

AEROSPACE INFORMATION REPORT

AIR5654™

REV. A

Issued 2009-04
Revised 2019-08
Reaffirmed 2025-04

Superseding AIR5654

(R) IEEE-1394b for Military and Aerospace Vehicles - Applications Handbook

RATIONALE

Update document to incorporate lessons learned during manufacturing, production, and flight test.

AIR5654A has been reaffirmed to comply with the SAE Five-Year Review policy.

TABLE OF CONTENTS

1.	SCOPE.....	4
1.1	Purpose	4
1.2	Background	4
2.	REFERENCES.....	4
2.1	Applicable Documents	4
2.1.1	SAE Publications.....	4
2.1.2	IEEE Publications.....	5
2.1.3	Other Publications.....	5
2.2	Definitions	5
3.	IN-DEPTH VIEW OF THE STANDARD.....	8
3.1	Introduction to AS5643 Network Architecture and Protocols.....	8
3.2	Highlights of AS5643 Determinism and Fault Tolerance	10
3.2.1	Determinism	10
3.2.2	System Integrity and Fault Tolerance Mechanisms.....	11
3.3	Failure Mode Analysis for AS5643 Architecture	13
3.3.1	Failure Modes and AS5643 Solutions.....	13
3.3.2	FMEA Scoring.....	17
3.4	Summary.....	20
3.4.1	Evaluation for Applications Other Than Military Applications	20
3.4.2	Enhancing Fault Containment, Fault Isolation, and Recovery.....	21
4.	CONTROL COMPUTER DESIGN	21
4.1	Number of Ports per Node	21
4.2	Control Computer Synchronization	21
4.3	Simultaneous Operation of Multiple Buses	22
4.4	Buffer-Fill and Packet-per-Buffer Modes.....	23
5.	REMOTE NODE DESIGN.....	24
5.1	Number of Connected Ports Considerations	24
5.2	Redundancy Considerations.....	24
5.2.1	System Integrity Management	24

SAE Executive Standards Committee Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2025 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, or used for text and data mining, AI training, or similar technologies, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER:
Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
http://www.sae.org

For more information on this standard, visit
<https://www.sae.org/standards/content/AIR5654A/>

Documents

Standard, visit Sharing Hub

5.3	Bandwidth and Throughput Considerations.....	27
5.3.1	Application Scheduling of 1394 Transmit Packets.....	27
5.4	Remote Terminal Design Lessons Learned.....	27
5.4.1	STOF Synchronization	27
5.4.2	Peak Load Handling.....	27
5.4.3	Payload Path Integrity.....	27
5.4.4	Failure Containment.....	27
5.4.5	Minimization of 1394 Bus Resets.....	28
6.	FAULT TOLERANT NETWORK ARCHITECTURE AND TECHNIQUES	28
6.1	Architectural Considerations	28
6.1.1	Redundant CCs.....	28
6.1.2	Cross-Channeling CCs and Remote Nodes	29
6.1.3	Looping Busses.....	29
6.1.4	Leaf Nodes.....	31
6.1.5	Other Redundant Architecture Example	31
6.1.6	Put All Pieces Together - The Network.....	32
6.2	Physical Network Layout Considerations.....	34
6.2.1	Distance Between Nodes.....	34
6.2.2	Repeaters.....	34
6.2.3	Overall Considerations.....	35
7.	TEST EQUIPMENT CONSIDERATIONS AND SUGGESTION	35
7.1	Bus Analyzer Requirements	36
7.2	Signal Integrity Requirements.....	39
7.2.1	Signal Integrity Test Tool Requirements.....	39
8.	BUS TIMING AND LATENCY	40
8.1	Establishing STOF Frequency.....	40
8.2	Establishing STOF Offsets for Each Node.....	41
8.3	Establishing the Process for Changing STOF Offsets.....	43
9.	CABLE DESIGN.....	44
9.1	Extended Cable Length.....	44
9.2	Harness Considerations for AS5643/1.....	46
9.2.1	Harness Construction.....	46
9.2.2	Testing of Harnesses	48
10.	LESSONS LEARNED IN SYSTEM INTEGRATION.....	57
10.1	Techniques for Mitigating Failures	57
10.1.1	Identifying/Avoiding Single Point Failures.....	57
10.1.2	Hardware Failures That Lead to Bus Resets	58
10.1.3	Handling Initialization Sequences and Bus Resets	61
10.1.4	Packet Data Structures	65
10.2	Considerations for Testing and Optimizing the System.....	65
10.2.1	Internal STOF Consideration	65
10.2.2	Device Settings for Optimal Throughputs	66
10.2.3	Bit Error Rate Verification.....	67
10.2.4	Suggestion for Robust Configuration	68
10.2.5	ASM Payload Size Clarification	68
10.2.6	Forced Root Node Setting	68
11.	FREQUENTLY ASKED QUESTIONS AND ANSWERS	69
12.	NOTES.....	96
12.1	Revision Indicator.....	96

Figure 1	Basic network with single CC	8
Figure 2	Basic network with single CC and a loop	9
Figure 3	Representative triplex CC architecture	10
Figure 4	Multiple 1394 buses with dedicated local memory	22
Figure 5	Multiple 1394 buses competing for common memory	23
Figure 6	Flowchart of Redundant System Integrity Management	26
Figure 7	Triplex network with multiple cross-channel connections	29
Figure 8	Basic network with single CC and a loop	30
Figure 9	Four nodes cross-connected to each other	32
Figure 10	Representative triplex CC architecture	33
Figure 11	Repeater	35
Figure 12	Cable testing using a triple FireSpy 1394 bus analyzer and repeaters	37
Figure 13	Cable testing using a QP-ICT interconnect tester with output level control	38
Figure 14	Example 38999 test fixture	39
Figure 15	QP-SQT beta signal quality tester	40
Figure 16	Timing diagram for node A with STOF	41
Figure 17	STOF offset effect on command path latency	42
Figure 18	Data latency timeline	42
Figure 19	Example sensed AOA to actuator motion	43
Figure 20	Example cable termination method from AS5643/1	46
Figure 21	Improved cable termination method	47
Figure 22	Eye pattern measurement	49
Figure 23	Harness test set-up	50
Figure 24	Bit error rate GUI	56
Figure 25	Harness with excessive right-angle bends	56
Figure 26	Basic network with single CC and a loop	58
Figure 27	Initialization and configuration timing	59
Figure 28	Typical disconnect and reconnect timing	60
Figure 29	Bus reset generation GUI	64
Figure 30	Host interfacing with network logic	65
Figure 31	BER test setup	67
Figure 32	Test times for various confidence levels and bit errors	68
Figure 33	IEEE-1394b PHY layer differential signals	70
Figure 34	The displacement of asynchronous stream packets with isochronous packets	78
Figure 35	1394b node under test	80
Figure 36	1394b node unit under test interconnection	81
Figure 37	Buffer fill mode versus packet per buffer mode	84
Figure 38	Node consideration diagram	85
Figure 39	Speed negotiation signaling diagram	86
Figure 40	S400 speed negotiation signaling example	87
Figure 41	S400 speed with acknowledge	87
Figure 42	S800 detect, speed, acknowledge, sync, and loss of sync	88
Figure 43	Example 512.04 ms network initialization	88
Figure 44	Example connection loop disabled to connection active diagram	93
Figure 45	Isolation PHY clears RHB	94
Table 1	Failure modes analysis	14
Table 2	FMEA score results	18
Table 3	Guidance for extended cable length	45

1. SCOPE

This Handbook is intended to accompany or incorporate AS5643, AS5643/1, AS5657, AS5706, and ARD5708. In addition, full understanding of this Handbook also requires knowledge of IEEE-1394-1995, IEEE-1394a, and IEEE-1394b standards.

This Handbook contains detailed explanations and architecture analysis on AS5643, bus timing and scheduling considerations, system redundancy design considerations, suggestions on AS5643-based system configurations, cable selection guidance, and lessons learned on failure modes.

1.1 Purpose

The purpose of this document is to provide application details, including explanations of AS5643, AS5643-based system design considerations, bus timing and scheduling, experiences on design tools, and lessons learned, that are not typically included in a SAE standard such as AS5643. It is intended to promote and support the use of AS5643, and to serve as a platform for information exchange.

1.2 Background

IEEE-1394 was invented by Apple Computer in the 1980s and is also known as Firewire. In 1995, the IEEE adopted it and created a specification to support its use. That specification has been continuously upgraded and improved. In 2002, the IEEE released 1394b, the version SAE has adopted for use in military and aerospace vehicles. IEEE-1394-2008, which combines all of the previous versions and errata into a single document, was released June, 2008. Answers to Q1 and Q3 in Section 11 will provide more details on different versions of IEEE-1394 standards.

Prior to its use in the Lockheed Martin F35 Lightning II (Joint Strike Fighter), IEEE-1394b had never been used as a flight critical or mission critical system data bus in any military or aerospace vehicle. The IEEE-1394b specification does not provide necessary functionalities, such as guaranteed determinism and information integrity for use in aerospace applications, such as the flight control system for aircraft. For that reason, the SAE variant of IEEE-1394b was conceived and implemented.

In addition to the F-35 program, the use of IEEE-1394b for safety critical/mission critical systems has been considered or is being considered by other major commercial aircraft program, space manned and unmanned vehicles for explorations, and defense systems other than fighters.

2. REFERENCES

2.1 Applicable Documents

The following publications form a part of this document to the extent specified herein. The latest issue of SAE publications shall apply. The applicable issue of other publications shall be the issue in effect on the date of the purchase order. In the event of conflict between the text of this document and references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

2.1.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or +1 724-776-4970 (outside USA), www.sae.org.

AS5643A	IEEE-1394b Interface Requirements for Military and Aerospace Vehicle Applications
AS5643/1	S400 Copper Media Interface Characteristics Over Extended Distances
AS5657	Test Plan/Procedure for AS5643 IEEE-1394b Interface Requirements for Military and Aerospace Vehicle Applications
AS5706	Test Plan/Procedure for AS5643/1 S400 Copper Media Interface Characteristics Over Extended Distances

SAE Aerospace Council of the SAE Technical Standards Board Organization and Operating Guide for Aerospace Standards Development Program, February, 2002.

SAE Aerospace Technical Report Style Manual, October, 2004.

SAE International Technical Standards Board Governance Policy, 7th Revision, May, 2004.

2.1.2 IEEE Publications

Available from IEEE Operations Center, 445 and 501 Hoes Lane, Piscataway, NJ 08854-4141, Tel: 732-981-0060, www.ieee.org.

IEEE Std 1212-2001	IEEE Standard for a Control and Status Registers (CSR) Architecture for Microcomputer Buses
IEEE Std 1394-1995	IEEE Standard for a High Performance Serial Bus
IEEE Std 1394a-2000	IEEE Standard for a High Performance Serial Bus - Amendment 1
IEEE Std 1394b-2002	IEEE Standard for a High Performance Serial Bus - Amendment 2
IEEE Std 1394c-2006	IEEE Standard for a High Performance Serial Bus - Amendment 3
IEEE Std 1394-2008	IEEE Standard for a High Performance Serial Bus (Combines all previous IEEE standards and amendments)

2.1.3 Other Publications

1394 Open Host Controller Interface Specification, January, 2000.

2.2 Definitions

The reader is encouraged to review the following terms and definitions before proceeding to the remainder of the document. By convention, these terms are expanded here only; in the remainder of this document, these terms are used in their shortened form.

ADS: Air Data System. Senses, computes, and outputs all parameters associated with aircraft movement through the atmosphere.

AOA: Angle of Attack. A term used in aerodynamics to describe the angle between the airfoil's chord line and the direction of airflow wind, effectively the direction in which the aircraft is currently moving. It can be described as the angle between where the wing is pointing and where it is going.

ASM: Anonymous Subscriber Messaging. Tailored to support deterministic, secure, low-latency communication between processors, sensors, instrumentation, and displays in mission-critical applications. It uses Message IDs to decouple the network traffic from physical addresses so application software can communicate without knowledge of network topology.

AWG: American Wire Gauge, also known as the "Brown and Sharpe" wire gauge. Used in the United States and other countries as a standard method of denoting wire diameter, especially for nonferrous, electrically conducting wire.

BER: Bit Error Rate. A parameter relating to the quality of a serial transmission system. BER is the percentage of bits having errors, relative to the total number of bits received in a transmission. BER is usually expressed as ten to a negative power.

BURSTABILITY: The ability to support burst-mode in which a device is transmitting data repeatedly without waiting for input from another device or waiting for an internal process to terminate before continuing the transfer of data. A high-speed data transfer ability like DMA that can transfer data at significantly higher rates. Ability to perform back-to-back burst operations.

BOSS: Bus Owner/Supervisor/Selector. The arbitration scheme defined by IEEE-1394b-2002 and implemented in 1394b-compliant LLCs. The principle features of BOSS arbitration are that the node making the arbitration decision varies, that arbitration requests may be overlapped with data transmission, and that both isochronous and asynchronous requests may be pipelined for the succeeding isochronous interval or fairness interval, respectively.

CC: Control Computer. The CC is the root node, cycle master (if used), and bus manager for its respective data bus. The CC “controls” the bus and generates the STOF packets.

CCDL: Cross-Channel Data Link. Interconnects a number of control computers or remote terminals together to improve the fault tolerance capability. See 6.1.2 for additional information.

COTS: Commercial Off-the-Shelf. A term for software or hardware, generally technology or computer products, that are ready-made and available for sale, lease, or license to the general public.

CRC: Cyclic Redundancy Check. An error detecting code commonly used in digital networks and storage devices to detect accidental changes to raw data. Blocks of data entering these systems get a short check value attached, based on the remainder of a polynomial division of their contents.

CHANNEL/CHANNEL NUMBER: The means by which Isochronous and Asynchronous Stream packets are addressed. Data is transmitted onto the bus with a particular channel number. Nodes on the bus wishing to receive the data are configured to accept packets that have been addressed to that channel number.

dB: Decibel. A logarithmic unit of measurement that expresses the magnitude of a physical quantity (usually power) relative to a specified or implied reference level.

ENQUEUE/ENQUEUEING: To add an item to a queue.

FIFO: First In, First Out. This expression describes the principle of a queue or first-come, first-served (FCFS) behavior: what comes in first is handled first, what comes in next waits until the first is finished, etc.

FMEA: Failure Mode and Effects Analysis. A risk assessment technique for systematically identifying potential failures in a system or a process. It is widely used in the manufacturing industries in various phases of the product life cycle.

FRAME: The time interval between consecutive STOF messages (e.g., 10.0 ms).

FEET: Feet or foot is a unit of length.

IBIT: Initiated Built-in-Test mode.

IRM: Isochronous Resource Manager. A function that an IEEE-1394b node can have to negotiate and allocate isochronous transaction bandwidth.

JSF: Joint Strike Fighter. The F-35 Lightning II is a single-seat, single-engine, stealth-capable military strike fighter, a multi-role aircraft that can perform close air support, tactical bombing, and air-to-air combat. The F-35 descended from the X-35 of the JSF program. Its development is being funded by the United States, the United Kingdom, and other partner governments.

LINK LAYER: The serial bus layer that defines the data transfer services. It also provides addressing, data checking, and data framing.

LLC: Link Layer Controller. The hardware component that performs the link layer services.

Mbps: Megabits per second. A measure of bandwidth (the total information flow over a given time) on a telecommunications medium.

MHz: Megahertz. A unit of frequency. 1 MHz is 10^6 Hz.

us OR μ s: Microsecond. A microsecond (us or Greek letter mu plus s) is one millionth (10^{-6}) of a second.

μV: Microvolt. A unit of potential equal to one millionth of a volt.

NASA: National Aeronautics and Space Administration.

NODE: An addressable device attached to the serial bus with at least the minimum set of control registers. A node may have one or more ports.

PHY: The hardware component that performs the physical layer services.

PHYSICAL LAYER: The serial bus physical layer that translates the logical symbols used by the link layer into electrical signals on serial bus media. The PHY is also responsible for performing the arbitration tasks for a node to gain access to the bus.

PREFETCH/PREFETCHABILITY: A technique which attempts to minimize the time spent waiting for instructions or data to be fetched from memory by preloading the instructions or data into a buffer or queue before the operation is initiated.

PORT: A physical layer entity in a node that connects to a cable and provides one end of a physical connection with another node.

QUADLET: Four bytes, or 32 bits of data. The normal word size in 1394 packets.

REMOTE NODE: A node, other than the CC, on a bus.

RESET:

1. Cold Reset - Resetting the system by starting the system from the power off state.
2. Warm Reset - Resetting the system without turning the power off (software- or hardware-initiated reset). The opposite of cold reset.
3. Hot Reset - Resetting the system without turning the power off and bypassing time consuming built-in-test functions to minimize startup time for critical systems.

ROM: Read-Only Memory. A class of storage media used in computers and other electronic devices. Because data stored in ROM cannot be modified (at least not very quickly or easily), it is mainly used to distribute firmware.

RPN: Risk Priority Number. A number used in FMEA evaluation to indicate the potential risk of a failure mode.

ROOT NODE: The node on the bus with the highest node ID. The root node may be the cycle master and is responsible for resolving arbitration in IEEE-1394 buses. The root serves this function when in 1394a mode on a 1394b bus, but when a bus can do 1394b BOSS arbitration, it is the BOSS node (node currently transmitting) that grants the bus (resolves arbitration).

STOF: Start of Frame. A packet sent by each CC at a periodic (frame) rate. The STOF packet is used to synchronize the bus.

VMS: Vehicle management system is an integrated avionics system that performs functions such as command and control, guidance and navigation, fault management, etc.

VPC: Vertical Parity Check. Is performed on the data area of each packet as an adjunct to the CRC performed by the 1394 physical layer devices. The VPC provides additional data integrity as the messages progress through the physical and software layers.

3. IN-DEPTH VIEW OF THE STANDARD

3.1 Introduction to AS5643 Network Architecture and Protocols

It is assumed that the reader is already familiar with the IEEE-1394b architecture and protocol. This section details some of the differences between traditional IEEE-1394b and AS5643. These changes have been made in support of creating a more robust network. Justification for each of these changes is outside the scope of this document. A considerable portion of this section has been taken directly from the AS5643 standard.

AS5643 is a set of enhancements to the IEEE-1394b standard. They include the use of asynchronous stream packets (see the answer to Q5 in Section 11) with no requirement for asynchronous packets or isochronous packets (except that provisions are made to provide for both types, if desired), a fixed frame rate synchronized with a STOF packet, addition of a VPC, static assignment of channel numbers, pre-assignment of bandwidth, use of ASM, and a static assignment of the root node. The root node is also referred to as the CC. The CC will be the cycle master (if used) and bus manager for each respective data bus. The differences described above will be discussed in more detail in this section and the answer to Q2 in Section 11. This section starts by looking at three different network architectures.

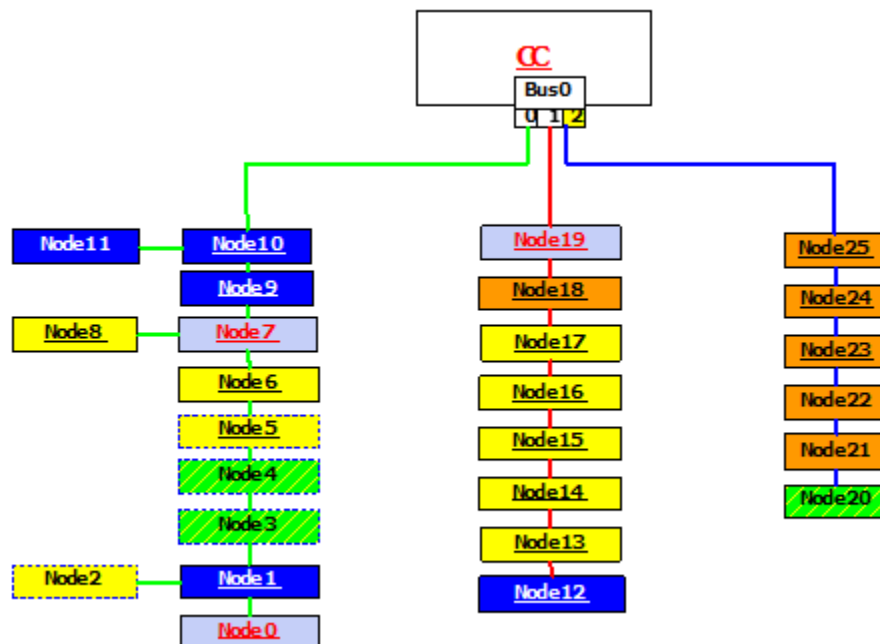


Figure 1 - Basic network with single CC

Figure 1 illustrates a basic network architecture with a single CC. Even though each of the three ports of the CC has remote nodes attached, it comprises a single IEEE-1394 bus.

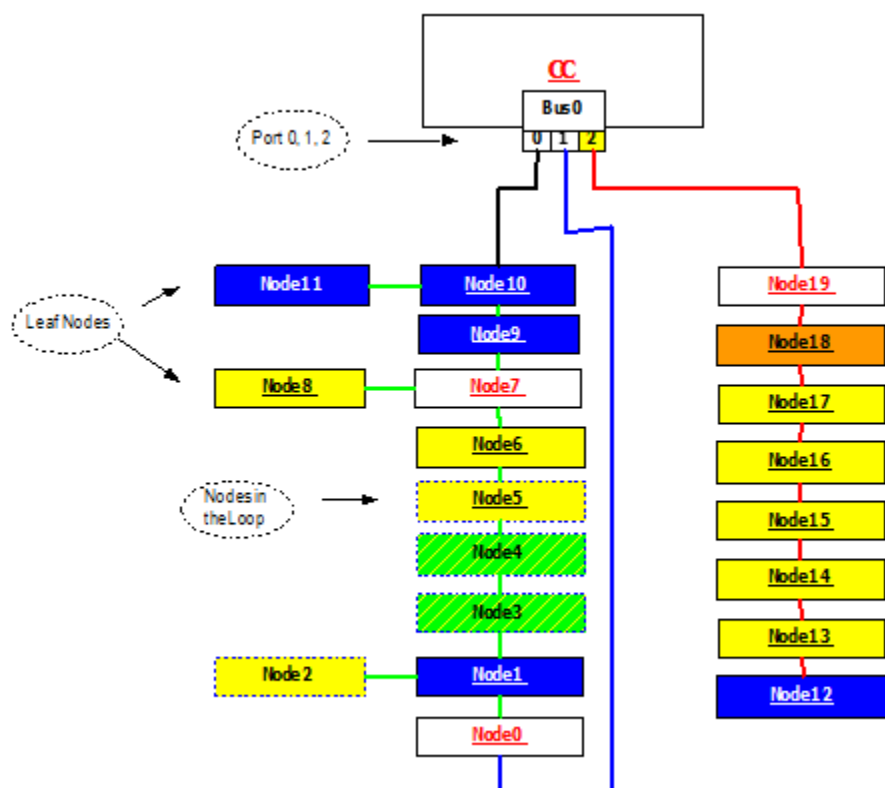


Figure 2 - Basic network with single CC and a loop

Figure 2 illustrates a basic network architecture utilizing a single CC and a loop created by connecting port 0 back to port 1 of the CC. Loops are not allowed in IEEE-1394 and IEEE-1394b PHYs will automatically detect and break the loop. Exactly where the loop is broken is unknown until the new architecture tree has been configured. After the PHYs break the loop, there will be two branches: one on port 0, and the other on port 1. If the cable is broken or the PHY layer of a node on either port should now fail, the bus will automatically reconfigure with the failed node on the “end” of one of the branches. (See 3.2.2.3 for a discussion of this loop failure/reconfiguration process.) All other nodes will still be enabled. This provides the first level of redundancy. Refer to 0 for additional information.

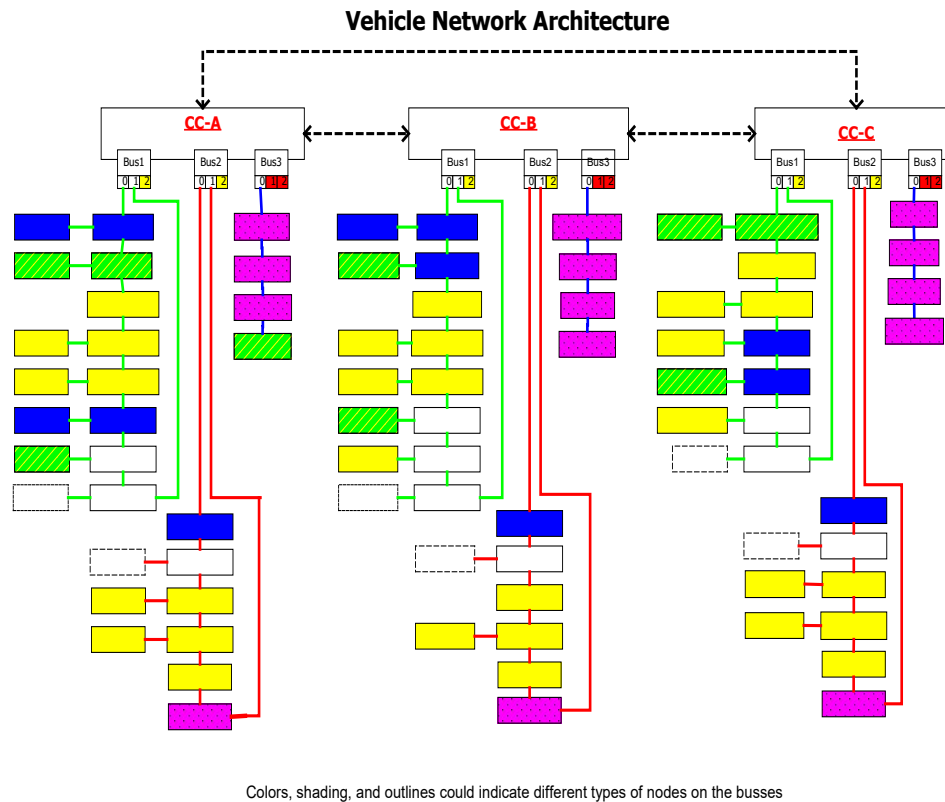


Figure 3 - Representative triplex CC architecture

Figure 3 illustrates an architecture for a representative triplex 1394 vehicle network adopted by JSF. The three CCs have been cross-channel linked, thus providing another level of redundancy.

3.2 Highlights of AS5643 Determinism and Fault Tolerance

In this section, we discuss main enhancements of AS5643, and benefits they provide for general space and military applications. We present these enhancements in terms of determinism and fault tolerance.

3.2.1 Determinism

IEEE-1394b does not provide sufficient determinism required by a typical space and/or military application. The only deterministic mechanism is its isochronous transmission mode where data transmission occurs uniformly in time and recurs at regular intervals. Within a transmission cycle (125 μ s), the transmission of isochronous packets start with the arriving of the cycle start packet. However, the arrival of the cycle start packet may be delayed by the unfinished transmission of asynchronous transaction packets, which leads to isochronous transmission delays and delay variations, but guaranteed to be a maximum of 125 μ s. Our previous study¹ has shown that, compared to the cycle time, 125 μ s, these delays and delay variations are significant enough to impact the determinism of a space and/or military vehicle network. Other features of IEEE-1394b, such as dynamic bandwidth allocation for isochronous and asynchronous transactions, re-election of a root node, and dynamic assignments of channel numbers, also cause insufficient determinism.

Designed for the F-35 Joint Strike Fighter, AS5643 significantly improves the network determinism over IEEE-1394b. In particular, improvements are made by the following enhancements to IEEE-1394b.

¹ Haowei Bai, Allalaghatta Pavan, Brian VanVoorst, Sabera Kazi, Vic Thomas, "On-Board High-Speed Avionics Data Network," Final Report, Honeywell AES IES CoE, 2003.

Pre-configured network topology: The network topology is configured by application requirements, and is likely the same for the lifetime of a vehicle.

Forced root nodes: Because of the pre-configured network topology, CC nodes are pre-configured to be forced roots. There are no re-elections of root nodes.

Use of asynchronous streaming: An asynchronous stream packet is actually an isochronous formatted packet transmitted in the fairness interval or asynchronous time frame. Packet transmissions are carried out in accordance with asynchronous arbitration rules, but without acknowledgements. Isochronous and asynchronous transactions are normally not used.

Global synchronization provided by STOF packets: The STOF packet can be generated by upper-layer software and transmitted at a periodic rate (e.g., 80 Hz), in order to provide a single synchronization source for nodes on multiple redundant buses. The IEEE-1394 standard provides a similar mechanism through the cycle master function. The cycle master is implemented in the 1394 link layer chip and it sends its cycle time to the local bus in cycle start packets 8000 times a second (125 μ s) to maintain synchronization with nodes on the local bus. Because cycle start packets are only sent to the local bus, it is difficult to maintain global synchronization among nodes on multiple redundant buses using only cycle start packets.

Static assignment of channel numbers: There are a total of 63 channels that can be assigned to each node. Channel numbers for each node on the bus are pre-assigned according to application requirements. Each node on a bus must be assigned a unique channel number. Channel numbers can be duplicated on separate busses (CC-A bus 0 and bus 1 would both have the CC as channel 0).

Pre-assignment of bandwidth: Because only asynchronous streaming is used normally in AS5643, all bandwidth is eligible to be allocated. AS5643 also accommodates the use of asynchronous and isochronous data streams, if desired. See 3.3.3 and FAQ Q31/A31. Transmit and receive times for each node on the bus are strictly regulated by offsets relative to STOF packets. Offset information is transmitted by CC nodes (to remote nodes) together with STOF packets. The offsets for each node on the bus are application specific.

TDMA-style packet transmission: CC nodes continuously send STOF and offset information for each channel once every STOF period (e.g., 12.5 ms or 80 Hz), this ensures that remote nodes will continuously receive STOF information even if powered up late or if the remote node(s) experience a power cycle. Remote nodes that need that information to get synchronized with the network only listen to it once. This is to avoid the remote node's loss of synchronization.

3.2.2 System Integrity and Fault Tolerance Mechanisms

The AS5643 architecture enhances the system integrity and the fault tolerance capability of the original IEEE-1394b in the following ways.

3.2.2.1 Enhanced Fault-Containment Schemes

VPC: VPC is performed on the data area of each packet as an adjunct to the CRC performed by the 1394 link layer devices. The VPC provides additional data integrity as the message progresses through the physical and software layers.

Health status word: The 32-bit health status word is the word 0 of the packet payload. The health status word is able to signal the following information.

- Packet error.
- Subsystem error.
- Node error.
- STOF offset acknowledgement.
- Status of each port of a node: connected, receiving OK, beta mode, and the negotiated data rate.

Heartbeat: The 32-bit heartbeat word is the word 1 of the packet payload. The purpose of the heartbeat is to ensure that applications running on CC nodes generate fresh data. The heartbeat is generated by application software, rather than just inserted by an independent timer.

CC status word: The 32-bit CC status word is the word 1 of the STOF packet payload. It signals failure states of each CC in the network.

Data transmission integrity detection: CC nodes monitor the inputs from remote nodes to verify proper IEEE-1394 bus operation and to verify that the remote node that produced the message is operating correctly. A data message shall be considered valid if all of the following conditions are met.

- The value of heartbeat word has updated since the last received message.
- The data validity indicators (e.g., VPC) are correct.
- The 1394 CRC is valid.

CC failure detection: Each remote node monitors the inputs from the CC (including the STOF message) to determine the failure state of the CC, to verify proper 1394 bus operation, and to verify the CC software that produced the message is operating correctly. In order for nodes to accept data from the CC during normal bus operation, all of the following conditions shall be met.

- STOF message timing is valid if determinable by the remote node.
- STOF message is valid.
- STOF message indicates the CC is in a legal operating mode and is in a "good" state.
- CC to node message is valid.

3.2.2.2 Enhanced Fault Isolation and Recovery

Cross-channel interconnection (optional): Three CC branches (a CC branch refers to a CC node as the root and all other nodes connected to the CC) are interconnected by another 1394b bus or a different type of data bus (e.g., MIL-STD-1553). All three CC branches process data simultaneously, constantly comparing results across channels to assure data integrity. In the case of divergent data, two processors can "vote" one processor or signal out. The detail of cross-channel interconnection is out of the scope of AS5643.

Port enabling and disabling: The ability of a node to enable or disable individual ports (a port is the physical interface to a link). A node in the bus is able to disable a link connected to a failed node, and enable a backup link to bypass the failed node.

PHY layer can be powered by cable connection: This allows the link-layer controller and the host processor to be powered off without affecting the capability of the physical layer to pass on messages. It is useful for isolating a failed processor during the fault recovery process.

3.2.2.3 Fault Protection by System-Level Redundancy

Loop breaking provides first-level redundancy: The PHY layer of AS5643 is based on the IEEE-1394b-2002 signaling standard, where automatic detection and breaking of loops are supported. Loops will be detected and broken during the bus initialization process. During normal bus operations, loops are not allowed because an IEEE-1394b network has a tree topology. Implementing a loop enhances redundancy by providing an alternate path to a node when another node on the bus fails by automatically reconfiguring with the failed node on the very end of a tree. See 6.1.3 for recommended further elaboration (loop breaking handled at PHY level).

Triple system redundancy example: Triplex 1394b network by interconnecting three CC branches. Each CC is connected to three independent buses (through three independent PHY within the same CC). Each bus has three physical ports.

3.3 Failure Mode Analysis for AS5643 Architecture

Fault tolerance is the ability of a system to continue satisfactory operation in the presence of one or more non-simultaneously occurring hardware or software faults (meaning that a second fault cannot occur until fully recovered from the first fault). It is therefore important to have a good understanding of system faults of the AS5643 architecture before we are able to analyze and further improve the fault tolerance capability. In this section, we first qualitatively evaluate failure modes of the AS5643 architecture, based on the information that has been released by Lockheed Martin to the SAE AS-1A3 working group. Secondly, our quantitative assessment of the AS5643 architecture is presented using a tool called FMEA. We would like to emphasize here that our failure mode analysis is based on limited JSF architecture information available to the public and generic application requirements. We are sure there are many ways we can improve our study in the future.

3.3.1 Failure Modes and AS5643 Solutions

Failure modes are evaluated in terms of the criticality of a failure (determined by the probability of occurrence and severity of the system), the detection scheme, and the recovery scheme. We make the following assumptions for our evaluation:

- Space applications are characterized by long mission periods, more availability than criticality², less weight and power consumption preferred.
- Fault detection and recovery schemes are based on AS5643.

We would like to point out that we did not use a quantitative definition for the probability of occurrence (the occurrence of a failure) in our analysis. As we know, currently two standards quantitatively define the probability of failure. FAA Advisory Circular 25.1309-1A defines the most well known 10^{-9} per flight hour definition for civil avionics. MIL-STD-1629 has a substantially different definition of probability of failure for military avionics. We are not aware of any standards for space applications (manned and unmanned). We want to emphasize that the definition may be application dependent. Manned space vehicles may have different requirements from satellites. An architecture with radiation-hardened components may also have different requirements from the one with more redundancy implemented by qualified COTS components.

With these assumptions in mind, some of the faults severe to military and/or commercial aircraft applications may not be that severe in space applications. For example, infrequent bus resets should be seriously considered in JSF fighter architecture. However, they may not be a big concern for a space vehicle, as most of application in the vehicle may be able to wait several hundred milliseconds for bus initialization. The failure mode evaluation results are shown in Table 1.

² Compared with military and commercial avionics, space missions have much longer durations. Therefore, availability is more important in space missions, but not at the price of criticality. Both availability and criticality are needed.

Table 1 - Failure modes analysis

Failure Mode Analysis for 1394b Fault Tolerant Architecture					
Assumptions: 1. Space application (long mission period, need more availability than criticality, less weight, less power consumption). 2. Fault detection and recovery analysis is based on AS5643 1394b architecture.					
Notations: Severity classification adopted from MIL-STD-882, Class I (catastrophic failure effect), Class II (critical effect), Class III (slight effect), and Class IV (no effect).					
Note: In this context, “not defined” means an answer to a specific question is not defined in the AS5643 standard; it does not necessarily mean that it is not defined for JSF architecture, as not all JSF information is released to the public yet.					
Faults	Failures	Criticality		Detection	Recovery
		Probability of Occurrence	Severity to System		
Bursty data error of more than 32 bits	Invalid data to application	Low	Class III	Not defined	Not defined
Bursty data error of fewer than 32 bits	Data is not passed to application	Medium	Class III	Bit 31 of health status word in data packets; VPC; CRC; heartbeat word	Not defined
Device memory failure	Invalid data	Medium	Class II	Bit 31 of health status word in data packets; VPC; CRC; heartbeat word	Not defined
Cable broken	Non-responsive	Medium	Class I	Bits 7, 15, and 23 of health status word in data packets; PHY port status register value	Redundant copy of disconnected node to take over
Node disfunction	Babbling	Low	Class I	Bit 29 of health status word in data	Not defined (but generally may be hard, as the bus may be re-partitioned if a PHY failure of a node)
Conflict of node ID/address	Masquerading	Low	Class II	Not defined	Not defined
Power down	Bus reset; non-responsive	Low	Class I	Heartbeat	Not defined
Functional node attachment	Bus reset	Low	Class IV	Bits 7, 15, and 23 of health status word in data packets; PHY port status register value	Bus initialization after reset (need manual static configuration for this newly added node to function)
Functional node detachment	Bus reset	Low	Class IV	Bits 7, 15, and 23 of health status word in data packets; PHY port status register value	Bus initialization after reset

Faults	Failures	Criticality		Detection	Recovery
		Probability of Occurrence	Severity to System		
Unexpected node attachment	Bus reset	Low	Class III	Bits 7, 15, and 23 of health status word in data packets; PHY port status register value	Bus initialization after reset (this newly added node will not affect the existing network, as long as it is not statically configured, e.g., channel assignments)
Unexpected node detachment	Bus reset, non-responsive	Medium	Class I	Bits 7, 15, and 23 of health status word in data packets; PHY port status register value	Bus initialization after reset; redundant node to take over
Expected reset requested by software	Bus reset	Medium	Class IV	PHY register values return to default; port connection indication bits in CC status word of STOF packets and health status word of data packets cleared	Bus initialization after reset
Unexpected reset requested by software due to bugs	Bus reset	Low	Class III	PHY register values return to default; port connection indication bits in CC status word of STOF packets and health status word of data packets cleared	Bus initialization after reset
Max arbitration time reached	Bus reset	Low	Class IV	Arbitration timer timing out; port connection indication bits in CC status word of STOF packets and health status word of data packets cleared	Bus initialization after reset

Faults	Failure	Criticality		Detection	Recovery
		Probability of Occurrence	Severity to System		
Port enable	Bus reset	Low	Class III	Bits 7, 15, and 23 of health status word in data packets; PHY port status register value; port connection indication bits in CC status word of STOF packets and health status word of data packets cleared	Bus initialization after reset
Functional port disable	Bus reset	Medium	Class IV	Bits 7, 15, and 23 of health status word in data packets; PHY port status register value; port connection indication bits in CC status word of STOF packets and health status word of data packets cleared	Bus initialization after reset
Unexpected port disable (all ports of a bus)	Bus reset; non-responsive	Low	Class I	Bits 7, 15, and 23 of health status word in data packets; PHY port status register value; port connection indication bits in CC status word of STOF packets and health status word of data packets cleared	Bus initialization after reset; redundant copy of disconnected node to take over
Rapidly drifting global clock (STOF offset)	Babbling; bus reset	Low	Class II	Interval between two consecutive STOF should not exceed $10\text{ ms} \pm 50\text{ }\mu\text{s}$ for 100 Hz frame rate (remote nodes perform this job)	Not defined
CC does not produce STOF	Non-responsive	Medium	Class I	Not defined	Not defined

Faults	Failure	Criticality		Detection	Recovery
		Probability of Occurrence	Severity to System		
CC does not produce STOF at the right timing	Timing violation	Low	Class I	Interval between two consecutive STOF should not exceed 10 ms ± 50 µs for 100 Hz frame rate (remote nodes perform this job)	If STOF does not arrive at the expected timing for three consecutive STOF, CC is considered failed
CC failed	Non-responsive	Medium	Class I	Heartbeat (32-bit word in data packets); CC status word in STOF packet; STOF does not arrive at the defined interval for three consecutive frames	Not defined in this standard (redundant CC to take over)
STOF offset (transmit, receive timing for a remote node) sent by CC is different	Timing violation	Low	Class I	Remote node to look for specific bits in STOF packets	Before a new bus reset; remote node to ignore the different offsets; after a new bus reset, remote node should use the new offsets
Application software bugs	Application does not refresh data	Medium	Class I	Heartbeat counter value is not incremented	Remote node ignores the message (does not pass to application layer); if fails for three consecutive STOF, CC is considered failed

3.3.2 FMEA Scoring

The FMEA evaluation for the AS5643 architecture focuses on a single CC branch. The system-wide failure mode, detection, and recovery schemes are application dependent. Some simulation studies may reveal further insights into the overall system behavior. The evaluation is an example only, without targeting at any specific defense and space applications. A separate evaluation is needed for each specific application.

The FMEA scoring results in Table 2 show the following failure modes have higher risks to the system, and therefore must be addressed further. The scoring system used in Table 2 is: 1 means low severity to customer requirements, not likely to occur, not difficult to detect; 3 means medium severity to customer requirements, medium likelihood to occur, somewhat difficult to detect; and 7 means high severity to customer requirements, very likely to occur, very difficult to detect.

The unexpected power-down of a node: This failure mode gets a high RPN because of the possible loss of application functionality due to the loss of the node together with the fact that application level logic is required to detect the loss of this functionality. The JSF avionics architecture addresses this problem by having triple-redundant networks. This solution may or may not be the best for space based systems where weight and power requirements may be more demanding than application recovery times. (Risk Item No. 7.)

Errors in device memory: Errors in device memory can result in faulty data being passed on to the application. The VPC specified by the AS5643 architecture may or may not be sufficient for space based applications. (Risk Item No. 3.)

Node joining and leaving the network unexpectedly: This may be an unlikely failure mode for space applications, but would be difficult to detect if it happens. (Risk Items No. 9 and 10.)

Some or all physical ports of a PHY unexpectedly enable and disable: This may be caused by hardware or software failures, or even mechanical failures of connectors and/or boards. As shown in Table 2, unexpected disables result in higher risks to the system performance as the application may lose functions due to port disables. (Risk Items No. 11, 12, and 13.)

Issues related to CC being a single point of failure: Solutions to be explored include the JSF approach of using redundant networks and the classical 1394b approach of electing a new node³ to take over CC function such as issuing STOFs. (Risk Items No. 14, 15, 16, and 17.)

Table 2 - FMEA score results

Functional Product Requirement	Potential Failure Mode	Potential Failure Effects	SEV	Potential Causes/Mechanisms	OCC	Current Design Evaluation or Control	DET	RPN
What is the function product requirement under consideration?	In what ways could the function product requirement fail to be fully met?	What would be the impact on the customer?	How severe is the effect to the customer?	What could cause the failure mode to occur?	What is the likelihood that the cause will occur?	What methods, tools, or measures will discover the cause before it design release?	How difficult is it to detect the cause of failure?	Risk Priority Number (SEV X OCC X DET)
Reliable data transfer	Application acts on bad data		3	More than xxx bits flipped	1	None	7	21
Reliable data transfer	Application does not get data packet		3	Fewer than xxx bits flipped	3	CRC	1	9
Reliable data transfer	Application acts on bad data		7	Device memory failure	3	Parity (device manufacturer dependent)	3	63
Reliable data transfer	Application does not get data		7	Broken cable/connector	3	Bits 7, 15, and 23 of health status word in data packets; PHY port status register value	1	21
Fair access to network	Network stops functioning		7	Babbling node	1	MAC layer protocol	1	7
Fair access to network	Unable to communicate with		7	Conflict in node ID/address	1	MAC layer protocol	1	7
All nodes are accessible	Unable to communicate with		7	Node is unexpectedly powered down	1	Application level detection	7	49
High network availability	Unexpected bus reset		3	Software bug	1	Bus resets affect network ops for a bounded time period	7	21

³ As mentioned previously, AS5643 uses forced root nodes. However, in space applications, re-election of root nodes may be allowed to increase flexibility and reconfiguration capability.

Functional Product Requirement	Potential Failure Mode	Potential Failure Effects	SEV	Potential Causes/Mechanisms	OCC	Current Design Evaluation or Control	DET	RPN
What is the function product requirement under consideration?	In what ways could the function product requirement fail to be fully met?	What would be the impact on the customer?	How severe is the effect to the customer?	What could cause the failure mode to occur?	What is the likelihood that the cause will occur?	What methods, tools, or measures will discover the cause before it design release?	How difficult is it to detect the cause of failure?	Risk Priority Number (SEV X OCC X DET)
High network availability	Network loses node; bus reset		7	Node unexpectedly drops out of network	3	Application level detection after network resumes operation from bus reset	7	147
High network availability + network	New node may affect network performance; bus		3	Node unexpectedly joins network	1	Application level detection after network resumes operation from bus reset	7	21
High network availability	Unexpected bus reset		3	Some ports disabled unexpectedly	1	Application level detection after network resumes operation from bus reset	7	63
All nodes are accessible	Unable to communicate with a node		7	All ports disabled unexpectedly	1	Application level detection after network resumes operation from bus reset	7	49
High network availability	Unexpected bus reset		3	One or more ports enabled unexpectedly	1	Application level detection after network resumes operation from bus reset	7	21
High network availability	No node is able to transmit		7	CC does not produce STOF	3	Timeouts	1	21
High network availability	No node is able to transmit		7	CC failed	3	Heartbeat (32 bit word in data packets); CC status word in STOF packet; STOF does not arrive at the defined interval for three consecutive frames	1	21

Functional Product Requirement	Potential Failure Mode	Potential Failure Effects	SEV	Potential Causes/Mechanisms	OCC	Current Design Evaluation or Control	DET	RPN
What is the function product requirement under consideration?	In what ways could the function product requirement fail to be fully met?	What would be the impact on the customer?	How severe is the effect to the customer?	What could cause the failure mode to occur?	What is the likelihood that the cause will occur?	What methods, tools, or measures will discover the cause before it design release?	How difficult is it to detect the cause of failure?	Risk Priority Number (SEV X OCC X DET)
High network availability	No node is able to transmit		7	STOF offset (transmit, receive timing for a remote node) sent by CC is different	1	MAC layer protocol (before a new bus reset: remote node to ignore the different offsets; after a new bus reset: remote node should use the new offsets)	1	7
High network availability	Unexpected bus reset		3	CC does not product STOF at the right time	1	MAC layer protocol	1	3
High network availability	No node is able to transmit		7	Rapidly shifting global clock (STOF offset) resulting in babbling node and bus reset	1	MAC layer protocol (interval between two consecutive STOF should not exceed 10 ms $\pm$ 50 μ s for 100 Hz frame rate)	1	7
Application robustness	Application does not refresh data		7	Application bug causing it to freeze	3	Heartbeat value not incremented (32 bit word in data packets)	1	21

3.4 Summary

We have shown extensive analysis results in previous sections. IEEE-1394b based high-speed avionics buses are also being considered as a candidate for next generation manned space vehicle and high-speed digital interconnects for missile and weapon systems. These applications may have different requirements from a military fighter. Avionics buses for a space vehicle require more considerations in availability than those for military vehicles. High-speed digital interconnects for missile and weapon systems require strong fault tolerance capabilities under stress environments such as high-dose rate radiation events.

3.4.1 Evaluation for Applications Other Than Military Applications

As previously mentioned, space vehicles may have different requirements from military applications, such as radiation (and associated system architecture to better recover from radiation events), vibration, temperature, etc. For example, given the fact that infrequent bus resets for system reconfiguration are allowed in a space vehicle, is the triplex bus architecture necessary? In yet another example, many dynamic and reconfiguration features of IEEE-1394b were turned off in JSF design due to the high system integrity requirement. With enough system integrity needed by a space vehicle, how many of them can be turned back on to enable system flexibility and reconfiguration capability that NASA is currently interested in?

It is also worthwhile to point out that a COTS IEEE-1394b network is a peer-to-peer network that allows reconfigurations. An AS5643 network is a command and control network (with control computers and remote terminals). If a space application requires peer-to-peer, then solutions based on IEEE-1394b architecture should be developed.

3.4.2 Enhancing Fault Containment, Fault Isolation, and Recovery

The main objective of this task is to develop fault-containment, fault-isolation, and fault-recovery schemes for those failures whose detection and recovery schemes were marked “Not Defined” in Table 2. Some enhancements to be considered are as follows:

- Asynchronous streaming acknowledgements and message retransmissions.
- Periodic fail-silence messages transmitted by CC nodes.
- Timers at the application layer to request bus resets.

4. CONTROL COMPUTER DESIGN

The CC is the root node, cycle master (if used), and the bus manager for its respective data bus(es). Figure 3 illustrates an architecture that represents a triplex redundant 1394 vehicle network in which three CCs have been cross-channel linked to provide a greater level of redundancy. For this example, each CC BRANCH, which includes one set of redundant resources (e.g., a CC including all of its buses and remote nodes) contains three independent 1394 nodes/data buses. Buses labeled as “Bus 1” and “Bus 2” are considered critical data buses and support three ports each and are connected in a loop configuration (per AS5643, 3.1.2). The bus labeled as “Bus 3” is considered a non-critical data bus and is connected in the basic tree configuration (per AS5643, 3.1.1).

4.1 Number of Ports per Node

Data bus(es) that have been identified as “critical” (bus 1 and bus 2) require a minimum of two ports per 1394 node in order to support the loop back configuration, which provides the first level of redundancy in the system. A third port is also beneficial to support an independent connection to a 1394 bus analyzer without affecting the connectivity of the “critical loop.” The 1394 bus analyzer port can be used to aid in test and debug of the CC and the vehicle network architecture.

Data bus(es) that have been identified as “non-critical” (bus 3) require a minimum of one port per 1394 node in order to support the standard tree architecture configuration. A second or third port is also beneficial to support the tree architecture, as well as providing an independent connection to a 1394 bus analyzer. The 1394 bus analyzer port can be used to aid in test and debug of the CC and the vehicle network architecture. Unconnected port(s) do not need to be terminated externally.

4.2 Control Computer Synchronization

In a redundant CC architecture (similar to triplex CC architecture illustrated in Figure 3), it is important for the redundant CCs to operate in a synchronous configuration with respect to each other. The synchronous operation allows the CCs to provide the STOF packet to the remote nodes on each independent bus at relatively the same time (within a specified tolerance). The synchronous operation allows the redundancy management and voting software within the CCs to hold tighter tolerances between redundant signal inputs and avoids signal select based on a mixed sample slice. Normally the maximum allowable synchronization skew between CCs is dependent on the periodic frame rate (e.g., for 100 Hz periodic frame rate the maximum CC skew is in the order of 50 μ s).

4.3 Simultaneous Operation of Multiple Buses

When a CC BRANCH is required to support multiple 1394 buses (as illustrated in Figure 3) and each CC BRANCH is required to support either sequential or simultaneous operation of those multiple buses, it is important to ensure that each 1394 interface operates in a fully autonomous fashion. In order to support autonomous operation, it is recommended that each 1394 bus (node) have local memory to store transmit and receive descriptors and for packet payload data (as illustrated in Figure 4). This local memory ensures that the 1394 LLC's transmit and receive buffers are never overwritten and incoming data is not lost due to the LLC's buffers being full. The local memory can be used to hold either static or dynamic transmit descriptor chains that can autonomously pull the message payload from local memory and transmit the messages over the 1394 bus. The LLC can also direct the incoming message content from the receive buffers and into the local memory where the CCs host control or processing element can access the data. The use of dedicated local memory per bus/node eliminates the need for multiple 1394 interfaces to arbitrate to gain access to a single bus or memory device (as illustrated in Figure 5), as well as eliminating stalling the host control or processing element in order to handshake with the 1394 interfaces to store/retrieve data from system memory.

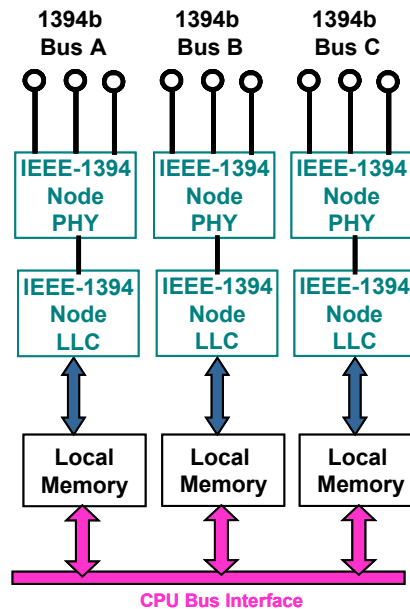


Figure 4 - Multiple 1394 buses with dedicated local memory

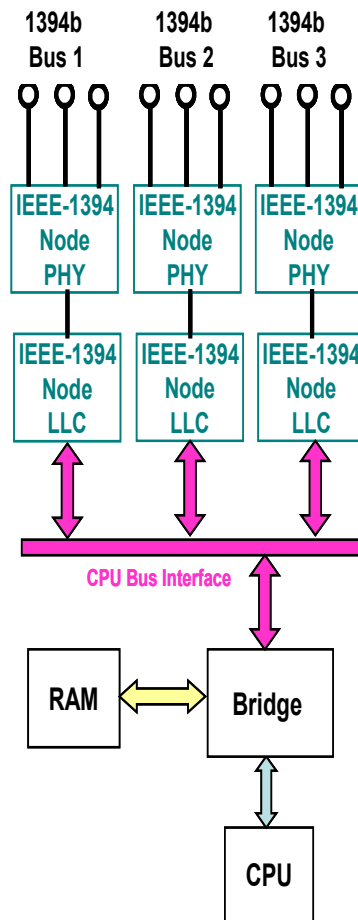


Figure 5 - Multiple 1394 buses competing for common memory

4.4 Buffer-Fill and Packet-per-Buffer Modes

The local 1394 bus/node receive descriptors can configure the use of the local 1394 memory into two different modes of operation. One single isochronous receive DMA (IR DMA) context can receive exactly one packet per buffer (packet-per-buffer) or can concatenate packets into a stream that completely fills each of a series of buffers (buffer-fill). Refer to 1394 Open Host Controller Interface Specification for additional information.

Using packet-per-buffer mode allows the 1394 local memory to be allocated to ensure that each incoming message is stored into memory at a predefined location that is based off the size of the largest allowable payload. Packet-per-buffer mode eliminates the need to search memory to locate the start and end of each message packet since the message is automatically stored into a predefined location. The disadvantage of using packet-per-buffer mode is that to ensure a flexible configuration, each message is normally defined a memory allocation equal to the maximum payload length allowable under AS5643, 3.2.4.1.7.6, which can force the local memory to be larger than necessary (e.g., 2 kilobytes allocated for message(s) that has only a few bytes of payload).

Using buffer-fill mode allows the maximum use of the available 1394 local memory by concatenating incoming packets into a stream that completely fills the available memory. Buffer-fill mode requires the host controller/processing element to search the memory to locate the start and end of each packet (since messages have different size payloads and can be received out of order) and to parse the messages prior to performing additional processing.

5. REMOTE NODE DESIGN

Requirements applicable to remote nodes can be found in 3.3.2 of AS5643.

5.1 Number of Connected Ports Considerations

Remote nodes that have been identified as “critical” (bus 1 and bus 2) require a minimum of two ports per remote node in order to support the standard branch in a tree architecture configuration. A third port is also beneficial to support an independent connection to a 1394 bus analyzer without affecting the connectivity of the “critical loop.” The 1394 bus analyzer port can be used to aid in test and debug of the CC and the vehicle network architecture.

Remote nodes that have been identified as “non-critical” require a minimum of one port per remote node in order to support the standard leaf in a tree architecture configuration. A second or third port is also beneficial for the remote node to act as a branch to support the tree architecture as well as providing an independent connection to a 1394 bus analyzer. The 1394 bus analyzer port can be used to aid in test and debug of the CC and the vehicle network architecture. Unconnected port(s) do not need to be terminated externally.

5.2 Redundancy Considerations

Remote node redundancy considerations are addressed in this section, as well as Section 6.

5.2.1 System Integrity Management

System Integrity Management of all remote nodes may be divided into two distinct categories: simplex systems and redundant systems. Simplex systems are single channel integrated systems where a remote node has no additional backup method for gathering data. Redundant systems are those integrated systems where a remote node has the ability to gather information from additional, adjacent or redundant sources and data buses such as a CCDL.

5.2.1.1 Simplex System Integrity Management

Each remote node will monitor the inputs from the CC (including the STOF message) to determine the failure state of the CC, to verify proper 1394 bus operation, and to verify the CC software that produced the message is operating correctly.

In order for nodes to accept data from the CC during normal bus operation, all of the following conditions should be met:

- STOF message timing is valid if determinable by the remote node.
- STOF message is valid.
- STOF message indicates the CC is in a legal operating mode and is in a “good” state.
- CC to node message is valid.

For further details see the System Integrity Management section of the baseline spec (AS5643).

5.2.1.2 Redundant System Integrity Management

Figure 6 shows the flow chart of the Redundant Systems Integrity Management. The baseline spec does not define System Integrity Management for redundant systems and is presented here as a possible approach for determining valid data and increasing the robustness for flight critical and safety critical remote nodes which have the ability to gather data from redundant sources such as a CCDL as illustrated in Figure 8.

For the simplex remote node, any interruption of the STOF message could terminate transmission and reception of data with the CC. The redundant remote nodes do not need to rely as heavily on the CC's STOF message (see 10.2.1 for additional information on remote node internal STOF considerations). Or, for that matter, the received messages from the CC. If the redundant remote nodes have the ability to cross channel data and have input signal management voting logic applied to the input stream of data from the 1394 data bus (STOF packets and receive offset packets), then the loss of communication with the primary CC channel should not result in the loss of the remote node. The remote nodes should continue to send transmit offset messages back to the CC in the case that the CC may still be receiving remote node transmissions.

The remainder of this section will define the major sections of the Redundant Systems Integrity Management Figure 6.

5.2.1.2.1 STOF Criteria (Condition 1)

The remote node should use the STOF packet data and proceed to Condition 2 if all the following criteria are true:

- STOF packet is received.
- STOF packet is within timing tolerance.
- STOF VPC is correct.

If any of the above criteria are false, the remote node should use the previously determined good STOF packet data, determine the transmit and receive offset time using its internal local clock, and proceed to Condition 3 if any of the above criteria are false.

5.2.1.2.2 Network Bus Mode (Condition 2)

The remote node should use the network bus mode and proceed to Condition 3 if the network bus mode is valid.

If the network bus mode indicates invalid, the remote node should use the previous network bus mode and proceed to Condition 3.

5.2.1.2.3 CC Status (Condition 3)

The remote node should use the STOF packet data and proceed to Condition 4 if any of the following criteria are true:

- The CC status indicates the CC is valid.
- The last remaining valid CC indicates its CC status has failed.
- All CC channels simultaneously indicate the CC status has failed.

With the exception of the above conditions, if the CC status indicates failed, the remote node should recognize the CC as failed and ignore any messages from the CC.

5.2.1.2.4 Bus Mode (Condition 4)

If the network bus mode is in IBIT mode, the remote node should use its internally generated system clock (local time reference) and its internal generated STOF (attention should be made to clock drift limits and duration of the IBIT mode) to determine the transmit and receive offset time and proceed to Condition 5.

If the network bus mode is not in IBIT mode, the remote node should conform to the definition under the AS5643 baseline spec (3.3.1.1.1.2) and proceed to Condition 5.

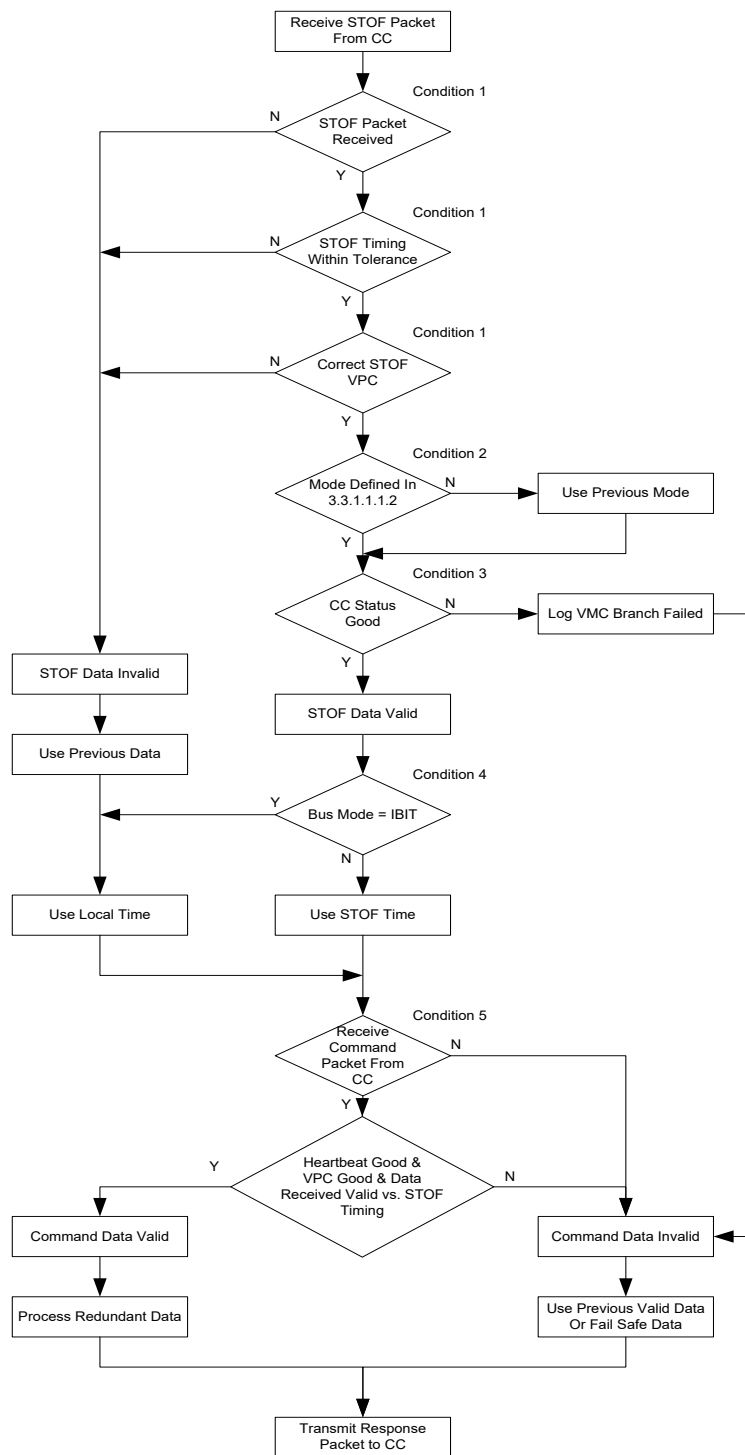


Figure 6 - Flowchart of Redundant System Integrity Management

5.2.1.2.5 Receive Valid Message (Condition 5)

The remote node should use the received data if both of the following criteria are true:

- The heartbeat in the ASM message header has incremented since the last received message.
- The data validity indicators (VPC and health status word) are correct.

With the exception of the above conditions, the remote node should ignore the message.



The remote node should continue to transmit its data to the CC at the appropriate time, regardless of the failure state of the received message.

5.3 Bandwidth and Throughput Considerations

5.3.1 Application Scheduling of 1394 Transmit Packets

The remote node will have to determine how best to schedule the passing of 1394 payloads from the application to Operating System (OS) to the link layer interface such as to minimize the 1394 data latency. Specifically, given the fact that Tx and Datapump offsets are defined as discrete points in the minor frame what mechanism will be used by the host to coordinate data gathering and handoff to the link layer interface. Several approaches of application scheduling are generally available; two examples include the use of interrupts or mailboxes. With interrupts, the host application SW can define the points in time that a gather routine has to be invoked to assemble the payload data and hand it off to the link layer for transmission before the defined offset time. This approach provides the least HW complexity but results in non-deterministic operation especially if offsets and payload sizes are altered. The second approach of mailboxes requires a hardware interface independent of the host that reads an OS mailbox just prior to the offset time. While this approach adds additional HW layer complexity between host and 1394 interface it decouples any timing relationship between the 1394 bus and application SW. It provides an advantage in detection of remote node faults by the CC or other remote nodes. For example, if the application SW fails and no mailbox update is made, the 1394 HW interface will transmit stale data which should be detected due to a heartbeat count not being updated.

5.4 Remote Terminal Design Lessons Learned

5.4.1 STOF Synchronization

Upon reset (either cold, warm, or hot, as defined in 2.2) the remote node needs to detect three consecutive valid STOF packets prior to starting its minor frame routines (slave synch to CC). This can be accomplished by HW timers measuring STOF intervals or time stamping STOF packets with internally generated time base for SW to measure. If no valid STOF sequence is detected within a predefined time, then host application on the remote node starts its minor frame and attempts to detect valid STOF sequence (foreground or background task). Generally speaking, the host should not attempt 1394b transmissions until valid STOF detection and synchronization, as the transmit offset is unknown. If redundancy is present, then the remote node can query other remote node channel(s) for 1394b bus health. Healthy remote node channel can announce to CC that cross remote node channel has STOF synch fault.

5.4.2 Peak Load Handling

The remote node should be designed with adequate resources such that it can accommodate continuous back-to-back 1394b receive packets of maximum payload size (external fault condition) without causing any impact to its application operation. This may be accomplished several ways either at the link layer level (overwriting of buffers) or at the host level (providing Direct Memory Access (DMA) capability and ample buffers to match incoming line rate) for example. The remote node should provide annunciation of this (e.g., overwriting of buffers) event back to the CC.

5.4.3 Payload Path Integrity

The remote node design must maintain integrity of 1394b payload data up to the host application. For example, the 1394b link layer device's CRCs maintains data integrity on the physical 1394b bus while the VPC is designed to maintain application to application layer integrity. If the VPC is done at the host/link layer boundary (perhaps by HW) and then stored in unprotected host memory (DPRAM, SRAM, etc.), then full data path integrity to application has been lost.

5.4.4 Failure Containment

The remote node design should consider mechanisms for limiting the fault propagation of any major internal system fault. If a HW fault occurs at the 1394b link layer level, the SW should have a means to disable the physical layer (e.g., port disable). Conversely, if a host SW fault occurs, then an independent HW mechanism such as a Watchdog monitor circuit should be able to disable the physical layer. This will result in a fail-silent remote node with no 1394b activity and the fail-silent condition can be easily detected by the CC.

Four Level Failure Containment/Error Recover Methods (listed from least severe to most severe impact on network):

1. CC transmits message to remote node to inform application to cease or reset communication.
2. Remote node to reset PHY (results in bus reset) - not applicable for Babbling Idiot Syndrome.
3. Remote node to disable PHY.
4. CC instructs adjacent connected node to disable port (isolate failed remote node).

5.4.4.1 Babbling Idiot Syndrome

Classic example of fault condition either at host or link layer level where remote node is constantly transmitting 1394b packets thus violating its STOF Tx offset. Remote node design can handle this condition several ways: independent external bus monitor who has authority to disable 1394b physical layer for example, wrap around receiver that signals host SW to take action either at application SW layer or at link/physical layer, or by adding an independent Watchdog monitor function/window internal to the remote node application SW layer transmit window to detect and disable 1394b physical layer.

A node can end up sending messages beyond its allocated transmitting window, if there is still data in the LLC buffer at the end of the transmitting window. In order to prevent data transmission outside of the transmitting window, the node should stop enqueueing data some period of time before the end of transmitting window. That amount of time depends on the amount of data that is allowed to be transmitted within a STOF frame. If the node is allowed to transmit only 1 kilobyte of data per STOF frame, then the node should stop enqueueing data about 20 μ s before the transmitting window ends, when operating at 400 Mbps. If 2 kilobytes of data are allowed per STOF frame, then the node should stop enqueueing approximately 40 μ s before the end of the transmitting window. The window size will be reduced by the remote node; however, it will help maintain order in the network and prevent unnecessary bus contention.

5.4.5 Minimization of 1394 Bus Resets

The remote node design should minimize the number of 1394b bus resets that occur as a result of internal faults. The remote node application should never initiate a bus reset unless directed to by the CC. Certain fault classes (e.g., parity fault, overflow exception, etc.) can be accommodated by soft resetting internal functions that were affected as opposed to taking approach of hard reset of entire remote node hardware including 1394 link and physical layers (thus causing a 1394 bus reset). Please refer to the 1394 Trade Association's "Bus Reset Handling" white paper for more details about bus resets.

6. FAULT TOLERANT NETWORK ARCHITECTURE AND TECHNIQUES

This section identifies network architecture and redundancy considerations in implementing a fault tolerant vehicle data network specified by AS5643 and AS5643/1 slash sheet.

6.1 Architectural Considerations

When setting up your network, an early decision to make in the design is how to interconnect the nodes of your vehicle. IEEE-1394b makes it possible to interconnect the three-port nodes in any configuration imaginable. Figures 1 through 3 illustrate three example architectures: basic network with single CC, basic network with single CC and a loop, and representative triplex network with loops. This is by no means an exhaustive list.

6.1.1 Redundant CCs

A first order of redundancy is the use of redundant CCs. To satisfy failure immunity requirements for your military/aerospace vehicle, it is very likely that you will use multiple CCs. If this is so, it makes sense to CCDL all CCs. If a 1394b CCDL interface is used, it is recommended that this interface should be independent of the vehicle's data buses. In fact, a CC will likely utilize a number of IEEE-1394b nodes, corresponding to an equal number of IEEE-1394b PHYs, for each bus, CCDL, and other IEEE-1394b connectivity that is required (e.g., test ports for diagnostic use, software loading, etc.).

6.1.2 Cross-Channeling CCs and Remote Nodes

With all CCs in a network cross-channel linked together, data collected from nodes on each CC can be shared with the other CCs as required. Further redundancy can be provided by having multiple remote nodes on a given piece of equipment, each connected to a different CC. This configuration enables the CCs to use the data provided by the redundant remote nodes in its input and output processing. Yet another option is to also cross-channel important remote nodes on different busses and/or CCs together. These possibilities are illustrated in Figure 8.

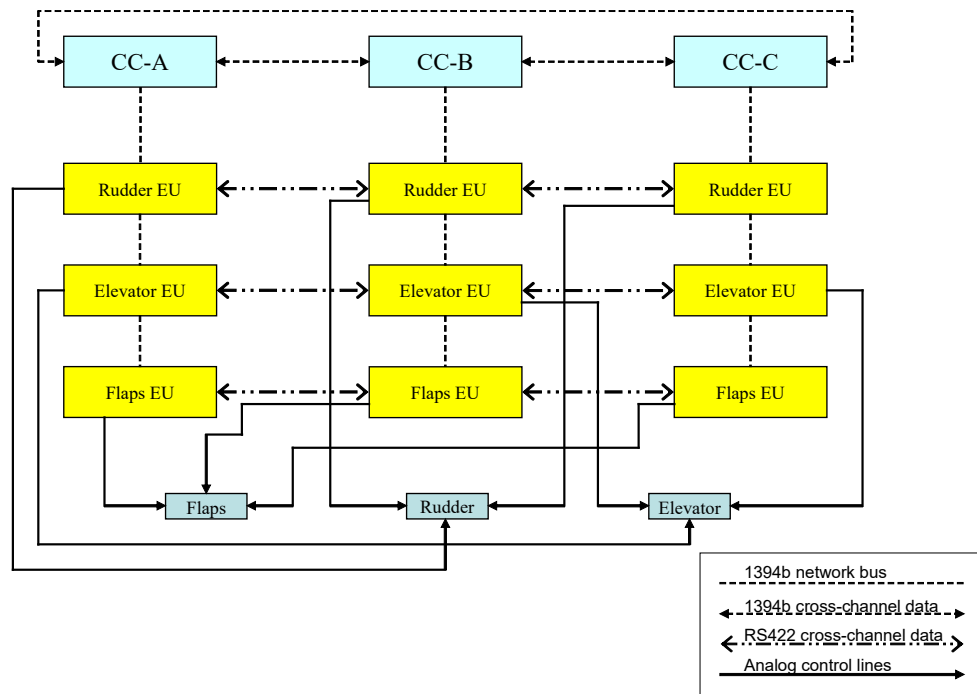


Figure 7 - Triplex network with multiple cross-channel connections

In this example, the cross-channel data connections between the three CCs are IEEE-1394b. It is not necessary that the cross-channel data connections be IEEE-1394b; a different data bus standard may be employed. Also note that it may not be necessary for data organization and timing to be based upon AS5643 format (use of STOFs, etc.), but may be at implementer's discretion.

Having the CCs cross-channel connected to one another allows each CC channel to have all three sets of input and output data for every computational frame. For example, the CC channel may select the mid-value or average for each input signal. If one channel's value for a particular signal parameter is different from the other two channels' values by a predetermined threshold for a predetermined persistence, that particular signal may be considered failed and latched out until an operator action is performed. In such case, all three CC channels can use the average of the two remaining values from the two good CC channels for that particular signal.

In order to determine the overall health of each CC channel, the CC software may compare each channel's output commands to one another in each computational frame. If one channel's value for a particular command output is different from the other two channels' values for that command output by a predetermined threshold for a predetermined persistence, that CC channel may be considered failed and latched out until an operator action is performed. In such case, all data from that CC channel should be considered failed and its command outputs ignored by the other subsystems.

6.1.3 Looping Busses

Figures 2 and 3 of AS5643 show some busses in the architecture as being looped (see Figure 8).