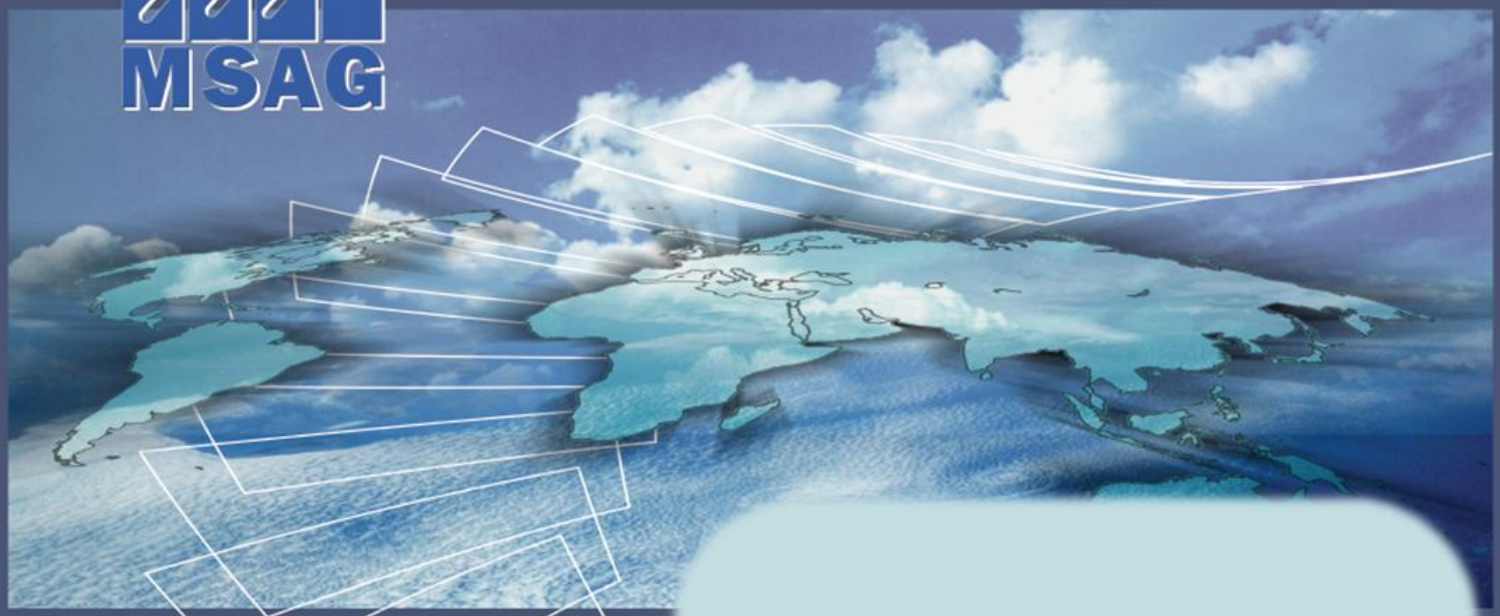
MSAG Vision Series®

AIRCRAFT • AEROSPACE



Global Harmonization of Commercial Aircraft Communications, Network, and Cyber Security Infrastructures to Support NextGEN and Single European Sky ATM Research (SESAR) Advanced Air Traffic Management (ATM)

September 2014

Author:

Terry Davis,
Chief Scientist
tdavis@msag.net

MSAG msag.net 703.538-0807

1. Background

Following the Chicago Convention in 1944, the aviation industry began to standardize the physical infrastructures needed for a global commercial aviation industry to emerge. Items like runway design, terminal gates, aircraft fuel and power connections, catering equipment, baggage handling, service vehicles, etc., were standardized so that airlines could use a common ground infrastructure to support their operations between airports anywhere in the world. This movement required aircraft design standardizations to conform to the new design standards; communications equipage followed suit. In the late 70's, the Aircraft Communications Addressing and Reporting System (ACARS) protocol was standardized by Aeronautical Radio, Incorporated (ARINC). Moreover, in the 80's existing global Open Systems Interconnection (OSI)-based communication networks for the Aeronautical Telecommunications Network (ATN) that supported air-to-ground global messaging for the Future Air Navigation System (FANS), controller–pilot data link communications **(**CPDLC), and ACARS, was developed and standardized.

Commercial aviation now requires a similar standardization effort to support envisioned NextGEN/SESAR advanced air traffic management functionality. It is unreasonable to update the existing OSI-based ATN to maintain legacy compatibility with existing fleets, provide increased bandwidth, and offer enhanced ATN functionality with the cyber security now required. Today, commercial aviation simply does not have the ability to support the creation of another global, custom network for NextGEN/SESAR when existing commercial alternatives are available; indeed, the development of such a network would likely delay advanced air traffic management for a decade. New functionality, updated communications, and security for advanced traffic management services will be provided using (commercial-off-the-shelf) COTS products that support Internet technologies over link types not previously approved for the safety of flight communications. Likely, these link types will include satellite communication (SATCOM) links (KU, Ka, L, X, etc.), a new Global System for Mobile Communications (GSM) (3G/4G/5G, etc.), and other new links like Wi-Fi, Worldwide Interoperability for Microwave Access (WiMAX), etc.

Using Internet technologies to create a consistent global infrastructure is not trivial, as there are literally hundreds of options on how to implement such an infrastructure. No aircraft design can be flexible enough to manage every communication service provider, navigation service provider, and airport implementing different suites of Internet services, without extreme development and operational overhead costs in their aircraft configuration management. Imagine the challenge of trying to support this vast amount of entities around the globe, using separate public key infrastructures (PKIs), and different encryption, key expiration times, key lengths, etc., on communications links. Alternatively, envision trying to establish links to an aircraft if each network service provider (NSP) uses different network addresses for the same aircraft and different message protocols.

Further, use of a fragmented infrastructure to support a new global ATN communications network, message routing and cyber security management becomes far more difficult for an

airline's operation staff to support. Finally, a globally fragmented, inconsistent advanced air traffic management network would unlikely ever achieve the availability and reliability needed to carry out flight critical communications.

2. Impacts to Commercial Aviation

Currently, a defined suite of standards does not exist for commercial aircraft to utilize in connecting to Internet capable media like SATCOM, 3G/4G, wireless, Broadband over Power, wired Ethernet, or any other Internet capable communication link. Every communication service provider, NSP, airport, etc., have their own Internet infrastructure in development for NextGEN, SESAR, and similar initiatives around the globe.

This inconsistency results in presenting varying sets of Internet technology standards to commercial aircraft on the different links from communication service providers, navigation service providers, and airports. Thus, an aircraft may be able to utilize a 4G link, but not a SATCOM link, even if available. Alternatively, an aircraft may be able to establish wireless terminal communications at one airport, but not the flight destination airport. The gravity of the lack of a common set of existing standards for commercial aircraft to utilize cannot be understated. This lack:

- Limits the ability of airlines to fully integrate their most valuable assets, their aircraft, into their corporate digital infrastructure forcing airlines to maintain operationally inefficient paper, manual, and voice interfaces for their aircraft.
- Limits the ability of airlines, airframers, and integrators to utilize multiple service providers for increased service, coverage, reliability, and/or cost savings.
- Prevents the implementation of new aircraft health management systems and in-flight technical and engineering assistance.
- Results in both airlines and airports installing duplicate link types, infrastructure, and network services to support aircraft utilizing different link connection standards.
- Makes coordinating airspace usage with UAVs more difficult.
- Increases the development cost of commercial aircraft, as standards enable airlines, airframers and their suppliers to provide lower cost solutions.
- Creates further delays in implementing the next generation of air traffic management services to improve airport capacities, as well as aircraft safety and flight operations.

Commercial aviation needs a single set of standards for all new airplane models, updates, and retrofits that utilize networks operating with Internet-based technology. Without these standards, the impact to airlines, air-framers, integration costs, implementation time, maintenance, system reliability and availability, are unwarranted. Additionally, the national airspace (NAS) rollout of new advanced air traffic management functionalities will be delayed causing system setbacks and additional costs for the entire aviation community.

3. Harmonization

Harmonization work should not involve the creation of new standards, but rather the selection of a suite of existing Internet Engineering Task Force (IETF) and Institute of Electrical and

Electronics Engineers (IEEE) technologies and standards, Internet services (i.e., Domain Naming System (DNS), Dynamic Host Configuration Protocol (DHCP), and Network Time Protocol (NTP), etc.) for commercial aircraft to utilize in connecting to aviation communication networks based on Internet and IEEE standards.

Initial harmonization efforts would focus on defining the high-level requirements for communications, network, and cyber security standards necessary to support global e-Enabled fleets with advanced communications and true NextGEN/SESAR air traffic management. The effort should also include the establishment of common communication protocol requirements, and the individual message types and to carry advanced air traffic management services between the various NSPs and commercial aircraft around the globe.

Following identification of the high-level requirements of harmonization, implementation priorities and timelines need establishing so that all aviation entities can participate in the rollout of these services and functionalities. Specific harmonization actions include:

- Identifying the Internet services required for aircraft network connectivity.
- Identifying the existing standards needed in the connectivity suite to provide said services.
- Analyzing the different standards available to provide said services, and providing suite recommendations for the standards supporting required services.
- Interfacing with other standards' organizations to reach consensus on the final requirements for incorporation in the connectivity suite.
- Ensuring coordination and compatibility with existing ARINC and other standards.
- Coordinating with the International Civil Aviation Organization (ICAO) to present the recommended suite for ICAO approval; this is especially important for encryption, authentication source location, encryption key length, and other cyber security services regulated by most nation/states and must be approved by ICAO.
- Determining what the digital aircraft identity is for advanced air traffic management, and whether it, and/or the transponder code, can be mapped into the Internet address assigned to the aircraft. This is similar to current usage of the transponder code and the OSI aircraft network address.

4. Basic Internet Functions and Service

The following key services and functions will likely require harmonization for globally, interoperable commercial aircraft connectivity.

4.1 Aircraft Internet Addressing Plans for Both Internet Protocol (IP) v4 and IPv6

A key part of harmonization is the development of addressing plans that account for legacy IPv4 existing addresses, and managing new IPv6 address allocation across the industry. It is critical that this plan clearly differentiates onboard aircraft internal IP address blocks, from blocks used for aircraft to ground links for ground infrastructure. Further, each aircraft will have at least three separate networks onboard to support the Passenger Information & Entertainment Services Domain (PIES), the Airline Information Services (AIS), and the Aircraft Control (AC) domains. Preliminary work performed in the past decade indicates that each of the three domains should

probably allow for somewhere between 16 and 64 sub-networks to further allow separation of functions. Each airline will need a conforming plan for its fleets as link service providers, NSPs, and airports. Without this base messaging routing is not possible, nor is maintaining domain isolation, and, network security and network operations are much more difficult.

4.2 Aircraft Link Address Allocation

Another particular concern is aircraft link address allocation for communication to a ground infrastructure; this is similar to connecting a laptop to a wireless hotspot. The problem is that there are numerous ways (fixed, DHCP, Link Local, etc.) to achieve this but the aircraft must know which one to use.

4.3 Aircraft Receipt of Network Services Location (Router, DNS Server, Radius/Diameter Authentication Servers, etc.)

For each link an aircraft uses anywhere on the globe, the aircraft must be given the addresses of the services that are critical to its use of that network. The installation of these addresses could occur in the aircraft configuration tables but will differ for each link and location used as addresses regularly change. Thus, the use of tabled information would become an operational nightmare for airlines. A dynamic method like DHCP or Service Location Protocol (SLP) could be used just as commercial hotspots are used to minimize operational issues.

4.4 Aircraft Network Identity Standard (i.e., Vehicle Identification Number (VIN) Equivalent)

In current OSI network addresses, transponder code is embedded and changeable. The industry must decide if the current transponder code is secure enough for advanced air traffic management, and whether an additional, permanent, aircraft digital ID is required. In either case, decisions on how transponder code or a digital ID can translate to the Internet-based implementation with functionality similar to OSI's, are necessary. There are several standard ways to embed ID's into the aircraft's network address.

4.5 Aircraft Authentication Standards (Type, Key Length, Hash, etc.)

Nations/states around the world have laws and regulations governing the use of PKI for authentication and encryption. Most authentication methods have some degree of conflict among nations/states. For example, many nations/states require that the certificate authority used be located on national soil. Others limit certain types of authentication and encryption technology, the permitted length of the keys, and the types of hashing functions used. Further, some require disclosure of the keys to the nation/state for either authentication or encryption. This is a severe problem for advanced air traffic management. To configure and maintain different configurations for each NSP its aircraft encounters, escalates airline operational costs. It will undoubtedly require the ICAO to take the lead in establishing the global standards in this area.

4.6 Aircraft Use of Link Encryption and the Supporting Encryption Standards

Harmonization must also include standardization of link encryption as many nation/states have very specific laws or regulations on the usage of encryption applying to their NSP's. This is

especially important as the communication aviation implements advanced air traffic management functions.

4.7 Aircraft Internet Naming (i.e., Tailnumber, Airline, PIES)

In order to utilize IPs, each aircraft and infrastructure component must have an Internet standard name (i.e., www.ICAO.int). The airline, the NSP, the communications service provider, airport, etc., must all have a common definition for aircraft's name to which they are contacting/connecting. Utilizing the IP address itself is not feasible from both a human function and operational fact for two reasons. First, the aircraft may have multiple active communications links with different addresses. Secondly, IPv6 addresses are 128 bits in length with the address represented as eight groups of four hexadecimal digits, which are not human usable. Internet naming hides the complexity of an address number, its recall from the Internet, and any address changes from aircraft or network operations. These Internet names could vary depending upon to which aircraft domain the unit is connected, or resides in. Additionally, the Internet allows names to have aliases. For instance, it might be appropriate to tie flight numbers to the associated aircraft. Again, the industry has to provide a single answer for the full utilization of Internet technologies by commercial aviation.

4.8 Aircraft Domain Separation Technology

The industry will also need to decide on the base technology needed to maintain separation between aircraft network domains. One option is in the network address plan itself by assigning the different aircraft domains to different address blocks. Other separation options include using virtual LANs (VLANs), network level encryption, multiple links, or other technologies that may be identified.

4.9 DNS

DNS services provide the link between the unit's actual IP address and its Internet name. Again, there are several options other than the use of generic public Internet DNS services. Dynamic DNS for example, will be required if the aircraft's link IPs change between service providers, NSPs, and airports. DNS is also an acknowledged weak point in the global Internet; DNS Security (DNSSec) significantly improves this but is extremely difficult and costly to implement on the public Internet. Government and business around the world use SplitDNS to allow visibility on the Internet, but to hide all internal infrastructure. Dark DNS can be created by the use of a private DNS infrastructure, and tunneled or encrypted links between entities. Dark DNS also makes the use of DNSSec much easier, if desired.

Finally, the question remains on the usage of Internationalized DNS names. This would allow DNS unit names to display in the owner/operators native language, but has two critical associated issues. First, the operational costs are very high in a mixed language network and it requires specialized tools. Second, it introduces cyber security issues that are extremely hard to manage in the mixed language networks.

4.10 Network Routing

There are numerous Internet standard routing systems with Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF) being predominant. Follow-on work for both are either standardized or in the process.

The use of BGP can be problematic if the aircraft's onboard networks are withdrawn from one continent's routing table and inserted into another as the aircraft changes ground stations between them. Although it works, it causes global routing storms, as hundreds of thousands of routers around the globe update their tables with the connection at the location of the new ground station. Verbal acknowledgement of the problem among the ICAO, the Federal Aviation Administration (FAA), Eurocontrol, the Internet Corporation for Assigned Names and Numbers (ICANN), the American Registry for Internet Numbers (ARIN), and the IETF occurred in 2008. At some point, with enough aircraft in flight, these storms could impact Internet service. Utilization of some specific BGP functions, network designs, or dark/cloaked/clandestine private networks can eliminate or minimize the risk of Internet routing storms. In any case, the routing technology of the global advanced air traffic network must be standardized in order to assure reliability in reaching the aircraft.

4.11 Network Authentication

Individual units/systems/aircraft can be forced to authenticate themselves prior to being given a network address in a new network domain. This could be an industry-wide requirement, or left to individual domain owners/operators. However, it will affect security services between domains as it has the potential to impact the flow of critical advanced air traffic communications to the aircraft. This should undergo industry study before implementations begin.

4.12 Network Time Service (NTS)

NTS is provided by the utilization of NTP. Synchronizing the time between units/systems/aircraft is critical to many applications, in some cases for security functions, but certainly to troubleshoot network or system problems. NTP allows a hierarchy of time servers to be created with a primary time server, referred to as a stratum 0, receiving high-precision timekeeping devices such as atomic (cesium, rubidium) clocks, global positioning system (GPS) clocks, or other radio clocks with lower stratum servers being further from the stratum source. An aircraft's time service can utilize ground servers, but in some cases, the link delays may cause its time to be different enough from the ground's servers to create issues. In some cases, the aircraft equipage includes GPS. It is possible for the aircraft's systems to use the GPS feed for time synchronization directly. Its use should be standardized as to the appropriate stratum or accuracy required, at least by key units/systems for advanced air traffic services.

4.13 Aircraft and Ground Firewall Standard Configurations

Standards must be developed to ensure accessibility for the use of systems/applications on known networks and authorized network port numbers. Basically, network port numbers are sub network addresses used by systems and applications to distribute network communication with the unit. The key suites of systems/applications in each aircraft domain will need to use standard

known port numbers. Normally, these standard sets of port numbers are utilized in both aircraft and ground firewalls, to permit messages destined for specific networks and known ports to pass while all other traffic is blocked. This standard is key for both aircraft security and global interoperability so that authorized known network and port messages can reach the aircraft or its corresponding ground infrastructure regardless of the link or location on the globe.

4.14 Cyber Security Standards

In all likelihood, key cyber security precautions like malware detection, anti-virus, web protections, and deep packet inspection will require standards. Any of these security functions can either inadvertently block critical messages or significantly delay their delivery. These standards are critical to ensure both link compatibility, and that messages reach their destinations reliably, within the required time window to support advanced air traffic management functions.

4.15 IPv4 to IPv6 Interoperability

All current e-Enabled aircraft, both new and by retrofit, utilize IPv4 addressing. The global pool of IPv4 addresses is now exhausted; none exist for new uses as the remaining addresses are reserved for support of existing critical systems. Therefore, the industry must plan for the use of IPv6 addresses in the development of advanced air traffic management systems; ICAO has already mandated this in Document 9896. To support both the legacy use of IPv4-based aircraft systems and new IPv6-based systems, standards need developing to ensure key interoperability. There are existing standards like Host Identity Protocol (HIP) that are v4/v6 agnostic and could be used; others are in development. The possibility also exists of the issue being solved at the network design level. Again, the industry will need to decide on a single solution if airlines want their legacy IPv4 aircraft and new IPv6 aircraft to be able utilize the same services and handle the same functions.

4.16 Other Functions or Services

This list is almost certainly incomplete. It should be expected that other functions and services requiring harmonization will be identified as the industry begins prototyping and implementation testing, such as the FAA System Wide Information Management (SWIM)-Connect demonstration.

5. Benefits

There are numerous benefits extending to all parts of the industry, in working on harmonization.

5.1 Benefits for Airlines

Some of the potential key benefits to airlines include:

- Having a consistent fleet-wide set of standards to utilize with their aircraft to interconnect globally.
- Aircraft Health Services (AHS) can become a reality.
- Support of remote electronic maintenance and diagnosis.
- Full integration of their aircraft into their digital corporate infrastructures.

- Aircraft can be pre-positioned to join and take advantage of next generation air traffic management services during manufacture or system updates.
- Aircraft links to Internet technology based networks are standard, regardless of provider or location.
- Operational complexity and maintenance support costs of the aircraft's communication systems are controlled.

5.2 Benefits for Airframe Manufacturers

Airframers benefit by having one set of standard, implementation services fully realizing their e-Enabled and AHS aircraft benefits to airlines.

5.3 Benefits for Avionics Equipment Suppliers

Equipment suppliers benefit by knowing exactly what Internet services their systems must support, and how to optimize them for fleet solutions that can span multiple airframers.

5.4 Airports and Link Service Providers

Standard infrastructure cannot support any aircraft fleet without customization.

5.5 Navigation Service Providers

Advanced air traffic management systems and functionalities can be implementations that improve airport and NAS capacities.

6. Conclusion

This paper's intent is to highlight some of the major issues the industry must confront if the vision of a new, advanced air traffic management is to come to fruition. The goals of any preliminary harmonization work are to identify key components that will guide prototype testing, functionality, and prioritizing implementation efforts to solve the roadblocks to global interoperability; and, to support the visions of NextGEN, SESAR, and the other advanced air traffic management initiatives around the globe.

Without this effort, unnecessary expenditures of resources will be required to empirically (trial and error) develop a solution that could have been identified, planned, and executed in advance adapting current commercial standards and protocols. The industry will move forward with the deployment of advanced air traffic management functions and commercial communication technologies. The question is at what cost.