International Avionics System Interoperability Standards (IASIS)

Draft C – February 2018

REVISION AND HISTORY

REV.	DESCRIPTION	PUB. DATE
Draft	Initial Release (Reference per SSCD XXXXXX, EFF. XX-XX-XX)	04-18-17
Draft A	Major update for September and Checkpoint Review	09-29-17
Draft B	Update based on NASA internal feedback	10-27-17
Draft C	Update based on Industry feedback	02-09-18

PREFACE

INTERNATIONAL AVIONICS SYSTEM INTEROPERABILITY STANDARDS

This International Avionics System Interoperability Standard establishes a standard interface to enable on-orbit crew operations and joint collaborative endeavors utilizing different spacecraft.

Configuration control of this document is the responsibility of the International Space Station (ISS) Multilateral Coordination Board (MCB), which is comprised of the international partner members of the ISS. The National Aeronautics and Space Administration (NASA) will maintain the IASIS Standard " International Avionics System Interoperability Standards" under Human Exploration and Operations Mission Directorate (HEOMD). Any revisions to this document will be approved by the ISS MCB.

INTERNATIONAL AVIONICS SYSTEM INTEROPERABILITY STANDARDS

CONCURRENCE

FEBRUARY 2018

Associate Administrator Human Exploration and Operations NASA	Date
Executive Director, Human Space Programs State Space Corporation “Roscosmos”	Date
Director of Human Spaceflight and Operations European Space Agency	Date
Director General, Space Exploration Canadian Space Agency	Date
Executive Director Japan Aerospace Exploration Agency	Date

TABLE OF CONTENTS

PARAGRAPH **PAGE**

APPENDIX

TABLE

FIGURE

1.0 INTRODUCTION

This International Avionics System Standard is the result of a collaboration by the International Space Station (ISS) membership to establish, interoperable interfaces, terminology, techniques, and environments to facilitate collaborative endeavors of space exploration in cis-Lunar and deep space environments.

Standards that are established and internationally recognized have been selected where possible to enable commercial solutions and a variety of providers. Increasing commonality while decreasing unique configurations has the potential to reduce the traditional barriers in space exploration: overall mass and volume required to execute a mission. Standardizing interfaces reduces the scope of the development effort and allows more focus on performance instead of form and fit.

The information within this document represents a set of parameters enveloping a broad range of conditions, which if accommodated in the system architecture support greater efficiencies, promote cost savings, and increase the probability of mission success. These standards are not intended to specify system details needed for implementation nor do they dictate design features behind the interface, specific requirements will be defined in unique documents.

1.1 PURPOSE AND SCOPE

The purpose of the International Avionics System Interoperability Standard is to provide basic common design parameters that allow developers to independently design compatible Avionics systems for the Deep Space Gateway and Transport (DSG&T).

This document specifies data link protocols and physical layer options that may be used to architect the interfaces between both spacecraft subsystems and vehicles themselves. Together, these technologies provide the ability to seamlessly integrate the three functional areas (defined in Section 2.6) within and across multiple spacecraft segments. Architectural considerations unrelated to these network interfaces, as well as their application to the functional areas described above, are beyond the scope of this document.

Because of Size, Weight, and Power (SWaP) challenges associated with an Exploration class Human Rated Vehicle, beyond those that already exist for Low Earth Orbit, a Distributed Integrated Modular Avionics (DIMA) Architecture was chosen as the working Avionics design for further development. This architecture allows SWaP benefits through the ability to aggregate functionality with less hardware. An example would be that because the architecture incorporates principles of time-space partitioning, critical and non-critical data can be collocated. This change in architecture selection translates into greater capability with a smaller footprint.

1.2 RESPONSIBILITY AND CHANGE AUTHORITY

Any proposed changes to this standard by the participating partners of this agreement shall be brought forward to the Avionics System Interoperability Standard committee for review.

Configuration control of this document is the responsibility of the International Space Station (ISS) Multilateral Coordination Board (MCB), which is comprised of the international partner members of the ISS. The National Aeronautics and Space Administration (NASA) will maintain the International Avionics System Interoperability Standard under HEOMD Configuration Management. Any revisions to this document will be approved by the ISS MCB.

1.3 PRECEDENCE

This paragraph describes the hierarchy of document authority and identifies the document(s) that take precedence in the event of a conflict between content. Applicable documents include requirements that must be met. If a value in an applicable document conflicts with a value here, then a conflict shall be resolved by the MCB or other applicable board identified or delegated.

Reference documents are either published research representing a specific point in time, or a document meant to guide work that does not have the full authority of an Applicable document. If a value in this document conflicts with a value in a referenced document, then it should be assumed that the value here was deliberately changed based on new data or a special constraint for the missions discussed.

2.0 DOCUMENTS

2.1 APPLICABLE DOCUMENTS

The following documents include specifications, models, standards, guidelines, handbooks, and other special publications. Applicable documents are levied by programs with authority to control system design or operations. The documents listed in this paragraph are applicable to the extent specified herein. Inclusion of applicable documents herein does not in any way supersede the order of precedence identified in Section 1.3 of this document.

IEEE 802.3ab	1000BASE-T Gbit/s Ethernet over twisted pair at 1 Gbit/s
SAE AS6802	Time-triggered Ethernet
ARINC 664-p7	Avionics Full-Duplex Switched Ethernet

2.2 REFERENCE DOCUMENTS

The following documents contain supplemental information to guide the user in the application of this document. These reference documents may or may not be specifically cited within the text of this document.

NASA/TM-2008-215108	A Primer on Architectural Level Fault Tolerance

2.3 INTERNATIONAL AVIONICS SYSTEM INTEROPERABILITY STANDARDS

2.4 GENERAL

The goal of establishing standards and agreeing on other assumptions is to maximize the success of future human spaceflight missions conducted as international partnerships. The ability of components, systems, or vehicles delivered from multiple sources to work together as an effective system is important to the success of actual missions. Good collaboration can make technology development and system maturation more efficient, by sharing the lessons learned and failures that drive requirements. Using standard assumptions can also make development more efficient by making tests conducted by one partner relevant and valid to multiple partners.

This document is focused on issues that drive system performance so much that they could rule out some technologies, and on issues that most directly affect interoperability between partner systems. Thought was given to coming up with a Network that was flexible and accommodating enough to include other entities and commercial providers as part of the DSG development effort, although care will need to be taken in designing and balancing bandwidth in support of time triggered, rate constrained, and best effort traffic on the network. Currently, this document is focused on how a Deep Space Gateway Inter-Element Network allows communications between potential Element providers to assist in an Integrated Avionics architecture that allows for the incorporation of desirable attributes associated with a more open architecture.

2.4.1 LEVERAGED STANDARDS

Currently, this standard document cites only existing data link standards (protocols), from which an interoperable spacecraft onboard communications system should be developed. The current approach is reflective of an agreed upon Avionics architecture currently employed by large commercial airline manufacturers and their suppliers. This approach allows for a homogenous network – where mating vehicles use the same protocol(s) for communication. A heterogeneous network – where mating vehicles use different protocols bridged via a protocol translator or other specialized device is a technical possibility that can't be precluded, but comes with penalties and associated tradeoffs that would need to be addressed. This is already expected to occur for Orion due to some differences in supporting data protocols and network selection (1000BaseCx vs. 1000BaseT). 1000BaseT is currently planned for the docking interface as well as the backbone network for DSG. Because Visiting Vehicles will need to interface with multiple DSG Elements as part of the build process, the expectation is that these vehicles will address the media and data converter aspects, when needed, so that the DSG elements can interact using CCSDS protocols and 1000BaseT and avoid/minimize point solutions for interactions between Visiting Vehicles and the various elements when they are mated. Deviation from the current approach should ideally be avoided because of the impacts to the overall architecture construct such as byzantine faults approach and realizing an overall fault tolerant construct that are part of a successful DIMA approach. The current International Docking System Standard (IDSS) accommodates the incorporation of Ethernet (IEEE 802.3), which is the backbone for critical and non-critical data transfer between docked Elements. The assumption is that all mated or docked vehicles and robotic interfaces will use this standard when designing their network interface to the Elements.

Standardization for external attachment points in support of science have not been currently addressed and may be an item that is determined at the Element level, but an Ethernet connection provides a viable option.

For additional revisions of this standard, it is expected that the list of data link standards cited in this document will be augmented by citing standards defining supplementary higher level communication services, which may not be defined for all individual data link protocols. Examples of such services may be those defined by CCSDS in the Spacecraft Onboard Interface Services (SOIS) area. This area is comprised of three groups: 1) the Wireless working group, 2) the Subnetwork working group, and 3) the Application Support working group.

The purpose of these services is to provide potential missing functionality and thus complete the layers in the communication stack needed to support the implementation of a common avionics framework. These layers provide different levels of abstraction from the data link to the application software in order to enable the integration of both hardware and software components related to the onboard communication system.

Together, the existing data link and future communication service standards will provide a layered communication framework upon which interoperable avionics systems may be developed. The lowest layers are currently described by the physical and data link standards referenced by this document. As additional architectural details emerge, higher level communication services will also be specified. For these reasons, this should be considered a living document until such time that the design matures. As the effort progresses, information captured and agreed upon in Section 5.0 Future Topics for Possible Standardization for further inclusion/development will be moved into Section 3.

2.4.2 ENGINEERING UNITS OF MEASURE

Engineering units, where applicable, will be in SI units (metric).

2.5 INTERFACES

There are numerous drivers that will ultimately decide the final human exploration class spacecraft architecture along with the actual networks and data link protocols that support this architecture. The focus of this standard is to allow communication between the various elements. Two aspects will be largely considered as a consequence; hardlined communications between Elements via the International Docking System and hardlined communications to the Elements via Robotic grapple fixtures. If the Robotic arm is to move between DSG Elements, Robotic Grapple fixtures will want to be common between the elements, utilizing common data protocols among those fixtures.

There are other datalink protocols and conversions that are expected to take place within a given Element. Although trade studies will eventually be deployed to identify and execute trade-offs among requirements, design, schedule, and cost, there exist common functions for human rated spacecraft that any network architecture will eventually need to accommodate. These tradeoffs will need to be assessed as part of the development effort in association with the following primary functional areas; vehicle command and control, crew interfaces and science, and specialty interfaces. This Standard makes no attempt to currently address what those intra-element datalink selection and tradeoffs are and is beyond the current scope for interoperability between the various elements addressed by this standard.

2.5.1 INTERFACE STANDARDS

The intent of the current draft is to address the device-to-device data link protocols (box-to-box) that may be utilized through both the International Docking System as well as the Robotic attachment points. Data links within devices (historically bussed backplanes but now evolving into serial backplanes) will not be addressed here and may be addressed for future considerations.

2.6 PERFORMANCE AND FUNCTIONAL AREAS

Historically, human rated spacecraft have had to address the functional areas of vehicle command and control, crew interfaces and science, and specialty interfaces. The following sections will discuss consideration of those areas. Although it is not the intent of this document to address all the decisions and tradeoffs associated with the actual implementation within the Elements that will comprise DSG, the intent is to show considerations within Elements that will need to be addressed and that the current DSG Inter-Element Network provides a foundation in which they can be addressed. An example of how the various functional areas will need to interact and consider different vehicle needs is provided below in Figure 1.

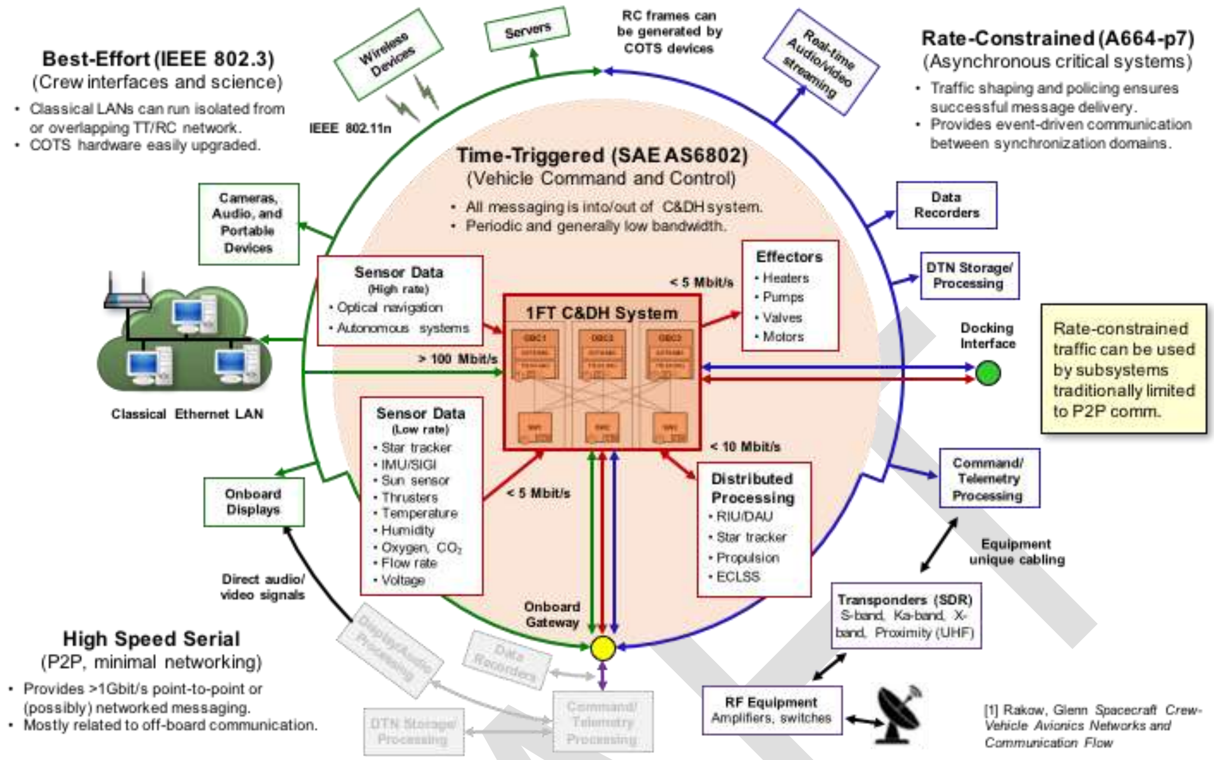

FIGURE 1

2.6.1 VEHICLE COMMAND AND CONTROL

The network needs for vehicle command and control have historically been low bandwidth (at least by today's standards) and periodic. The networks typically support a failure tolerant C&DH system that addresses critical functions. Fault tolerant systems are usually designed to handle more than just fail-stop faults, so inevitably some form of voting must be employed. Networks in support of vehicle command and control functions need to support various voting schemes such as exact match, fault-tolerant averaging, and mechanical.

Options currently exist where rather than having a dedicated vehicle command and control network, mixed types of data and criticality can occur over the same network. An example currently employed by some Aircraft manufacturers and Orion would be the utilization of strong space-time partitioning to accommodate these mixed criticality and data types.

2.6.2 CREW INTERFACES AND SCIENCE

Exploration networks will be expected to support crew interfaces and science as well. This can often be accommodated via classical Ethernet LANs utilizing best effort protocols such as IEEE 802.3 that can run isolated or overlapping with a Time-triggered/Rate Constrained type of network. Typically, COTS hardware in terrestrial applications, may be replaced with newer, faster elements so long as they conform to the network protocol. This approach would allow a vehicle, assembled over years to take advantage of advances in systems without disrupting the performance of hardware delivered earlier.

Examples of devices that would be supported would be onboard displays, cameras, audio, portable devices, wireless devices such as those utilizing IEEE 802.11 based protocols, and servers.

2.6.3 SPECIALTY INTERFACES

Exploration networks often have a need for off-board communications that require a high speed serial link. This is often accommodated with a Point-to-Point (P2P) network.

Examples of equipment that would be supported would be RF equipment such as amplifiers and switches, transponders that support protocols such as S-band, Ka-band, X-band and Proximity (UHF).

3.0 TIME-TRIGGERED ETHERNET SYSTEM CHARACTERISTICS

3.1.1 TIME-TRIGGERED ETHERNET GENERAL REQUIREMENTS

3.1.1.1 REDUNDANT NETWORK PLANES

The DSG Inter-Element Network shall support 3 redundant Network Planes of 1000BaseT per each of the two International Docking System (IDS) docking umbilical connectors.

Rationale: The current DSG Distributed Integrated Modular Avionics (DIMA) architecture is dependent upon 3 redundant planes as part of an overall integrated Avionics architecture that meets expected reliability, safety, fault tolerance, and fault containment.

3.1.1.2 802.3-2008 1000BASE-T STANDARD

One DIMA network plane connection shall be comprised of 8 wires following to the 802.3-2008 1000BaseT standard.

Rationale: Currently one Ethernet Network plane connection utilizing 1000BaseT utilizes 8 20AWG connectors at the docking umbilical interface. Planned FRAM alternative based connectors for NDS Block 2 are planned to contain enough connections to accommodate the 3 network planes.

3.1.1.3 SAE AS 6802 TIME TRIGGERED PROTOCOL

Each of the 3 DSG Inter-Element Network planes shall support the Time-Triggered Ethernet Protocol SAE AS 6802 or an agreed upon tailored implementation of said standard.

Rationale: Orion and ESA's Ariane 6 launcher both incorporate TTE, which helps better meet size, weight, and power challenges. Three planes of Ethernet will facilitate safety, redundancy, and reliability concerns as it allows connectivity for communication with Orion's 3 ODN planes for critical communication as well as communication between the DSG Elements. TTE, in conjunction with a time/space partitioned software standard such as ARINC 653, allows for partitioned access to shared resources for both critical and non-critical applications within the same processor (e.g., frame memory), greatly reducing what would otherwise be separate hardware with its subsequent size, weight, and power penalties. The networks, likewise, can transfer critical and non-critical data over the same network, likewise reducing size, weight, and power. Also, Ethernet in general, allows for utilization of more COTS applications/hardware due to its relative ubiquity in industry.

3.1.2 NETWORK DATA FORMATS

3.1.2.1 TIME TRIGGERED ETHERNET DEVICES

A Time-Triggered Ethernet device shall provide the following classes, at a minimum:

a) Protocol control frames
b) Time-triggered traffic

c) Rate-constrained traffic
d) Best-effort traffic

Rationale: General Concept is that Time Critical Data is Time Triggered. Rate Constrained Traffic can be used for intercommunications and off vehicle data. Best Effort/COTS Traffic is used by COTS End Systems and Network Maintenance functions and is reserved for non-critical data. Protocol control frames are used to synchronize the network in accordance with SAE AS 6802.

3.1.3 MAJOR COMPONENTS

3.1.3.1 MAJOR NETWORK COMPONENTS

The DSG Inter-Element Network shall address/utilize the following major network components:

Hardware

- Network Switches
- Network Interface Cards
- Cables & Connectors

Software

- Network scheduler
- Device loader
- Network Configuration Tables
- Network Design Database

Rationale: Standard Network related equipment and software will be required to support the network.

3.1.4 DATA TRANSFER

3.1.4.1 END SYSTEM TRANSFER

The DSG Inter-Element Network shall transfer data between end systems using three traffic classes (Time-Triggered, Rate Constrained, or Best Effort) per the TBD configuration table definitions.

Rationale: This requirement establishes the need to prioritize Time-Triggered, Rate Constrained, and BE network traffic. It forms the basis of the Network Partitioning Rule that: Lower priority traffic class faults and overloading conditions do not propagate to higher priority traffic classes.

3.1.5 LRU PROCESSING SYNCHRONIZATION

3.1.5.1 LRU TO NETWORK SYNCHRONIZATION

The DSG Inter-Element Network shall provide a means of an LRU to synchronize internal processing to the network.

Rationale: In order for the end systems to move traffic in their assigned windows, their NIC must be synchronized to the overall network schedule and operation. This requirement ensures that the network performs this network-wide synchronization.

3.1.6 NETWORK TIME COORDINATION

3.1.6.1 TIME SYNCHRONIZATION

The DSG shall synchronize network time on all end systems to allow time coordination between LRUs.

Rationale: The DSG hardware maintains sync after network time has been initialized, but the initialization is a FSW function.

3.1.7 NETWORK TOPOLOGY

3.1.7.1 DSG TOPOLOGY

The DSG topology shall be per TBD drawing part number.

Rationale: The DSG topology will not be static for the life of the program. Rather new modules, systems, visiting vehicles and payloads will be added to and removed from DSG throughout its operational life. Therefore the topology will need to be configuration managed throughout its life cycle.

3.1.8 NETWORK INITIALIZATION

3.1.8.1 DSG INTER-ELEMENT NETWORK POWER UP AND SYNCHRONIZATION

The DSG Inter-Element Network shall power up and gain synchronization within TBD milliseconds.

Rationale: This requirement assumes all DSG components are powered on without failure.

3.1.9 SYNCHRONIZATION

3.1.9.1 SAE AS 6802 SYNCHRONIZATION COMPLIANCE

The DSG Inter-Element Network shall perform network synchronization in compliance with SAE AS 6802 sections:

> 4 SYNCHRONIZATION PROTOCOL CONTROL FLOW
>
> Appendix C TIME-TRIGGERED ETHERNET REALIZATION ON IEEE 802.3 (GENERIC ETHERNET)
>
> Appendix D TIME-TRIGGERED ETHERNET REALIZATION ON ARINC 664-P7

Rationale: TBD

3.1.9.2 INDICATION OF SYNCHRONIZATION STATUS

The DSG Inter-Element Network synchronization function shall transmit synchronization state for indication of synchronization status.

Rationale: Synchronization must be established within the tolerance of the system to address temporary loss of an End-System or Switch. The protocol control frame (PCF) Message transmits the current sync state over the DSG Inter-Element Network.

3.1.9.3 COMPRESSION MASTER

The DSG Inter-Element Network shall be configured with at least one compression master (CM) for each Network Plane.

Rationale: TBS

3.1.9.4 SYNC MASTERS

The DSG Inter-Element Network shall be configured with at least TBD sync masters (SM).

Rationale: Configuration based on the number of NICs.

3.1.10 LOW POWER OPERATION

3.1.10.1 SINGLE PLANE OPERATION

The DSG Inter-Element Network shall remain operational in a single plane configuration.

Rationale: In order for fault tolerant systems to function they need to operate in a standalone mode without dependencies on the other redundant systems.

3.1.11 NETWORK FAULT RESPONSE

3.1.11.1 RESTART UPON FAULTS

The DSG Inter-Element Network shall reset and restart upon major faults such as switch hard and transient faults, sync master hard and transient faults, link faults and detected cliques.

Rationale: TBS

3.1.12 PCF FRAMES

TBD

3.1.13 CLOSED LOOP TESTING

TBD

3.1.14 DATA TIME TAGGING PRECISION

TBD

3.1.15 COTS END SYSTEM INTERFERENCE

3.1.15.1 HIGHER PRIORITY COMMUNICATIONS

The DSG Inter-Element Network shall prevent lower priority end systems from disrupting higher priority communication.

Rationale: The DSG Inter-Element Network prevents Best Effort data sources from interfering with the Protocol Control Frames, Time Triggered messages and Rate Constrained messages. DSG Inter-Element Network configuration tools need to be able to configure discoverable pre-determined and prohibited COTS data paths.

3.1.16 NETWORK TABLE LOADING

TBD

3.1.17 NETWORK HEALTH STATUS

3.1.17.1 STATUS MESSAGES

The Network Health Status messages shall be transmitted periodically.

Rationale: TBS

3.1.17.2 STATUS MESSAGES

The Network Health Status messages shall be available for downlink as needed.

Rationale: TBS

3.1.18 NETWORK DESIGN DATA

TBD

3.1.19 END SYSTEM IDENTIFICATION

3.1.19.1 UNIQUE IDENTIFIERS

The DSG Inter-Element Network End Systems (Network Switch, NIC hosting LRUs) shall be uniquely identified in the configuration tables.

Rationale: Configuration tables are used to define the Source MAC Address.

3.1.20 TEST PORT ACCESSIBILITY

3.1.20.1 LAB OPERATIONS

The DSG Inter-Element Network shall provide test ports on each network plane to support lab operations.

Rationale: This requirement specifically calls for the wiring system to provide access to the test ports. A test port is used to capture data that flows on the DSG Inter-Element Network for fault isolation.

3.1.21 NETWORK SWITCH

The Network Switch is the component that forwards data between End Systems.

3.1.21.1 PHYSICAL PORTS

The Network Switch shall have a minimum of TBD (8-16 likely) physical ports.

Rationale: TBS

3.1.21.2 CONTROL REGISTERS

The Network Switch control registers shall be accessible over the DSG Inter-Element Network.

Rationale: TBS

3.1.21.3 STATUS REGISTERS

The Network Switch status registers shall be accessible over the DSG Inter-Element Network.

Rationale: TBS

3.1.21.4 MEMORY

The Network Switch shall have a minimum of TBD of memory to buffer network traffic.

Rationale: TBS

3.1.21.5 NETWORK TRAFFIC PRIORITY

The Network Switch shall process network traffic in priority order. That priority would be:

1. Protocol Control
2. Time-Triggered (TT)
3. Rate Constrained (RC)
4. Best Effort (BE)

Rationale: This requirement establishes prioritization order PCF, TT, RC and BE network traffic. It forms the basis of the Network Partitioning Rule: Lower priority traffic class faults and potential overloading conditions do not propagate to higher priority traffic classes.

3.1.21.6 NETWORK PLANE INDEPENDENCE

Each Network Switch shall be connected to a single (one) network plane.

Rationale: The DSG Inter-Element Network is configured in a topology to support up to three switch planes and prevent propagation of faults between the planes.

3.1.21.7 HIGH INTEGRITY PROCESSING AND FAULT CONTAINMENT

The Network Switch shall be in a COM/MON configuration to allow for high integrity processing and fault containment.

Rationale: The Network Switches are the core of a DSG Inter-Element Network plane, providing the DSG Inter-Element Network Schedule enforcement that protects the overall system from end system failure. An overview is included in Appendix B of SAE AS 6802.

3.1.21.8 CLOCK OUT OF TOLERANCE RESPONSE

In response to Network Switch Clock being out of tolerance, the Network Switch Clock Monitor shall reset and hold the Switch in reset until the power is cycled or the clock comes back into tolerance.

Rationale: If the clock is out of specification, predictable device operation is not assured. The devices need to be held in reset until power is cycled.

3.1.21.9 POWER MONITOR TRIP LIMITS

The Network Switch Power Monitor trip limits shall be set to keep the power supplied to the parts and the power monitor within specification values.

Rationale: TBS

3.1.21.10 TRANSITION TO FAIL PASSIVE STATE

The Network Switch shall transition to a fail passive state upon detection of a shared internal power failure.

Rationale: This is accomplished by a guaranteed reset that when asserted results in outputs transitioning to a passive state.

3.1.21.11 COM/MON FUNCTIONS

The Network Switch shall provide two independent, separated functions (i.e. COM-MON) where each function performs the processing of all network message traffic.

Rationale: The motivation to keep the switches high integrity is due to the fault propagation impact on multiple subsystems/partitions/functions in an integrated environment. Complete failure of the Switch does not propagate beyond the subsystem boundary. Intermittent Switch faults are prevented by power and clock monitors and COM/MON. These two functions will not be co-located in the same silicone. An overview of COM/MON fault containment is included in Appendix B of SAE AS 6802.

3.1.21.12 NETWORK SWITCH MON

The Network Switch MON lane shall monitor COM TX packet transmissions and force packet syntax errors prior to the completion of the transmission for each packet that does not match the MON lane expected transmit packet.

Rationale: The length field detects packets shortened by COM hardware faults within the message that may otherwise escape CRC detection.

3.1.21.13 DISABLED TRANSMIT-PACKETS

The Network Switch shall count the occurrences of disabled transmit-packets on a per port basis and make results accessible to the Network Management Function.

Rationale: Need to track the number of disabled packets to assess the status of the hardware. Fault Counters only count the number of failed packets. This count does not include packets that were scheduled but not sent by the host. If this is necessary it is up to the application layer to provide this capability.

3.1.21.14 DUAL CRC MONITORS

The Network Switch shall have independent, dual CRC monitors that detect invalid received packet CRCs per CRC:

$$G(x) = x^{32}+x^{26}+x^{23}+ x^{22}+ x^{16}+ x^{12}+ x^{11}+ x^{10}+ x^{8}+ x^{7}+ x^{5}+ x^{4}+ x^{2}+ x+1$$

Rationale: This is the IEEE-802.3 CRC32. Both COM and MON have packet CRC monitors.

3.1.21.15 DISCARDING INVALID PACKETS

The Network Switch shall provide independent means for both COM and MON to detect when a received packet's CRC is invalid..

Rationale: A failed CRC check indicates the data has been corrupted in the signal path and should not be used.

3.1.21.16 PACKET LENGTH MONITORING

The Network Switch shall provide independent means for both COM and MON to detect when a received packet's length is shorter than that specified in the packet header.

Rationale: TBD

3.1.21.17 COM AND MON CONGRUENCY

The Network Switch shall provide an independent means to ensure congruency between COM and MON. It ensures received packets are either accepted by both COM and MON, or otherwise discarded.

Rationale: It is necessary to keep the operations of COM and MON from diverging due to weak reception that is perceived differently between COM and MON.

3.1.21.18 VIRTUAL LINK MONITORING

The Network Switch shall provide an independent means for both COM and MON to monitor network packet VLs against a predefined schedule contained in the configuration tables.

Rationale: The schedule contains information as to Virtual Link allocation and associated time base. This allows determination of message timing as well as validity. (TT Only)

3.1.21.19 PROTECTING TIME TRIGGERED PRECEDENCE

The Network Switch shall discard received packets that would interfere with Time Triggered data allocations.

Rationale: This monitor detects ensures that this class of traffic data has priority. (TT Only)

3.1.21.20 BANDWIDTH ALLOCATION GAP MONITORING

The network switch shall provide a mechanism for COM to independently monitor the network packet bandwidth allocation gap (BAG) to protect Rate Constrained allocations.

Rationale: This allows determination of message validity. (RC Only)

3.1.21.21 HANDLING PRIORITY DISAGREEMENT

The Network Switch shall discard received packets that disagree with the predefined schedule in the configuration tables.

Rationale: Limits one network element from consuming network bandwidth beyond its predetermined allocation (RC Only).

3.1.21.22 CONFIGURATION TABLE LOADING

The Network Switch shall be capable of loading a configuration table from the network, whether an existing configuration table is loaded or is valid.

Rationale: The Network Switch needs to be capable of loading a configuration table from the network.

3.1.21.23 BUILT-IN-TEST

The Network Switch shall contain Built-In-Test that can be initiated on power-up and provide the ability to externally execute the test.

Rationale: CRC checks of the loaded table contents during BIT are performed.

3.1.21.24 OPERATION MODE TABLE LOADING

The Network shall allow loading a configuration table while the switch is in operation mode.

Rationale: The Network will support two configuration tables in Non-Volatile Memory.

3.1.21.25 CONFIGURATION CRC CHECKS

The Network Switch shall perform an IEEE CRC-32 over the configuration tables prior to use after a cold-start or reset.

Rationale: The network schedule and other configuration information in the configuration table needs to be verified prior to use.

3.1.21.26 COMPRESSION MASTER

The Network Switch shall be capable of functioning as a Compression Master as defined in SAE AS 6802.

Rationale: TBD

3.1.21.27 NETWORK SYNCHRONIZATION

The Network Switch synchronization function shall establish network synchronization such that no 2 healthy network time sources differ by more than TBD microseconds.

Rationale: Synchronization requires enough network resources be available in all mission modes. It is assumed that a high integrity component synchronization messages are valid when received but may not be seen by all other End-Systems or Switches.

3.1.21.28 SYNCHRONIZATION WITH NETWORK FAULTS

The Network Switch synchronization algorithm shall establish network synchronization in the presence as many as of TBD faulty NICs or TBD faulty NIC and TBD faulty Network Switch within a network plane when more than one network plane is operating.

Rationale: Synchronization requires enough network resources be available in all mission modes. It is assumed that a high integrity component synchronization messages are valid when received but may not be seen by all other End-Systems or Switches.

3.1.21.29 SYNCHRONIZATION INTEGRATION PERIOD

The Network Switch synchronization algorithm shall maintain the established network synchronization for up to one integration period without receiving synchronization messages.

Rationale: Synchronization protocol messages can be dropped due to SEU or other transients and will not result in the loss of synchronization. The fault tolerance of the network is implied by the topology and the setup of the timing and compression masters.

3.1.21.30 SYNCHRONIZATION DURING POWER APPLICATION

The Network Switch synchronization function shall establish synchronization within TBD milliseconds of power application and release from reset when the required timing masters are available

Rationale: Synchronization must be established within the tolerance of the system to address temporary loss of an End-System or Switch due to transient upsets.

3.1.22 NETWORK INTERFACE CARDS (NIC)

The NIC is a single thread network interface for internal and third party use. The NIC receives Ethernet frames through the network ports, checks them and may put them into Host Interface memory per the configuration tables. The NIC takes Ethernet frames from the egress ports, formats them and transmits them on the DSG Inter-Element Network.

3.1.22.1 POWER INTERFACE

The NIC shall receive power via the host interface connection.

Rationale: TBS

3.1.22.2 NETWORK TIME CAPTURE INTERFACE

The NIC shall receive a discrete input time pulse from a source external to the hosting LRU or from the hosting LRU to trigger a network time capture.

Rationale: TBS

3.1.22.3 NETWORK TIME CAPTURE

The NIC shall capture the network time upon receipt of a discrete input time pulse.

Rationale: TBS

3.1.22.4 NETWORK TIME CAPTURE LATENCY

The NIC shall capture the network time in an internal register within TBD microsecond of either the internal discrete input time pulse or external discrete input time pulse being received.

Rationale: TBS

3.1.22.5 CONFIGURATION TABLE INTEGRITY CHECKS

The NIC shall perform a CRC over the configuration tables prior to use after a cold-start or reset.

Rationale: The network schedule and other configuration information in the configuration table needs to be verified prior to use.

3.1.22.6 CONFIGURATION TABLE INTEGRITY CHECKS FAULT RESPONSE

The NIC shall inhibit all network traffic except for maintenance communication using dedicated maintenance messages when the configuration table CRC is invalid.

Rationale: This requirement supports the fail-silent redundancy architecture. Maintenance communication can be used to load the switch schedule.

3.1.22.7 HIGH INTEGRITY NETWORK INTERFACE SYNCHRONIZATION

A device with a high-integrity network interface shall be configurable as a synchronization master or a synchronization client.

Rationale: The terms high-integrity, standard integrity, synchronization master and synchronization client are as defined in SAE6802.

3.1.22.8 STANDARD INTEGRITY NETWORK INTERFACE SYNCHRONIZATION

A device with a standard-integrity network interface shall, at a minimum, be able to function as a synchronization client.

Rationale: The AS6802 standard allows for standard integrity synchronization masters.

3.1.22.9 DATA TRANSFER BUFFER MEMORY

The NIC shall have a minimum of TBD MBits of memory for buffering DSG Inter-Element Network traffic.

Rationale: TBS

3.1.22.10 TRAFFIC CLASSES

The NIC shall prioritize network traffic processing such that PCF first, Time-Triggered is processed next followed by Rate Constrained and then BE traffic within the available network bandwidth.

Rationale: This requirement establishes the need to prioritize Time-Trigger, Rate Constrained and BE network traffic. It forms the basis of the Network Partitioning Rule that: Lower priority traffic class faults and overloading conditions do not propagate to higher priority traffic classes.

3.1.22.11 DMA CHANNELS

The NIC shall support TBD DMA channels to allow data transfer from the NIC memory.

Rationale: TBS

3.1.22.12 HOST SIDE BUS VOLTAGE

The NIC shall be compatible with TBD PCI volt power.

Rationale: The NIC is used with a variety of different devices (Display Units, Audio Systems, & Video Systems). These require standards based interface.

3.1.22.13 HOST SIDE BUS TRANSFER RATE

The NIC shall be compatible with PCI TBD MHz transfer rate.

Rationale: The Standard Integrity NIC is used with a variety of different devices (Display Units, Audio Systems, & Video Systems). These require standards based interface.

3.1.22.14 HOST SIDE BUS INTERFACE

The NIC shall be compatible with PCI TBD bit interface definition.

Rationale: The NIC is used with a variety of different devices (Display Units, Audio Systems, & Video Systems). These require standards based interface.

3.1.23 CABLES AND CONNECTORS

The DSG Inter-Element Network Physical Layer is based on Ethernet 1000BASE-T standard, which includes:

- Copper media
- Dedicated TX and RX wire pairs per link with full duplex signaling on each pair.
- Connectors (Electrical Characteristics for LRU Connectors) Zero Force, Bulkhead, LRU)

3.1.23.1 NETWORK HARNESS

The DSG Inter-Element Network harness shall be routed in a manner to minimize Single Faults that will result in failure of multiple Avionics devices or multiple Network Planes.

Rationale: Each DSG Inter-Element Network Plane is considered redundant function. In order to preserve this redundancy, DSG Inter-Element Network Planes 1 and 2 should be separated to maintain that redundancy wherever possible. DSG Inter-Element Network Plane 3 can be split by power zones and routed with Planes 1 and 2 when needed.

3.1.23.2 WIRING INTERNCONNECTS

The DSG Inter-Element Network wiring interconnections shall be per Interconnect Drawing Part Number TBD.

Rationale: TBS

3.1.23.3 BIT ERROR RATE (BER)

The DSG Inter-Element Network shall provide network communications with a Bit Error Rate (BER) per physical layer connected selected for each port.

Rationale: The BER needs to be at a reasonable level to prevent frequent loss of data disrupting system operation.

3.1.23.4 WIRE GAUGE

The TTE cable shall use at least 24AWG wire to ensure maximum cable length.

Rationale: TBS

3.1.23.5 JUMPER CABLE SEGMENTS

When designing Jumper Cable segments, 1.5dB margin shall be allocated for manufacturing and environmental issues.

Rationale: 1.5 dB is practical to allow for environmental and manufacturing anomalies.

3.1.23.6 TRANSFORMER COUPLING

The NIC and Network Switch shall provide isolation/surge protection transformers between the Network Interface connectors and the NIC PBA circuitry to protect against signal levels referred in this section.

Rationale: TBS

3.1.23.7 LIGHTNING

The NIC and Network Switch will meet all operational performance requirements in the event of a lightning event within TBD levels.

Rationale: TBS

3.1.24 CONFIGURATION TABLES

The Network Scheduler impacts the DSG Inter-Element Network and all equipment that interfaces to that network. The Network Scheduler does the following:

- Aligns processing & dataflow across the network to meet
  - Producer/Consumer Requirements
  - Latency & Jitter
- Lays out network communications while not exceeding physical constraints (link size, end system memory size, tenure times, etc.)
- Provides an export of network traffic information for network end system builder
- Provides processing timeline start times/(offset to marker) and other IO information for the Processors
- Provides major, minor and sub minor frame schedule information for Processors with linkage to processing timeline
- Provides an export to a Vehicle ICD
- Produces reports/data coordinated processing timelines, dataflow and other information for other tooling for design & verification use.

3.1.24.1 NETWORK SCHEDULER PARAMETERS

The Network Scheduler will implement the SAE AS6802 Section 11 parameters.

Rationale: TBS

3.1.24.2 CRITICAL TRAFFIC NETWORK COMMUNICATIONS SCHEDULE

The Network Scheduler should schedule Critical Traffic (CT) network communications such that the communication links, End System Memories, and Switch Memories do not exceed TBD % of overall utilization rates.

Rationale: CT traffic comprises both the TT and RC traffic. This allows the adequate bandwidth be reserved for Best Effort Traffic.

3.1.24.3 IDENTICAL CRITICAL TRAFFIC SCHEDULES

The Network Critical Traffic schedules for redundant Network Planes shall be identical to maintain symmetry.

Rationale: TBS

3.1.24.4 CONFIGURATION FILE VERIFICATION

Every Switch shall verify that a configuration file is intended for its use by a TBD identification code associated with each switch.

Rationale: This prevents the loading of the wrong configuration file to a switch.

3.1.24.5 CONFIGURATION FILE VERIFICATION

Every Switch shall verify the configuration file received was not corrupted prior to loading.

Rationale: This prevents the loading of the wrong configuration file to a switch.

3.1.24.6 CRITICAL TRAFFIC CLASSES

The Network Scheduler shall schedule network data for critical traffic classes (TT & RC) to meet the data transfer requirements.

Rationale: This requirement establishes the need to prioritize Time-Triggered, Rate Constrained while leaving adequate room for BE network traffic. Lower priority traffic class faults and overloading conditions do not propagate to higher priority traffic classes.

3.1.24.7 ORDERING VIRTUAL LINKS

The Network Scheduler shall support ordering of specific VLs transmitted on the DSG Inter-Element Network.

Rationale: TBS

3.1.24.8 SCHEDULER CONSIDERATIONS

The Network Scheduler shall use the produce/consumer data, the network topology model, LRU latency model, and jitter & latency allocations to schedule network traffic.

Rationale: TBS

3.1.24.9 NIC AND NETWORK SWITCH SCHEDULING

The Network Scheduler shall create configuration tables for the NIC and Network Switch.

Rationale: TBS

3.1.25 NETWORK CONFIGURATION TABLES

3.1.25.1 CONFIGURATION TABLES IN FLIGHT COMPONENTS

The DSG Inter-Element Network shall use configuration tables in each flight component that allow configuration management (unique part number), error checking and loading of flight components.

Rationale: TBS

3.1.25.2 SWITCH POSTIONS

The Network Switch Configuration Tables shall uniquely identify the switch position within the network.

Rationale: TBS

3.1.25.3 NETWORK END SYSTEM CONFIGURATION TABLES UNIQUIE ID

The Network End System Configuration Tables (NICs) shall be uniquely identified for an end system position within the network.

Rationale: TBS

3.1.25.4 CONFIGURATION DOCUMENTATION

The data required to configure the DSG Inter-Element Network shall be documented in TBD.

Rationale: TBS

3.2 PHYSICAL LAYER ATTRIBUTES CONSIDERED

Physical layer attributes - TBS

The physical layer defines the cable, connector, the electrical signaling levels, and the line encoding method for the information. The physical layer for the protocols outlined in this document will be discussed as well as some of the considerations for comparing the different physical layers.

The Ethernet standards have different physical layers depending upon the signaling rate.

The 1000BaseT (802.3ab 1999) uses PAM-5 coded signaling as well as at least Category 5e cable with four twisted pairs cabling. Each pair is used in both directions simultaneously.

4.0 VERIFICATION AND TESTING

TBS

Define how standard implementation will be verified.

4.1 TIME-TRIGGERED ETHERNET SYSTEM CHARACTERISTICS

4.1.1 TIME-TRIGGERED ETHERNET GENERAL VERIFICATION

4.1.1.1 REDUNDANT NETWORK PLANES

Verification of 3 redundant Network Planes of 1000BaseT per each of the two International Docking System (IDS) docking umbilical connectors shall be done through Inspection and Test. Verification will be considered complete when signal quality can be verified through each connection.

4.1.1.2 802.3-2008 1000BASE-T STANDARD

Verification of one DIMA network plane connection comprised of 8 wires following the 802.3-2008 1000BaseT standard shall be verified by inspection.

4.1.1.3 SAE AS 6802 TIME TRIGGERED PROTOCOL

Verification of each of the 3 DSG Inter-Element Network planes supporting the Time-Triggered Ethernet Protocol SAE AS 6802 or an agreed upon tailored implementation of said standard shall be verified by test and analysis.

4.1.2 NETWORK DATA FORMATS

4.1.2.1 TIME TRIGGERED ETHERNET DEVICES

Verification of a Time-Triggered Ethernet device provide the following classes, at a minimum:

a) Protocol control frames

b) Time-triggered traffic

c) Rate-constrained traffic

d) Best-effort traffic

shall be verified through a combination of analysis and test.

4.1.3 MAJOR COMPONENTS

4.1.3.1 MAJOR NETWORK COMPONENTS

Verification of the DSG Inter-Element Network addressing/utilizing the following major network components:

- Network Switches
- Network Interface Cards
- Cables & Connectors
- Network scheduler
- Device loader
- Network Configuration Tables
- Network Design Database

shall be verified through analysis and inspection.

4.1.4 DATA TRANSFER

4.1.4.1 END SYSTEM TRANSFER

Verification of the DSG Inter-Element Network transferring data between end systems using three traffic classes (Time-Triggered, Rate Constrained, or Best Effort) per the TBD configuration table definitions shall be verified by test.

4.1.5 LRU PROCESSING SYNCHRONIZATION

4.1.5.1 LRU TO NETWORK SYNCHRONIZATION

Verification of the DSG Inter-Element Network providing a means of an LRU to synchronize internal processing to the network shall be verified by test.

4.1.6 NETWORK TIME COORDINATION

4.1.6.1 TIME SYNCHRONIZATION

Verification of the DSG synchronizing network time on all end systems to allow time coordination between LRUs shall be verified by test.

4.1.7 NETWORK TOPOLOGY

4.1.7.1 DSG TOPOLOGY

Verification of the DSG topology shall be per inspection of TBD drawing part number.

4.1.8 NETWORK INITIALIZATION

4.1.8.1 DSG INTER-ELEMENT NETWORK POWER UP AND SYNCHRONIZATION

Verification of the DSG Inter-Element Network powering up and gain synchronization within TBD milliseconds shall be verified by test.

4.1.9 SYNCHRONIZATION

4.1.9.1 SAE AS 6802 SYNCHRONIZATION COMPLIANCE

Verification of the DSG Inter-Element Network performing network synchronization in compliance with SAE AS 6802 sections:

4 SYNCHRONIZATION PROTOCOL CONTROL FLOW

Appendix C TIME-TRIGGERED ETHERNET REALIZATION ON IEEE 802.3 (GENERIC ETHERNET)

Appendix D TIME-TRIGGERED ETHERNET REALIZATION ON ARINC 664-P7

shall be verified by test.

4.1.9.2 INDICATION OF SYNCHRONIZATION STATUS

Verification of the DSG Inter-Element Network synchronization function transmitting synchronization state for indication of synchronization status shall be verified by test.

4.1.9.3 COMPRESSION MASTER

Verification of the DSG Inter-Element Network configuring with at least one compression master (CM) for each Network Plane shall be verified by analysis and test.

4.1.9.4 SYNC MASTERS

Verification of the DSG Inter-Element Network configuring with at least TBD sync masters (SM) shall be verified by analysis and test.

4.1.10 LOW POWER OPERATION

4.1.10.1 SINGLE PLANE OPERATION

Verification of the DSG Inter-Element Network remaining operational in a single plane configuration shall be verified by test.

4.1.11 NETWORK FAULT RESPONSE

4.1.11.1 RESTART UPON FAULTS

Verification of the DSG Inter-Element Network resetting and attempting restart upon major faults such as switch hard and transient faults, sync master hard and transient faults, link faults and detected cliques shall be verified by analysis and test.

4.1.12 PCF FRAMES

TBD

4.1.13 CLOSED LOOP TESTING

TBD

4.1.14 DATA TIME TAGGING PRECISION

TBD

4.1.15 COTS END SYSTEM INTERFERENCE

4.1.15.1 HIGHER PRIORITY COMMUNICATIONS

Verification of the DSG Inter-Element Network preventing COTS End Systems from disrupting higher priority communication shall be verified by analysis and test.

4.1.16 NETWORK TABLE LOADING

TBD

4.1.17 NETWORK HEALTH STATUS

4.1.17.1 STATUS MESSAGES

Verification of the Network Health Status messages being transmitted periodically and are available for downlink as needed shall be verified by analysis and test.

4.1.18 NETWORK DESIGN DATA

TBD

4.1.19 END SYSTEM IDENTIFICATION

4.1.19.1 UNIQUE IDENTIFIERS

Verification of the DSG Inter-Element Network End Systems (Network Switch, NIC hosting LRUs) being uniquely identified in the configuration tables shall be verified by analysis and test.

4.1.20 TEST PORT ACCESSIBILITY

4.1.20.1 LAB OPERATIONS

Verification of the DSG Inter-Element Network providing test ports on each network plane to support lab operations shall be verified by test.

4.1.21 NETWORK SWITCH

The Network Switch is the component that forwards data between End Systems.

4.1.21.1 PHYSICAL PORTS

Verification of the Network Switch having a minimum of TBD (8-16 likely) physical ports shall be verified by analysis and test.

4.1.21.2 CONTROL REGISTERS

Verification of the Network Switch control registers being accessible over the DSG Inter-Element Network shall be verified by test.

4.1.21.3 STATUS REGISTERS

Verification of the Network Switch status registers being accessible over the DSG Inter-Element Network shall be verified by test.

4.1.21.4 MEMORY

Verification of the Network Switch having a minimum of TBD of memory to buffer network traffic shall be verified by analysis and test.

4.1.21.5 NETWORK TRAFFIC PRIORITY

Verification of the Network Switch prioritizing network traffic processing such that Protocol Control Frames are the highest priority, Time-Triggered are the next priority, followed by Rate Constrained and then BE traffic within the available network bandwidth shall be verified by analysis and test.

4.1.21.6 NETWORK PLANE INDEPENDENCE

Verification of each Network Switch being connected to a single (one) network plane shall be verified by analysis and test.

4.1.21.7 HIGH INTEGRITY PROCESSING AND FAULT CONTAINMENT

Verification of the Network Switch being in a COM/MON configuration to allow for high integrity processing and fault containment shall be verified by analysis and test.

4.1.21.8 CLOCK OUT OF TOLERANCE RESPONSE

Verification of the Network Switch Clock Monitor response to the clock being out of tolerance to reset and holding the Switch in reset until the power is cycled or the clock comes back into tolerance shall be verified by test.

4.1.21.9 POWER MONITOR TRIP LIMITS

Verification of the Network Switch Power Monitor trip limits being set to keep the power supplied to the parts and the power monitor within specification values shall be verified by test.

4.1.21.10 TRANSITION TO FAIL PASSIVE STATE

Verification of the Network Switch transitioning to a fail passive state upon detection of a shared internal power failure shall be verified by analysis and test.

4.1.21.11 COM/MON FUNCTIONS

Verification of the Network Switch providing two independent, separated functions (i.e. COM-MON) where each function performs the processing of all network message traffic shall be verified by some combination of test and analysis.

4.1.21.12 NETWORK SWITCH MON

Verification of the Network Switch MON lane monitoring COM TX packet transmissions and forcing packet syntax errors prior to the completion of the transmission for each packet that does not match the MON lane expected transmit packet shall be verified through some combination of test and analysis.

4.1.21.13 DISABLED TRANSMIT-PACKETS

Verification of the Network Switch counting the occurrences of disabled transmit-packets on a per port basis and making results accessible to the Network Management Function shall be verified through some combination of test and analysis.

4.1.21.14 DUAL CRC MONITORS

Verification of the Network Switch shall have independent, dual CRC monitors that detect invalid received packet CRCs per CRC:

$$G(x) = x^{32}+x^{26}+x^{23}+ x^{22}+ x^{16}+ x^{12}+ x^{11}+ x^{10}+ x^{8}+ x^{7}+ x^{5}+ x^{4}+ x^{2}+ x+1$$

shall be through test and analysis.

4.1.21.15 DISCARDING INVALID PACKETS

Verification of the Network Switch CRC monitor discarding packets received containing invalid received packet CRCs shall be verified through test and analysis.

4.1.21.16 PACKET LENGTH MONITORING

Verification of the Network Switch providing independent means for both COM and MON to detect when a received packet's length is shorter than that specified in the packet header shall be verified through test and analysis.

4.1.21.17 COM AND MON CONGRUENCY

Verification of the Network Switch providing an independent means to ensure congruency between COM and MON shall be verified through test and analysis. Verification will ensure received packets are either accepted by both COM and MON, or otherwise discarded.

4.1.21.18 VIRTUAL LINK MONITORING

Verification of the Network Switch providing an independent means for both COM and MON to monitor network packet VLs against a predefined schedule contained in the configuration tables shall be verified through test and analysis.

4.1.21.19 PREDEFINED SCHEDULE DISAGREEMENT

Verification of the Network Switch discarding received packets that disagree with the predefined schedule in the configuration tables shall be verified through text and analysis.

4.1.21.20 BANDWIDTH ALLOCATION GAP MONITORING

Verification of the network switch providing an independent means for both COM and MON to monitor the network packet bandwidth allocation gap (BAG) against a predefined schedule in the configuration tables shall be verified by test and analysis.

4.1.21.21 SCHEDULE DISAGREEMENT

Verification of the Network Switch discarding received packets that disagree with the predefined schedule in the configuration tables shall be verified through test and analysis.

4.1.21.22 CONFIGURATION TABLE LOADING

Verification of the Network Switch being capable of loading a configuration table from the network, whether an existing configuration table is loaded or is valid shall be verified through test and analysis.

4.1.21.23 BUILT-IN-TEST

Verification of the Network Switch containing Built-In-Test that can be initiated on power-up or provide the ability to externally execute the test shall be verified by test.

4.1.21.24 OPERATION MODE TABLE LOADING

Verification of the Network allowing loading a configuration table while the switch is in operation mode shall be verified by test.

4.1.21.25 CONFIGURATION CRC CHECKS

Verification of the Network Switch performing an IEEE CRC-32 over the configuration tables prior to use after a cold-start or reset shall be verified by test and analysis.

4.1.21.26 COMPRESSION MASTER

Verification of the Network Switch being capable of functioning as a Compression Master as defined in SAE AS 6802 shall be verified by test and analysis.

Rationale: TBD

4.1.21.27 NETWORK SYNCHRONIZATION

Verification of the Network Switch synchronization function establishing network synchronization such that no 2 healthy network time sources differ by more than TBD microseconds shall be verified by test and analysis.

4.1.21.28 SYNCHRONIZATION WITH NETWORK FAULTS

Verification of the Network Switch synchronization algorithm establishing network synchronization in the presence as many as of TBD faulty NICs or TBD faulty NIC and TBD faulty Network Switch within a network plane when more than one network plane is operating shall be verified by test.

4.1.21.29 SYNCHRONIZATION INTEGRATION PERIOD

Verification of the Network Switch synchronization algorithm maintaining the established network synchronization for up to one integration period without receiving synchronization messages shall be verified by test and analysis.

4.1.21.30 SYNCHRONIZATION DURING POWER APPLICATION

Verification of the Network Switch synchronization function establishing synchronization within TBD milliseconds of power application and release from reset when the required timing masters are available shall be verified by test and analysis.

4.1.22 NETWORK INTERFACE CARDS (NIC)

The NIC is a single thread network interface for internal and third party use. The NIC receives Ethernet frames through the network ports, checks them and may put them into Host Interface memory per the configuration tables. The NIC takes Ethernet frames from the egress ports, formats them and transmits them on the DSG Inter-Element Network.

4.1.22.1 POWER INTERFACE

Verification of the NIC receiving power via the host interface connection shall be verified through test and analysis.

4.1.22.2 NETWORK TIME CAPTURE INTERFACE

Verification of the NIC receiving a discrete input time pulse from a source external to the hosting LRU or from the hosting LRU to trigger a network time capture shall be verified through test and analysis.

4.1.22.3 NETWORK TIME CAPTURE

Verification of the NIC capturing the network time upon receipt of a discrete input time pulse shall be verified by test and analysis.

4.1.22.4 NETWORK TIME CAPTURE LATENCY

Verification of the NIC capturing the network time in an internal register within TBD microsecond of either the internal discrete input time pulse or external discrete input time pulse being received by test and analysis.

4.1.22.5 CONFIGURATION TABLE INTEGRITY CHECKS

Verification of the NIC performing a CRC over the configuration tables prior to use after a cold-start or reset shall be verified by test and analysis.

4.1.22.6 CONFIGURATION TABLE INTEGRITY CHECKS FAULT RESPONSE

Verification of the NIC inhibiting all network traffic except for maintenance communication using dedicated maintenance messages when the configuration table CRC is invalid shall be verified through test and analysis.

4.1.22.7 HIGH INTEGRITY NIC SYNCHRONIZATION

Verification of a device with a high-integrity network interface being configurable as a synchronization master or a synchronization client shall be verified through test and analysis.

4.1.22.8 STANDARD INTEGRITY NIC SYNCHRONIZATION

Verification of a device with a standard-integrity network interface, at a minimum, being able to function as a synchronization client shall be verified through test and analysis.

4.1.22.9 DATA TRANSFER BUFFER MEMORY

Verification of the NIC have a minimum of TBD MBits of memory for buffering DSG Inter-Element Network traffic shall be verified through analysis.

4.1.22.10 TRAFFIC CLASSES

Verification of the NIC prioritizing network traffic processing such that PCF first, Time-Triggered is processed next followed by Rate Constrained and then BE traffic within the available network bandwidth shall be verified through test and analysis.

4.1.22.11 DMA CHANNELS

Verification of the NIC supporting TBD DMA channels to allow data transfer from the NIC memory shall be through test and analysis.

4.1.22.12 HOST SIDE BUS VOLTAGE

Verification of the NIC being compatible with TBD PCI volt power shall be verified through test and analysis.

4.1.22.13 HOST SIDE BUS TRANSFER RATE

Verification of the NIC being compatible with PCI TBD MHz transfer rate shall be verified through test and analysis.

4.1.22.14 HOST SIDE BUS INTERFACE

Verification of the NIC being compatible with PCI TBD bit interface definition shall be verified through analysis.

4.1.22.15 ENDIAN

Verification of the NIC using a PCI host interface that is configurable to provide network data in big and little endian format without software swapping of ingress and egress data shall be verified by test and analysis.

4.1.23 CABLES AND CONNECTORS

The DSG Inter-Element Network Physical Layer is based on Ethernet 1000BASE-T standard, which includes:

- Copper media
- Dedicated TX and RX wire pairs per link – full duplex w/o signal mixing
- Connectors (Electrical Characteristics for LRU Connectors) Zero Force, Bulkhead, LRU)

4.1.23.1 NETWORK HARNESS

Verification of the DSG Inter-Element Network harness being routed in a manner to minimize Single Faults that will result in failure of multiple Avionics devices or multiple Network Planes shall be verified through analysis and inspection.

4.1.23.2 WIRING INTERNCONNECTS

Verification of the DSG Inter-Element Network wiring interconnections being per Interconnect Drawing Part Number TBD shall be through inspection.

4.1.23.3 BIT ERROR RATE (BER)

Verification of the DSG Inter-Element Network providing network communications with a Bit Error Rate (BER) per physical layer connected selected for each port shall be verified through analysis and analysis of test data.

4.1.23.4 WIRE GAUGE

Verification of the TTE cable using at least 24AWG wire to ensure maximum cable length shall be verified through inspection.

4.1.23.5 JUMPER CABLE SEGMENTS

Verification of Jumper Cable segments using 1.5dB margin for manufacturing and environmental issues shall be verified through analysis and test.

4.1.23.6 TRANSFORMER COUPLING

The NIC and Network Switch provide isolation/surge protection transformers between the Network Interface connectors and the NIC PBA circuitry to protect against signal levels referred in this section.

4.1.23.7 LIGHTNING

Verification of the NIC and Network Switch meeting all operational performance requirements in the event of a lightning event within TBD levels will be through analysis.

4.1.24 CONFIGURATION TABLES

The Network Scheduler impacts the DSG Inter-Element Network and all equipment that interfaces to that network. The Network Scheduler does the following:

- Aligns processing & dataflow across the network to meet
    - Producer/Consumer Requirements
    - Latency & Jitter
- Lays out network communications while not exceeding physical constraints (link size, end system memory size, tenure times, etc.)
- Provides an export of network traffic information for network end system builder

- Provides processing timeline start times/(offset to marker) and other IO information for the Processors
- Provides major, minor and sub minor frame schedule information for Processors with linkage to processing timeline
- Provides an export to a Vehicle ICD
- Produces reports/data coordinated processing timelines, dataflow and other information for other tooling for design & verification use.

4.1.24.1 NETWORK SCHEDULER PARAMETERS

Verification of the Network Scheduler implementing the SAE AS6802 Section 11 parameters will be through analysis.

4.1.24.2 CRITICAL TRAFFIC NETWORK COMMUNICATIONS SCHEDULE

Verification of the Network Scheduler scheduling Critical Traffic (CT) network communications such that the communication links, End System Memories, and Switch Memories do not exceed TBD % of overall utilization rates shall be through analysis and test.

4.1.24.3 IDENTICAL CRITICAL TRAFFIC SCHEDULES

Verification of the Network Critical Traffic schedules for redundant Network Planes being identical to maintain symmetry shall be through analysis and test.

4.1.24.4 CONFIGURATION FILE VERIFICATION

Verification of every Switch being able to verify their configuration file shall be through test.

4.1.24.5 CRITICAL TRAFFIC CLASSES

Verification of the Network Scheduler scheduling network data for critical traffic classes (TT & RC) to meet the data transfer requirements shall be through test.

4.1.24.6 ORDERING VIRTUAL LINKS

Verification of the Network Scheduler supporting ordering of specific VLs transmitted on the DSG Inter-Element Network shall be through test.

4.1.24.7 SCHEDULER CONSIDERATIONS

Verification of the Network Scheduler using the produce/consumer data, the network topology model, LRU latency model, and jitter & latency allocations to schedule network traffic shall be through analysis and test.

4.1.24.8 NIC AND NETWORK SWITCH SCHEDULING

Verification of the Network Scheduler creating configuration tables for the NIC and Network Switch shall be through analysis and test.

4.1.25 NETWORK CONFIGURATION TABLES

4.1.25.1 CONFIGURATION TABLES IN FLIGHT COMPONENTS

Verification of the DSG Inter-Element Network using configuration tables in each flight component that allow configuration management (unique part number), error checking and loading of flight components shall be verified by analysis and test.

4.1.25.2 SWITCH POSTIONS

Verification of the Network Switch Configuration Tables uniquely identifying the switch position within the network shall be verified through analysis and test.

4.1.25.3 NETWORK END SYSTEM CONFIGURATION TABLES SWITCH POSITION

Verification of the Network Switch Configuration Tables uniquely identifying the switch position within the network shall be verified by analysis and test.

4.1.25.4 NETWORK END SYSTEM CONFIGURATION TABLES UNIQUIE ID

Verification of the Network End System Configuration Tables (NICs) being uniquely identified for an end system position within the network shall be verified by analysis and test.

4.1.25.5 CONFIGURATION DOCUMENTATION

Verification of the data required to configure the DSG Inter-Element Network be documented in TBD shall be verified by inspection.

5.0 FUTURE TOPICS FOR POSSIBLE STANDARDIZATION

5.1.1 DESCRIPTION OF FUTURE TOPIC AREAS

TBD/TBS

5.1.2 FUTURE TOPIC AREAS STANDARDS

TBD/TBS

Potential areas for future standards interoperability selection for avionics could include the areas of Command and Data Handling (Processors, Networks, and Instrumentation), Human Interfaces (Displays and Controls, Audio, Imagery, and Wearable Technology), and Electronic Design (EEE Parts, EMI/EMC, Radiation, and Manufacturing). As the Interoperability Standards development proceeds, assessments as to which areas should be addressed as well as when in the document development cycle this would occur will be decided at a future time.

APPENDIX A ACRONYMS AND ABBREVIATIONS

AFDX	Avionics
BAG	Bandwidth Allocation Gap
BE	Best-Effort
BER	Bit Error Rate
BIT	Built In Test
C&DH	Command and Data Handling
CA	Collision Avoidance
CCSDS	Consultative Committee for Space Data System
CIS	Cross Support Services
CM	Compression Master
COM/MON	Command/Monitoring
COTS	Commercial Off The Shelf
CRC	Cyclic Redundancy Check
CT	Critical Traffic
CXP	CoaXPress
DIMA	Distributed Integrated Modular Avionics
DMA	Direct Memory Access
DSG	Deep Space Gateway
ECSS	European Cooperation for Space Standardization
EMI	Electromagnetic Interface
ETG	EterCAT Technology Group
FSW	Flight Software
HEOMD	Human Exploration and Operations Mission Directorate
IDSS	International Docking System Standard
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IOAG	Interagency Operation Advisory Group
ISS	International Space Station
LAN	Local Area Network
LLC	Logical Link Control
LRU	Line Replacement Unit
MAC	Media Access Control
MCB	Multilateral Coordination Board
MOIMS	Mission Operations and Information Management Services
MTBF	Mean Time Between Failure
NASA	National Aeronautics and Space Administration

NIC	Network Interface Cards
ODN	Onboard Data Network
P2P	Point-to-Point
PBA	Printed Board Assembly
PCI	Peripheral Component Interconnect
PLC	Programmable Logic Controller
QoS	Quality of Service
RC	Rate-Constrained
RID	Review Item Disposition
SEA	System Engineering
SIS	Space Internetworking Services
SLS	Space Link Services
SM	Sync Masters
SOIS	Spacecraft Onboard Interface Services
SWaP	Size, Weight, and Power
TBD	To Be Determined
TBS	To Be Supplied
TCP	Transmission Control Protocol
TT	Time-Triggered
TTE	Time-Triggered Ethernet
TT-GbE	Time-Triggered Gigabit Ethernet
UHF	Ultra High Frequency
VL	Virtual Links
VRRP	Virtual Router Redundancy Protocol

APPENDIX B GLOSSARY

Synchronous

A synchronous network (sometimes referred to as scheduled networks) is a network in which global timing on the network is controlled for communications to occur across network components deterministically. Please note this is not to be confused with synchronous interfaces where data and clock are provide to clock a data signal.

Asynchronous

An asynchronous network (sometimes referred to as event driven networks) is a network in which communications occurs between components randomly based upon when data is collected and ready for transmission with no regard to the receiver(s) timing in the network. Please note this is not to be confused asynchronous interface where data is sent without clocking information and oversampling must be performed to interrupt the data.

Isochronous

Isochronous communication is a transmission method that ensures data flows at a steady rate so that data received at the destination is received at close to the same data rate as that generated at the source. It is accomplished by interrupting at controlled intervals the data stream being transmitted. Isochronous timing is a characteristic of a repeating event whereas synchronous timing refers to the relationship between two or more events. Video is an example of where isochronous communications is used.

Determinism

For this context is a desired property of communication in which: 1) the max message latency is bounded and known a priori, 2) the order messages are received matches the order they were sent, and 3) messages sent simultaneously will be received in an a priori known order for all recipients..

Nondeterminism

For this context, nondeterminism refers to communication where communication is does not have an upper and lower timing jitter for receipt.

Latency

A measure of time delay experienced by the system.

Jitter

The deviation from true periodicity of a presumably periodic signal, often in relation to a reference clock signal.

Switch

A switch is a device that connects multiple network components via point-to-point full duplex links. The switch makes decisions on the destination (either final or intermediate) of an received message from a point-to-point link based upon the addressing information in the message (usually in the header of the message). Messages are usually referred to as packets (could be a portion of a packet if the packet is segmented) and are bound by an upper limit in size. A switch has multiple (more than two) ports (point-to-point links) for communicating in a full duplex fashion on each port. Simultaneous communication is possible through the switch when no contention for ports exist.

Bus

A bus or logical bus is a network topology where all network components are attached to a shared medium. The bus (logical bus) is half duplex communication where only one network component may transmit at a time (half duplex). The method for when a network component is permitted to transmit varies based upon the protocol. The bus at the physical layer is also referred to as a multi-drop bus where all components connect (usually through a impedance matched coupler) to the backbone differential pair. The physical layer for the logical bus is a broadcast hub which has a point-to-point link from each network component, which is functionally the same as the multi-drop bus backbone.

APPENDIX C OPEN WORK

TBS

Table C-1 lists the specific To Be Determined (TBD) items in the document that are not yet known. The TBD is inserted as a placeholder wherever the required data is needed and is formatted in bold type within brackets. The TBD item is numbered based on the section where the first occurrence of the item is located as the first digit and a consecutive number as the second digit (i.e., <TBD 4-1> is the first undetermined item assigned in Section 4 of the document). As each TBD is solved, the updated text is inserted in each place that the TBD appears in the document and the item is removed from this table. As new TBD items are assigned, they will be added to this list in accordance with the above described numbering scheme. Original TBDs will not be renumbered.

TABLE C-1 TO BE DETERMINED ITEMS

TBD	Section	Description

Table C-2 lists the specific To Be Resolved (TBR) issues in the document that are not yet known. The TBR is inserted as a placeholder wherever the required data is needed and is formatted in bold type within brackets. The TBR issue is numbered based on the section where the first occurrence of the issue is located as the first digit and a consecutive number as the second digit (i.e., <TBR 4-1> is the first unresolved issue assigned in Section 4 of the document). As each TBR is resolved, the updated text is inserted in each place that the TBR appears in the document and the issue is removed from this table. As new TBR issues are assigned, they will be added to this list in accordance with the above described numbering scheme. Original TBRs will not be renumbered.

TABLE C-2 TO BE RESOLVED ISSUES

TBR	Section	Description

APPENDIX D SYMBOLS DEFINITION

TBS

APPENDIX E NETWORK ARCHITECTURE ATTRIBUTES

There are a number of approaches that could be used to eventually determine the types of datalink protocols that could be utilized for Exploration based upon their various attributes. One approach utilized here is based upon types of Network Architecture needs and attributes. Please note that some of these attributes are not mutually exclusive, i.e., a synchronous network may be implemented over a bus or a switch fabric, etc.

Asynchronous networks

An **asynchronous network** is one in which messages are generated and consumed in response to events or changes in system state (i.e. event-driven). Unlike in synchronous networks, in which all communication is coordinated through use of some synchronization service or external clock signal, participants within an asynchronous network may produce messages at any point in time.

As a result of this event-driven architecture, contention may occur if messages produced by different network participants contend for shared network resources. In a multidrop bus network, contention occurs if multiple nodes attempt to transmit data over the same bus simultaneously. In a switched network, contention occurs if multiple frames must be forwarded through the switching fabric to the same egress port. Asynchronous networks require some arbitration scheme in order to resolve this contention in a timely and fair manner. Some examples of common arbitration methods include Carrier Sense Multiple Access with Collision Detection and Arbitration on Message Priority (CSMA/CD+AMP) used in Controller Area Network (CAN), and the Round-Robin Matching (RRM) algorithm used in many Ethernet switch fabrics.

One disadvantage of the need for arbitration in asynchronous networks is that transmission time is inherently less predictable than in synchronous network technologies, as the delay a message experiences depends heavily on contention from competing inputs and the arbitration method used. Even priority based arbitration schemes do not guarantee predictable behavior, as minor variations in system timing can alter which messages contend at a given arbitration cycle. Asynchronous networks are also generally less composable than their scheduled counterparts. When multiple independently developed subsystems are integrated together, the resulting system often contains unintended system states and transitions caused by the interaction of event-triggered traffic between subsystems. Attempts to increase the composability of event-driven networks generally require 1) more resources dedicated to coordinating actions between subsystems at run-time (e.g. announcements, handshaking), and 2) limiting communication between subsystems as much as possible (i.e. keeping traffic internal to a given subsystem).

Compared to scheduled communication, the main advantage of asynchronous networks is their relative flexibility regarding design and implementation. First, it is not required to know the traffic patterns of all network participants at design time. Networks may be expanded incrementally over time (e.g. through the addition of new devices) without necessitating changes to the original design of the network – provided the QoS requirements of all participants are still met. Moreover, asynchronous networks do not require synchronization between node, which eliminates the need for external timing hardware or dedicated synchronization services. Also, the lack of a global communication schedule enables increased utilization of the network bandwidth and overall higher effective throughput (10Gbit/s+ for some technologies).

Overall, asynchronous networks prioritize flexibility and responsiveness over predictability, though some asynchronous technologies discussed in later sections do provide mechanisms to improve their determinism. Generally, they are best suited for systems required to respond quickly to unpredictable external events, systems that are expected to grow or change over time, or in systems requiring transmission speeds so high that concerns regarding determinism are diminished. These applications include crew interfaces and science, real-time audio/video streaming, telemetry and data processing, and general purpose onboard LANs.

Synchronous Networks

One common problem in the implementation of a shared network is the occurrence of contention, in which multiple nodes (or the messages they produce) may compete for access to shared network resources. Asynchronous networks address this problem through the use of arbitration, but introduce unpredictability regarding message transmission time and unintended system states.

A **synchronous network** is a network in which some clock service is used to coordinate the transmission of messages such that this contention *cannot occur*, so no arbitration method is required. This coordination is commonly achieved using a Time Division Multiple Access (TDMA) access scheme, in which specific time slots in which to communicate are allocated to each transmitter. Generally, communication is scheduled offline and devices are pre-configured using static messaging tables. Some method of synchronization is required to maintain a common time base between devices, and is generally provided by means of a common external reference or distributed global clock. By nature of its scheduled communication, synchronous networks are generally able to provide improved determinism over asynchronous technologies – that is, near constant latency (jitter <10 µs for some technologies) with guaranteed in-order message delivery.

However, synchronous networks have downsides that make them impractical for some spacecraft applications. Considerable effort is required to specify the timing properties and access patterns of all participants upfront, and once deployed, changes to this network configuration or the addition of new devices necessitate changes to the communication schedule. Moreover, depending on the granularity at which scheduled events may occur, the overall effective throughput of synchronous traffic may be severely limited.

Overall, scheduled communication sacrifices flexibility in order to ensure predictable network loading and deterministic traffic performance. By nature of their designs, synchronous networks are generally best suited for critical applications requiring hard real-time distributed control, periodic communication, and which do not require extensive modification once deployed. These domains include networking for vehicle command and control (e.g. onboard computers (OBCs), inertial measurement units (IMUs), star trackers, sensors/actuators, and telerobotics (e.g. motor controllers, embedded processors).

Traditionally, vehicle control networks have been implemented using a multi-drop bus network. This choice of topology is partially motivated by the transaction patterns generally found in this application, in which traffic flow is required between end devices (e.g. sensors/effectors) and one or more OBCs, but not between the end devices themselves. Furthermore, the required throughput in most vehicle control networks is relatively low (e.g. < 2Mbit/s), which can be accommodated by multiple modern deterministic buses.