

# 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

1

## 2 CONTRIBUTOR GROUP

3

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

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

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

7 Jabbar, Abdul <jabbar@ge.com>

8 Lawton, Grant <glawton@wlgore.com>

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

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

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

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

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

14

15

16

17

18

19

## TABLE OF CONTENTS

20		
21	1. Scope .....	3
22	1.1 Definitions.....	3
23	1.2 Symbols and Abbreviations.....	3
24	1.2.1 Symbols.....	3
25	1.2.2 Abbreviations.....	3
26	2. Introduction to Aerospace networks .....	3
27	2.1 Current Network Architecture.....	3
28	2.2 Considerations for Future TSN based network architecture .....	4
29	2.3 Time Synchronization in Aerospace.....	7
30	3. Aerospace Use Cases .....	8
31	3.1.1 General.....	8
32	3.1.2 Small Business Aircraft .....	10
33	3.1.3 Large Passenger Aircraft .....	11
34	3.1.4 Large Passenger Aircraft (Cabin).....	13
35	3.1.5 Small and Combat Military Mission Network.....	15
36	3.1.6 Large Military Aircraft Mission Network.....	16
37	3.1.7 Small, Combat, and Large Military Flight Network (VMS).....	17
38	3.1.8 Unmanned Military Aircraft Network.....	19
39	3.1.9 Rotary Wing Mission Network .....	20
40	3.1.10 Rotary Wing Flight Network .....	21
41	3.1.11 Satellite Network .....	22
42	3.1.12 Fibre Channel over TSN backbone (AS6509) .....	25
43	3.1.13 Summary of Use Cases .....	27
44	4. Aerospace Traffic Types .....	28
45	4.1 Traffic Definitions.....	28
46	5. Aerospace TSN Requirements .....	28
47	5.1 Interoperability and Interconnection .....	28
48	5.2 Aerospace Mode of Operations .....	29
49	5.3 Configuration Requirements .....	29
50	5.4 Network Availability Requirements.....	29
51	5.5 General Bridge 802.1Q requirements .....	30
52	5.6 Time Synchronization Requirements .....	30
53	5.7 Traffic Shaping Requirements.....	30
54	5.8 Filtering and Policing Requirements .....	30
55	5.9 Other Requirements That Were Considered .....	31
56		
57		
58		

## 1. SCOPE

This document captures aerospace network use cases that may potentially use TSN profile. It includes use cases for both commercial 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.

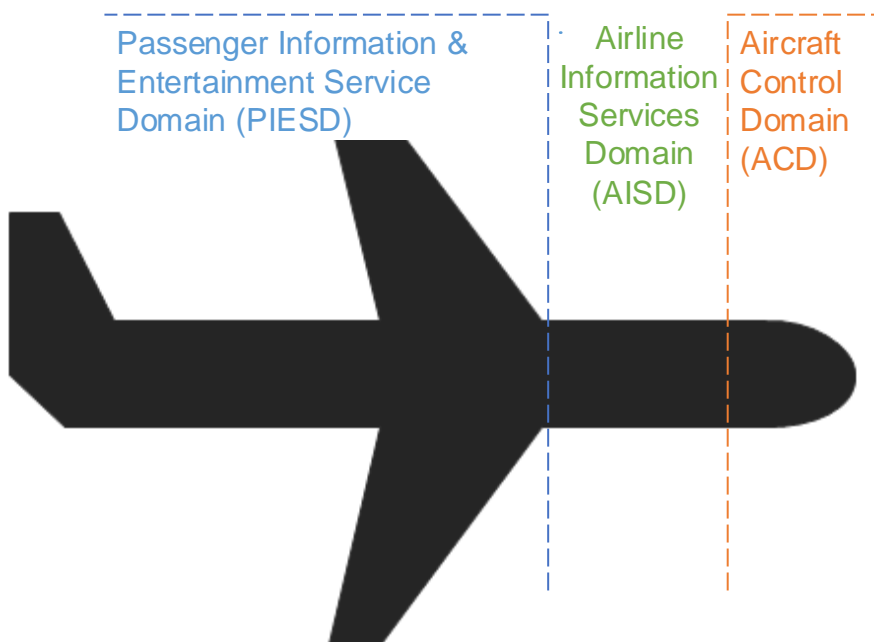


Figure 1: Commercial Aircraft Network Domains

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

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

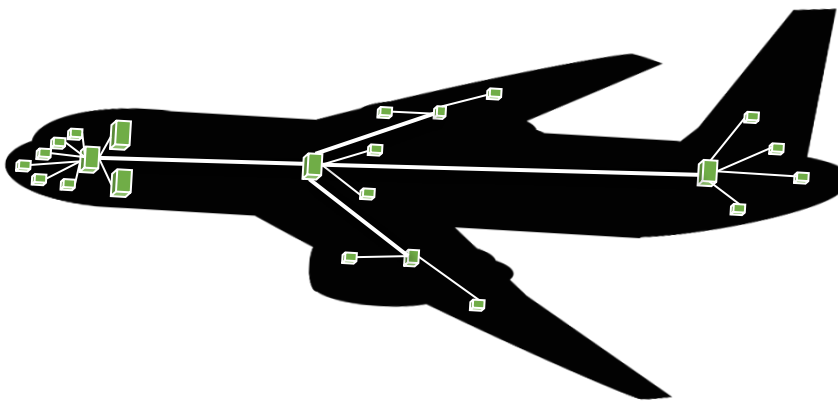


Figure 2: Commercial Integrated Modular Avionics Depiction

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

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

## 102 Military Aircraft

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

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

## 110 2.2 Considerations for Future TSN based network architecture

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

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

114 Technical Performance requirements vs. certification requirements.

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

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

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

- 183 ○ Benefit when design has legacy retrofit potential
- 184 ○ Growth path for increased medium speeds
- 185 ● Security Resilience
  - 186 ○ Network must not preclude security features common in modern infrastructure network communications,  
187 or new technologies built upon standard Ethernet packet formats.
  - 188 ○ Provision or support of mechanisms to segregate different networks (with different security  
189 levels/requirements) from each other

190

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

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

198 5. Cost (see notes in Objectives list above)

199 6.Key dealbreakers for this network.

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

202 Complexity (configuration and jeopardizes certifiability)

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

204 Interoperability between vendors and tools is key.

205 2.3 Time Synchronization in Aerospace

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

- 207 ● Local/Working clock [Note that these can be met with a globally synchronized as well]
    - 208 ○ Age of data to validate data transport Integrity
    - 209 ○ Latency Reduction
    - 210 ○ Age of data for sensor age
    - 211 ○ Synchronization of the Arinc 653 partition scheduler and partition
    - 212 ○ Fault Correlation (time stamp in logs)
    - 213 ○ Flight data recorder for data/event recording
    - 214 ○ Security (key rotation, cybersecurity attack logs)
  - 215 ● Universal/Global Clock
    - 216 ○ Database applicability (Do I have the latest database)
    - 217 ○ Navigation (adhering to flight plan) FMS must be synchronized to GPS time
    - 218 ○ Flight data recorder general date and time
    - 219 ○ Security (cert validation, cybersecurity attack logs)
- 220

221 **How is time synchronization done today?**

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

224 Network Time Synchronizaion

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

227 Out of band synchronization – discrete lines (1PPS, IRIG-B)

228 Number of different/isolated synchronization for subsystems

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

230

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

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

235 - Clearly benefit for 802.1 AS like network time synchronization

236 - Particular interest in distributing global time (GPS)

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

238 **Integrity, availability of time synchronization**

239 Aerospace primarily concern with time synchronization is fault tolerance.

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

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

244

245 **3. AEROSPACE USE CASES**

246 **3.1.1 General**

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

255 **[TODO] Add a row to each use case on certification requirement**

256 **[TODO] Add a row to each use case on supported traffic types**

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

258



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 maximum 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 topologies 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 stream requires three functions by the bridge: stream identification, stream policing, and stream shaping. These functions serve 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 or more redundancy architectures may be specified
Redundancy Mode	Denotes the mode of redundancy. Options include standby, active, hot-active, active-active with voting  One or more modes may be specified.
Data Rate	Denotes the data rate(s) of the physical 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 worst 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	Specify if it is Mandatory, Desired, Do Not Care.
Supported Traffic Types	Listing of Traffic Types from section 4 that exist in this use case

259

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

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

267

268 3.1.2 Small Business Aircraft

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

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

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

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

283

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

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

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

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

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

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

303

### 304 3.1.3 Large Passenger Aircraft

305 1-2: Large Passenger Aircraft use case is roughly defined as aircraft carrying 100 passengers or more in a commercial  
306 airline operation. Examples of this use case in aerospace industry would be AirbusA220, Boeing 787, Airbus  
307 A350, Boeing 777x, etc.[reference]

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

### 327 3.1.4 Large Passenger Aircraft (Cabin)

328 [1-2]: This use-case belongs to the same type of Aircraft as the one before, carrying more than 100 passengers. However,  
 329 there are significant differences between cabin networks and avionics networks, which justify a separation within this  
 330 document:

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

348 Dedicated examples of cabin use-cases:

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

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

364 [3]: Due to the stretched geometry of aircraft cabins, cabin networks often consist of daisy-chained switches in the cabin,  
 365 connected to central servers in the electronics bay of the Aircraft. Each switch may connect to end-devices or to further

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

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

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

374 Today, only the Cabin Management System provides redundancy in terms of a second server operating in hot standby.  
 375 (tbd: IFE?). In addition, the Cabin Management System's Network architecture provides some redundancy: more clients  
 376 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.  
 377 one daisy-chain), the relevant functions can still be served by the remaining chains and clients, respectively.

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

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

386

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: <ul style="list-style-type: none"> <li>- Two servers</li> <li>- 2-4 independent network lines in the cabin, each serving the same functions</li> </ul>	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

387

388 3.1.5 Small and Combat Military Mission Network

389 Combat Military Aircraft mission network are constrained by SWaP availability. Instead major constraints would come from  
390 interoperability and flexibility to be able to interface with legacy and current systems, and scalability to modifications.  
391 Combat Military Aircraft mission networks are purpose built for specific operational needs.

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

395  
396 DO-178/DO-254 style safety certification does not generally apply to combat military aircraft networks, although it is  
397 becoming more relevant.  
398

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; <b>Redundancy dependent on data transport tech.</b>	
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. <b>Dissimilarity: HW dissimilarity, SW dissimilarity?</b>	

	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)	

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

402  
403 Certification of compact Military Aircraft mission networks are typically dependent on their acquisition authority, the safety  
404 criticality level associated to their functions most typically aligns with that of DO-178/DO-254 Design Assurance Level C to  
405 E, i.e. safety-involved to non-criticality for mission criticality.

406  
407 [Sample text on supported traffic types] Typical scenarios include tens of TT13 type traffic on this platform. Therefore an  
408 aggregate bandwidth or rate of 100 Gbps is needed/required. This scenario only supports three types of traffic – all which  
409 are high bandwidth flows with relaxed latency requirements

410

### 411 3.1.6 Large Military Aircraft Mission Network

412  
413 This use case captures how an SAE AS-6675 based data transport infrastructure satisfies the typical characteristics and  
414 qualities of a large Military Aircraft mission network.

415  
416 Large Military Aircraft mission networks are not constrained by SWaP availability. Instead major constraints would come  
417 from interoperability and flexibility to be able to interface with legacy, and scalability to modifications. Large Military Aircraft  
418 mission networks are purpose built for specific operational needs.

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

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

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

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

428

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 Gbps, 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		

429

430

431

432

433

434

435

436

437

438

439

440

441

442

443

444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

460

461

462

463

464

465

466

467

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 aircraft. 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 significantly 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.

468 Small Military Aircraft flight networks and combat military aircraft flight networks are significantly constrained by SWaP  
 469 availability and are purpose built for specific safety and operational needs. Large aircraft flight networks are not  
 470 constrained in by SWaP availability, but are purpose built for specific safety and operational needs.  
 471 Changes to the flight capability occur infrequently and with very slow pace, about once every two to five years. Overall  
 472 aircraft lifespan is expected to last 50+ years.  
 473 There are small number of sub-systems and limited data transport infrastructure on-board the aircraft. Each sub-system  
 474 has a defined interface and performance requirements for a defined set of messages which instantiate a required  
 475 behavior, all of which must be validated to perform safely and reliably. The flight network composes of periodic and  
 476 aperiodic messages with safety-critical requirements.  
 477 DO-178/DO-254 style safety certification does not generally apply to combat military aircraft networks, although it is  
 478 becoming more relevant.  
 479

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		

480  
 481 Although the absolute number of nodes is not expected to increase significantly, it is expected that more nodes will  
 482 natively adopt the converged AS-6675 network interace to communicate and in doing so the topology moves to a  
 483 traditional switched topology with redundant interfaces for flight systems, utilizing a maximum of 1 switch per aircraft.  
 484 Besides, non-switched topologies are also applicable with similar guarantees for performance and determinism to be  
 485 provided.  
 486  
 487 Militiary flight control network shall support safety-criticality functionalities with strict latency requirements but not  
 488 demanding bandwidth requirements.

489 Periodic and aperiodic messages have to be managed with latency or deadline requirements. Latency requirements shall  
 490 be the range of sub milli seconds-100ms, while bandwidth requirements shall be in the range of 100kbps-100Mbps.  
 491 During the convergence to AS-6675 network, end-to-end latency with non-AS-6675 interfaces cannot be guaranteed.  
 492 Also, interfacing with legacy part of the network shall be developed.  
 493 Military flight control networks shall support for time synchronization.

494  
 495 Availability of the network infrastructure will be actively monitored and faults will be logged for maintenance. The number  
 496 of streams will increase as additional legacy nodes such as aircraft sensors and discrete inputs adopt the converged AS-  
 497 6675 network interface.

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

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

502  
 503 While certification of Military Aircraft flight networks are typically dependent on their acquisition authority, the operational  
 504 performance most typically aligns with that of DO-178/DO-254 Design Assurance Level A to B.

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

### 508 3.1.8 Unmanned Military Aircraft Network

509 **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		
<b>Supported Traffic Types</b>		

## 512 3.1.9 Rotary Wing Mission Network

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

515 A rotary wing aircraft mission network is significantly constrained by space, weight, and power availability, and is purpose  
 516 built for specific operational needs. Therefore, there are a minimum number of sub-systems and limited data transport  
 517 infrastructure on-board the aircraft. Each sub-system has a defined interface and performance requirements for a defined  
 518 set of messages which instantiate a required behavior, all of which must be validated to perform safely and reliably. DO-  
 519 178/DO-254 style safety certification does not generally apply, although it is becoming more prevalent in recent years.  
 520 Changes to the operational capability occur infrequently, with minor updates one to two times per year, and major updates  
 521 about once every five to ten years. Overall aircraft lifespan is expected to last 50 years.

522

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		

523 Given its space, weight, and power constraints, the absolute number of nodes is not expected to increase significantly,  
 524 however, it's expected that more nodes will natively adopt the converged AS6675 network interface to communicate. In  
 525 doing so the topology moves largely to a traditional Ethernet star topology with redundant interfaces for mission critical  
 526 systems, utilizing two or four switches per aircraft. Availability of the network infrastructure will be actively monitored and  
 527 faults will be logged for maintenance. The number of streams will increase as additional legacy nodes such as aircraft  
 528 sensors and discrete inputs adopt the converged AS-6675 network interface. Bandwidth of these streams will increase  
 529 significantly as higher fidelity video and mission sensor data is transmitted over the mission network, driving a need for  
 530 100Gbps and even 1Tbps line rates in the 2030 timeframe. The mission network should support high utilization of this  
 531 bandwidth, with scheduled traffic supporting deterministic behavior at >90% utilization. While today's mission network is a  
 532 mix of various interfaces and media such as MIL-STD-1553 over coaxial cable and ARINC-429 over copper twisted pair,  
 533 the future converged AS-6675 mission network will utilize Ethernet over copper and/or fiber optic cabling.

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

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

### 539 3.1.10 Rotary Wing Flight Network

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

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

550

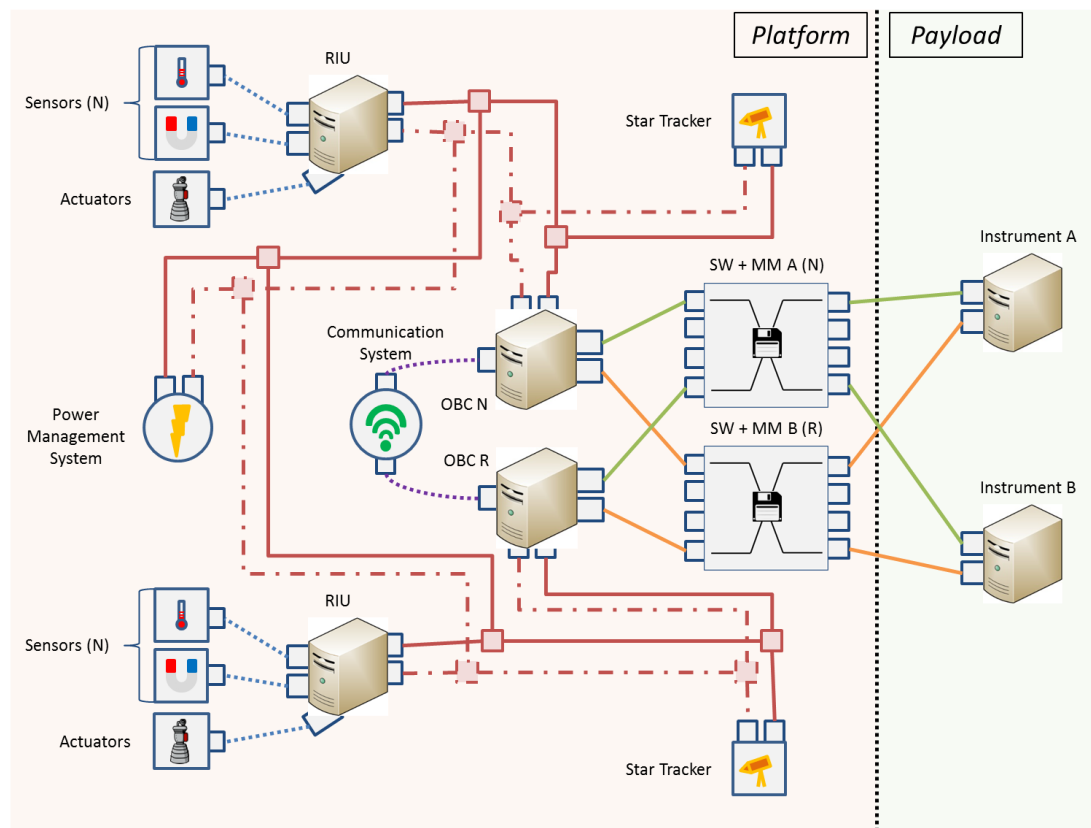
Topology Characteristic	Present / Today	Projected or Desired (if known)
Number of nodes	10-20	10-20
Physical topology	Master/slave Bus; point-to-point	Star
Number of switched hops	0-2	1-2
Number of streams per switch	50-200	Significant increase would come from individual sensors being connected directly (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
<b>Supported Traffic Types</b>		

551 Given its space, weight, and power constraints, and its bounded functionality, the absolute number of nodes on the flight  
 552 network is not expected to increase significantly, however, it's expected that more nodes will natively adopt the converged  
 553 AS6675 network interface to communicate. In doing so the legacy point-to-point and point-to-multipoint topologies move  
 554 largely to a traditional Ethernet star topology with redundant interfaces for guaranteed availability of safety critical data,  
 555 utilizing two or three switches per aircraft for duplex or triplex redundant flight control, respectively. Availability of the  
 556 network infrastructure will be actively monitored, and faults will be logged for maintenance. The number of streams will  
 557 increase as additional legacy nodes such as aircraft sensors, analog inputs, and discrete inputs adopt the converged AS-  
 558 6675 network interface. Bandwidth of these streams will likely remain low, and current ethernet line rates should exceed  
 559 future requirements with relatively low utilization for safety critical needs. Scheduled traffic supporting highly deterministic  
 560 behavior will be used for closed loop systems, such as those impacting flight control surfaces. While today's flight  
 561 network is a mix of various interfaces and media such as RS-422, RS-485 and ARINC-429 over copper twisted pair, the  
 562 future converged AS6675 mission network will utilize Ethernet over copper and/or fiber optic cabling.

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

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

568  
 569 **3.1.11 Satellite Network**



571 *Figure 3 - Current Network Topology*  
 572

573 **Actual network configuration**

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

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

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

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

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

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

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

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

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

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

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

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

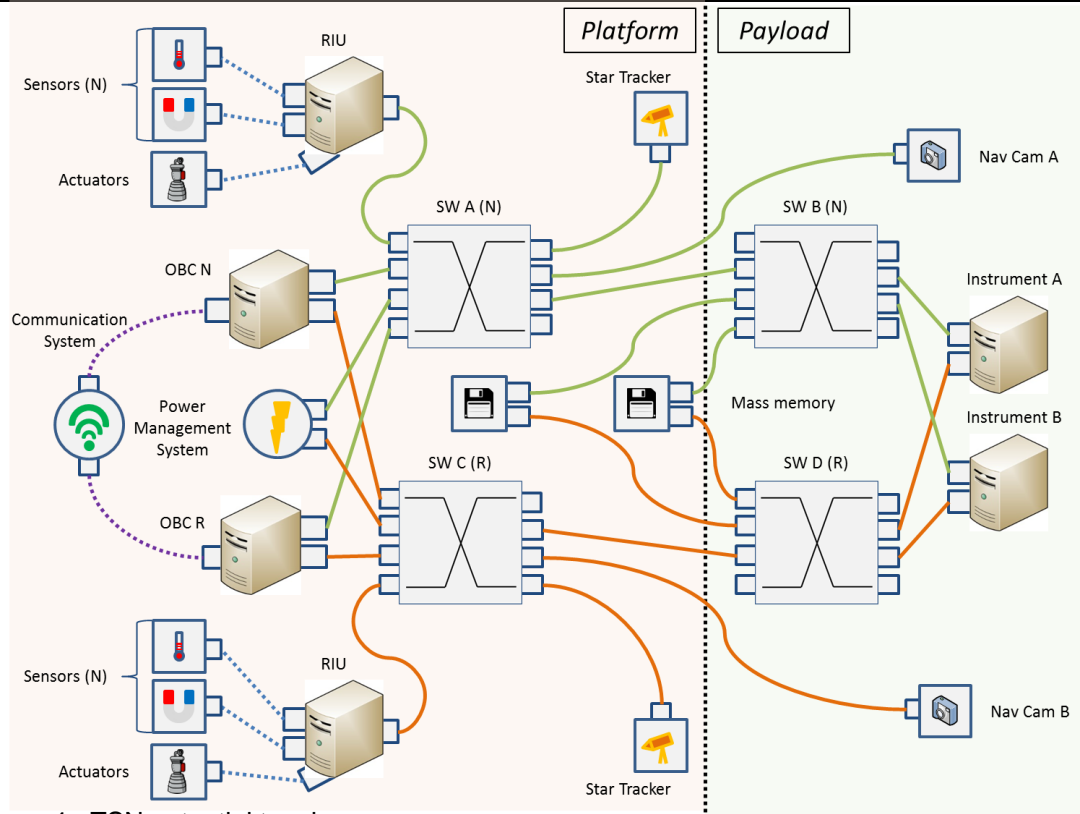


Figure 4 - TSN potential topology

**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  $1\mu\text{s}$ . 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.

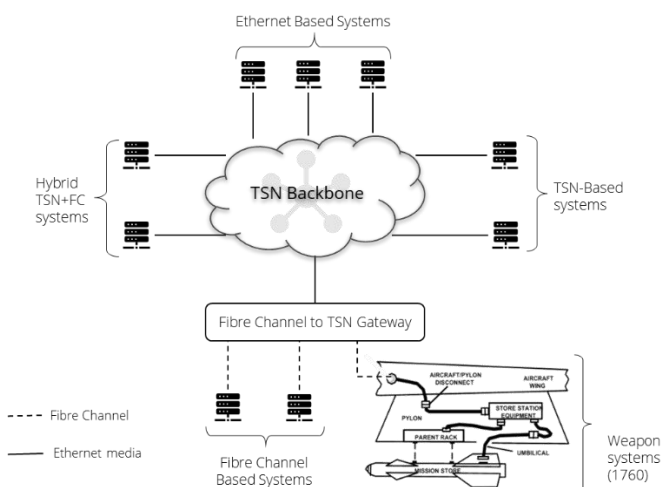
Fibre Channel (as defined in FC-AE an other ANSI INCITS standards) is currently used in various military/aerospace platforms including F/A-18E/F, F-16, F-35, E-2D, AH-64, various radar systems, and numerous others. Applications for

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

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

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

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



670  
 671 *Figure 5 Fibre Channel over TSN Backbone*

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

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

680 Virtual links, in conjunction with gateways, can be used to provide connections through a TSN network between:

- 681 1) A Fibre Channel switch port and another Fibre Channel switch port A (i.e. an E-Port to an E-Port).  
 682 2) A Fibre Channel switch port and a Fibre Channel node port (i.e. an F-port and an N-port).  
 683 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-  
 684 port).

- 685 4) A Fibre Channel node port and another Fibre Channel node port (i.e. an N-port and an N-port).
- 686 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-  
687 port).
- 688 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  
689 virtual N-port to a virtual N-port).  
690

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		

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

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

695 3.1.13 Summary of Use Cases

696 [TODO] Fill out this section at the end

697 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			

698

699 4. AEROSPACE TRAFFIC TYPES

700 4.1 Traffic Definitions

701 **[TODO] Fill this section**

702 This document uses the table x to define the characteristics of each data flow in an aerospace on-board communication network.  
703

704 Convert traffic classification xlsx file into words and tables

705 **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**  
706

707

708 5. AEROSPACE TSN REQUIREMENTS

709 5.1 Interoperability and Interconnection

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

711

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)

712

## 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	

## 727 5.5 General Bridge 802.1Q requirements

## 728 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

## 729 5.6 Time Synchronization Requirements

## 731 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

## 732 5.7 Traffic Shaping Requirements

## 734 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

## 735 5.8 Filtering and Policing Requirements

## 737 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	

738

739 5.9 Other Requirements That Were Considered

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

741 b.They only communicate with like-devices in the network and expect TSN treatment (some impact on one or more of  
742 stream identification, Qbv shaping, Policing, and forwarding on the bridge). Like-devices means no FRER.743 c.They communicate with TSN-devices in the network (impact on one or more of stream identification, Qbv shaping,  
744 Policing, and forwarding on the bridge, FRER)

745

746 Envisioned features subset – To be moved Elsewhere

747

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

749

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

750

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

751

752