AEROSPACE TSN USE CASES, TRAFFIC TYPES, AND REQUIRMENTS

REV. 0.6

Date: March 4, 2021

Document in support of IEEE 802.1DP and SAE AS6675: TSN Profile for Aerospace

CONTRIBUTOR GROUP

Fischer, Wolfgang <wolfgang.fischer2@airbus.com>

Gelish, Joseph <gelish@ddc-web.com>

Hegarty, Michael <hegarty@ddc-web.com>

Jabbar, Abdul <jabbar@ge.com>

Lawton, Grant <glawton@wlgore.com>

Nelson, Brent <brent.nelson@collins.com>

Rang, John <john.rang@ge.com>

Scanlon, Gregory <gregory.scanlon@lmco.com>

Santinelli, Luca <luca.santinelli@airbus.com>

Zaehring, Jamie <Jamie.Zaehring@boeing.com>

TABLE OF CONTENTS

1. SCOPE

This document captures aerospace network use cases that may potentially use TSN profile. It includes use cases for both commerical and military platforms. Furthermore, the use cases could be based on traditionally Ethernet based networks (e.g. ARINC664) or non-ethernet based communication sub-systems (e.g. Fibre Channel or FireWire). The use cases cover all domains of an aerospace platform.

1.1 Definitions

1.2 Symbols and Abbreviations

1.2.1 Symbols

1.2.2 Abbreviations

2. INTRODUCTION TO AEROSPACE NETWORKS

This captures the high level aerospace architecture along with specific examples of the use cases (from the ppt slide on topology and instances).Generic description of the aircraft network/domains from a commercial and military perspective.

2.1 Current Network Architecture

Commercial Aircraft

Networks are used in commercial aircraft to support varying levels of capabilities from supporting passenger entertainment to the actual control of the aircraft. Modern commercial aircraft can be subdivided into three networking domains: Aircraft Control Domain (ACD), Airline Information Services Domain (AISD), and the Passenger Information and Entertainment Services Domain (PIESD) as shown in Figure 1.

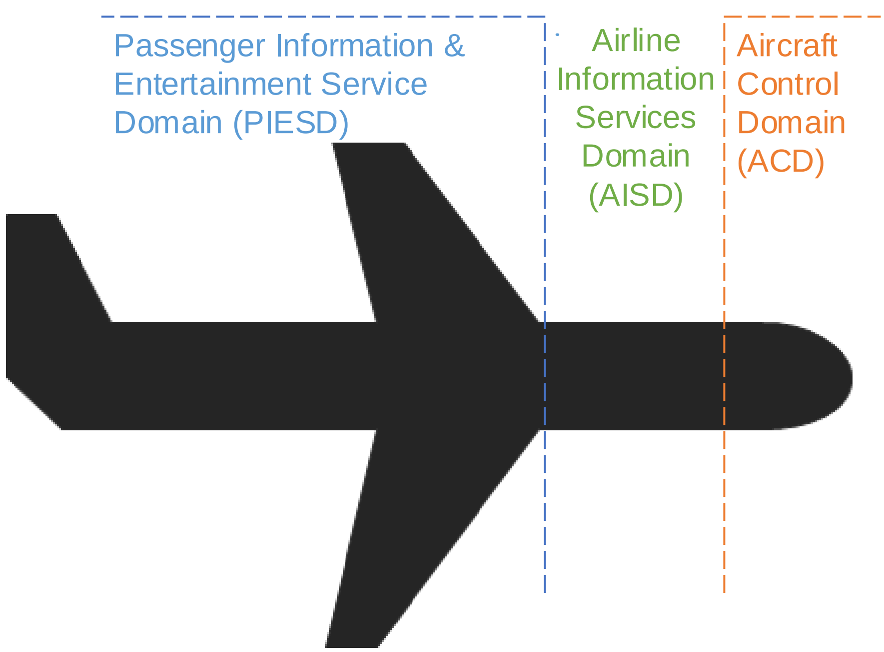

Figure 1: Commercial Aircraft Network Domains

The Aircraft Control Domain (ACD) networks host equipment that contribute to the safe flight of the aircraft. Functions typically hosted on the ACD network include electronic flight instrument system (EFIS), engine-indicating and crew alerting system (EICAS), flight management system (FMS), flight controls, and other control systems. Due to the high criticality of the functions hosted, the ACD network has high safety requirements and deterministic behavior is required.

In the ACD, networks were initially brought on the aircraft in order to reduce size, weight, and power (SWaP). In legacy aircraft, function specific federated equipment was interconnected by lower bandwidth point to point databuses such as ARINC 429. Modern aircraft employ integrated modular avionics (IMA) that reduces the amount of federated equipment and wires. In an IMA system, a general purpose processor is used to host the applications from multiple systems. The network provides an interconnect between the IMA processing, other functions hosted on the network, and to data concentrators that provide legacy interfaces. SWaP savings occur due to the reduction in equipment needed and the reduction in wiring in due to consolidated buses as depicted in Figure 2.

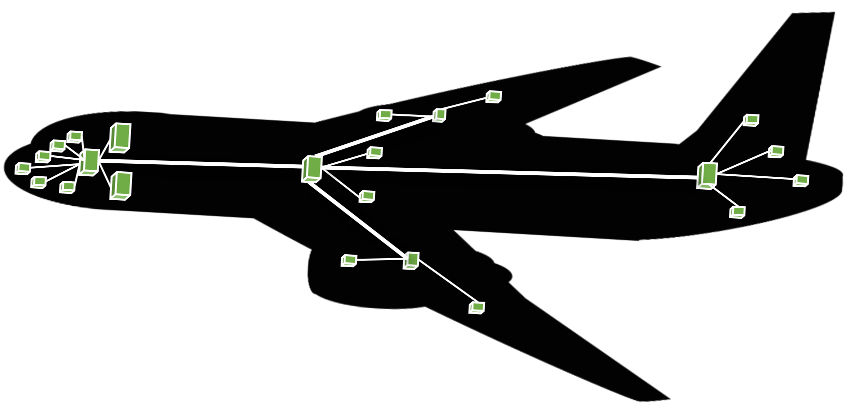

Figure 2: Commercial Integrated Modular Avionics Depiction

The Airline Information Service Domain (AISD) supports non-essential airline operational activities. It typically provides ageneral purpose processing platform as well as connectivity offboard the aircraft and between the other domains on the network. The AISD has high security requirements, but limited safety and determinism requirements due to the non-essential functions supported.

The Passenger Information and Entertainment Services Domain (PIESD) provides passenger network and entertainment services. On large commercial aircraft, this includes supporting the needs of hundreds of passengers. This drives high performance requirements. Interestingly, the PIESD has high availability requirements due to customer affinity.

Military Aircraft

Military aircrafts also use onboard networks to support functionality from the flight critical to mission oriented. A military aircraft can be subdivided into two domains: Air Vehicle System (AVS) and Mission System (MS). The AVS of the military aircraft is similar to the ACD of commercial aircraft. It encompasses the systems necessary for safe flight of the aircraft.

The Mission System of the military aircraft is responsible for supporting the varied mission of the aircraft. Depending on the type of aircraft, this could be delivering a weapon, search-and-rescue operations, and transport of equipment or personel. The requirements for the MS network vary based on the mission equipment installed. The MS equipment may include one or more high performance mission computers and typically has higher bandwidth needs than the AVS.

2.2 Considerations for Future TSN based network architecture

[TODO]: Clean up this section and add some text around these bullet points. Does a table make sense?

There is variablility in the use cases. For example, fly-by-wire would have different requirements compared with infotainment system

Technical Performance requirements vs. certification requirements.

Although the network architecture of these systems vary by aircraft, an aerospace profile of TSN appears to balance the following objectives:

- Performance (supports needs of system design)
  - Bandwidth needs of connected nodes
  - Latency/Jitter –end to end bounded latency requirements
- Cost (NRE Engineering, not Component parts, necessarily)
  - Industry supported standards tend to cheaper than custom interfaces. AFDX™, ARINC 664, ARINC 429, SAE 6509/6675, TSN Standardized, etc.
  - Cross Industry collaboration is required for Aerospace use cases to achieve sufficient scale for maximal cost savings (per part, as NRE)
- Longevity/Obsolescence (Large Passenger aircraft have service life of 20-30 yrs +)
- Available
  - Industry supported standards generally reduce risk of single supplier, usually means multiple available suppliers. ARINC 664, ARINC 429, etc
  - Interoperability is key between multiple suppliers (helped by standardized test profiles)
- Maturity
  - Certified, DO-254 Design Assurance Level up to A, depending on use-case and aircraft domain (ref. 3.1). Flying technology presents less risk to certification than novel technology. However, I believe exceptions are made by Integrators when there is a problem that can only be solved with novel solutions.
    - What problems is this novel solution solving (that cannot be solved by changes to existing technologies)? This is the true test of evolutionary technology leaps.
- Safety Critical
  - Supports Integrity Requirements of Architecture/System Depending on System Design, could be anywhere between 1E-5 and 1E-10 or smaller.
  - No Single Failure Regardless of Probability (JAR 25.1309B) for Failure Cases leading to Catastrophic effects
  - Simultaneous Segregation / Isolation of multiple criticalities, etc. Logical segregation between flows/between QoS classes. Protection against babbling idiot (eg traffic filtering)
  - Extensive understanding of failure cases (loss of frame, undetected erroneous frame/CRC failure and new failure cases introduced by TSN eg loss of synchronization, loss of synchronization capability …)
- Certifiable
  - Government is requiring Civil Certification/Processes in new contracts
  - Supports DO-178/DO-254 up to DAL A design assurance, depending on use-case and aircraft domain (ref. 3.1)

    - ARP 4761/JAR 25.1309B
    - DO-297
    - AC 20-156
- Deterministic
    - Support System Level Failure Tolerance/Architectures
        - Related to Certifiable at the Systems Level, if TSN has a vulnerability that allows a single failure to defeat synchronous operation (or inability to recover, etc), this fails to meet Deterministic (and certification) goals.
            - Erroneous Best Master, Grand Master Transition Logic
        - Bounded Latency/Jitter, etc
        - Demonstration can be done with theoretical analysis (eg Network Calculus) or simulation but ultimately methods have to be validated by Aviation Authorities. Tools and simulations might have to be certified at similar level as endpoints/switches.
- Flexible
    - Flexibility on one network to support both synchronous needs and asynchronous needs. For example, supporting synchronous closed loop networking brings with it necessary system complexities, such as voting at the receiver and/or ultra low latency requirements. A flexible network also at the same time supports asynchronous network designs, legacy equipment or data flows, that does not require the same ultra low latency as synchronous networks demand.
    - This also may support the needs of mission systems and flight critical systems on the same network.
    - Support of Deterministic trafic and non deterministic traffic on the same network (eg safety critical vs dataloading)
    - Technology can accommodate architectures of multiple type of and size
    - Technology needs to be incremental ie the effort to modify and certify architectures should be low
- Ease of Integration
    - Ease of Configuration
    - Ease of Analysis
    - Interoperability between multiple suppliers
        - Standard/COTS
        - Test Specs? What exactly does Interoperability look like?
    - COTS 802.3 Compatibility
    - Test Equipment (available, reasonably priced)
    - Scalability (both number of nodes and speed of medium)
- Upgrade path / Retrofit Options

- Benefit when design has legacy retrofit potential
- Growth path for increased medium speeds

- Security Resilience
    - Network must not preclude security features common in modern infrastructure network communications, or new technologies built upon standard Ethernet packet formats.
    - Provision or support of mechanisms to segregate different networks (with different security levels/requirements) from each other

4.Certification Requirements for Large Passenger aircraft would be that it did not preclude certification compliance to the following standards:

- DO-178/DO-254 up to DAL A design assurance, depending on use-case and aircraft domain (ref. 3.1)
- ARP 4761/JAR 25.1309B
- DO-297
- AC 20-156
- DO.160 for the HW components

5. Cost (see notes in Objectives list above)

6.Key dealbreakers for this network.

Clear upgrade pathway for accomodation of legacy databuses, the clearer and more robust the mapping, the more likely widespread adoption will occur. This includes: ARINC 664 Part 7, ARINC 429, CAN (including CAN FD), ARINC 629,

Complexity (configuration and jeopardizes certifiability

High cost means not competitive vs other solutions eg ARINC 664 part 7/CAN

Interoperability between vendors and tools is key.

2.3 Time Synchronization in Aerospace

What is the use of time synchronization in aerospace on-board communications?

- Local/Working clock [Note that these can be met with a globally synchonized as well]
    - Age of data to validate data transport Integrity
    - Latency Reduction
    - Age of data for sensor age
    - Synchronization of the Arinc 653 partition scheduler and partition
    - Fault Correlation (time stamp in logs)
    - Flight data recorder for data/event recording
    - Security (key rotation, cybersecurity attack logs)
- Universal/Global Clock
    - Database applicability (Do I have the latest database)
    - Navigation (adhering to flight plan) FMS must be synchronized to GPS time
    - Flight data recorder general date and time
    - Security (cert validation, cybersecurity attack logs)

How is time syncrhonization done today?

GPS source of global clock: Gross date and time distributed to select devices using proprietery/rudimentary method/protocol

Network Time Synchronizaion
Proprietary method/protocols to synchronize working clocks (not tied to global clock)
very course/gross synchronization (relative to worse case bounded latency to high priority traffic)

Out of band synchronization – discrete lines (1PPS, IRIG-B)
Number of different/isolated synchronization for subsystems

What are the performance and reliability requirements (today) for time synchronization

What are the future benefits of a network wide time synchronization tied to global clock?

We need to talk here about the fact that use of synchronous operation with time sync and 802.1Qbv is to achieve a higher level of determinism and bounded latencies. But it is also fine if one were to use the asynchronous operation with qav or qcr. AS6675 will support both.

- Clearly benefit for 802.1 AS like network time synchronization
- Particular interest in distributing global time (GPS)

What would be the requirements and challenges of TSN time sync solution?

Integrity, availability of time synchronization

Aerospace primarily concern with time synchronization is fault tolerance.

Concern is that 802.1AS-Rev allows for failed silence of time synchronization mechanism. However that is not acceptable in aerospace

Has to consider both: a) failure causing loss; b) time sync failure causing **undetected erroneous** function – leading to some functional failure

3. AEROSPACE USE CASES

3.1.1 General

This section presents various aerospace use cases. The objective is to inform the reader (and standards committee) of potential aerospace use cases for time sensitive networking and the corresponding requirements for TSN aerospace profile. Beyond that, the use cases listed do not have a special status from a standardization perspective. Furthermore, the inclusion of a use case does not necessarily mean that the TSN profile shall support the use case. Similarly, the exclusion of a use case does not imply that it is not supported by the TSN profile. In accordance with the committee rules, all relevant use cases provided by participants shall be included. Lastly, a varying degree of overlap between use cases is to be expected. A summary of the use cases that captures a non-overlapping set of aerospace networking features is presented at the end in section 3.1.13.

[TODO] Add a row to each use case on certification requirement
[TODO] Add a row to each use case on supported traffic types

The characteristics defined in Table 1 are used to define aerospace use cases

Characteristic	Description
Number of Nodes	Denotes the total number of networking nodes in an instantiation of the use case. Includes both end stations and bridges. May be specified as a range or a maxium value
Physical Topology	Denotes the type of physical topology in use, where in “physical topology” represent the hardware level connectivity between devices. Examples include star, ring, mesh, and point-to-point.. One or more topolgies may be specified
Number of Switched hops	Denotes the number of hops between source and destination. May be specified as a range or a maximum value
Number of Streams Per Switch	Denotes the number of unique data streams traversing a bridge in the network. Each unique data streams requires three functions by the bridge: stream identification, stream policing, and stream shaping. These functions server the overall aerospace requirement that the bridge is able to maintain isolation between unique data streams and provide guaranteed quality of service for each data stream May be specified as a range or a maximum value.
Network Redundancy	Describes the network redundancy architecture in the current instantiations of the use case. One of more redundancy architectures may be specified
Redundancy Mode	Denotes the mode of redundancy. Options include standy, active, hot-active, active-active with voting One or more modes may be specified.
Data Rate	Denotes the data rate(s) of the phyiscal media. May be specified as one or more rates
Media Type	Denotes the type of media, which may include the physical medium as well as MAC protocol. Examples include 100Base-Tx, Shielded Twisted Pair, May be specified as one or more media types
Worst Case Link Utilization	Denotes the link utilization of the most congested link in the network. Due to aerospace certification requirements, the worst case link utilization as designed/configured may be different from the works case utilization as realized on the wire. This field can be used to specify both the “as configured” and “as realized on wire” variants of the link utilization May be specified as a range or maximum value.
Dissimilarity, Integrity, Maintainance, Monitoring, Security [DIMMS]	When applicable, denotes the use of dissimilarity, integrity, maintainance, monitoring, or security features. Additionally, the method by which such a feature is achieved in the current instantiation of the use case may be specified May specify one or more features in use.
Certification	Specify if any certification requirements apply to this use case.

Requirements	Speficy if it is Mandatory, Desired, Do Not Care.
Supported Traffic Types	Listing of Traffic Types from section 4 that exist in this use case

Template of what should we address for each of the use cases 4.1.2 to 4.1.11 below:

1. Definition of the Use Case. What is the purpose of the use case?
2. Introduction/General context: to this use case. Examples of this use case
3. Description of the characteristics table. Wordify the table below to the extent necessary.
4. Certification requirements for this use case, if any.
5. Cost pressures or lack thereof, if any.
6. Key dealbreakers for this network.

3.1.2 Small Business Aircraft

This use case captures how an SAE AS-6675 based data transport infrastructure satisfies the typical characteristics and qualities, as previously defined in section 3.1.1, of a small business aircraft. In this section, “small” business aircraft is encompassing of single and dual engined turboprops and light jets through super mid-sized jets.

The avionics systems of small business aircraft are constrained for size, weight, and power (SWAP). Additionally, the quantity of any one type of aircraft produced tends to be much lower than large passenger aircraft, resulting in a more product line approach to the avionics systems rather than a purpose built for this aircraft approach.

The avionics networks in this market segment are used primarily to interconnect the integrated avionics systems of a single provider. These systems host a range of functions requiring safety and design assurance levels ranging from A to D (ARP-4754 / DO-178 / DO-254). Based on SWAP constraint, the avionics networking components are often integrated into other multipurpose equipment, such as displays or processing units.

Major updates to these avionics systems / networks on a aircraft type occur every 7 to 10 years, where major is defined as the system is mostly replaced. This market segment tends to be early adopters of new features / functions resulting in incremental updates throughout the lifecycle. For instance, Synthetic Vision System (SVS) has been essentially standard for much of the last decade where it has not yet been signifcantly adopted in large commercial aircraft.

Topology Characteristic	Present / Today	Known future requirement vs. Desired feature
Number of nodes	10-20	30-40 (as legacy boxes become Eth/TSN boxes)
Physical topology	Hub and spoke (star) Point to Point (direct)	TBD as more switching gets distributed
Number of switched hops	1-2	TBD
Max number of flows/streams per switch	50-500	
Network Redundancy	No redundancy on point-to-point links; Two separate LANs between switched nodes	

	(ARINC664 type redundancy) Redundancy is mostly used for DAL-A/B systems in this scenario	
Redundancy Mode	Frame Failover (Hot Active)	
Data Rates	10 – 100 Mbps	1 Gbps will be required
Media	Copper (shielded twisted pair) 10Base-Tx or 100Base-Tx (ARINC664 compliant)	Preference to stick to copper for serviceability. Fiber only if absolutely necessary
Worst Case Link Utilization	50% as configured (for bounded worst-case latency) 20% as realized on the wire	
Dissimilarity, integrity, maintenance, security [DIMS]	No Dissimilarity requirement; SNMP based fault and status information;	Dissimilarity may be needed if used for fly-by-wire; security is a consideration;
Certification Requirements		
Supported Traffic Types	All listed traffic types (TT2 through TT14)	Future desire to support TT1 traffic as well

The network architecture of these systems vary by aircraft and supplier. For smaller systems, point to point interconnects between equipment is common. As the quantity of nodes increases, switches, often integrated into multifunction equipment, become more common. It is expected that future systems will have more nodes primarily due legacy units migrating to network interfaces.

Redudancy is an important characteristic to these systems to achieve the safety goals, but the application varies by system. In smaller systems, redudancy is primarily limited to right side / left side equipment with interconnections in the point to point network. As the systems get larger and switches are added, ARINC664p7 style redudancy with LAN A/B starts to become more common.

Depending on the system, the quantity of flows on the network varies greatly. The data flows include periodic and aperiodic messaging. For periodic data, the highest rates tend to be on the order of 50-100 Hz with most sensor/parmetric data falling in the 5-20 Hz range. Event driven, large data transfers are also common. At initial certification, it is highly desirable to keep the worst case utilization to less than 50% to support future growth on the platform.

In this market segment, copper is the preferred physical medium due to the ease of installation and maintenance. Fiber optics require specialized tooling and training that is less desireable. The maintenance operations in this market segment tend to support a wide variety of aircraft.

To date, dissimilarity of the network has not been required. In the future, it could become a necessity as capabilities fly-by-wire are introduced. However, it is more likely that architectural mitigations would be applied to prevent the need for dissimilarity.

3.1.3 Large Passenger Aircraft

1-2: Large Passenger Aircraft use case is roughly defined as aircraft carrying 100 passengers or more in a commercial airline operation. Examples of this use case in aerospace industry would be would be AirbusA220, Boeing 787, Airbus A350, Boeing 777x, etc.[reference]

These aircraft (and their networks) have high requirements placed on them for performance, efficiency, and high dispatch reliability. Additionally, due to their size and commercial operation, they often have multiple network domains, including high criticality Aircraft Control Domain (ACD) networks, Aircraft Information Services Domain (AISD), as well as Passenger Information Entertainment System Domains (PIESD). There will be a range of design assurance levels, from DAL E in PIESD, to DAL C-D for AISD, to DAL A-C for ACD. The onboard presence of multiple domains, especially when interconnected, as well as design assurance levels drives a wide variety of traffic requirements and additional security requirements on network implementations.

3. The typical Large Passenger aircraft currently will have approximately 50-100 nodes, most often in a switched star topology, with a maximum of 2-3 switch hops for any node to any other node. It is likely that the switches will be standalone modules or LRUs with 10-24 ports. Currently primarily implemented using ARINC 664 Part 7, uniquely statically configured streams are in the 100s-1000s per switch, and expected to climb with increasing node capabilities and stream bandwidths. Redundancy is accomplished with redundant and physically separate LANs, with nodes being dual homed (two physical ports). The redundancy mode is frame failover (ARINC 664 P7), with data rates between 10-100mbps, and expected to climb as bandwidth of streams increase and maximum allowed latencies decrease. Media types include copper for 10 and 100mbit, although the weight savings and reduced electromagnetic susceptability of fiber becomes important with faster speeds or long distance runs. Worst case utilization would have some nodes configured as high as 70-95% of the medium capability, although the typical nominal bandwidth would be expected to be 20-50% loading.

Large Passenger Aircraft have the characteristics listed below:

Topology Characteristic	Present / Today	Projected or Desired (if known)
Number of nodes	50-100	100-500 (as legacy A429/A629/CAN boxes become Eth/TSN boxes) No more than 1000 network elements expected
Physical topology	Primarily multiple Hub and spoke (switched star)	Large networks will likely stay switched star, but certain small scale networks might use linear, ring, or hybrid topologies.
Number of switched hops	2-3	Same or Larger
Max number of flows/streams per switch	100s-1000s (1000+ streams per switch) Does TSN silicon support 1000s of stream identification entries?	4096+ streams per switch **may** be possible to rearchitect streams to minimize number of unique streams
Network Redundancy	Two separate LANs between switched nodes (ARINC664P7 type redundancy) End systems are dual homed to redundant (physically separate) LANs.	Same as Today
Redundancy Mode	Frame Failover (Hot Active)	Same as Today
Data Rates	10 – 100 Mbps	1 Gbps will be required Trunk lines between switches may require 10-40+ Gbps link to support aggregate BW (even higher if high resolution video utilizes the network)
Media	Copper (shielded twisted pair) and Multimode Fiber 10Base-Tx/Sx or 100Base-Tx/Sx (ARINC664 compliant)	Preference to stick to copper for serviceability for short runs and low medium speeds. Fiber for weight gains for long runs and high speeds.
Worst Case Link Utilization	70%-95% as configured (for bounded worst case latency) 20%-50% as realized on the wire	Probably similar depending on selected determinism demonstration method
Dissimilarity, integrity, maintenance, security [DIMS]	Dissimilarity requirement required for fly-by-wire or critical processing; periodic broadcast fault and status information, with centralized maintenance management software. Security requirements exist for isolation between design assurance levels and cross-domain	Same, with potential increase in dissimilarity requirements in future certifications

	traffic.	
Certification Requirements		
Supported Traffic Types		

3.1.4 Large Passenger Aircraft (Cabin)

[1-2]: This use-case belongs to the same type of Aircraft as the one before, carrying more than 100 passengers. However, there are significant differences between cabin networks and avionics networks, which justify a separation within this document:

- Safety Level: Although use-cases in the cabin cover all three domains as per ARINC664-P5 (ACD, AISD, PIESD), the safety criticality of the use-cases is DAL C in maximum (exception: cargo smoke detection DAL B).
- Configurability: Cabin layouts are highly customer dependent, and so are the underlying networks. Network configuration for cabin shall be easy to change and maintain per head of version. Ideally, it would be self configuring or at least provide “plug’n’play” mechanisms to support self-configuration. On the other hand, determinism is not required for most cabin use-cases.
- Life-Cycles: Typically, the cabin of a commercial aircraft is overhauled every 7 years, including exchange of (network) equipment. Software Lifecycles can be shorter, upcoming products like open software platform principles will allow for frequent remote software changes, e.g. in an overnight stop. This requires flexibility in network configurations as well as low cost hardware. Commercial off the shelf (COTS) hardware and open standards are prefered to reduce cost. Lack of reliabiliy may be recovered by sufficiently redundant network architectures.
- Wireless: to support layout flexibility as well as mobility of users, wireless networks as WiFi and Bluetooth gain more and more importance in the aircaft cabin. To support use-cases end to end, a TSN profile for commercial aircraft cabin shall support wireless networks as well.
- Security: Cabin networks provide open interfaces to passengers. For this reason, high security standards must be kept especially for the gateways between different networks and between different domains, respectively.

Dedicated examples of cabin use-cases:

- the Cabin Management System, providing all functions to monitor and control the aircraft cabin (e.g. lights and temperature control, passenger announcements, crew intercommunication, crew alerting, signs, …). Design Assurance Level (DAL) between C and D.
- the In-Flight Entertainment System, providing video (and audio) streams to every passenger seat and/or personal device, either wired or wireless. This is often combined with a connectivity system, providing (internet) connectivity during flight, most often using satellite links. DAL D-E.
- Video Surveillance System, which interconnects several surveillance cameras within the cabin with suitable monitoring devices (e.g. the Flight Attendant Panel or a mobile cabin crew device) and (optionally) a video recording device. DAL D in most cases.
- Wireless Networks: as already mentioned, WiFi networks in the cabin are mainly used for In-Flight-Entertainment purposes. However, usage for mobile cabin crew operations is intended as well. In general it is expected, that the number of wireless use-cases in the cabin will grow in coming years, e.g. regarding Internet of Things applications.

IFE, Video and Wireless systems are mainly buyer furnished equipment, for more detailed descriptions and as support to achieve a broad standards acceptance, the related manufacturers should be involved.

[3]: Due to the stretched geometry of aircraft cabins, cabin networks often consist of daisy-chained switches in the cabin, connected to central servers in the electronics bay of the Aircraft. Each switch may connect to end-devices or to further

star-topology sub-structures. Switches often serve as gateways to e.g. CAN, RS485 or other field busses. Ring topologies to enhance redundancy/reliability are in discussion for future evolutions and should be regarded in this standardisation activity.

The number of nodes varies with cabin configurations and number of passengers. For a large Aircraft like A350, Cabin Management as well as IFE can serve ~500-5000 end devices each (the exact number will heavily depend on the intelligence of the end devices), with the number of nodes by factor 5-10 lower (~1000 in maximum). In a daisy chained network, the number of hops could go up to 15 (or the double number in a ring topology).

The number of streams per hop needs a deeper analysis of stream classes and refering use-cases.

Today, only the Cabin Management System provides redundancy in terms of a second server operating in hot standby. (tbd: IFE?). In addition, the Cabin Management System's Network architecture provides some redundancyt: more clients than required are installed and connected to a multiple of daisy-chains. In case of a failure of a part of the network (i.e. one daisy-chain), the relevant functions can still be served by the remaining chains and clients, respectively.

Today, 100 Base Tx and 1000 Base T copper Ethernet networks are in use for cabin networks. In future, fibre optical networks with datarates between 1-10Gbps are intended for the backbone network (ideally combining Cabin Management, Video surveillance and IFE) as well as 100/1000 Base T1 2-wire Ethernet (or PoDL) for subnetworks (e.g. replacing CAN, RS485 and other field buses).

Dissimilarity is not applied in cabin networks. The Cabin Management System is connected to the Aircraft central fault management, providing power-on test results and regular health messages. Security logs are available for the last 90 days as well. Selected health messages and maintenance procedures are available on the Flight Attendant Panel for Cabin Management System and connected systems, and on the IFE control panel (if available) for the IFE.

Topology Characteristic	Present / Today	Projected or Desired (if known)
Number of nodes	Cabin Management: not switched Ethernet today IFE: ~100 (2 per seat-row + wall disconnect boxes) Video: ~10	~200-300, when Cabin Management will be implemented as switched network as well
Physical topology	Daisy chained switches with star-topology substructures	Ring-topology in discussion for Cabin Management System
Number of switched hops	Up to 5 in IFE, depending on implementation	Up to 15 in future Cabin Management Networks, up to 30 if realized as ring topology
Max number of flows/streams per switch	Tbd	Tbd
Network Redundancy	Only Cabin Management System: - Two servers - 2-4 independent network lines in the cabin, each serving the same functions	As today, ring topology as replacement of independent network lines in discussion
Redundancy Mode	Hot standby for Cabin Management Server	Same as Today
Data Rates	IFE: 1Gbps Video surveillance: 100Mbps Cabin Management: 10Mbps Each system providing several network lines with above bandwidth.	5-10Gbps for all, several network lines per system.
Media	Copper (shielded twisted pair), 100Base Tx or 1000Base T	Common multi-fiber backbone (5-10Gbps) for all cabin use-cases in discussion. Multi-mode fibres combined in multi-fibre cables of

		12/24/48 fibres per cable. 100/1000Base T1 or PoDL in discussion as replacement of CAN, RS485 and other field buses “on the last mile”.
Worst Case Link Utilization	Cabin Management System: 99% IFE: depending on usage by passenger (up to 70%?) Video: below 20%	design goal: 50% in maximum with entry into service
Dissimilarity, integrity, maintenance, security [DIMS]	See text	Same
Certification Requirements	Cabin Management System: up to DAL C IFE: DAL E-D Video: DAL D	no change, downgrade of Cabin Management System DAL C functions desired
Supported Traffic Types	Tbd	Tbd

3.1.5 Small and Combat Military Mission Network

Combat Military Aircraft mission network are constrained by SWaP availability. Instead major constraints would come from interoperability and flexibility to be able to interface with legacy and current systems, and scalability to modifications. Combat Military Aircraft mission networks are purpose built for specific operational needs. Changes to the operational capability occur frequently, with minor updates one to two times per year, and major updates about once every 2-3 years. Changes to the mission capability occur frequently with different operational conditions possible. Overall aircraft lifespan is expected to last 50+ years.

DO-178/DO-254 style safety certification does not generally apply to combact military aircraft networks, although it is becoming more relevant.

Topology Characteristic	Present / Today	Projected or Desired (if known)
Number of nodes	10-70	10-70
Physical topology	Master/slave Bus, point-to-point, ring, star.	
Number of switched hops	0- 2	0-2
Number of streams per switch		Could increase dramatically when converged to TSN (as opposed to federated)
Network Redundancy	Mostly subsystem level; Redundant network connections to separate networks; Redundancy dependent on data transport tech.	
Redundancy Mode	Bus Failover (Standby); Limited hot – active.	
Data Rate	100kbps, 1 Mbps, 10 Mbps, 100Mbps, 1 Gbps	10-100 Gbps needed
Media	Copper: 1553, 1760, ARINC 429 buses, ARINC 818	Copper, fibre
Worst case link utilization	50% under max load for congestion prone bus 90% for “deterministic” buses like 1553 (mostly to avoid missing deadlines for safety critical)	
Dissimilarity, integrity, maintenance, monitoring, security [DIMMS]	Maintenance: active in-flight health monitoring. MIBs are design specific, but definitely exist. Same with logs for maintenance. Dissimilarity: HW dissimilarity, SW dissimilarity?	

	Integrity and determinism needed for mission and operational capabilities. Emphasis is on security	
Certification Requirements	Generally self-certified by acquisition authority, analogous to DO-178/DO-254 DAL C/D/E	
Supported Traffic Types	TT1, TT5, TT13 (data hog)	

The topology for combact Military Aircraft mission networks could converge to a star topology with redundant interfaces for mission critical systems, utilizing a maximum of one switch per aircraft. Besides, non-switched topologies exist and no changes with similar guarantees for performance and determinism to be provided.

Certification of combact Military Aircraft mission networks are typically dependent on their acquisition authority, the safety criticality level associated to their functions most typically aligns with that of DO-178/DO-254 Design Assurance Level C to E, i.e. safety-involved to non-criticality for mission criticality.

[Sample text on supported traffic types] Typical scenarios include tens of TT13 type traffic on this plaform. Therefore an aggregate bandwidth or rate of 100 Gbps is needed/requiredThis scenario only supports three types of traffic – all which are high bandwidth flows with relaxed latency requirements

3.1.6 Large Military Aircraft Mission Network

This use case captures how an SAE AS-6675 based data transport infrastructure satisfies the typical characteristics and qualities of a large Military Aircraft mission network.

Large Military Aircraft mission networks are not constrained by SWaP availability. Instead major constraints would come from interoperability and flexibility to be able to interface with legacy, and scalability to modifications. Large Military Aircraft mission networks are purpose built for specific operational needs.

Changes to the operational capability occur frequently, with minor updates one to two times per year, and major updates about once every 2-3 years. Changes to the mission capability occur frequently with different operational conditions possible. Overall aircraft lifespan is expected to last 50+ years.

There are considerable number of sub-systems and limited data transport infrastructure on-board the aircraft. Each sub-system has a defined interface and performance requirements for a given set of messages which instantiate a required behavior, all of which must be validated to perform reliably and with high integrity.

The mission network composes of periodic and aperiodic messages with safety-involved/mission critical requirements to non-criticality requirements for the functions using such.

DO-178/DO-254 style safety certification becomes applicable to large military aircraft networks.

Topology Characteristic	Present / Today	Projected or Desired (if known)
Number of nodes	10-200	
Physical topology	Many different topologies: Master/slave Bus; point-to-point, star, ring.	
Number of switched hops	0-4	
Number of streams per switch	100s – 500	
Network/Media/Bus/communication Redundancy	Mostly subsystem level; Redundant network connections to separate networks Redundancy dependent on data transport tech.	
Redundancy Mode	Bus Failover (Standby);	
Data Rate	100kbps, 1 Mbps, 10 Mbps, 1 Gpbs, multi gigabit,	10-100 Gbps needed

Media	Copper: 1553, 1394, FC/copper; smaller subsystems that control actuators, etc, may have 485,422 buses; Fibre: FC	Copper, fibre
Worst case link utilization	50% under max load (mostly to avoid missing deadlines for safety critical)	
Dissimilarity, integrity, maintenance, monitoring, security [DIMMS]	Dissimilarity in SW & HW (but same data transport technology) Data integrity mechanisms used Dissimilarity: HW dissimilarity, SW dissimilarity? Integrity and determinism: needed for mission and operational capabilities. Emphasis is on security.	
Certification Requirements	Generally self-certified by acquisition authority, analogous to DO-178/DO-254 DAL C/D/E.	
Supported Traffic Types		

Although the absolute number of nodes is not expected to increase significantly, it is expected that more nodes will natively adopt the AS-6675 network interace to communicate. The topology can converge to a switched topology with redundant interfaces for mission critical systems, utilizing a maximum of 3 switches per aicraft. The case of non-switched mission network exists but it is limited to portion of the network; the portions have to be integrated with the majority of the networks which is switched.

Large Military Aircraft mission networks should support functions of mixed criticalities, from safety-involved to non-critical, with both bandwidth and guaranteed latency requirements for operational capability.
Periodic and aperiodic messages have to be managed with latency requirements and/or bandwidth requirements. Latency requirements shall be in the range of 5-100ms, while bandwidth requirements shall be in the range of 100Kbps-1Gbps. During the convergence to AS-6675 network, end-to-end latency with non-AS-6675 interfaces cannot be guaranteed. Also, interfacing with legacy part of the network shall be developed.
Large Military Aircraft mission networks shall support for non-time synchronization.

The availability of the network infastructure will be actively monitored and faults will be logged for maintenance. The number of streams will increase as additional legacy nodes such as aircraft sensors and discrete inputs adopt the converged AS-6675 network interface.
In order to improve operational capabilities and mission network performance, latency requirements will reduce sensibly driving the need for ms constraints. The bandwidth will increase signifcantly as higher fidelity video and misson sensor data is exchanged over the mission network, driving a need for triple-digit Gbps. The mission network should support high utilization of this bandwidth, with scheduled traffic supporting deterministic behavior at >50% utilization.
While today's mission network is a mix of various interfaces and media, the future converged AS-6675 mission network will utilize copper and fibre optic media.

Certification of large Military Aircraft mission networks are typically dependent on their acquisition authority, the safety criticality level associated to their functions most typically aligns with that of DO-178/DO-254 Design Assurance Level C to E, i.e. safety-involved to non-criticality for mission criticality.
It is expected that a AS-6675 converged mission network should result in cost savings and cost avoidance when compared to legacy mission system data transports, while forming the foundation for a modular open systems architecture. During the transition, interfacing with legacy mission system has to be considered.

[Sample text on supported traffic types]

3.1.7 Small, Combat, and Large Military Flight Network (VMS)

This use case captures how an SAE AS-6675 based data transport infrastructure satisfies the typical characteristics and qualities, as previously defined in section **Error! Reference source not found.**, of a small, combat, and large Military Aircraft flight network.

Small Military Aircraft flight networks and combat military aircraft flight networks are significantly constrained by SWaP availability and are purpose built for specific safety and operational needs. Large aircraft flight networks are not constrained in by SWaP availability, but are purpose built for specific safety and operational needs.

Changes to the flight capability occur infrequently and with very slow pace, about once every two to five years. Overall aircraft lifespan is expected to last 50+ years.

There are small number of sub-systems and limited data transport infrastructure on-board the aircraft. Each sub-system has a defined interface and performance requirements for a defined set of messages which instantiate a required behavior, all of which must be validated to perform safely and reliably. The flight network composes of periodic and aperiodic messages with safety-critical requirements.

DO-178/DO-254 style safety certification does not generally apply to combact military aircraft networks, although it is becoming more relevant.

Topology Characteristic	Present / Today	Projected or Desired (if known)
Number of nodes	5-20 (10-50)	10-100
Physical topology	1394 – Tree and leaf topology implemented as a physical ring Master/slave Bus; point-to-point, star, ring.	
Number of switched hops	0-2	
Number of streams per switch	10s – 500	Will increase generally. Dramatic increase would come from individual sensors being connected separately (as opposed to going to RDCs)
Network Redundancy	Redundant failover with a ring (usually a ring). 1394 Loops Also has full system level redundancy (dual, tri, or quad) Redundancy dependent on data transport tech.	Future TSN based implementation could use CB like network redundancy depending on design
Redundancy Mode	Hot Active with voting; Most simplistic mode – Standby; Active/Active Voting	
Data Rate	100Kbps, 200-400 Mbps (1394-s4), 1 Mbps, 10 Mbps, 1 Gpbs, multi gigabit,	No desire at the moment for even higher BW
Media	Copper: 1394 Fibre: FC; Ethernet/fibre	
Worst case link utilization	50% but can go as high as 80% due to fewer buses	
Dissimilarity, integrity, maintenance, monitoring, security [DIMMS]	Dissimilarity in SW & HW (but same data transport technology) Data integrity mechanisms used Dissimilarity: HW dissimilarity, SW dissimilarity? Integrity: needed for safety-criticality. Emphasis is on security.	
Certification Requirements	Generally self-certified by acquisition authority, analogous to DO-178/DO-254 DAL A/B/C. DAL C?	
Supported Traffic Types		

Althought the absolute number of nodes is not expected to increase significantly, it is expected that more nodes will natively adopt the converged AS-6675 network interace to communicate and in doing so the topology moves to a traditional switched topology with redundant interfaces for flight systems, utilitizing a maximum of 1 switch per aircraft. Besides, non-switched topologies are also applicable with similar guarantees for performance and determinism to be provided.

Militiary flight control network shall support safety-criticalitity functionalities with strict latency requirements but not demanding bandwidth requirements.

Periodic and aperiodic messages have to be managed with latency or deadline requirements. Latency requirements shall be the range of sub milli seconds-100ms, while bandwidth requirements shall be in the range of 100kbps-100Mbps. During the convergence to AS-6675 network, end-to-end latency with non-AS-6675 interfaces cannot be guaranteed. Also, interfacing with legacy part of the network shall be developed.

Military flight control networks shall support for time synchronization.

Availability of the network infastructure will be actively monitored and faults will be logged for maintenance. The number of streams will increase as additional legacy nodes such as aircraft sensors and discrete inputs adopt the converged AS-6675 network interface.

Latency requirements will reduce sensibly to 10us-100us for performance improvements. Bandwidth will not increase signifcantly with the need of at most 1Gbps. The flight network should support high utilization of this bandwidth, with scheduled traffic supporting deterministic behavior at >50% utilization.

The future converged AS-6675 mission network will utilize copper and fibre optic media.

While certification of Military Aircraft flight networks are typically dependent on their acquisition authority, the operational performance most typically aligns with that of DO-178/DO-254 Design Assurance Level A to B.

It is expected that an AS-6675 converged flight network should result in cost savings and cost avoidance when compared to legacy mission system data transports, while forming the foundation for a modular open systems architecture. During the transition, interfacing with legacy flight system has to be considered.

3.1.8 Unmanned Military Aircraft Network

Add some text describing use case as well as describe the table contents.

Topology Characteristic	Present / Today	Projected or Desired (if known)
Number of nodes	10-50	
Physical topology	Master/slave Bus, point-to-point, star.	
Number of switched hops	0-2	
Number of streams per switch	50 – 500	
Network Redundancy	Mostly subsystem level; Redundant network connections to separate networks; Redundancy dependent on data transport tech.	
Redundancy Mode	Bus Failover (Standby); Limited hot – active.	
Data Rate	100Kbps, 1 Mbps, 10 Mbps, 100Mbps, 1 Gbps, 10GBase-T	10-100 Gbps need
Media	Copper, Fiber Optic: 1 Gig -10Gb Ethernet, 1553, 1394, Fibre Channel, Ethernet/fibre	Copper, fiber
Worst case link utilization	75%	
Dissimilarity, integrity, maintenance, monitoring, security [DIMMS]	Maintenance: active in-flight health monitoring. Same with logs for maintenance. Emphasis is on security.	
Certification Requirements		
Supported Traffic Types		

3.1.9 Rotary Wing Mission Network

This use case captures how an SAE AS6675 based data transport infrastructure satisfies the typical characteristics and qualities of a rotary wing aircraft mission network.

A rotary wing aircraft mission network is significantly constrained by space, weight, and power availability, and is purpose built for specific operational needs. Therefore, there are a minimum number of sub-systems and limited data transport infrastructure on-board the aircraft. Each sub-system has a defined interface and performance requirements for a defined set of messages which instantiate a required behavior, all of which must be validated to perform safely and reliably. DO-178/DO-254 style safety certification does not generally apply, although it is becoming more prevalent in recent years. Changes to the operational capability occur infrequently, with minor updates one to two times per year, and major updates about once every five to ten years. Overall aircraft lifespan is expected to last 50 years.

Topology Characteristic	Present / Today	Projected or Desired (if known)
Number of nodes	10-50	10-100
Physical topology	Master/slave Bus, point-to-point, star.	Star
Number of switched hops	0-2	
Number of streams per switch	100 – 500	Could increase dramatically if converged to TSN (as opposed to current federated)
Network Redundancy	Mostly subsystem level; Redundant network connections to separate networks; Redundancy dependent on data transport tech.	Future TSN based implementation could use IEEE 802.1CB like network redundancy depending on design
Redundancy Mode	Bus Failover (Standby); Limited hot – active.	
Data Rate	100Kbps, 1 Mbps, 10 Mbps, 100Mbps, 1 Gbps	10-100 Gbps need
Media	Copper: 1553, 1760, RS-485/422, ARINC 429 buses	Copper, fiber
Worst case link utilization	50% under max load for congestion prone bus 90% for “deterministic” buses like 1553	
Dissimilarity, integrity, maintenance, monitoring, security [DIMMS]	Maintenance: active in-flight health monitoring. MIBs are design specific, but definitely exist. Same with logs for maintenance. Emphasis is on security.	
Certification Requirements	Generally self-certified by acquisition authority, analogous to DO-178/DO-254 DAL C.	
Supported Traffic Types		

Given its space, weight, and power constraints, the absolute number of nodes is not expected to increase significantly, however, it’s expected that more nodes will natively adopt the converged AS6675 network interface to communicate. In doing so the topology moves largely to a traditional Ethernet star topology with redundant interfaces for mission critical systems, utilizing two or four switches per aircraft. Availability of the network infrastructure will be actively monitored and faults will be logged for maintenance. The number of streams will increase as additional legacy nodes such as aircraft sensors and discrete inputs adopt the converged AS-6675 network interface. Bandwidth of these streams will increase significantly as higher fidelity video and mission sensor data is transmitted over the mission network, driving a need for 100Gbps and even 1Tbps line rates in the 2030 timeframe. The mission network should support high utilization of this bandwidth, with scheduled traffic supporting deterministic behavior at >90% utilization. While today’s mission network is a mix of various interfaces and media such as MIL-STD-1553 over coaxial cable and ARINC-429 over copper twisted pair, the future converged AS-6675 mission network will utilize Ethernet over copper and/or fiber optic cabling.

While certification of rotary wing aircraft mission systems are typically dependent on their acquisition authority, the operational performance most typically aligns with that of DO-178/DO-254 Design Assurance Level C.

It is expected that an AS-6675 converged mission network should result in cost savings and cost avoidance when compared to legacy mission system data transports, while forming the foundation for a modular open systems architecture.

3.1.10 Rotary Wing Flight Network

This use case captures how an SAE AS6675 based data transport infrastructure satisfies the typical characteristics and qualities, of a rotary wing aircraft flight network.

A rotary wing aircraft flight network supports the safety critical aviation and navigation of the aircraft, and is significantly constrained by space, weight, and power availability. Aircraft flight safety has traditionally required a limited number of avionics components and minimal bandwidth connectivity between them. Each avionics sub-system has a defined interface and performance requirements for a defined set of messages which contribute to the flight safety, all of which must be validated to perform safely and reliably. DO-178/DO-254 style safety certification does not generally apply in the military domain, although it is becoming more prevalent in recent years as FAA style certification becomes more commonplace. Changes to the flight network operational capability occur very infrequently due to costly certification impacts. Overall aircraft lifespan is expected to last 50 years.

Topology Characteristic	Present / Today	Projected or Desired (if known)
Number of nodes	10-20	10-20
Physical topology	Master/slave Bus; point-to-point	Star
Number of switched hops	0-2	1-2
Number of streams per switch	50-200	Significant increase would come from individual sensors being connected directly (as opposed to going through data concentrators)
Network Redundancy	Hot active redundant failover Also has full system level redundancy (dual, tri, or quad)	Future TSN based implementation could use IEEE 802.1CB like network redundancy depending on design
Redundancy Mode	Hot Active with voting; Most simplistic mode – Standby; Active/Active Voting	
Data Rate	100Kbps, 1 Mbps, 10 Mbps, 100Mbps	No desire at the moment for even higher BW
Media	Copper: RS-485/422, ARINC 429 buses, 1553, Ethernet	
Worst case link utilization	50% but can go as high as 80% due to fewer buses	
Dissimilarity, integrity, maintenance, monitoring, security [DIMMS]	Emphasis is on integrity, monitoring, and maintenance.	
Certification Requirements	Generally self-certified by acquisition authority	FAA style certification (DO-178/DO-254 DAL A) becoming more prevalent
Supported Traffic Types		

Given its space, weight, and power constraints, and its bounded functionality, the absolute number of nodes on the flight network is not expected to increase significantly, however, it's expected that more nodes will natively adopt the converged AS6675 network interface to communicate. In doing so the legacy point-to-point and point-to-multipoint topologies move largely to a traditional Ethernet star topology with redundant interfaces for guaranteed availability of safety critical data, utilizing two or three switches per aircraft for duplex or triplex redundant flight control, respectively. Availability of the network infrastructure will be actively monitored, and faults will be logged for maintenance. The number of streams will increase as additional legacy nodes such as aircraft sensors, analog inputs, and discrete inputs adopt the converged AS-6675 network interface. Bandwidth of these streams will likely remain low, and current ethernet line rates should exceed future requirements with relatively low utilization for safety critical needs. Scheduled traffic supporting highly deterministic behavior will be used for closed loop systems, such as those impacting flight control surfaces. While today's flight network is a mix of various interfaces and media such as RS-422, RS-485 and ARINC-429 over copper twisted pair, the future converged AS6675 mission network will utilize Ethernet over copper and/or fiber optic cabling.

Certification of rotary wing aircraft flight systems are typically dependent on their acquisition authority, with both commercial and military domains now using FAA style certifications aligning with that of DO-178/DO-254 Design Assurance Level A.

It is expected that an AS6675 flight network should result in cost savings and cost avoidance when compared to legacy flight system data transports, while forming the foundation for a modular open systems architecture.

3.1.11 Satellite Network

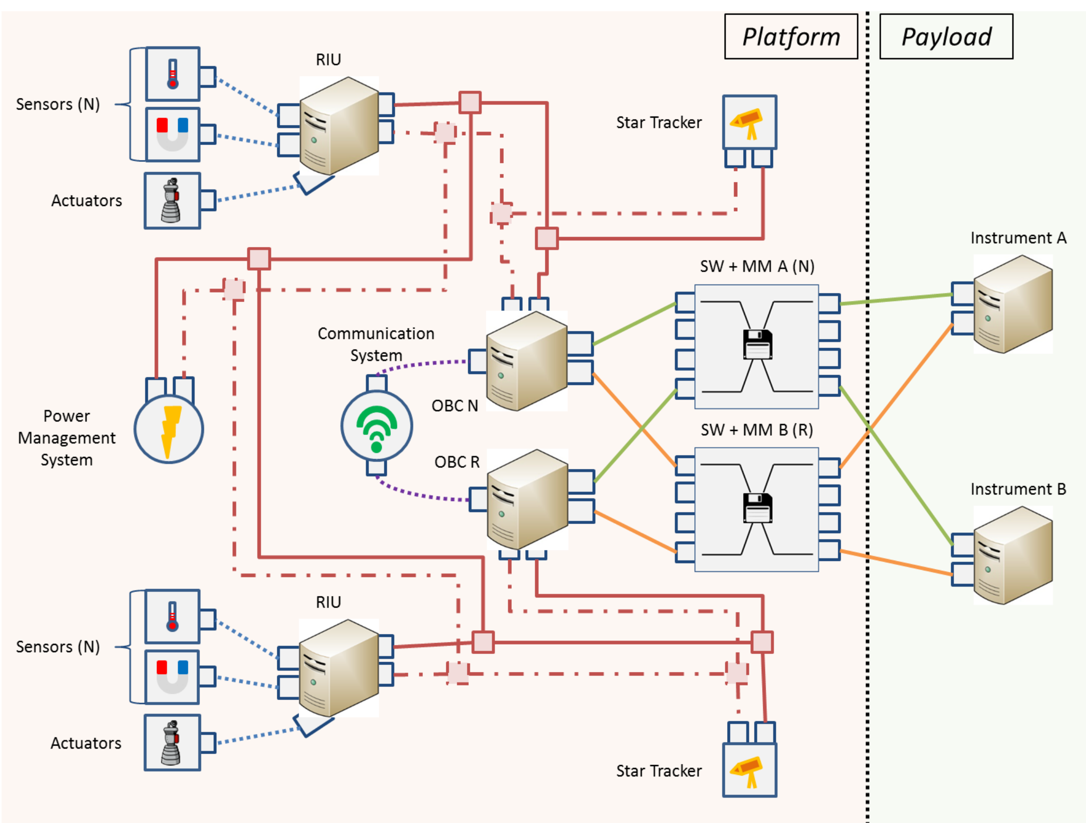

Figure 3 - Current Network Topology

Actual network configuration

The figure above represents a simplified but generic view of current satellite network topology summarizing the architecture. The network is "divided" into two sub-networks: platform and payload.

On the one hand, the platform network is in charge of conveying all the necessary information in order to guarantee the nominal behavior of the satellite. It transmits data from sensors as well as, among others, flight control actuators commands. This kind of traffic, often described as time critical traffic, requires bounded latency and low jitter communications. However, due to the small size and small volume of messages, a low data rate is enough to achieve the platform needs.

On the other hand, the payload network might require a very high data rate in order to convey the huge amount of raw data generated by the payload instruments such as pictures from optical instrument, TMs from a weather sensor or IoT (Internet of Things) data. However, the constraints are less stringent for a payload network as it is more demanding in term of maximum observed delay and far more robust to jittery deliveries.

These two networks are linked with each other through the On-Board Computer (OBC). The payload network is generally supported by SpaceWire, or custom point to point connection while the platform network is generally supported by a MIL-STD-1553B bus or CAN bus. The OBC plays the role of platform bus controller.

In both networks, links are duplicated (one nominal, one redundant) for guaranteed availability. Terminal Devices in these networks are duplicated, working in a hot/warm or cold redundancy depending on the mission needs and constraints.

Each OBC must be able to reach nominal and redundant devices (cross-strapping), this means that there should be at least a path to the nominal equipment and a path to the redundant equipment from the OBC.

Most legacy sensors are behind a gateway for the end station in the 1553-bus that is interrogated by the OBC in order to get sensor information and control the satellite’s actuators.

Mixed cold/warm/hot redundancy schemes can coexist, and this scheme is mission dependent, however equipments most often operate in cold redundancy.

The usual data rate for these networks is 10kbits/s for the platform and 100-200Mbits/s for the payload.

For the future satellite architecture, one could envision there would be only one network, bearing the traffic of both platform and payload devices.

The topology introduced hereafter is one of the possible topologies identified so far with switch (s) dedicated to the platform devices and switch (s) dedicated to the payload devices.

The switches would be duplicated (for availability purposes) so that there would be a nominal and a backup switch on both sides (platform & payload). Eventually, a cross strapping between nominal platform switch & backup payload switch and nominal payload & backup platform could be introduced. The payload switch may also be increased in size (number of ports) depending on the number of Payload Instruments

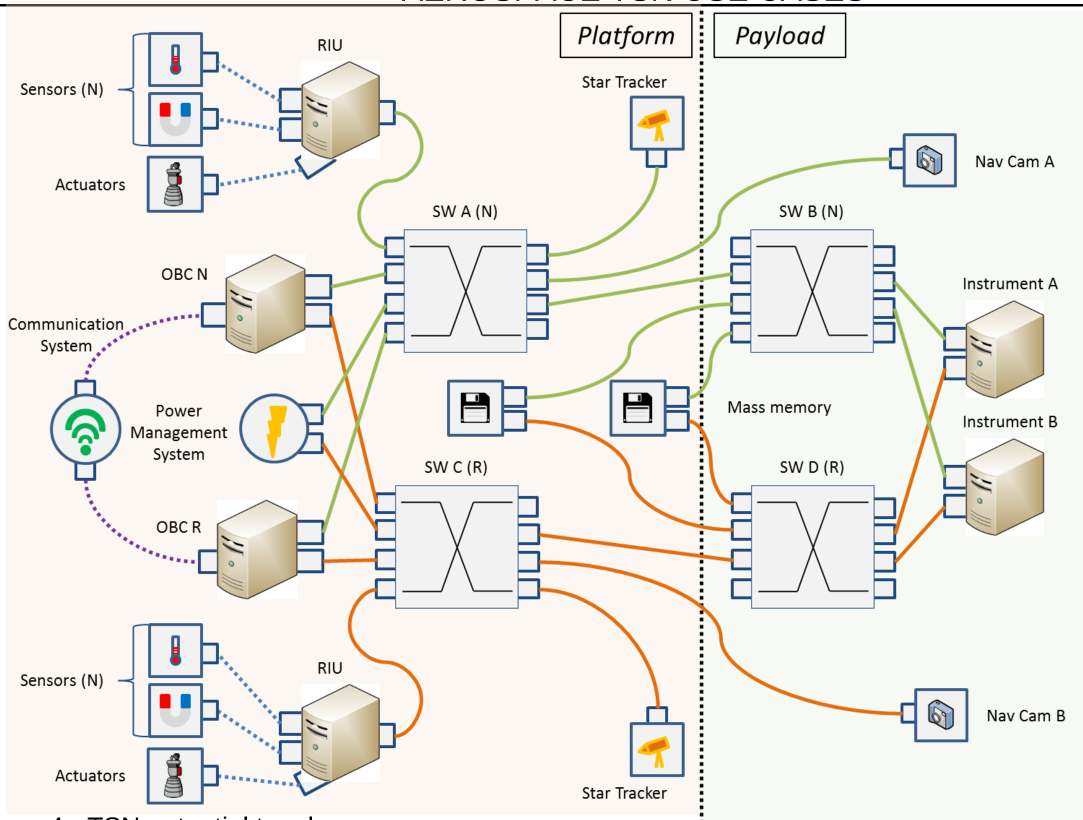

Figure 4 - TSN potential topology

Time Distribution/Synchronization service: In space domain, the time management function maintains the satellite on-board time (OBT), which is used on the space to ground interface for time stamping TM packets or scheduling time-tagged TC.

The OBT is given by the master spacecraft elapsed time (SCET) counter of the OBC SCTM module. This SCET is reset only at OBC power on and is generated by the OBC master clock (or RTC). This master clock is used to generate synchronization pulses to on-board units (e.g. 1Hz, 4Hz, 8Hz or 16 Hz external signal depending on the mission) or to the CSW (1Hz signal called internal PPS or 16Hz interrupt also depending on the mission). This clock can be synchronized with the GPS 1Hz pulse (PPS).

Synchronisation with GPS PPS is often used on-board in a lot of missions. The difference between the date of the GPS and internal PPS is evaluated periodically by the CSW to adjust both RTC clocks and achieve the synchronization of both PPS. The synchronization of the OBC internal PPS with the GPS one is achieved with accuracy better than 1µs. The smooth synchronization process is still performed every second to keep the difference between both PPS under the targeted threshold. If the error becomes greater than this threshold or if the GPS pulse is lost, the CSW autonomously comes back to a “research for synchronisation” state.

The targeted time distribution precision is in the sub microsecond range, as it is deemed reachable with PTP like protocols on top of simple local 100 Mbps network.

The network solution shall also provide hardware support to timestamp received packets at hardware level, and potentially timestamp sent packet as well for observability purpose.

Fault Detection Isolation and Recovery Aspects: Fault Detection Isolation and Recovery Aspects (FDIR) at network level covers the following topics:

- Management of cold/warm/hot redundancy and reconfiguration at unit/interface level
- Detection of nodes misbehaviour such as “babbling idiot”, causing an excessive packet rate to the Processor Module, and associated mitigation measures, which most likely imply traffic policing at switch level
- To provide to the Processor Module report of every error detected (and potentially recovered) locally at network E/S and switch level.

- To provide requirements on E/S failure groups, i.e. for terminals that are not cross-strapped to the switch, which combinations of those terminals may be reconfigured in case of a switch single-point failure affecting interface to those terminals.
- To provide failure recovery strategy at switch level.
- To provide protection against network communications against packet loss, at least for critical data.
- To provide isolation means, detecting and mitigating impersonation whether intentional (security) or due to a malfunction

In case of failure the reporting mode can be either through:

- an immediate failure status dispatch mechanism
- a continuous monitoring based on confirmation, thresholds, and predefined metrics and statistics computation.

It is expected the TSN based technology to provide such metrics through an Ethernet MIB or equivalent that can be collected at OBC level.

Topology Characteristic	Present / Today (TBD even if is not TSN!)	Projected or Desired (if known)
Number of nodes	5-30	5-50
Physical topology	Master/slave Bus, point-to-point, star.	Star (hierarchical)
Number of switched hops	1-2	1-2
Number of streams per switch		100-500
Network Redundancy	Hot active redundant failover Full system level redundancy (dual)	Mandatory for reliability/availability
Redundancy Mode	Hot/warm or cold redundancy depending on the mission needs and constraints	Cold and/or Hot
Data Rate	10kbits/s for the platform; 100-200Mbits/s for the payload	200 Mbps 1 Gbps
Media	Copper	Copper Fiber Optic
Worst case link utilization		>90% (payload)
Dissimilarity, integrity, maintenance, monitoring, security [DIMMS]	Monitoring	Essentially driven by reliability and availability
Certification Requirements	ECSS level B	
Supported Traffic Types		

Certification aspects: For the most stringent missions such as earth observation or science/exploration, the hardware architecture should support compliance demonstration vs ESA standards: ECSS-E-ST-20C and ECSS-Q-ST-60-02C for Hardware qualification, ECSS-Q-ST-80C for Development tools and ECSS-Q-ST-80 & ECSS-Q-ST-40 for Software Qualification. Satellites platform systems are usually qualified up to ECSS level B.

Comment: Compliance to ESA SAVOIR OSRA & OSRA-NET guidelines are also envisioned. This could imply to find a way to involve ESA, CNES, DLR and main European actors such as GMV in the loop of this standardization activity.

3.1.12 Fibre Channel over TSN backbone (AS6509)

This section presents the use case of Fibre channel systems connected via a TSN-profile defined backbone network.

Fibre Channel (as defined in FC-AE an other ANSI INCITS standards) is currently used in various military/aerospace platforms including F/A-18E/F, F-16, F-35, E-2D, AH-64, various radar systems, and numerous others. Applications for

Fibre Channel include data storage, video processing, sensor data, mission computers, DSP clusters, and serial backplanes. These applications share a common need for a high performance localized network between compute resources and high bandwidth I/O sources and sinks. Fibre Channel, with its streamlined data transport framework, served as an attractive networking solution for these applications.

In 2008 the SAE AS-1A2 task group extended the use of Fibre Channel in military systems with the release of the AS5653 High Speed Network for MIL-STD-1760 Aerospace Standard. AS5653 defines the characteristics and requirements for a high speed network interface incoporated within a MIL-STD-1760 interface connector (i.e. the standardized connector between aircraft and stores) thus extending the use of Fibre Channel to include high speed communication with aircraft stores.

While a large number of current systems utilize Fibre Channel, TSN is emerging as an attractive networking solution for future systems. TSN provides a number of enhancements over legacy networks, especially with regard to determinism, redundancy, security and scalability. Future systems are envisioned to have a combination of data communication technologies including Fibre Channel and TSN (as well as others).

This use case describes a system that includes multiple networking domains interconnected with a TSN backbone and focuses specifically on the interconnection of Fibre Channel based systems through the TSN backbone (see Figure 5). The goal of the TSN backbone is provide seamless end to end communication between Fibre Channel based systems, consisting various combinations of Fibre Channel switches and nodes. The envisioned architecture will utilize a Fibre Channel to TSN Gateway to transition between the Fibre Channel and TSN domains.

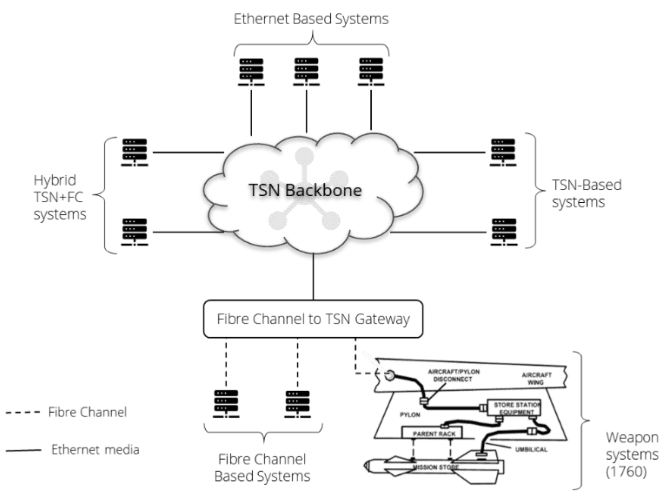

Figure 5 Fibre Channel over TSN Backbone

The Fibre Channel based systems may include legacy equipment (such as data storage, sensors, displays, DSP processors, etc) as well as interfaces to next generation stores (via a high speed 1760 interface). The architecture includes an option for hybrid systems that include a mixture of TSN and Fibre Channel (i.e. Ethernet end systems that implement Fibre Channel upper layer protocols and communicate with other Fibre Channel based systems).

The network architecture of the envisioned systems will utilize TSN to interconnect Fibre Channel elements in place of physical Fibre Channel links (i.e. physical links within a Fibre Channel network will be replaced by virtual links through the TSN network). The goal of the virtual links is to provide connectivity between fibre channel elements without modifying the Fibre Channel or TSN protocols.

Virtual links, in conjunction with gateways, can be used to provide connections trhough a TSN networok between:

1) A Fibre Channel switch port and another Fibre Channel switch port A (i.e. an E-Port to an E-Port).

2) A Fibre Channel switch port and a Fibre Channel node port (i.e. an F-port and an N-port).

3) A Fibre Channel switch port and a Fibre Channel protocol stack on a TSN end point (i.e. an F-port to a virtual N-port).

4) A Fibre Channel node port and another Fibre Channel node port (i.e. an N-port and an N-port).

5) A Fibre Channel node port and a Fibre Channel protocol stack on a TSN end point (i.e. an N-port and a virtual N-port).

6) A Fibre Channel protocol stack on a TSN end point and a Fibre Channel protocol stack on a TSN end point (i.e. a virtual N-port to a virtual N-port).

Topology Characteristic	Present / Today	Projected or Desired (if known)
Number of nodes	10 to 50	10-500 (as legacy boxes become Eth/TSN boxes)
Physical topology	Hub and spoke, Point to Point	TBD as more switching gets distributed
Number of switched hops	0-2	TBD
Max number of flows/streams per switch	10-500	
Network Redundancy	Redundant networks, system level redundancy	
Redundancy Mode	Hot active with voting, standby redundant	
Data Rates	1-2 Gbps links between Fibre Channel elements (switches and nodes)	>1 Gbps will be required
Media	Copper (shielded twisted pair and coax), Fiber Optic	Preference to stick to copper for serviceability. Fiber only if absolutely necessary
Worst Case Link Utilization	<50% but can go above 90%	
Dissimilarity, integrity, maintenance, security [DIMS]	No Dissimilarity requirement; SNMP based fault and status information;	Security is a consideration;
Certification Requirements		
Supported Traffic Types		

The number of TSN gateway nodes/virtual links will vary based on the number of nodes in the Fibre Channel network and how the TSN backbone is used to interconnect those nodes. It is envisioned that the Fibre Channel fabrics could be partitioned based on function with the TSN backbone providing connectivity between partitions.

Examples: large commercial aircraft, Gen 5 military aircraft, etc

3.1.13 Summary of Use Cases

[TODO] Fill out this section at the end

Perhaps have a summary table of the use cases

Topology Characteristic	Lower Bound	Upper Bound	Use Case Driving the Bounds
Number of nodes			
Physical topology	2	500	
Number of switched hops			

Max number of flows/streams per switch		5000	
Network Redundancy			
Redundancy Mode			
Data Rates	10 Mbps	100 Gbps	
Media			
Worst Case Link Utilization			
Dissimilarity, integrity, maintenance, security [DIMS]			
Certification Requirements			
Supported Traffic Types			

4. AEROSPACE TRAFFIC TYPES

4.1 Traffic Definitions

[TODO] Fill this section

This document uses the table x to define the characteristics of each data flow in an aerospace on-board communication network.

Convert traffic classification xlsx file into words and tables

NOTE: We should address future bandwidth intensive traffic types in this section…beyond what we captured in the excel sheet. As an example, 10 4K video feeds, etc

5. AEROSPACE TSN REQUIREMENTS

5.1 Interoperability and Interconnection

These requirements are based on UC10 (refers to interoperability with legacy fiber channel systems)

R1	Interoperability and Interconnection
R1.1	Bridges and End Stations shall be interoperable
R1.2	The TSN Aerospace Profile (TSN-AP) shall be media independent.
R1.3	TSN-AP shall be compatible with higher link (>10Gbps) speeds
R1.4	TSN-AP shall support MPDU of 2200 Bytes
R1.5	TSN-AP shall support COTS <-> COTS communication with TSN traffic shaping
R1.6	TSN-AP should support COTS<-> TSN communication with TSN traffic shaping
R1.7	TSN-AP should support TSN<->COTS communication with all TSN features (shaping and frer);
R1.8	TSN-AP should support Unidirectional devices to communicate with COTS or TSN devices .
R1.9	TSN-AP shall support heterogenous/mixed link speeds in the network (10 Mbps to >10Gbps)

5.2 Aerospace Mode of Operations

R2	Aerospace Mode of Operations
R2.1	TSN-AP shall support an engineered/pre-configured network/devices
R2.2	TSN-AP should support Best Effort Ethernet Device connectivity without pre-configuration
R2.3	
R2.4	
R2.5	
R2.6	
R2.7	
R2.8	
R2.9	

Notes:

R2.1 is a type of “Plug and play” in this context wherein no stream reservation and TSN configuration is needed prior to connecting and operating an ethernet device on the network. In other words, the network behaves like a traditional/cots ethernet LAN for best effort devices

5.3 Configuration Requirements

R3	Configuration Requirements
R3.1	
R3.2	
R3.3	
R3.4	
R3.5	
R3.6	
R3.7	
R3.8	
R3.9	

5.4 Network Availability Requirements

R4	Network Availability Requirements
R4.1	TSN-AP shall support interface redundancy at end stations
R4.2	TSN-AP shall support frame redundancy
R4.3	TSN-AP shall support A-B network redundancy
R4.4	TSN-AP shall support seamless (hot-active) and switchover (hot-standby) redundancy
R4.5	
R4.6	
R4.7	
R4.8	
R4.9	

5.5 General Bridge 802.1Q requirements

R5	General Bridge 802.1Q requirements
R5.1	TSN-AP should support one-way Ethernet links. Implies no auto negotiation
R5.2	TSN-AP shall have 8 or more egress queues per port on aggregation bridges
R5.3	TSN-AP shall have 2 or more egress queues per port on constrained bridges (e.g. bridged end stations)
R5.4	
R5.5	
R5.6	
R5.7	
R5.8	
R5.9	

5.6 Time Synchronization Requirements

R6	Time Synchronization Requirements
R6.1	TSN-AP shall use preconfigured time distribution trees and grandmaster selection
R6.2	TSN-AP shall enable a network time synchronization error of less than 100 nsec over 3 hops
R6.3	TSN-AP shall enable a end-to-end data jitter of less than 1 usec over 3 hops
R6.4	
R6.5	
R6.6	
R6.7	
R6.8	
R6.9	

5.7 Traffic Shaping Requirements

R7	Traffic Shaping Requirements
R7.1	TSN-AP shall support time aware shaper (Qbv)
R7.2	TSN-AP shall support non-time aware traffic shapers (Qav, Qcr)
R7.3	
R7.4	
R7.5	
R7.6	
R7.7	
R7.8	
R7.9	

5.8 Filtering and Policing Requirements

R8	Filtering and Policing Requirements
R8.1	TSN-AP shall support 802.1Qci (PSPF)
R8.2	TSN-AP shall support policing of up to 4096 streams per aggregation bridge
R8.3	
R8.4	
R8.5	
R8.6	

R8.7	
R8.8	
R8.9	

5.9 Other Requirements That Were Considered

a.They only communicate with like-devices in the network and expect non-TSN treatment (no impact)

b.They only communicate with like-devices in the network and expect TSN treatment (some impact on one or more of stream identification, Qbv shaping, Policing, and forwarding on the bridge). Like-devices means no FRER.

c.They communicate with TSN-devices in the network (impact on one or more of stream identification, Qbv shaping, Policing, and forwarding on the bridge, FRER)

Envisioned features subset – To be moved Elsewhere

The table below summarizes the currently targeted sub-standards and the rationale for it

Ref.	Name	Target	Rationale
IEEE 802.1AS	Timing and Synchronization	mandatory	Time distribution and synchronization & FDIR
IEEE 802.1Qci	Per-Stream Filtering and Policing	mandatory	Policing + QoS management at Layer 2
IEEE 802.1CB	Frame Replication and Elimination (FRER)	mandatory	Availability of the network and the system (RAMS)
IEEE 802.1 Qbv	Scheduled Traffic	mandatory	For scheduled traffic, TBC
IEEE 802.1Qav	Credit Based Shaper	mandatory	For Quality of Service
IEEE 802.1 Qcc	Time Sensitive Network Configuration	mandatory	Static configuration part is mandatory
IEEE 802.1Qbu & IEEE 802.3br	Frame Preemption	TBD	Not necessary for 1Gbits/s
IEEE 802.1Qch	Cyclic Queuing and Forwarding	TBD	(It is actually a combination of other standards)
IEEE 802.1 Qat & IEEE 802.1 Qcc	*Stream Reservation Protocol Stream Reservation Protocol Enhancement*	*not requested*	*Dynamic (re)configuration hence not targeted for now*
IEEE 802.1 Qca	*Path Control*	*not requested*	*Dynamic (re)configuration hence not targeted for now*
IEEE 802.1 Qcc	*Stream Reservation Protocol Enhancement*	*not requested*	*Dynamic (re)configuration hence not targeted for now*

Comment: The profile shall also focus on keeping the functional scope compliant with an implementation in state of the art rad hard/tolerant FPGAs…