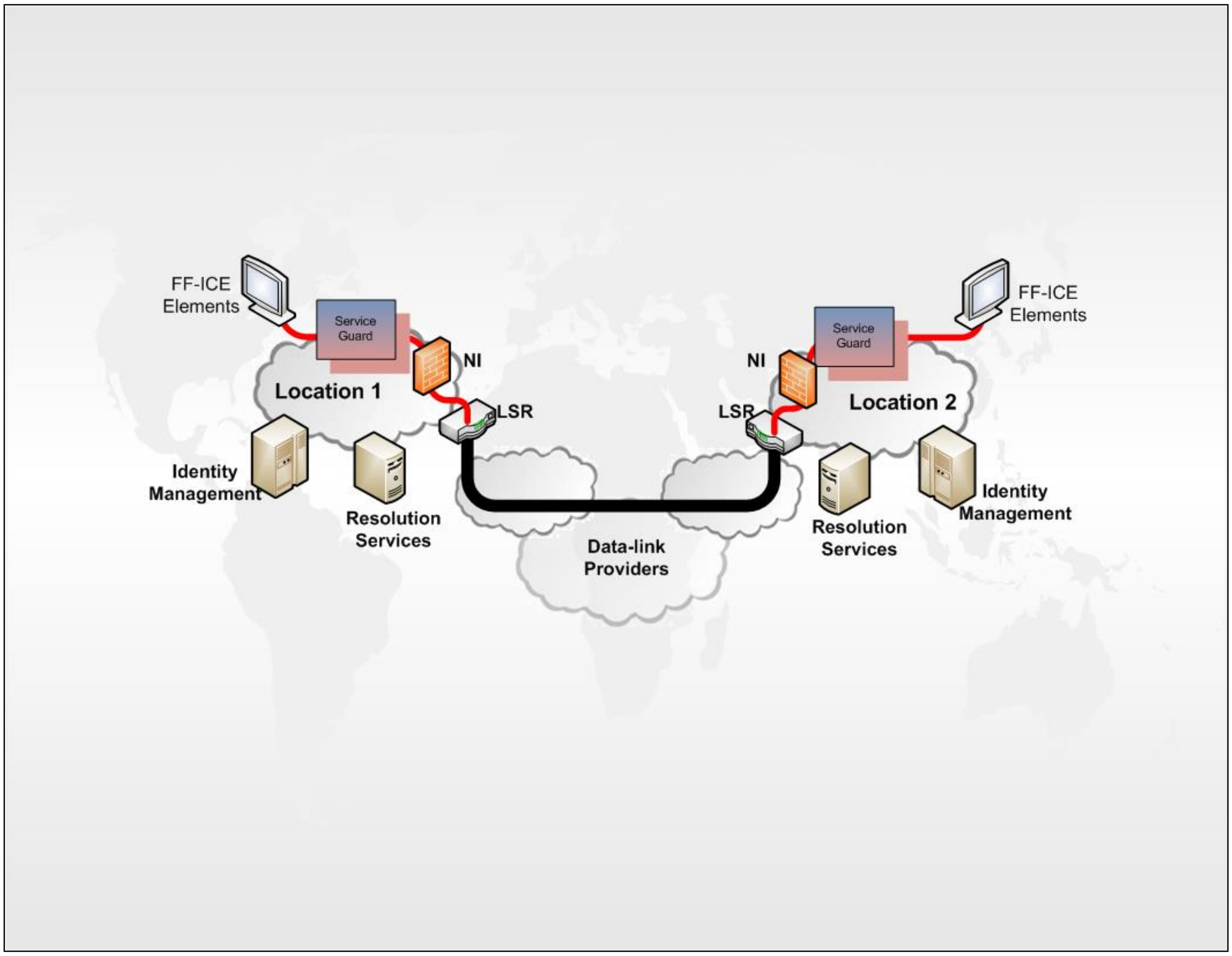


Figure 4 Network Architecture showing overlay model with protected paths between Service Guards.

5.4.3 Time

The network architecture includes support for a globally consistent view of time. Time scales vary between technologies and context, which results in confusion when not understood. Many security functions, including PKI certificate validation and auditing systems, require a consistent time scale. This means that a policy about time is needed to ensure operational protocols and procedures work system-wide.

The aviation community and Civil Society refer to time using an imprecise scale that periodically adjusts to align with the earth's rotational relationship to the sun, known as Coordinated Universal Time (UTC). Computational systems are not so forgiving or flexible and generally use a simple precise count of events since the counter was last at zero, known as an epoch. The duration of an epoch is determined by the event being counted, and the size of the counter. Different computational systems have different starting dates and sizes for their counters, so even if they happen to align at some point, one will eventually reset before another. While it might be tempting to view a preferred Global Navigation Satellite System (GNSS) as an adequate time source, different systems already use different time scales, and those differ from UTC. Any legacy equipment intended to be based on UTC which does not include the capability to compensate leap-seconds[5] is currently incorrect by 37 seconds (roughly increasing by 5 seconds every 6 years). Existing policies about aircraft spacing include a generous margin and can mask clock inconsistencies. As airspace efficiency rises through better situational awareness and tighter spacing, the need for clock consistency will rise in importance independent of any network protocol requirements.

There is no hard requirement for International Civil Aviation to continue to use UTC, but there needs to be an unambiguous and bi-directional mapping to UTC because that is the time scale used by Civil Society when interacting with the aviation community. Policy needs to be established selecting one of the available time scales as the system-wide reference. If UTC is selected, additional policy will be needed to establish procedures for how computational systems interpret between precise counters and the pseudo-random non-linearity events inherent in UTC.[6]

5.5 Network Addressing

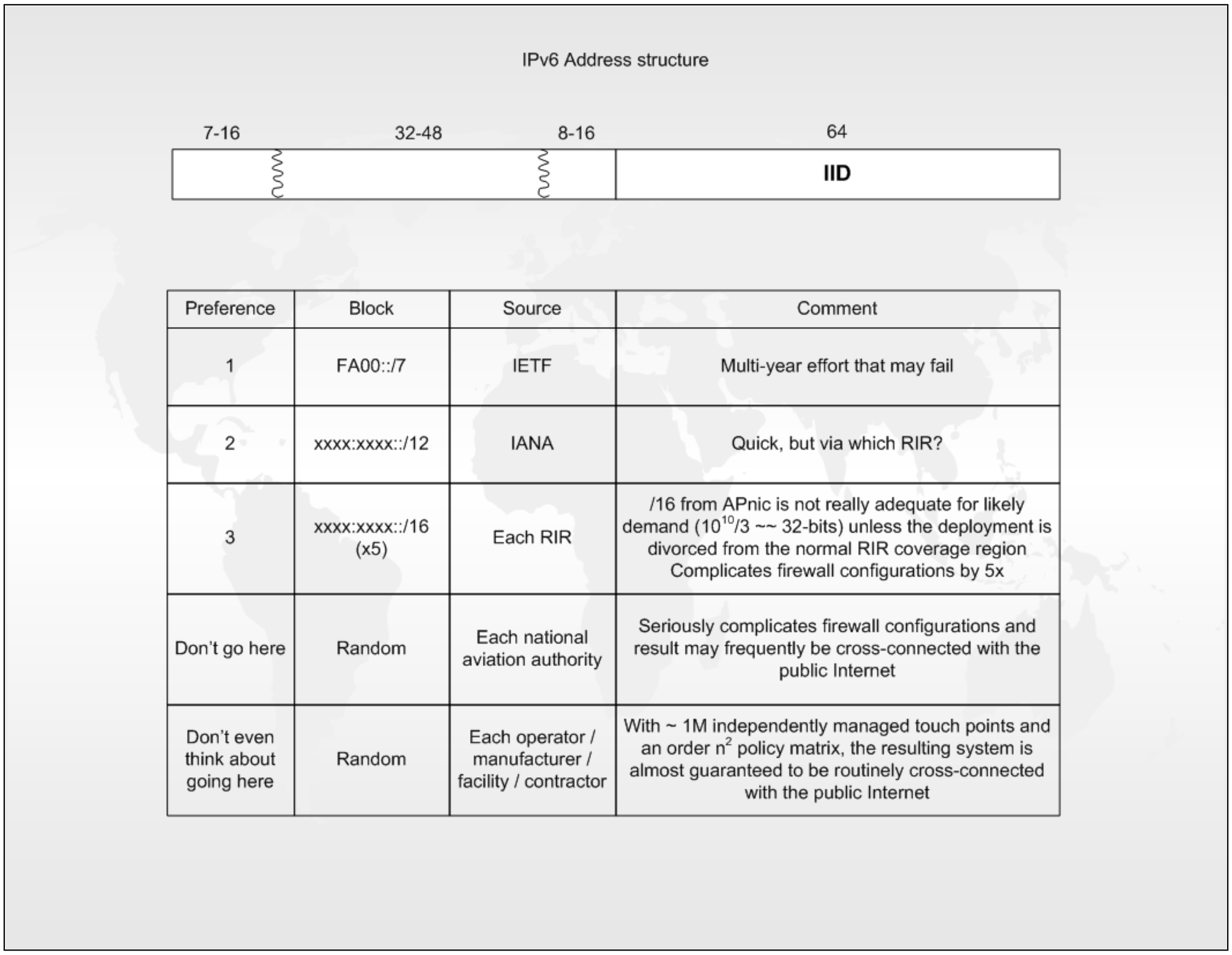
The independent Information Realms within the AANS operate in a members-only or closed context similar to a private enterprise network using technologies that are in widespread use across the public Internet and global enterprise networks. Network addressing will use IPv6, as it has sufficient scale to address the global nature of the network and current alternatives are being deprecated in operational use or removed from products. While the AANS Information Realms collectively constitute a private enterprise environment, it is expected there will be over one million touch-points between those operational realms or domains and the public Internet through various operators, manufacturers, facilities, and contractors. Acquiring an address range that is globally unique and well known allows public Internet Service Providers to provide an additional layer of isolation by rejecting direct routes to that block as they do for other documented private use blocks. Connections that use the public Internet for transport within or between realms or domains will have path-protected Service Guards. The Link Security Routers providing the path protection will have public Internet addresses for talking to each other over the Internet so knowledge of the private range is not required by the public routing system.

For more than a decade there have been a variety of proposals about IPv6 addressing for use in aviation.[7] Most, if not all of these proposals, look at the issue from the perspective of resource management, and simple integration with existing ICAO identifiers, not from the perspective of impact on routing. The impact of those proposed approaches where ICAO identifiers are used as routing tokens (which are constantly moving to different attachment points) present serious instability in the routing system. The endpoint identifier belongs in the part of the IPv6 address space architected for that purpose leaving the routing part to align with a stable routing system. That said, the route needs to track with aircraft as they move so routing needs to extend into the aircraft in a way that is not disruptive. The AANS will be deployed using a hybrid mix of dynamic mobility with stable addresses (usually consistent for an entire flight) to balance the conflicting requirements of routing stability and device stability as the aircraft moves throughout the network.

[5] https://www.itu.int/net/pressoffice/press_releases/2015/53.aspx
https://en.wikipedia.org/wiki/Leap_second

[6] https://www.itu.int/dms_pub/itu-r/oth/0a/0e/R0A0E0000960007PDFE.pdf slides 8-12

[7] APC-WGG I-07/WP-02
CP-WGI 20/WP01
ACP-WG-I/14 M



IPv6 Address structure

7-16
32-48
8-16
64
IID

Preference	Block	Source	Comment
1	FA00::/7	IETF	Multi-year effort that may fail
2	xxxx:xxxx::/12	IANA	Quick, but via which RIR?
3	xxxx:xxxx::/16 (x5)	Each RIR	/16 from APnic is not really adequate for likely demand (10^{10}/3 ~~ 32-bits) unless the deployment is divorced from the normal RIR coverage region Complicates firewall configurations by 5x
Don't go here	Random	Each national aviation authority	Seriously complicates firewall configurations and result may frequently be cross-connected with the public Internet
Don't even think about going here	Random	Each operator / manufacturer / facility / contractor	With ~ 1M independently managed touch points and an order n^2 policy matrix, the resulting system is almost guaranteed to be routinely cross-connected with the public Internet

Figure 5 IPv6 address block options for the members-only private overlay network

The exact structure for the IPv6 routing prefix will be determined after acquisition of space by industry. Several options exist, each with their own complications and trade-offs. The general form will be an identifier or set of identifiers as assigned by the source, a globally distributed pool of routing tokens, and a subnet pool for each location. Policy about pool sizes and administration will need to be developed.

5.6 Cyber Security and Resilience

This ConOps is designed to minimize cyber security risks. To do this, it assumes a layered defense where network, system, and applications have their own individual cyber security and do not share security implementations between them. It further assumes that the new AATCC and SWIM systems are implemented as a message passing system similar in design to the existing ACARS, FANs, and CPDLC systems. Besides being easier to secure, this type of service design uses minimal communications bandwidth and has minimal processing overhead.

The use of this type of service design eliminates the potential of many types of cyber and malware attacks. The service operates as an application; thus, an attacker has increased difficulty in attacking the service application host system as it does not have a direct access point to the operating system. Messages have within them a label that defines what the message contains, its length, the data type, and a message authentication block. With that information, the receiving service can check the authentication to validate the sender then process the message within those boundaries. This reduces the chances that corrupted or spoofed messages are even processed by the service but rather simply dropped if the contents do not fit the label. Controlling the size of messages help make corrupted or spoofed packets easier to detect, and malware more difficult to insert. Encryption mitigates simple eavesdropping, though it does introduce a denial-of-service attack vector attempting to decrypt spoofed packets. Finally, there is no direct access to the core of the system hosting the application, so the only data exposed is what the service allows.

In addition, the design assumes that the service communication passes through a Service Exchange environment that includes multiple types of access controls and processes. While implementation of specific services and processes may vary at each Service Exchange based on local cost-benefit threat analysis, the full set is available at every instance to ensure rapid response to changing threats. At the most basic level, a simple white-list access control firewall precludes outsiders from impacting the more processing intensive controls. One of the additional processes in each Service Exchange is a Service Guard to do a sanity check of the message on the ground-side before it is placed on the data link and through another Service Guard on the receiving side on the aircraft. The Service Guards provide the same basic checking of the message as the application does but can do much more if needed. The Service Guards also provide a point to which protections against new cyber threats can be added virtually overnight to protect the aircraft.

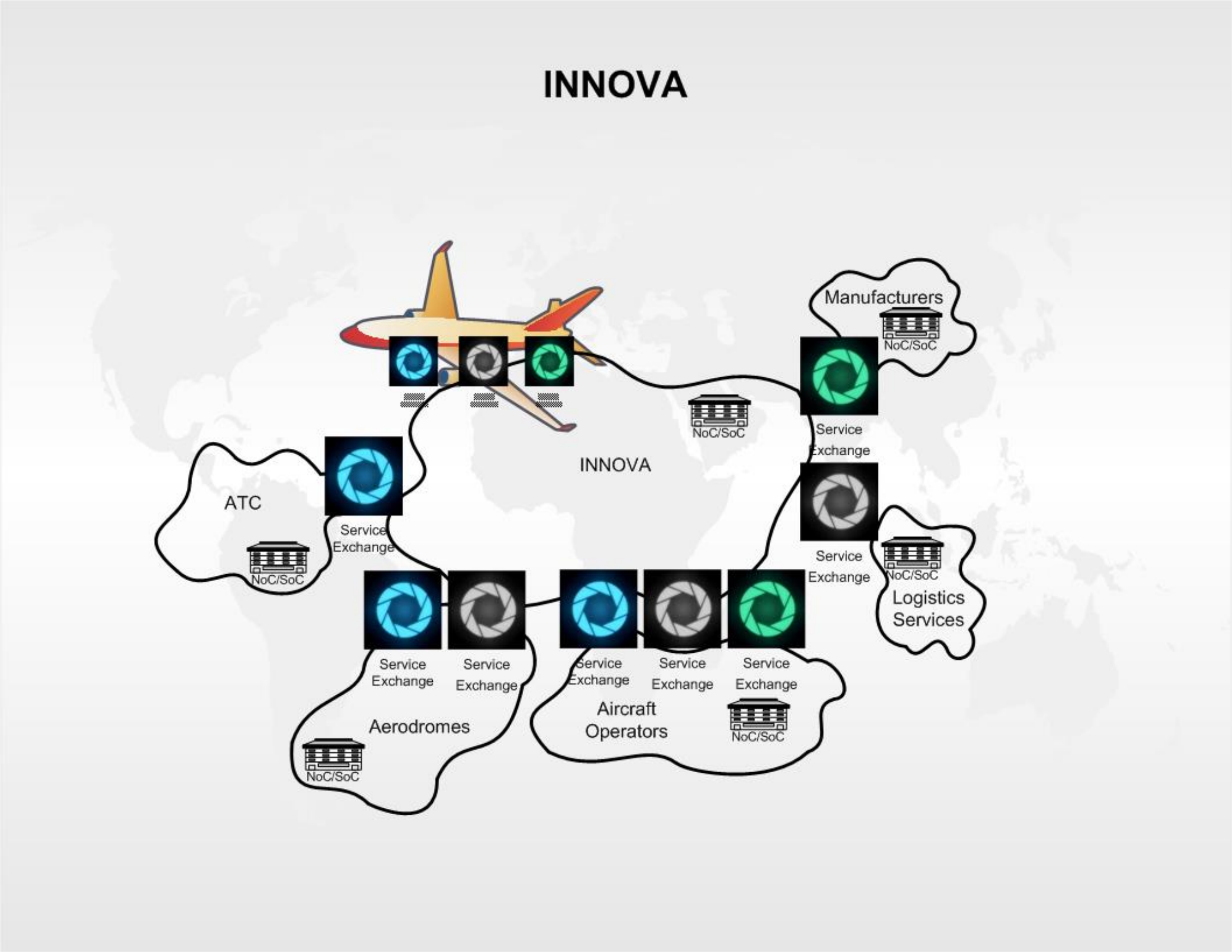


Figure 6 Cyber Resilience perspective of the members-only architecture, including isolated realms (for detail on the ATC components, please see Figure 7).

It is a basic assumption of most cyber security professionals that no system, application, or network can be guaranteed to be cyber secure. Even if direct cyber vulnerabilities cannot be found by an attacker, the system still depends on some sort of secret kept by its human operators; thus, it can still be vulnerable to cyberattack.

To counter this, cyber researchers and designers are increasingly looking at system designs that produce resiliency to the corruption of a single system allowing the overall set of systems to remain functional. ICAO Members should encourage this sort of research and work on resilient system design.

5.7 Services Based Application and Message Systems

The Service Oriented Architecture is often implemented as a Publish/Subscribe (PubSub Pattern) data distribution model where message originators 'publish' data without concern for consumers, and message consumers 'subscribe' to data without concern for who the publisher is. The linkage through common Service Names, allows subscribers to identify data of interest, while the supporting resolution services manages where the subscriber is directed to acquire it. Introduction of new, or evolution of existing, data types are managed by publishing a different service endpoint which can coexist while consumers are updated to subscribe to the new endpoint Service Name.

Message Screening ensures contents are within bounds, that the publisher is authorized to publish, and that the subscriber is authorized to subscribe.

Establishing a service delivery communication method focused on simple messages minimizes both system complexity and hardware requirements. This approach allows both the aircraft operators and the Member States to have increased control of their transition approach and implementation timelines. Local business needs and policies will drive the decision about when to deploy the new AATCC and ground-to-ground systems that integrate with the rest of the global ATC infrastructure. In many cases, ANSPs will be able to leverage their legacy systems to deploy new services, while at the same time they can easily interface with and transport legacy protocols securely over the new virtual topology. This should speed implementations of specific states to begin utilizing systems like AAtS through Service Exchanges that can place specific messages into new IPv6 services that are globally interoperable. States can also readily define specific services and Service Classes between themselves for exchange of flight planning, management, and handoffs.

As stated earlier, in a message-based service like ACARS, messages have within them a label that defines what the message contains, its length, the data type, and a message authentication block. If defined adequately, messages can readily use the label to determine key items:

- The Service Class of the message (i.e. delivery to the ACD, AIS, or PIES aircraft domain).
- The prioritization for delivery meeting Required Communications Performance (RCP) Content requiring a high security data link (i.e. flight control data).
- The ability for the destination aircraft or control center to utilize this service message type. If the destination is not equipped to handle it, the message is simply dropped.

This Service Class concept allows the message stream to an aircraft to be completely tailored for that aircraft manufacturer, model, and equipage. Thus, providing a way for industry to both continuously add capability to new aircraft without impacting in-service aircraft and to allow aircraft operators to make equipage decisions based on their own economic analysis or fleet requirements.

As a consequence of its message labeling and integrity properties, it also facilitates leveraging transitional use of existing IPv4 Internet services and of legacy network protocols where service quality requirements can be met. As an example, existing IPv4 links could provide transit between LSRs that in turn utilize IPSec protocols to encapsulate FANs or CPDLC. This secure virtual link between ground stations and the aircraft minimize the chance of messages being corrupted or spoofed.

An additional benefit is that member legacy ground systems can communicate messages to and from a Service Exchange in any protocol they choose. If their existing ground systems have the data for a service message, small custom Service Exchange specific to an ANSP can be created regardless of their legacy systems communication protocol. It can receive the message from a legacy system in native protocol, format it to match the new AANS service and place it on the data link to the aircraft and likewise in reverse to receive messages from the aircraft.

In the event that SOA message formats are determined to consume more bandwidth than the constrained air-to-ground links can support, a Digest Exchange service can be integrated into the Service Guard. This Digest Exchange would be used to transform verbose SOA constructs into a concise form, appropriate for transmission over any constrained bandwidth link types, before forwarding through the NI/LSR. The receiving Digest Exchange would in turn transform the concise variant back into the full SOA construct before handing to the Service Guard for Message Screening and/or forwarding.

Finally, small Service Exchange points can be created on the aircraft itself to securely allow data messages to be passed between aircraft domains. This could allow ACARS messages such as weight and balance or gate clearances, to be transmitted up via ACARS and sent to a Service Exchange for forwarding to the ACD. Similarly, weather data could be received via an IPv4 PIES data link, forwarded to a secure Service Exchange for delivery to a cockpit display in the ACD.

The concept of service-based message exchange should provide the industry with the ability to rapidly evolve ATC services when and where needed. However, it allows Member States and aircraft operators to set their timelines to utilize new ATC services while significantly aiding to minimize cyber threats by minimizing the cyberattack surfaces. The AANS architecture can be implemented on small systems, roughly the size of current smart phones, due to its focus on minimal air-to-ground bandwidth utilization. This approach is expected to reduce costs for all stakeholders.

6 Migration to the New Network Infrastructure and Communications Services

Implementation strategies for the AANS infrastructure need to build incrementally both for recognition that stakeholders will have different time horizons, and to recognize that a system of this complexity and scale will simply take time to complete. The definitions for the services described are crafted in such a way as to permit existing operations to continue using their current and functional services for as long as necessary, in parallel with the introduction of new infrastructure. That said, some of the benefits related to authenticity assurance and overall resilience will not be available until the legacy systems are retired.

As a message-oriented service carried by a members-only overlay network, there is extreme flexibility designed into the architecture to simplify migration at a technical level. There will be challenges where historical operational procedures and future trust relationships are not aligned, but those are outside the scope of the infrastructure itself. Part of these challenges can be aided by the use of Smart Services such that the Message Screening process in the Service Guards can validate that the receiving aircraft is equipped to support a given message and simply not forwarding the message if it is not.

In any case, the Airline Information Services Domain remains on its current evolutionary trajectory. The primary impacts from this document are to provide structure to the Network Services and scale the ICAO-ID to deal with the number of objects sharing the airspace.

The Passenger Internet and Entertainment and Passenger Electronics Domains remain on their current evolutionary trajectory. The primary impact is to provide structure to the Network Services to enforce isolation from other Information Realms sharing the air-to-ground links. From a policy perspective these domains should be considered equivalent to the open public Internet because it will not be possible to determine when or if a passenger device is acting as a routing conduit for a device outside the aircraft.

The system is architected around the air-to-ground link being the most constrained resource in the system, both for capacity and flexibility or options. It is expected that the deployments will occur first in the ground-to-ground environment, likely focusing on inter-ANSP interconnections as the starting point. This will deliver the most initial value while it starts the building process. Getting to the point where the ground-side infrastructure necessary to accept air-to-ground virtual paths will take some time. Once that is in place, introducing the AANS Service Exchanges on the air-side is expected to be relatively simple.

7 Governance and Operational Considerations

The industry should investigate the need for additional legal frameworks that may be necessary to enable full interoperability. Technology selection should be driven by appropriateness for resilience and flight safety requirements, not by existing legal restrictions. Cyber Incident response efforts need to have pre-established procedures and policies to permit timely action.

The industry should establish policies and procedures that facilitate a framework for global trust between participants in the AATM/AATCC network infrastructure. The inherent nature of the Service Exchange is a 'trust but verify' model, which at its core requires a framework for trust before anything else happens.

Early establishment of these concepts as the overall direction will enable airframe manufacturers to start the process of integrating the architecture components even before the ground infrastructure is ready. This is particularly urgent for the remotely-piloted recreation airframe manufacturers, as they are desperately searching for a way to improve airspace situational awareness related to their products. Being relatively nimble, these manufacturers could help provide early validation of the overall system, including air-to-ground, during its initial phases of deployment.

The aviation industry should insist that all air-to-ground network providers conform to the same standards used at the IP network layer. This ensures that during flight the aircraft can use any digital data links it has available to receive or send AATCC messages and that the aircraft can be contacted by ATC at any time when at least one link is operational.

To improve infrastructure flexibility and longevity, the industry should avoid using proprietary protocols for routing or other network services. This is also true for protocol standards that are planned for deprecation or have limited commercial usage. Focusing on technologies and protocols in widespread use reduces deployment costs, at the same time it increases the availability of staff trained in its operation and use.

ICAO policy about a globally consistent timescale needs to be established system-wide. This policy is necessary to deal with certificate validation, and audit procedures, as well as the ability for protocols to detect replay events. PKI relationships and procedures need to be established and iterated with operational practice for Flight and Flow. The network components can move the bits to arbitrary locations as necessary, but policy about Flight and Flow coupled with the constraints imposed by the PKI system needs to define which locations are allowed to interact.

Finally, the operational policies and procedures to permit implementation, oversight, auditing, and routine monitoring of the infrastructure components need to be established. This includes any cyber incident coordination that may be necessary between participants in the ATM/AATCC network. Ensuring the mechanisms are in place and understood before any response event is necessary to enable timely action.

8 Benefits and Summary

This ConOps discusses the network architecture, addressing, naming, and supporting components of the ecosystem needed to enable the vision and services described in FF-ICE. By defining applications, structures, and protocols necessary for AATCC within the AANS architecture and then standardizing on the technologies described here, ICAO will enable Member States, regions, and other global stakeholders to begin deployment of the AANS infrastructure at their own pace.

The approach described in this ConOps will improve resilience for communications that have historically had limitations. The ability to send and receive data with resilience and integrity, to and from an aircraft will improve efficiency for the aircraft operator as well as airspace management.

Beyond improving existing use cases, additional missions and new entrants will be easier to integrate as the framework enables sharing the limited air-to-ground resources by parallel structures comparable to FF-ICE for other Information Realms. This makes the long-term impact difficult to predict with any precision, but efficient use of the airspace has historically been a benefit to society as a whole.

With a focus on incremental deployment, the initial impact of this approach is the cost of the ground infrastructure necessary to support the number of aircraft in simultaneous use along any supported routes. At the same time, these concepts greatly reduce the financial and operational risks associated with AATCC deployment and aircraft equipage over the long term through standardized interfaces and concise digital messaging. By establishing a framework for continuous evolution, this approach cleanly separates existing in-service legacy aircraft and communications leaving them untouched from AATCC implementation unless or until the ANSP and aircraft operator choose to retrofit. This choice is entirely based on when or if it makes economic and operational sense to do so. The concepts can be further extended to allow existing aircraft with Internet IPv4 links to provide “secured” ACARS and ATN services to them with only an IPv4 interface to the CMU required. However, AATCC services will still require an end-to-end IPv6 AANS due to IPv4 public routable address space exhaustion.

To maximize their gains from the deployment of the ecosystem described here, the ICAO Member States, regions, and other stakeholders should begin developing infrastructure test labs and cyber ranges for the AANS in parallel with finalization of the standardization work. Feeding this practical experience back into the standards discussions will improve the resulting outcome and lower overall costs and effort.

That said, allowing each stakeholder to go out and build their own environment without a guiding global architecture virtually assures that there will be no way to plug the various networks together to create a resilient infrastructure. Basic network operations such as message routing, or cyber risk control would prove to be incredibly complex or impossible to manage, driving up operating costs for the entire industry. Evolving in parallel towards a common vision is very different than attempting to fit pieces from completely unrelated puzzles together.

Failure to deploy, or even delay in deployment, will result in reduced safety-of-flight as the number of AUs, primarily interested in personal recreational aircraft, vastly exceeds the number of trained pilots that routinely interact with ANSPs today. Untold millions of recreational airframes will be acquired globally over the next few years and the loss of situational awareness or management of the airspace will be difficult to regain until they are retired. Airspace usage rules are helpful as long as operators are aware and choose to follow them. Fully integrating these AUs will require adoption of technologies and approaches comparable to those described here.

By moving expeditiously and adopting these recommendations, ICAO will be able to maintain their long history of continuous improvements to flight safety.

Appendix

A) Terminology

Advanced Air Traffic Control Communications (AATCC)

Aircraft Communications Addressing and Reporting System (ACARS) – Is a digital data link system for transmission for messages between aircraft and ground stations via radio or satellite communication systems.

Aircraft Control Domain (ACD) – Isolates systems that perform functions necessary to the aircraft flight safety. This includes Air Traffic Control communications.

Aircraft Information System (AIS) – Isolates systems that perform aircraft operational management for example ACARS communications.

Controller Pilot Data Link Communications (CPDLC) – Allows pilots to read and reply to messages received via ground control.

Coordinated Universal Time (UTC) - Time scale used throughout the aviation community and civil society to provide an imprecise measure of the earth’s rotational relationship with the sun.

Digest Exchange - Handles transformation between verbose SOA constructs and a concise form used for transport over the constrained air-to-ground links.

Digital Identity - Unique, persistent, and invariant electronic tag used as an anchor when resolving between various aliases (also-known-as) strings

DNS Security Extensions (DNSSEC) - Extension standards for DNS to mitigate various threats and vulnerabilities discovered in operational practice of the original protocol.

Domain Name System (DNS) - An IETF protocol and, as deployed as a collection of independently managed data sets that through the protocol present the appearance of a coherent database.

Dynamic Host Configuration Protocol (DHCP) - An IETF protocol for administration of network locators, commonly called addresses.

Dynamic Multipoint Virtual Private Network (DMVPN) - Protocol suite and operational practice that establishes a virtual IP network over links or other networks, which may be using IP or non-IP protocols. The primary characteristic of the Multipoint aspect is that traffic flows directly between spokes rather than having to transit a hub location. After motion events the IPsec path between the spokes needs to be reestablished.

Electronic Flight Bag (EFB) - A set of processes or applications that helps flight crews perform flight management tasks with less paper than the traditional 23kg attaché full of charts. Typically packaged and described as a stand-alone appliance due to certification policies, but functionally independent of packaging.

Flight Flow-Information for a Collaborative Environment (FF-ICE) – Manual to describe the information environment.

Future Air Navigation System (FANS) – Provides communication between the pilots and the ground air traffic controllers.

Global Navigation Satellite System (GNSS) - Constellation of satellites providing signals used for timing and positioning. Currently deployed systems include GPS, GLONASS, Galileo, and BeiDou.

Information Realm - The set of participants sharing common policies about data handling.

Internet Engineering Task Force (IETF) - An open international community that develops and documents the standards used by the global public Internet, as well as by other organizations for private networks.

Internet Protocol version 6 (IPv6) - Protocol defined by the IETF for interoperation of devices within and between networks. The version 6 variant features 128-bit addresses (~ $80x10^{27}$ IPv4 Internets worth). The well-known version 4 variant uses 32-bit addresses, which has limitations resulting in its ability to uniquely identify less than $4x10^{9}$ devices.

Internet Service Provider (ISP) - Operator of network infrastructure, usually for hire as a public or private service offering. Initially these organizations were distinguished from PSTN providers that offered data link services which were unaware of the IETF protocols. Over time most of these organizations were absorbed and became indistinguishable from the PSTN provider other than the technical characteristics of service interface.

Internet Protocol Security (IPsec) - Protocol suite used to authenticate and optionally encrypt sessions between parties speaking the same version of the Internet Protocol.

Legacy Exchange - Handles transformation between legacy bus or IPv4 network systems and constructs.

Link Access Manager (LAM) - System or process responsible for assigning LSR pairings. In a DMVPN deployment model, LAM is the Hub while the LSR is the spoke. Used for topology management only as normal traffic is handled between LSRs (spoke-to-spoke).

Link Management Domain - Label for the Information Domain that is used to interconnect other Information Domains. The Link Management Domain contains Link Security Routers, data link provider infrastructure, private or leased circuits, and the public Internet.

Link Management Router (LMR) - Enforces the Service Classes a given data link is authorized to carry and manages prioritization consistent with policy. The LMR transports opaque packets between LSRs or between an LSR and other data link provider networks.

Link Security Router (LSR) - Establishes the virtual infrastructure as an overlay network using IPsec or its successors. The LSR interacts with LAM to determine LSR pairings then carries normal traffic between LSRs. In a DMVPN deployment model, LSR is the spoke while LAM is the hub.

Local Area Network (LAN) - Network infrastructure, usually operating in a local area, that provides transport for Internet Protocol packets. The primary distinction is that LAN protocols are generally designed with expectations of very short response times and a limited number of possible destinations, where Internet protocols allow for responses that may take seconds with minimal limitation on possible destinations.

Messages described in FF-ICE (4DT) - Messages are passed between Service Guards in this format.

Network Interchange - Enforces access controls at the network level (layer 3 firewall). The NI handles all processes and services that are necessary between the LSR's overlay abstraction, and the Service Guard's message passing abstraction. These include at least DNS, DHCP, NTP, Certificate-Server caching, and network routing within the virtual infrastructure.

Network Time Protocol (NTP) - An IETF protocol for distribution and synchronization of time on a global basis

Next Hop Routing Protocol (NHRP) – An IETF protocol for redirecting DMVPN clients to establish the spoke-to-spoke topology.

Passenger Internet and Entertainment System (PIES) – Supports cabin passenger entertainment, internet and voice communications.

Personal Autonomous Aircraft (PAA) – Low cost, consumer class UAS with self-contained control system.

Public Switched Telephone Network (PSTN) - Infrastructure provided by telephony operators on a local, regional, national, or global scale.

Quality of Service (QoS) - Protocol options allowing end systems to inform network infrastructure of relative priority or expectations about data handling.

Remotely Piloted Aircraft Systems (RPAS) - ICAO doc 10019 Manual on remotely piloted aircraft systems.

Request for Comment (RFC) - The IETF document series providing a stable historical reference. Some RFC's are considered standards, while others are informational or historical.

Service Class - Identifies technical performance requirements, policy groupings, and minimum-security expectations.

Service Guards - Enforce content policies at the messaging or application level.

Service Exchange - Identifier for the collection of processes and infrastructure that provide services between the Message Publishers in an Information Realm and the data link providers connecting locations or between realms. This includes at least the Service Guard, the Network Interchange, and the Link Security Router.

Unmanned Aerial Vehicle (UAV) - Aircraft without a pilot onboard. Vehicles generally controlled from the ground though autonomous operations would also fit this broad category.

Unmanned Aircraft Systems (UAS) - An aircraft without a human pilot onboard, plus the control system

B) Use Cases

To better understand the interactions of this ConOps, some example use cases will be illustrated for a proposed implementation framework. These examples will highlight different aspects of the infrastructure while discussing three different use case scenarios. All aspects of the infrastructure are used the same way in all scenarios. The scenario discussions are split to draw particular attention to design choices that enable new entrants, mission types, or use cases beyond the current perspective of Flight and Flow operations.

To focus on various components of the system, the description will follow the phases of flight sequence. To simplify the discussion, bundles of data exchanges that are described in FF-ICE will be collapsed showing where the bundles are handled at each step, rather than every message in an extended transaction. Even the phases of flight will be collapsed into pre-flight, weather acquisition and ANSP handoff. The intermediate steps have been removed to simplify the explanation.

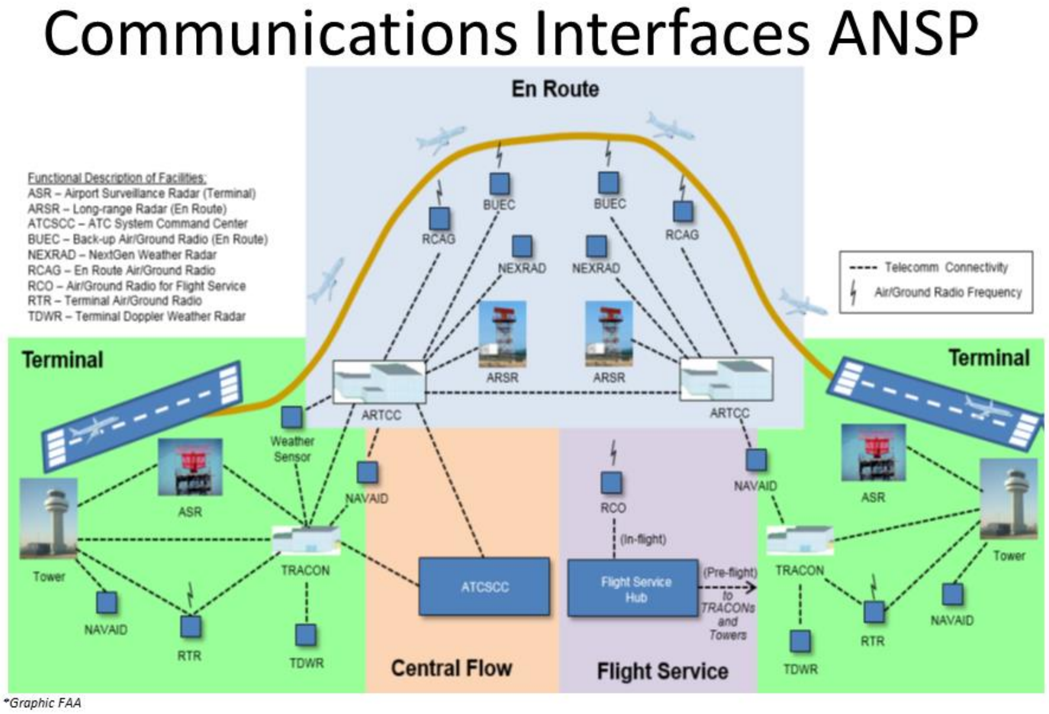

Communications Interfaces ANSP
En Route
Functional Description of Facilities:
ASR – Airport Surveillance Radar (Terminal)
ARSR – Long-range Radar (En Route)
ATCSCC – ATC System Command Center
BUEC – Back-up Air/Ground Radio (En Route)
NEXRAD – NextGen Weather Radar
RCAG – En Route Air/Ground Radio
RCO – Air/Ground Radio for Flight Service
RTR – Terminal Air/Ground Radio
TDWR – Terminal Doppler Weather Radar
Telecomm Connectivity
Air/Ground Radio Frequency
BUEC
BUEC
RCAG
RCAG
NEXRAD
NEXRAD
ARSR
ARSR
ARTCC
ARTCC
Terminal
Terminal
Weather Sensor
NAVAID
NAVAID
ASR
ASR
Tower
Tower
TRACON
TRACON
NAVAID
NAVAID
RTR
RTR
TDWR
TDWR
ATCSCC
RCO
(In-flight)
Flight Service Hub
(Pre-flight) to TRACONs and Towers
Central Flow
Flight Service
*Graphic FAA

Figure 7 Timeline of information provision relative to events pertaining to a single flight, referenced sections detail FF-ICE activities in more detail

Scenario 1 Passenger Flight International Handoff

Pre-flight

The process of negotiating 4D Trajectory (4DT)[8] between the AU and the relevant ANSPs requires collecting necessary data, offering a 4DT proposal to the initial ANSP, which handles subsequent ANSP interactions as necessary, then receiving the constraints associated with that proposal. This process iterates as necessary until a 4DT is accepted by the AU and relevant ANSPs. The messages necessary to conduct this negotiation are passed through the infrastructure as

[8] FF-ICE C-5 & C-6

necessary to align with existing trust relationships as expressed through services like a public key infrastructure (PKI).

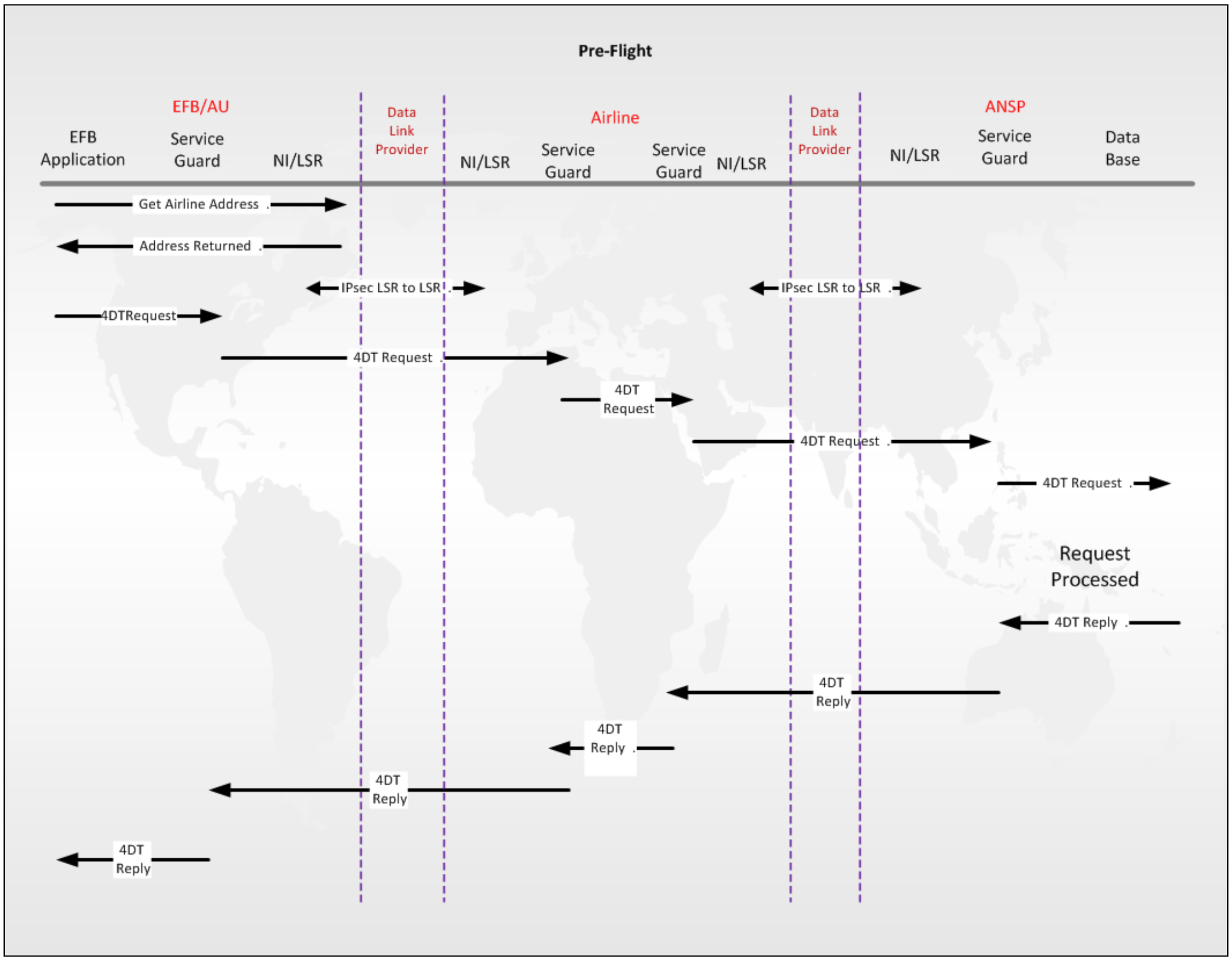


Figure 8 Preflight data exchange between Service Guards via protected paths established between LSR functions

The 4DT messages described in FF-ICE are passed between the Service Guards over the virtual topology created by the LSRs. The chain of participating Service Guards is defined by the trust relationships and authentication mechanisms available. The sequence depicted above assumes a trust model where the ANSP is not able to authenticate the EFB appliance directly but trusts that the Airline has done so.

A sequence similar to this could also be used to pass messages that would be the basis for a session level trust directly between the ANSP and the EFB appliance.

Weather

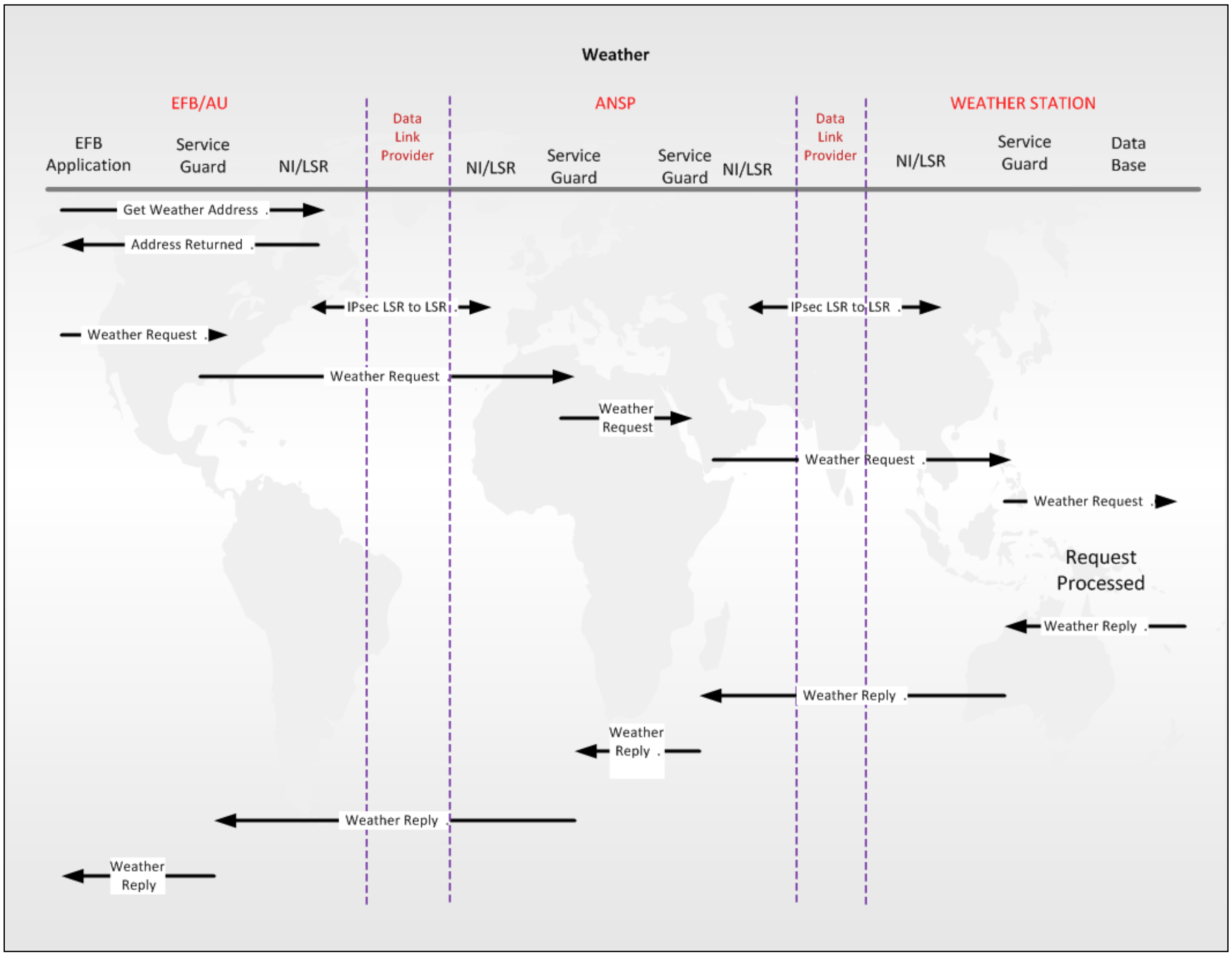


Figure 9 Weather acquisition sequence

Weather services are acquired via the ANSP and need a pass-through message passing model between Service Guards. This is comparable to the pre-flight sequence in Figure 8 and, depending on trust relationships, the weather sequence may also include the Airline as depicted there. For simplicity and clarity in the diagram, any additional parties are not shown, though the model can accommodate any chain of messaging passing Service Guards that complies with policy.

As with the pre-flight sequence, the LSRs establish a protected path, and then messages are passed between Service Guards where sanity checks are performed before forwarding to the appropriate next party.

Aircraft Pre-flight Weight & Balance

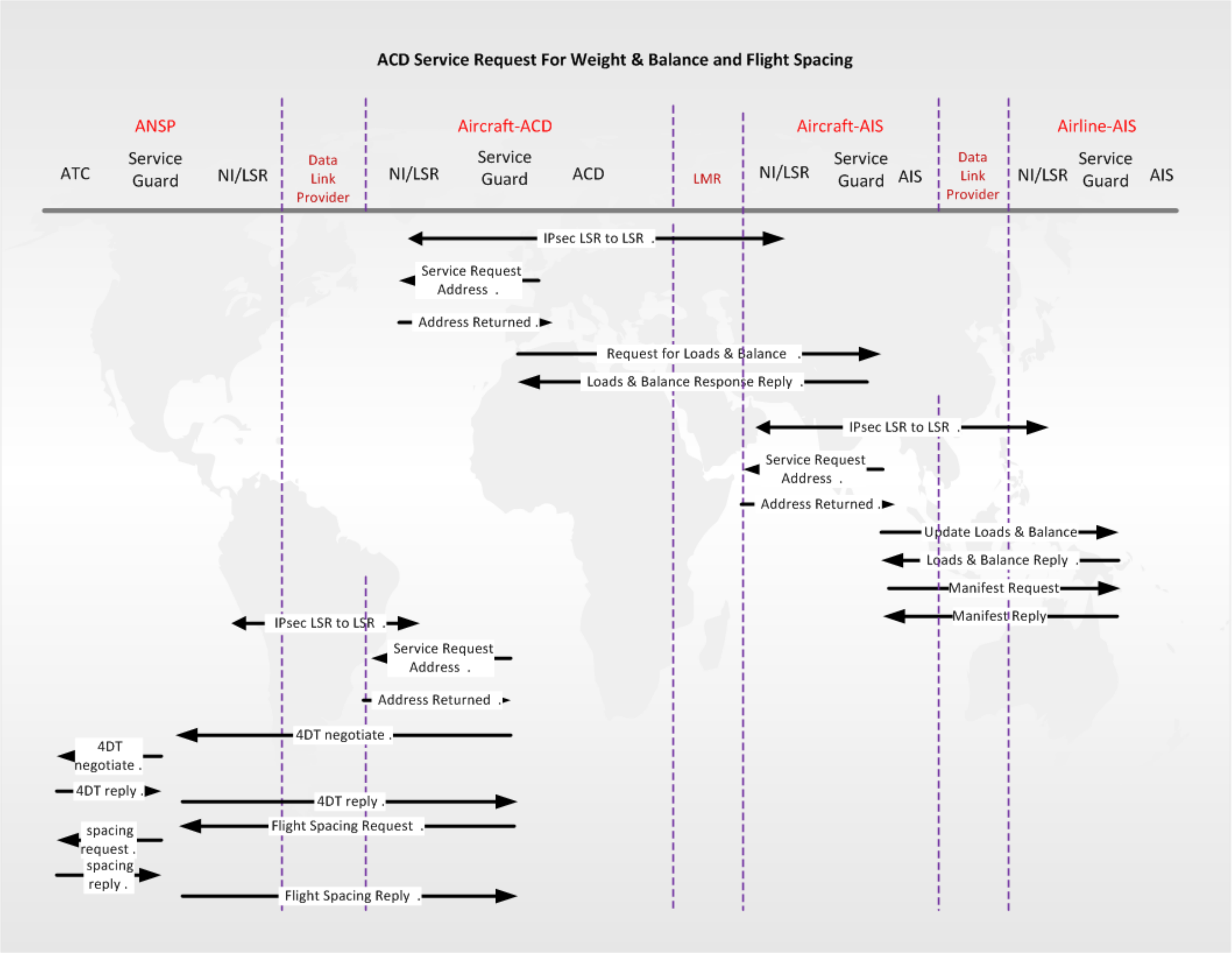


Figure 10 Message Service interactions to acquire weight & balance, and manifest before negotiating spacing

This example flow above demonstrates how an ACD service could request information from a limited service interface out of the AIS domain. Such a service could be designed to send only aircraft weight and balance information from the AIS domain on the aircraft, then validate that it is within bounds before accepting it for direct digital input to the air flight controls. The service could also be designed where the query from the flight deck triggered an automatic update to the airline ground infrastructure, which in turn triggered an automatic transmission of any passenger manifest. Once all the appropriate information has been exchanged and processed, an update to the 4DT negotiation for current spacing can take place.

Aircraft Handoff Sequence

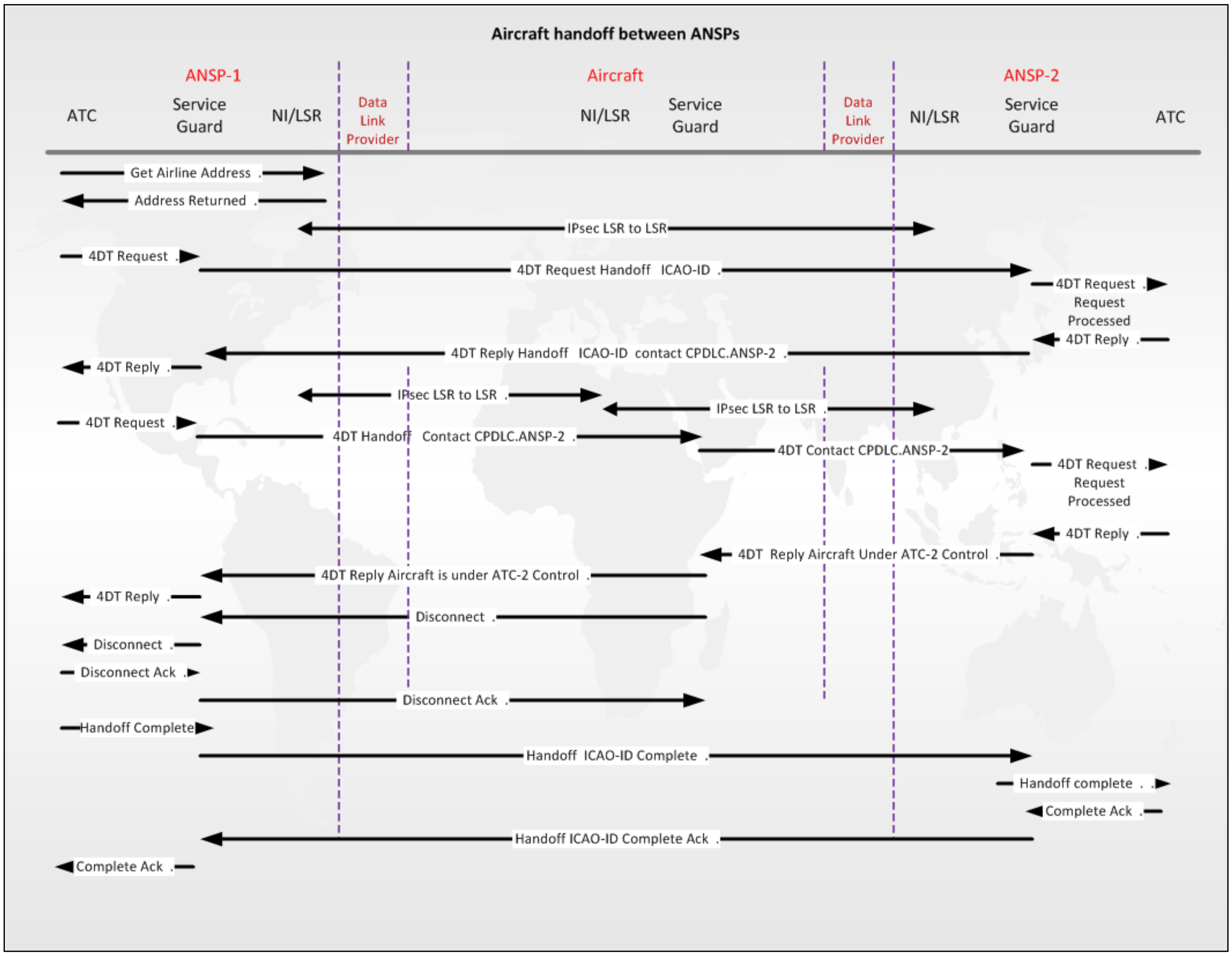


Figure 11 Aircraft handoff sequence between ANSPs

The sequence depicting aircraft handoff between ANSPs includes disjoint communications, where the preceding examples of pre-flight and weather were pass-through. This appears to be a complex sequence but is intended to follow a hypothetical work flow that might traditionally be handled over various radios, telephone, or data systems. The primary difference in the AANS approach is that technology is consistent throughout, and that structured Service Names are used rather than radio frequencies or phone numbers as the target for the next communication. In all cases, the path across the data link providers is protected with IPsec by the Link Security Routers and the messages are authenticated and sanity checked between the Service Guards.

Scenario 2 Air-Ambulance Flight International Handoff

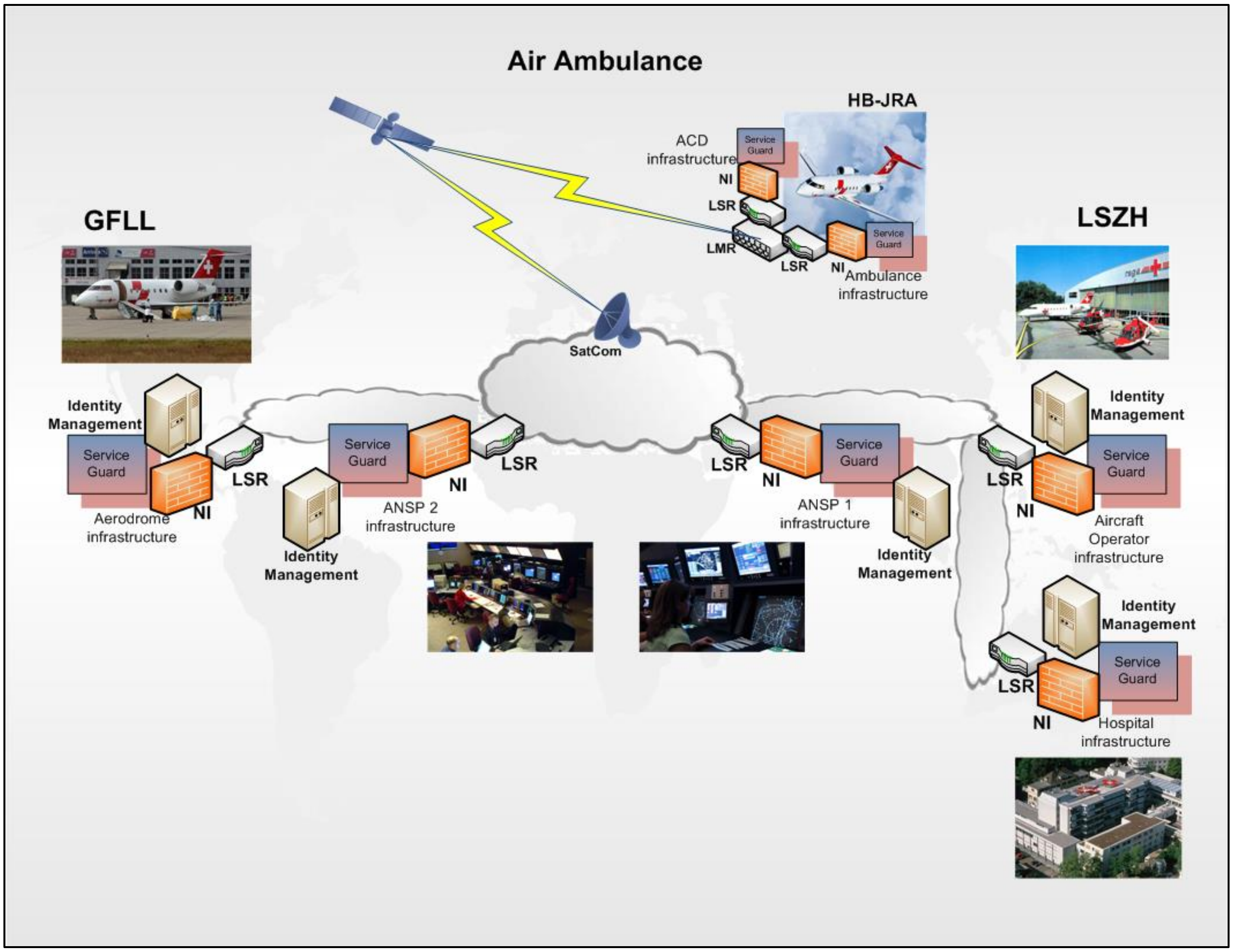


Figure 12 Air ambulance sharing air-to-ground link between FF-ICE realm, and Medical Information Realm

Through the AANS architecture, an air ambulance Medical Information Realm may share air-to-ground resources with AATCC Flight and Flow, as long as the Service Exchange for that realm conforms to the interface requirements necessary to ensure safety of flight. Using the same protection technologies and strategies, but with isolated access controls, policies, and implementations, the independent Information Realms are totally unaware of each other. While the boxes look identical in the figure above, they are not all in the same logical network. For the Medical Information Realm, the Ambulance LSR would establish a virtual path with the Hospital LSR, while the FF-ICE Information Realm and the ACD LSR would establish virtual paths as assigned between origin and destination aerodromes or ANSP LSRs. The content and message formats for any Information Realm outside FF-ICE is beyond the scope of this document, except the addressing and QoS marking policy as that interacts with FF-ICE. The ability of the LMR to recognize and enforce QoS parameters on the IPv6 packets allows it to interleave life-safety messages in between flight-safety and routine information. Policy will need to be established about QoS groupings that ensure the highest priority goes to flight-safety, while leaving room for aircraft operators to establish markings appropriate for each mission type.

Scenario 3 Autonomous Cargo Flight International Handoff

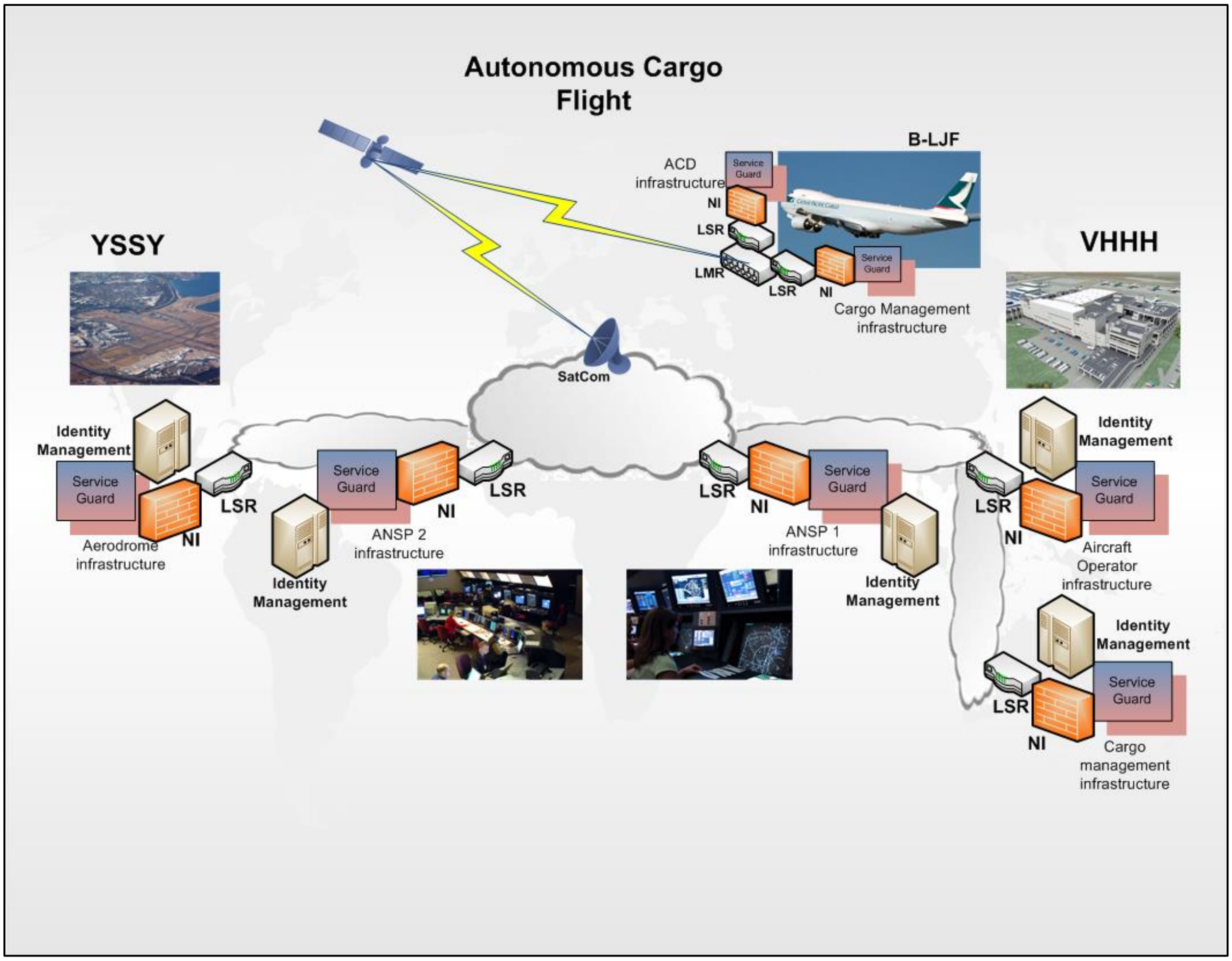


Figure 13 Autonomous cargo flight sharing air-to-ground link between FF-ICE realm, and Cargo Management realm

The autonomous cargo flight uses the data handling procedures in Flight and Flow as demonstrated in the previous examples. Though at the same time, the aircraft operator likely needs isolated parallel facilities to participate in third-party flight management more directly than would be the case with direct controller pilot data exchanges. The primary aspect of this scenario is that it relies on a robust identity and communications infrastructure, as there is no human judgment onboard to detect and mitigate errant instructions. When policies are in place to enable this type of mission, the monitoring and management of the cargo takes place in complete isolation from the FF-ICE realm, even if the aircraft operator could participate in both realms.