NASA/TM—2006–

Comparison of Communication Architectures for Spacecraft Modular Avionics Systems

D.A. Gwaltney and J.M. Briscoe
Marshall Space Flight Center, Marshall Space Flight Center, Alabama

April 2006

The NASA STI Program Office…in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA Scientific and Technical Information (STI) Program Office plays a key part in helping NASA maintain this important role.

The NASA STI Program Office is operated by Langley Research Center, the lead center for NASA's scientific and technical information. The NASA STI Program Office provides access to the NASA STI Database, the largest collection of aeronautical and space science STI in the world. The Program Office is also NASA's institutional mechanism for disseminating the results of its research and development activities. These results are published by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA's counterpart of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or cosponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and mission, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services that complement the STI Program Office's diverse offerings include creating custom thesauri, building customized databases, organizing and publishing research results…even providing videos.

For more information about the NASA STI Program Office, see the following:

- Access the NASA STI Program Home Page at ***http://www.sti.nasa.gov***

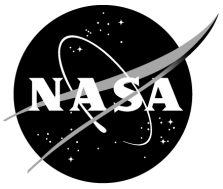
- E-mail your question via the Internet to help@sti.nasa.gov

- Fax your question to the NASA Access Help Desk at 301–621–0134

- Telephone the NASA Access Help Desk at 301–621–0390

- Write to:
  NASA Access Help Desk
  NASA Center for AeroSpace Information
  7121 Standard Drive
  Hanover, MD 21076–1320
  301–621–0390

NASA/TM—2006–



Comparison of Communication Architectures for Spacecraft Modular Avionics Systems

D.A. Gwaltney and J.M. Briscoe
Marshall Space Flight Center, Marshall Space Flight Center, Alabama

National Aeronautics and
Space Administration

Marshall Space Flight Center • MSFC, Alabama 35812

April 2006

TRADEMARKS

Trade names and trademarks are used in this report for identification only. This usage does not constitute an official endorsement, either expressed or implied, by the National Aeronautics and Space Administration.

Available from:

NASA Center for AeroSpace Information
7121 Standard Drive
Hanover, MD 21076–1320
301–621–0390

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161
703–487–4650

TABLE OF CONTENTS

LIST OF ACRONYMS

AE	avionics environment
AFDX	avionics full duplex switched
ANSI	American National Standards Institute
ARINC 659	Aircraft Radio, Inc.
ASIC	application specific integrated circuit
BC	bus controller
BIU	bus interface card
BOSS	bus owner/supervisor/selector
CAN	controller area network
CRC	cyclic redundancy check
CSMA/CD+AMP	carrier sense multiple access with collision detection and arbitration on message priority.
CDMA	code division multiple access
EBR–1553	enhanced bit rate 1553
ESA	European Space Agency
ESMD	Exploration Systems Mission Directorate
FC–AE	Fibre Channel avionics environment
FDIR	fault detection, isolation, and recovery
FPGA	field-programmable gate array
GOF	glass optical fiber

LIST OF ACRONYMS (Continued)

I2C	inter-IC bus
IO	input/output
IP	intellectual property
ISAACC	integrated safety critical advanced avionics for communications and control
ISHM	integrated system health management
JPL	Jet Propulsion Laboratory
LAN	local area network
LRM	line replaceable module
LVDS	low-voltage differential signaling
MMSI	miniature munitions/store interface
MSFC	Marshall Space Flight Center
NGLT	next generation launch technology
PHIAT	propulsion high-impact avionics technology
POF	plastic optical fber
RT	remote terminal
RX	receiver
SAN	storage area nets
SPI	serial peripheral interface
SSME	Space Shuttle main engine
SPIDER™	scalable processor-independent design for electromagnetic resilience
TCP	transmission control/protocol

LIST OF ACRONYMS (Continued)

TDMA	time division on multiple access
TM	Technical Memorandum
TTA	time-triggered architecture
TTCAN	time-triggered controller area network
TTP	time-triggered protocol
TTP/C	time-triggered communication protocol
UDP	user datagram protocol
VL	virtual link

low criticality that are used offline for vehicle maintenance decisions after the mission is over. Using one communications architecture to support all these functions would mean that some systems would not provide an adequate return on investment, while others could not perform in an optimal manner due to system limitations. This survey provides coverage of a range of communication architectures that can support many different tiers of critical functionality. The goal is to provide information that can be used to align communication architectures with the functionality needed to support modular avionics for the next generation spacecraft.

In the context of this document, serial communication architectures are those that define a physical layer, media access control, and possibly a protocol with data flow control and some level of error detection/correction. Such architectures are not just electrical specifications. Therefore, simpler serial buses such as RS–232, RS–485/422, and low-voltage differential signaling (LVDS) are not considered by themselves, but only when they specify the physical layer for a communication architecture. Serial communication standards, primarily for chip-to-chip or board-to-board communications, are not considered because these are usually not suitable for long-haul communications and generally support only minimal media access control and protocols in typical applications. Examples of this type standard are serial peripheral interface (SPI) and inter-IC (I2C) bus.

2. CANDIDATE ARCHITECTURES

The architectures selected have either extensive aerospace or aeronautic deployment history, are deployed in new vehicles, or have some potential to be included in future vehicles. If the net is cast widely, the number of serial communication architectures that exist is immense. There are several communication architectures used in industrial distributed control systems for factory and process automation. Additionally, there are communication architectures used to control the lighting, heating and elevator services in buildings. While these architectures are successful in their application field, the requirements for manned and robotic space vehicles differ significantly from those for industrial applications, and much work may need to be done to convert such architectures for aerospace work. The goal of this study is to leverage off-the-shelf components as much as possible, and to minimize the changes needed to field the selected communication architectures. Communication architectures developed specifically for use in manned vehicle distributed control have a better chance of being ported to the aerospace environment unchanged. This may also apply to many of the more extensively used communication architectures, such as Ethernet, as its wide use has spawned commercial interest in using it in manned vehicles.

The communication architectures selected for study include event-triggered systems and time-triggered systems. Event-triggered communication refers to a system in which messages are generated based only on the need to transmit a new or changed piece of information, or to request that some information be transmitted to the requester. Ethernet is a good example of such a system. Used in communication between computers (nodes) that are part of a network, either local or over the Internet, messages are sent over Ethernet when an individual at a network node decides to look at a Web page or send e-mail. For instance, transmitted messages are sent when the user enters a Web page address in a browser, and messages are received when the Web server (another node) sends back the requested content. These messages are sent based on an event that can occur at any time, with no discernable regularity. Time-triggered communication occurs at specified times based on a globally agreed upon time base. Such communication is scheduled with the passage of time and each node that is part of the network is given a finite amount of time, or a slot, in which to transmit a message in each communication cycle. The sequence of message slots in the schedule is repeated over and over to create periodic message transmission slots for each node. Messages are sent by nodes that are part of a network at a predefined moment in time as referenced to a global time base. The time base is generated either on a clock reference message sent by a network master node, or by combining clock messages from several nodes. The latter method is a masterless approach to generating a time base, and generally employs a fault-tolerant clock algorithm to produce clock corrections for each node in the network. This masterless approach to creating a global time base creates a masterless communication protocol in which the failure of any node does not prevent the other nodes from communicating with each other.

When the PHIAT team began exploring available options for real-time communications in safety critical distributed control systems, the information available indicated a clear preference for communication architectures with time-triggered protocols (TTPs) over those with event-driven protocols.

A report written in 2001 by Rushby gives a comparison of bus architectures targeted toward safety critical sys-tems.[1] Rushby includes an extensive list of references that provide further insight into the capabilities of these systems. The following systems are reviewed in the report and all employ a TTP: SAFEbus™, Time-Triggered Protocol (TTP™/C), FlexRay™, and SPIDER™. These architectures, with the addition of time-triggered controller area network (TTCAN), are the primary architectures targeted for safety critical systems. TTPs are considered by many to be a requirement for safety critical distributed control systems, because the bus loading is known and constant, the message latency and jitter are known and constant, and the time-triggered nature of the communication supports composability. Composability means that the nodes, which are part of the time-triggered communication network, have precisely defined communication interfaces that can be developed by different manufacturers and will be guaranteed to integrate into the communication network. These time-triggered networks also employ different methods for fault tolerance and the ability to detect communication and node failures. All of the known time-triggered communication architectures are included in the study with the exception of SPIDER, which is intended as a case study for DO–254 "*Design Assurance Guidance for Airborne Electronic Hardware*." The purpose of case study DO–254 is not necessarily to create deployable hardware, but to gain experience in the lab with hardware adhering to the new guidance document.[2] As such, there is no hardware that can be purchased openly or procured from the system designer for implementation. SPIDER is therefore inappropriate for consideration at this time. More details are provided on these buses in sections 2.3 through 2.6.

While time-triggered systems offer a great deal in terms of addressing safety and highly dependable operation, there are tradeoffs made to attain the high level of reliability needed. It is true that time-triggered communication provides a well-defined sequence of messages that ensure maximum bus loading stays at a prescribed level with no contention between the nodes for access to the bus, which is very important in the proper verification and operation of a hard real-time control system. However, there is a significant amount of upfront design that must be done to create the message schedule model and coordinate it with the timing of tasks at each node that require the data, and as such, a strict configuration of the system is imposed. This strict configuration does not allow the addition of new nodes or messages without redesigning the message and task schedule. Event-based systems have no such constraints; so new nodes with new message requirements can be added simply by attaching them to the physical layer. In some systems event-based communication may be more efficient, as the number of messages passed in a given amount of time may be sparse or the data payloads may be large. In the former case, the message slots in a time-triggered architecture (TTA) would still exist even if the nodes in the network had no new information to send. This means empty slots are taking network bandwidth that could be used to send larger messages. So, if large data payloads must be transmitted, a TTA may require splitting the data up into chunks transmitted over several transmission cycles. In some systems, this may be unacceptable. For instance, when transmitting a video data stream, breaking up the data could lead to choppy motion, depending on the rate of the communication cycles, which would be annoying to a viewer. On the other hand, the video stream need not be hard real-time with guaranteed delivery. In most cases, a viewer can tolerate the occasional loss of a frame better than consistently choppy video. In this scenario, a high-speed, event-based system may be a better choice than time-triggered communication. These issues are part of the trade space that will be dictated by the functionality of the modules that are interconnected with the communication architecture.

High-speed, event-driven communication architectures are included in the survey to provide the system designer with the information needed to make a choice based on communication throughput, reliability, and real-time requirements for the distributed system being designed. Clearly, there will need to be other considerations than just criticality when designing a system to transmit and manage the expected large data load required for comprehensive ISHM. The following communication architectures that provide high-speed throughput are included in this survey:

- Avionics Full Duplex Switched (AFDX) Ethernet, currently in service on Airbus A380
- Fibre Channel, used in the Joint Strike Fighter
- Ethernet, operational in commercial aircraft and on the *International Space Station*, also frequently proposed for new spacecraft avionics
- Gigabit Ethernet has not yet been deployed in an aeronautic or aerospace application, it uses Fibre Channel physical layer and proposed for use in military systems
- IEEE1394–B, used in the Jet Propulsion Laboratory X2000 spacecraft distributed avionics architecture, to date has not flown
- SpaceWire, utilized in robotic spacecraft missions by the European Space Agency (ESA) and NASA

A description of each bus is provided in sections 2.7 through 2.12.

One important point to make concerns the determinism of real-time communications. Many of the users and distributors of particular communication architectures call the communication over that medium real time and deterministic. There are two definitions for deterministic: (1) The term describing a system whose time evolution can be predicted exactly and (2) algorithms that may be part of a system whose correct next step depends only on the current state. For real-time communications only the first definition applies. Any communication architecture that uses arbitration cannot be deterministic in this sense, because minor variations in the timing of system functions will cause changes in which messages are arbitrated and transmitted at any given time in a particular communication cycle. So the messages transmitted will vary and not be exactly predictable. As a rule, TTPs do not use arbitration. However, some exceptions exist to provide time limited windows, or slots, for event-triggered messages. In this survey, only TTCAN and FlexRay specifically provide for arbitrated event-triggered message windows. MIL–STD–1553 is referred to as deterministic because it is a master-slave protocol. During normal fault-free operation, the master is in complete control of the message traffic on the bus. If specified messages are sent by the master in a predefined order, then MIL–STD–1553 is deterministic with respect to time. For example, IEEE1394–B, Ethernet, and Fibre Channel all use arbitration to send messages in their standard form and cannot claim to be deterministic with respect to time unless modifications to the standard implementation are made.

MIL–STD–1553 is included because it is the most widely deployed serial communication architecture in military and aerospace applications. It will be present in such systems for some time to come

due to its reliability and long historical use. However, it is beyond its prime, and despite efforts to increase its speed and capabilities, it is expected to eventually be supplanted by newer communication architectures in future military and space vehicles.

The salient features of the communication architectures selected are compared in appendix A, table 1. While such tables are a good way to compare summarized data at a glance, they do not always provide a means of describing the compared items well. A brief description of each of the candidate architectures is given in sections 2.1 through 2.12.

2.1 MIL–STD–1553

The aircraft internal time division command/response multiplex data bus is a military standard with the designation MIL–STD–1553b. This revision was published in 1978 and the last change notice was published in 1996.[3,4] MIL–STD–1553 represents one of the first communication data bus standards for transmission of digital data between systems and subsystems over a common set of wires. The first users of the original version A, published in 1975, were the U.S. Air Force's F–16 and the Army's AH–64A Apache helicopter.[5] MIL–STD–1553 has found many applications including satellites, the Space Shuttle and the *International Space Station*.

The standard defines a dual redundant pair of serial communication buses that are used to interconnect nodes on a network. The transmission media is a twisted shielded pair consisting of the main bus and numerous stubs to create a multidrop topology. There is currently no maximum bus length defined in the standard, and working systems with a main bus length of several hundred meters have been implemented. However, it is highly recommended that the bus topology be built and tested prior to deployment to ensure proper performance. Time division multiple access (TDMA) allows communication between the interconnected nodes, while a single node designated as the bus controller (BC) supervises the bus access. The remaining nodes are remote terminals (RTs). They do not use a global clock and are only allowed to transmit data on the bus after it is requested, or commanded, by the BC. Commands from the BC may be asynchronous or they may follow a periodic pattern based on local timing at the BC. Nodes, acting as backup BC's, may exist on the network to take over in the event of the primary BC failure. Data is not transmitted over the dual redundant bus simultaneously, but rather one bus is used to transmit data for communication during normal operation and the other is in hot backup status used only to send commands in the event of node failure causing the primary bus to be monopolized by one node. The BC would send a transmitter shutdown message on the backup bus in an attempt to stop the node from babbling on the primary bus. The secondary bus could also be used to resume normal communication in the event the primary bus fails entirely due to physical damage.

Communication over the bus is limited to 1 MB/s, which is very slow if message data contains more than a few bytes of data. Recently, the development of new standards called enhanced bit rate 1553 (EBR–1553) and the miniature munitions/store interface (MMSI) have increased the speed to 10 MB/s. They require a star, or hub, topology to provide the higher data rate, and therefore require additional components to implement the architecture.[6] Additionally, there are reports that two companies are working for the Air Force on a new transmission standard using existing MIL–STD–1553 cabling. The idea is to overlay high-speed communication without disturbing the existing legacy communication. Laboratory prototypes reaching 200 MB/s have been reported. The prototype systems may become the basis for

MIL–STD–1553C. It is notable that the high-speed communication is separate from the legacy 1 MB/s communication, so the new systems will not communicate with legacy systems at the high rate. There is currently no publicly available information on MIL–STD–1553C other than a couple of articles in trade magazines and no announced time frame for completion of the standard. These standards are relatively new; therefore, components based on them do not have substantial deployment at this time. This is likely to change in the near future for EBR–1553, since MIL–STD–1553B components are in wide use and components based on the new standards should provide an upgrade path with existing software reuse. These standards are not included in this trade study due to the lack of publicly available standards documents and their current limited use.

MIL–STD–1553 also served as the basis for a fiber optic version called MIL–STD–1773. This standard still only provided for 1 MB/s and has not enjoyed wide use. A new standard called AS 1773 provides for 20 MB/s, but still has not been popular communication architecture in military and aerospace systems.

Systems based on MIL–STD–1553 are considered to be extremely reliable and have been widely used in military and space applications. However, the need to transmit larger amounts of data at near real-time rates has led many designers of new military avionics to pursue other communication architectures. The cost of components is also high relative to components used in commercial communication architectures, such as Ethernet, due to the niche market that is targeted by suppliers of MIL–STD–1553 components. The information in this section is a very brief overview. Complete details can be found in the standard and in manufacturer component and test equipment publications.

2.2 SAFEbus

SAFEbus is the registered trademark for the Honeywell implementation of ARINC 659 and is, by definition, the backplane bus in a computing cluster housed in a cabinet. It is currently part of the Boeing 777 avionics architecture. Communication with other cabinets and control and monitoring subsystems is achieved through input/output (IO) modules using other bus protocols. This architecture requires a quad redundant bus, in which two data lines and one clock line comprise each bus. Full duplication of bus interface units (BIUs) is provided at each of eight nodes (four processing nodes and four IO nodes) providing a powerful but expensive architecture. The standard defines the capability to have shadow nodes waiting in hot backup to take over if the primary node fails. SAFEbus has limited bus length, but has a transmission rate of 60 MB/s.

The level of reliability and redundancy provided by SAFEbus is extremely high, as it was specifically designed to support safety critical functions in commercial passenger aircraft. Most of the functionality is in the BIUs that perform clock synchronization and control data transmission based on message schedules. Each node has a pair of BIUs that drive different pairs of bus lines, but can read all four lines. BIUs act as the bus guardian for their partner BIUs by monitoring transmitted data and transmission scheduling and controlling its partner's access to the bus lines. This prevents a faulty BIU from becoming a babbling idiot or transmitting erroneous data. Data transmission is time-triggered and is governed by a message schedule. Synchronized timing of messages delivered is maintained using a global clock. The clocks are synched via periodic pulses on the dedicated clock line. Because the message schedules include sender and recipient information, the data packets include no header information,

but are pure data. There is also no cyclic redundancy check (CRC) or parity information transmitted with the data because the BIU pairs check all data transmitted on the bus signal pairs by the node they support. Each BIU checks its data and its partner's data for errors. These features result in a very efficient, masterless transmission protocol.

A system that is designed to be fault tolerant should have a fault hypothesis by which its performance can be evaluated. The fault hypothesis for the SAFEbus architecture states that it is guaranteed to tolerate one arbitrary fault, but may tolerate multiple faults. At most, one component of any pair can fail (i.e. the BIU, the processing module, or one of the dual redundant bus lines). When one component of a node fails, the node must fail-silent, thus removing itself from operation. Nodes with important functions must be redundant to be able to continue normal operation.

The SAFEbus architecture is considered to be very dependable for safety critical functions, but it is also very expensive. The hardware is redundant as a pair of pairs at all levels and the components are proprietary to Honeywell. The components are not available as commercial off-the-shelf products. Despite the creation of the ARINC 659 standard, it does not appear that other independent companies have created ARINC 659 compliant components. More information on SAFEbus can be found in the standard.[7,1,8]

2.3 Time-Triggered Communication Protocol

The TTA developed at the University of Vienna uses a time-triggered communication protocol called TTP/C. Specifications for TTP/C were first published in 1993.[9] The C in TTP/C stands for automotive class C referring to the hard real-time communications requirement. Indeed, the automobile industry funded much of the TTA development and the TTP/C protocol to support future drive-by-wire applications. TTTech, a company based in Austria, has commercialized TTP/C and the communication controller integrated circuit devices are now available for purchase. These devices implement the protocol in hardware and are openly available to any system developer. TTP/C has been applied to a wide variety of manned transportation vehicles including the Airbus A380 cabin pressure control system, full-authority digital engine controllers for military aircraft, and railway signaling and switching systems in Switzerland, Austria, and Hungary. It has also been used in drive-by-wire concept cars. TTP/C is designed to provide a high level of reliability and availability at a cost suitable for mass production.

TTP/C is a fault-tolerant TTP providing important services such as autonomous message transport based on a schedule with known delay and bounded jitter over dual redundant communication channels. TTA, and therefore TTP/C, supports the implementation of redundant nodes or redundant functions executing on multiple nodes. Current implementation of the communication controller chip includes a fault-tolerant global clock to establish a time base, membership services to inform all nodes of the health status of the other nodes, and message status set by both the sender and the receiver. The protocol is masterless, which allows communication to continue between the remaining nodes on the network when other nodes fail. Bus guardians are included in the TTP/C communication controller hardware, but are part of the same device and share a common clock. TTP/C is designed to be physical layer independent. Current controller chips support communication at 5 MB/s over RS–485 and 25 MB/s over the Ethernet physical layer. There is reported to be an effort to develop a 1 GB/s implementation using Gigabit Ethernet as the physical layer. The TTP/C fault hypothesis guarantees that the communication system

can tolerate any single fault in any component of the architecture. It can tolerate multiple faults depending on the application. More information on TTP/C can be found in the specification.[10] The specification document is available free upon request from TTTech.

2.4 FlexRay

The FlexRay protocol is specifically designed to address the needs of a dependable automotive network for applications like drive-by-wire, brake-by-wire, and power train control. It is designed to support communication over single or redundant twisted pairs of copper wire. It includes synchronous frames and may include asynchronous communication frames in a single communication cycle. The synchronous communication frames are transmitted during the static segment of a communication cycle. All slots are the same length and are repeated in the same order every communication cycle. Each node is provided one or more slots whose position in the order is determined at design time. Each node interface is provided only with the information concerning its time to send messages in this segment and must count slots on each communication channel. After this segment, the dynamic segment begins with the time divided into minislots. At the beginning of each minislot there is the opportunity to send a message, if one is sent the minislot expands into the message frame. If a message is not sent the minislot elapses as a short idle period. Messages are arbitrated in this segment by sending the message with the lowest message ID. It is not required that messages be sent over both communication channels when a redundant channel exists.

No membership services are provided by FlexRay to detect faulty nodes. Clock synchronization, through messages sent by specific nodes, is the only service provided. There is also no bus guardian specification currently published and no published fault hypothesis. The FlexRay consortium, consisting of many major automotive companies, has indicated it has no interest in any field of application other than the automotive industry. The hardware that has been developed is only available to the consortium members and cannot be purchased by nonmembers. Only recently have the protocol and physical layer specifications been publicly available.[11,12] FlexRay is included because it has the potential to be applied to aerospace applications, despite the current lack of interest by the consortium

2.5 Time-Triggered Controller Area Network

The TTCAN specification is an extension to the standard controller area net (CAN) to provide time-triggered communication. Standard CAN uses carrier sense multiple access with collision detection and arbitration on message priority (CSMA/CD+AMP) for message arbitration. Simply stated, when there is an attempt by two nodes to send a message simultaneously, the message with the lowest ID number is transmitted. Additionally, standard CAN controllers will retransmit a message when no acknowledgement is received.

TTCAN can be implemented in software or hardware to use a system matrix that defines a schedule for message transmission over a communication cycle. This schedule includes slots for specific messages that are sent every cycle and slots for standard arbitration, so event-triggered messages can be transmitted. TTCAN still uses CSMA/CD+AMP, as implemented in standard CAN controllers, to ensure proper arbitration during the arbitrated frames. During the scheduled frames there should be

no bus contention, and the arbitration service will not be used. TTCAN can only be implemented on CAN controllers with the capability to turn off the retransmit feature.

Clock synchronization is achieved by designating one node as the time master. This node sends a reference frame to begin the communication cycle. The maximum transmission rate is 1 MB/s but is typically lower in application, on the order of 500–650 Kbits/s. TTCAN is targeted to the automotive industry, but CAN has found applications in industrial automation and some military systems. So it is included for its potential to be used in aerospace applications. TTCAN is specified by the international standard ISO 11898–4 "Time-Triggered Communication on CAN." There is also information in papers published on the subject.[13,14]

2.6 IEEE 1394b

IEEE 1394 (Firewire) is a communication architecture that has generated much interest in aerospace applications, as evidenced by the Jet Propulsion Laboratory's use of the legacy IEEE 1394–1995 in the X2000 fault-tolerant avionics system for the Deep-Space System Technology Program. Interest in IEEE 1394 for space applications stems from the fast communication rates over copper wiring, and the availability of intellectual property (IP) cores for use in the fabrication of application specific integrated circuit (ASIC) devices. This survey covers IEEE 1394b that supports data rates from 100 MB/s up to 3.2 GB/s and also supports the specifications in the legacy standards. Communication is specified over twisted, shielded and unshielded, pairs as well as plastic and glass optical fiber. The transmission medium and the length of the medium effects the maximum transmission rate.[16]

The communication protocol used is characterized by an isochronous transmission phase and an asynchronous transmission phase. Isochronous transmission refers to broadcast transmissions to one node or many nodes on the network without error correction or retransmission. This is useful for video data where loss of a frame now and then is acceptable, but choppy error-free video is not desirable. Asynchronous transfers are targeted to a specific address (another node) on the network and are acknowledged by the recipient, allowing error checking and the retransmission of messages. This is used for data that must be transmitted error free. Arbitration for bus access occurs for each transmission phase. IEEE 1394b speeds up the arbitration process by using bidirectional communication in which the arbitration frames are sent while data frames are being sent.

IEEE 1394 uses point-to-point connections in a tree topology and does not support loops. However, there exists the capability to disable ports, so a loop may be connected, and in the event a link fails the disabled port can be enabled to reestablish connectivity with all the nodes. At start up, an identification process is used to provide addresses to the nodes, select root nodes, and isochronous master. Adding or removing devices requires the identification process to execute again. The family of standards specifying the legacy architecture of IEEE 1394–1995, IEEE 1394a, and the updated architecture IEEE 1394b are available for purchase from IEEE.

2.7 SpaceWire

SpaceWire, developed in Europe for use in satellites and spacecraft, is based on two existing standards—IEEE 1355 and LVDS.[17,18] It has found application on the NASA's Swift spacecraft and

several ESA spacecraft such as Rosetta, and has been proposed for use on the James Webb Telescope. The European Cooperation for Space Standardization has published a SpaceWire specification.[19]

The transmission physical layer is shielded twisted pair and point-to-point. A large network of devices can be created using cascades of hubs or switches that route messages from one node to another. This requires the message packet to contain address or routing information that is used by the hubs and switches to send the data to the recipient. The standard does not specify the arbitration schemes that will be needed at the hubs and switches. It does however establish the concept of port credit to regulate message flow across a link. Senders must not exceed the data buffering capacity of a port. Buffer space availability is tracked by flow control tokens. The SpaceWire specification indicates the maximum data transfer rate is 400 MB/s. Data transmission is event triggered in this architecture

2.8 Ethernet 10/100 Base-T

Ethernet is one of the most widely used communications architectures for computer networks at business, government, and educational institutions. It has also found military and aerospace application, and is currently used on the *International Space Station*. The 802.3–2002 IEEE Standard defines Ethernet while the current revision of this standard includes specifications for Gigabit Ethernet. Because the 10/100 Base-T implementation of Ethernet and the 1/10 G Base-X implementation have some significant differences, Gigabit Ethernet is described separately in section 2.11.

As the designation suggests, 10/100 Base-T Internet provides data transmission rates of 10 MB/s and 100 MB/s over unshielded twisted pair. Ethernet can operate in half-duplex mode (all nodes share the same cables) or full-duplex mode (nodes can communicate over dedicated cabling with one other device). In half-duplex operation CSMA/CD governs the way computers share the channel. This works by only initiating data transmission when the line is idle. If two nodes initiate transmission at the same time, a collision is detected and transmission ceases. Each node then waits until the line is idle, and then waits a random amount of time to begin transmitting again. The two nodes will hopefully select different random wait times and gain access to the bus. Clearly, this can result in extremely inefficient communication, especially when data traffic is heavy. Full-duplex mode is possible when the nodes are connected to a switch that allows a dedicated connection between the switch port and the node. The switch is now responsible for routing the message to the intended recipient without contention.

The protocol used to send messages affects the reliability of the transmission, the overhead in the message packet, and the time required to complete a message transaction. Two popular protocols are: (1) User datagram protocol (UDP) and (2) transmission control protocol (TCP). UDP is an unreliable connectionless protocol with no guarantee that the data will reach its destination. It is meant to provide barebones service with very little overhead. TCP adds significant overhead to the transmission process, when compared to UDP, but it provides a reliable connection that requires the sender (client) and receiver (server) to open a connection before sending data, ensures messages are received properly, sequences packets for transmission, and provides flow control. IEEE Standard 802.3–2002 is the most recent revision of the standard specifying Ethernet.[20]

2.9 Avionics Full-Duplex Switched Ethernet

AFDX Ethernet is a trademark of Airbus. It was developed for use in the A380 passenger plane. It is a standard that defines the electrical and protocol specifications for the exchange of data between avionic subsystems using IEEE 802.3 (100 Base-TX) for the communications architecture. The ARINC 664, Part 7 standard builds on the proprietary standard developed by Airbus. The AFDX communication protocol has been derived from commercial databus standards (IEEE 802.3 Ethernet medium access control (MAC) addressing, IP, and UDP) and adds deterministic timing and redundancy management with the goal of providing secure and reliable communications of critical and noncritical data. It capitalizes on the huge commercial investment and advancements in Ethernet.

The issue of deterministic communications is addressed by defining communication virtual links (VLs) with specified maximum bandwidth and frame size during system design. These VLs must share the 100 MB/s physical link. The switches are provided with a configuration table that defines the network configuration. Queues at each port and switches used to route the messages may introduce jitter in the message latency, or receive time of the message. This jitter is due to random delays in transmission based on the message transmission volume at a given time, and is required to be less than 500 μs. Messages on VL are sent with a sequence number that is used on the receiving end to verify that the sequence numbers within a VL are in order. This is referred to as integrity checking.

A redundant set of switches and physical links is required by the AFDX standard. Data is replicated and passing on the first valid message received on one channel and discarding the duplicate provides redundancy management. The redundancy management function may also introduce message-timing jitter that is included in the overall transmission jitter requirement of less than 500 μs. AFDX provides message error detection and the capability for switches to enter quiet mode in the event of catastrophic failures within the switch. Node failures resulting in inappropriate messages cause the switch to discard the messages. No mechanism is specified to inform the receiving node of sending node errors. AFDX has no published fault hypothesis. More information concerning AFDX is found in the ARINC standard.[21,22]

2.10 Fibre Channel

As specified by a large collection of standards published by the American National Standards Institute (ANSI), Fibre Channel is designed to be a high-performance data transport connection technology supporting transmission via copper wires or fiber optic cables over long distances. It is designed to support a variety of upper level protocols mapped onto the physical delivery service. Fibre Channel was originally developed for storage applications and is primarily used to implement storage area nets (SAN). It has been selected for use in military aircraft avionics, most notably the F/A–18 Hornet Fighter-Bomber avionics upgrades and the Joint Strike Fighter. One ANSI standard addresses the application of Fibre Channel to the avionics environment.

Fibre Channel is a full-duplex communication architecture that supports a variety of topologies such as point-to-point, arbitrated loop, and switched fabric. The switched fabric topology is used in the Joint Strike fighter. As described in section 2.8, the switches must keep track of address information

to send messages from one node to another. Fibre Channel supports several classes of transmission as follows:

- Class 1—Provides a dedicated connection with acknowledgment, guaranteeing delivery and message sequence,
- Class 2—Connectionless and may provide messages out of order, delivery confirmation is provided,
- Class 3—Connectionless and unconfirmed. Flow control is provided based on port credit, similar to SpaceWire. Data is only sent when the credit counter indicates buffer space is available.

While Fibre Channel is extremely fast, it is not deterministic in its standard form. Delays through switches increase as network traffic increases. With large network sizes, it is impossible to analyze these delays, as they are functions of multiple variables.[23] Fibre Channel also has many characteristics that make it attractive, including the availability of off-the-shelf components, capability for plug-and-play, and support of hot-swappable components. To address the determinism issue, the Fibre Channel avionics environment (FC–AE) working group developed standards pertaining to upper-level protocols with the goal of augmenting Fibre Channel to provide deterministic latency. Of particular interest is FC–AE–1553, that involves creating a deterministic command/response protocol that can leverage existing system designs based on MIL–STD–1553, but make full use of the Fibre Channel characteristics. The comparison table entries are primarily for the switched topology implementation of Fibre Channel and the standard characteristics. The FC–AE related standards are not included in this TM because coverage of all upper-level protocols that could run on Fibre Channel is outside the scope of this survey. The numerous standards that specify Fibre Channel are also not referenced in this survey. More information can be found at www.t11.org and the standards in their final published form may be purchased from ANSI.

2.11 Gigabit Ethernet

1000/10 G Base-X Ethernet is included as a separate section because it is a combination of the IEEE 802.3 standard and the Fibre Channel physical layer standards. It is widely used in networks for commercial, government, military, and educational institution networks and typically uses TCP/IP or UDP/IP, as is done with Ethernet. It supports both copper wire and fiber optic transmission media. The transmission rate is very fast and it can be implemented over long distances (40 km is reported). The maximum length of the transmission medium is determined by the medium itself. 10 G Ethernet only supports full-duplex operation, while 1 G Ethernet will support half-duplex transmission. Other than the differences in the physical layer, 1000/10 G Base-X operates the same as 10/100 Base-T. Like Fibre Channel, there is much interest in implementing Ethernet in military systems, however; no publicly available information exists on any deployment in military systems. IEEE Standard 802.3ae-2002 specifies 1000/10 G Base-X Ethernet.

3. SELECTION RATIONALE

Early in the project, the PHIAT team needed to select the communication architecture to support a hard real-time distributed control system for safety critical systems in a manned spacecraft. These systems include propulsion, spacecraft navigation and attitude control, automated docking, vehicle health management, and life support. Based on requirements developed by the PHIAT team, the resulting distributed system had to support fault detection, containment, and tolerance while providing high reliability and high availability. Additionally, the system must employ modular components at all levels for high reusability, flexibility, and scalability, and these components must support plug-and-play and be hot swappable wherever possible. Also required was the capability to distribute functionality and intelligence to enable the use of existing radiation-hardened processors and provide complex functionality for fault detection, isolation, and recovery (FDIR) and health monitoring. Finally, the system must be sustainable with respect to nonrecurring engineering, upgrade, and maintenance costs. The capability to transmit large amounts of data at an extremely high rate was not a requirement. Most control loops operate at a rate of 100 Hz or less. The SSME controller operates at a rate of 50Hz and the flight control loop in the Space Shuttle general purpose computers executes at 25 Hz.[25,26]

These requirements were best met by TTP/C for several reasons. TTP/C is designed specifically for safety critical, hard real-time distributed control. As such, it provides the guaranteed latency and jitter that is needed to ensure that the data required for distributed control functions is delivered in a timely and predictable fashion. The use of a predefined message schedule with a fault-tolerant global clock provides known and exactly predictable communication bus loading and message sequencing. Most importantly, the protocol is masterless. The failure of a single node, or even several nodes, does not prevent synchronized communication from continuing between the remaining nodes. Fault detection, containment, and tolerance are provided via the membership services, message status, data consistency checks, and bus guardian functions implemented in the hardware. TTP/C imposes a physically and functionally distributed architecture that partitions the application hardware and the communication network. This not only prevents application errors from propagating from one node to another, but also simplifies software development due to the implementation of protocol components in the hardware. The communication network looks like shared memory to the application software on each node. All that is required for communication is periodic reading from and writing to the memory locations.

TTP/C supports hot swap of nodes on the network. Faulty nodes can be replaced and new nodes integrated without powering down the rest of the system. This along with the strict interface specification supports modularity in system upgrades and new system integration. Modules can be upgraded and swapped with existing modules without disturbing the system and without full-system requalification. The strict interface definition allows different manufacturers to create modules and essentially guarantees successful integration if the interface definitions are enforced.

The communication rates supported by TTP/C hardware currently available are suitable for the real-time control requirements of all safety critical vehicle subsystems. Higher data rates are only

needed if noncritical data is transmitted along with critical data. From a control system standpoint, there is no need to transmit data like a video stream or vibration data streams from multiple channels. Rather, this data would be transmitted directly to a local processing node that would then transmit the analyzed results obtained from this data to the components that need it. In the case of a video stream for automated docking, the information transmitted across the hard real-time network would be the coordinates of the target that are needed by the controller for the reaction control system. Since TTP/C is designed to be physical layer independent, higher speed transmission can be obtained by moving to an appropriate physical layer, if the need arises.

Finally, TTP/C represents a cost-effective solution. The communication controller and supporting development software are commercially available at a reasonable cost to any interested party wanting to purchase them. The communication controller can be implemented in a radiation-tolerant FPGA or in a radiation-hardened ASIC device for deployment in space. The distributed system architecture supported by TTP/C allows the use of currently available radiation-hardened processors in the implementation of complex control and monitoring functions. Implementation of the protocol in the hardware reduces the complexity and cost of software development. The capability to network nodes at distances up to 100 m allows components to be placed in confined locations and reduces long runs of bulky wiring bundles by placing the nodes close to the system components being monitored and controlled. The wiring connections to multiple sensors and actuators can be shortened and only the lightweight twisted pair buses will be routed over significant lengths.

TTCAN is slow at 1 MB/s, but may be useful as a secondary field bus to interface with less critical control and monitoring components. SAFEbus is a proprietary implementation and is not commercially available as components. Furthermore, it is a backplane bus that cannot support the physical distribution of networked nodes. FlexRay could provide the functionality needed, but the associated hardware is less mature and is only available to members of the FlexRay consortium. Additionally, FlexRay does not implement services such as membership, message status, and consistency. These would have to be implemented in the application software.

While AFDX shows some promise, it does not have inherent fault tolerance and would require additional software and hardware implementation to meet the same level of reliability and fault tolerance as TTP/C. Furthermore, the event driven nature of the standard has the potential to make it difficult to truly implement real-time communication with known latency. Without a bus guardian function, AFDX is subject to a faulty node monopolizing a link. SpaceWire suffers similarly, but has the attraction of having been deployed in space. A TTP/C implementation over SpaceWire, switched Ethernet, or Fibre Channel is possible with some, most likely significant, development cost. All these switched fabrics should have the capability to support a time-triggered upper level protocol with some modification to the transmission medium.

Taking all this into account, the choice is to use TTP/C to implement the modular real-time control system that the PHIAT team is tasked to develop. This control system architecture has come to be known as the integrated safety critical advanced avionics for communication and control (ISAACC) system. Based on this survey, TTP/C provides all the functionality needed to meet the requirements defined by the PHIAT team.

4. CONCLUSION

This survey is intended to provide data to aid in the selection of communication architecture for future spacecraft avionics systems. It is not an exhaustive survey, but it provides good coverage of the communication architectures currently being used or proposed for aircraft and aerospace vehicles.

The rationale for selection of TTP/C for the ISAACC system is presented. This shows how the PHIAT team used the data to select communication architecture suitable to complete the task of implementing a modular, distributed, and hard real-time control system for manned spacecraft. Other designers may come to a different conclusion to meet the requirements of the avionics systems they are tasked to design. It is the opinion of the PHIAT team members that there will be several different communication architectures in manned spacecraft to support integrating the critical functions needed to ensure safety with the functions needed for vehicle health monitoring. This is inevitable, as the differing system requirements are traded against the real costs of system implementation. The major challenge will be in defining what the systems will do and how the systems will be implemented.

APPENDIX A

Feature	MIL–STD–1553	Safebus	TTP/C	FlexRay	TTCAN	IEEE–1394B	SpaceWire	Ethernet 10/100 Base-T	AFDX	Fibre Channel	Gigabit Ethernet
Description	Military standard defining electrical and protocol characteristics for a data bus Centralized messaging control	Backplane bus that is the basis for ARINC 659, a standard for transfer of digital data between line replaceable modules (LRMs) within an integrated modular avionics cabinet Used	TTP governed by TTP/C specification developed by University of Vienna and TTTech Synchronous and fault-tolerant protocol developed for safety-critical, real-time distrbuted systems	Deterministic and fault-tolerant bus system for high-speed automotive control applications, based on standards developed by FlexRay consortium	TTCAN is an extension to the unchanged CAN protocol, introducing to CAN networks time-triggered communication and systemwide global network time with high-precision TTCAN controllers can be seen as CAN controllers enhanced with a frame synchronization entity TTCAN is internationally standardized as ISO DIS 11898–4	The IEEE 1394 standard enables simple, low-cost, high-bandwidth data interfacing between computers, peripherals, and consumer electronics products.	SpaceWire is based on two existing commercial standards, IEEE–1355 and LVDS, which have been combined and adapted for use onboard spacecraft	The family of LAN products covered by IEEE 802.3 standard that defines what is commonly known as the CSMA/CD protocol	AFDX is a standard that defines the electrical and protocol specifications, (IEEE 802.3 and ARINC 664, Part 7) for the exchange of data between avionics subsystems	Defined by a collection of ANSI standards, a high-bandwidth (100 MB/s) serial communication bus supporting several topologies, protocols, and media	Combines IEEE 802.3 Ethernet CSMA/CD standard with ANSI X3T11 Fibre Channel physical layer specifications
Application	Primarily military aircraft and spacecraft, some commercial	Developed by Honeywell for commerical aircraft	Applicable to all manned vehicles, commercial and military to date	Automotive electronics	Automotive drive-by-wire	Primarily consumer electronics. Has been proposed for automotive and used in aerospace applications	Developed in Europe for use in satellites and spaceborne experiments	Widely used for non-critical LAN applications in all sectors, including aerospace	Developed by Airbus Industries for commercial aircraft	Targeted for use in mass data storage and transport applications for large computing networks SAN standards exist defining use in an AE	Widely used for non-critical LAN/WAN applications in commercial and public sectors
Deployed Systems	*ISS*, Shuttle payloads, military aircraft, and ships	Aircraft information system (AIMS) on Boeing 777	Airbus A380 cabin pressure control Full-authority digital engine control for Aermacchi M–346 and Lockheed Martin F–16 aircraft, railway switching/interlocks	Prototype in-vehicle testing	Concept/prototype automobiles No widely reported deployment in publicly available literature	Widely used in personal computers and peripherals Planned for use in automotive telematics applications Used in JSF and a noncritical Space Shuttle camera system	IEEE 1355-based communication used on several ESA spacecraft, such as Rosetta SpaceWire-like hardware on NASA SWIFT spacecraft Proposed for James Webb Space Telescope and several ESA missions	Nearly all commercial, educational, military, and government facilities Implements *ISS* LAN	Used on Airbus A380 Planned for Boeing 787	Deployed in SANs for commercial computing networks Used in upgrades to existing military avionics Selected for use in Joint Strike Fighter	Nearly all commercial, educational, military, and government facilities
Communication Control Event-/Time-Triggered, etc.	Event-triggered, (command/response) requires bus controller	Time-triggered, based on communication schedules in pre-loaded tables Masterless	Time-triggered, autonomous and independent of host Masterless	Time and event triggered Event messages sent during specified dynamic slots	Time and event triggered (event in arbitrating frame)	Cycle master (root) broadcasts cycle start package For isochronous transmission in broadcast mode Isochronous resource manager arbitrates requested isochronous transfers Any time left used for asynchronous transfers arbitrated by root	Event triggered	Event, employs CSMA/CD for half-duplex implementation	Event-triggered, based on host message generation, bandwidth predefined and guaranteed by hard limits	Event-triggered, based on host message generation and arbitration as required based on topology	Event, employs CSMA/CD

Feature	MIL–STD–1553	Safebus	TTP/C	FlexRay	TTCAN	IEEE–1394B	SpaceWire	Ethernet 10/100 Base-T	AFDX	Fibre Channel	Gigabit Ethernet
Maximum Data Rate (MB/s)	1 MB/s	60 MB/s	5 MB/s using RS–485 phy, 25 MB/s using Ethernet phy	10 MB/s	1 MB/s maximum high-speed CAN: 125 KB/s max for low-speed/fault-tolerant CAN	800 MB/s currently available (3,200 MB/s defined) Limited by cable media and length and the slowest device between transmitting node and receiving node	400 MB/s	100 MB/s (10 MB/s)	100 MB/s using ethernet phy.	1, 2, 4 and 10 GB/s	10 GB/s(1 GB/s)
Message Size	640 bits (512 data bits)	1 to 256 32-bit data words, no overhead in packet, programmable gap from 2 to 9 bits	24 120-bit overhead 2-240 byte data	8-bytes overhead, 0-254 bytes data	Standard: 51 bits overhead Extended: 72 bits overhead; 0-8 bytes data	Based on transmission rate and mode 4,096 bytes asynch. and 8,912 isoch. at 800 MB/s for beta packets	5 bytes overhead, data payload not limited by standard	TCP: 66–118 byte overhead 1,416–1,460 byte data UDP: 53 byte overhead 17–1,471 byte data	53 byte overhead 17–1,471 byte data	21,248 bytes (36 bytes overhead, 4–2,112 bytes payload)	TCP: 66–118 byte overhead 1,416–1,460 byte data UDP: 53 byte overhead 17–1,471 byte data
Message CRC (Yes/No)	No, app. level data CRC	No, not required due to self-checking bus pairs	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Provide All Nodes With Data Transmitted by Other Nodes for Local Node Use as Required	No RT to all, only through broadcast messages, BC to all RT	Yes, must be specified in message table memory	Yes, by default	Yes	No, only nodes with proper message ID filter see particular messages	Using isochronous broadcast only	Can be done via packet distribution at routing switches	No, unless computing node is configured to snoop or data is broadcast (UDP)	Only if all messages sent as broadcast	Multicast with switched fabric only	Multicast with switched fabric only
Duplex	Half	Half	Half	Half	Half	Full, Legacy: Half	Full	Half and Full	Full	Full	Half and full for 1 G, Full only for 10 G
Media Access	TDMA, Manchester II	TDMA	TDMA	TDMA for static data and minislottting for dynamic (event) data	TDMA for exclusive windows, with CSMA/CD+AMP in arbitrating windows	Overlapping arbitration and data transfer called BOSS Legacy requires arbitration for transmission via request during specific periods	Flow control via tokens (port credit)	CSMA/CD (collision avoidance) for half duplex, direct for full duplex with processing by switch for delivery	Traffic shaping by end system based on VL definition. Filtering (validation) and policing at switch	Flow control based on port credit	CSMA/CD (collision avoidance) for half duplex, direct for full duplex with processing by switch for delivery
Media Access Without Arbitration (Yes/No)	Bus master only	Yes	Yes	Yes for static segment, no for dynamic segment	Yes for exclusive windows and no for arbitrating windows.	No	No	No, half duplex Yes, full duplex	No	No	No, half duplex Yes, full duplex
Clock Synchronization	Available through master commmand (not required)	Clock synchronization is scheduled and all BIUs participate	Tight synchronization/ fault tolerant	Yes	Level 1 via master reference message Level 2 via global synched clock using data in ref. message	Cycle master handles clock sync. for scheduling isochronous transfers	Not required, but facility for time master exists for time reference	Not required	No	Not required	Not required
Global Time Base (Yes/No)	No	Yes	Yes, fault tolerant, masterless	Yes	Yes, synched to clock master via reference message, backup masters can be present	No	No	No	No	No	No
Latency Jitter	<12 μs for RT response (may be extended to >20 μs)	Goal is <2 bit times	Programmable (1–10 μs)	Programmable, 1–6 μs	<100 μs	<0.02 μs	Variable based on topology, estimated <=10 μs	>=50 μs and variable due to CSMA/CD in half-duplex mode Small, but varies based on size of network and traffic in a switched full-duplex configuration	<=500 μs	Small, but varies based on size of network and traffic	Small, but varies based on size of network and traffic in a switched full-duplex configuration

Feature	MIL–STD–1553	Safebus	TTP/C	FlexRay	TTCAN	IEEE–1394B	SpaceWire	Ethernet 10/100 Base-T	AFDX	Fibre Channel	Gigabit Ethernet
Processor Required at Each Node	Yes for BC No for modules with DMA/glue logic for simple RT	No	Yes	Yes	Could be done with complex VHDL design implemented on an FPGA	Yes	No, only on one end of a point-to-point connection if simple protocol used	Yes	Yes	Yes	Yes
Maximum Number of Nodes on Single Bus	31	32 (theoretical AIMS implementation uses 8–10)	64	64	120	63 on a bus with up to 1,023 buses supported by addressing	224 (logical addresses per cluster) allows regional addressing of 224×224	1 node per segment, 1,024 segments (10/100 Base-T)	Governed by number of switched ports available	127 on arbitrated loop, 224 million logical limit on switched fabric	Governed by number of switched ports available
Physical Layer Length	No limit specified, can be >100 m	<1.5 m (estimate)	Depends on physical layer, 30 nodes on 100-m length for multi-drop topology Cable length of up to 1 km possible	24 m, point-to-point or total bus length	30 m for 1 MB/s	Point-to-point: 4.5 m nominal any type, 50 m over POF at 200 MB/s, 100 m over GOF at 3,200 MB/s, 100 m over CAT5 at 100 MB/s	10 m	100 m between TX/RX	Same as Ethernet 10/100 Base-T	30 m electrical, at least 2 km optical (10 km reported)	1 G:25 m electrical, 5 km optical 10 G: 40 km optical
Physical Layer Independent (Yes/no)	No	No	Yes	No, has physical layer spec.	No	No, 1394 phy. controller required.	No	No	No	No	No
Implementation Physical Layer	Electrical characteristics defined by standard as twisted pair or coax, can be transformer coupled	IEEE 1194.1, copper	Currently RS-485 (MFM) or Ethernet phy. (MII) using COTS devices. Custom over optical fiber.	Twisted pair	CAN controller supporting TTCAN level 1 or 2 with CAN transceiver and twisted pair	1394 physical layer controller or phy./link controller. Requires additional external transceivers for optical connections	LVDS	10/100 Base-T MAC/phy. hardware, twisted pair	Ethernet 100 Base-T MAC/phy., twisted pair	Fibre Channel compatible transceiver over copper or fiber	1,000/10 G Base-T MAC/phy. hardware, twisted pair, or fiber
Topology (Tree, Point-to-point, Multi-drop, Daisy Chain)	Multidrop	Redundant multidrop	Multidrop and point-to-point (hub supports star)	Multidrop and point-to-point (hub supports star)	Multidrop	Cable—peer-to-peer with repeater (tree), noncyclic (1394b disables ports to break loops)	Point-to-point and switched	Generally spanning tree (hub), can be point-to-point and switched	Switched fabric	Point-to-point, arbitrated loop, tree (hub), switched fabric	10 G supports full duplex (point-to-point or switched fabric only) 1 G also supports half duplex (shared bandwidth using repeaters)
Supports Hot Swap of Same Type Nodes	Depends on implementation	Yes	Yes	Not specifically addressed	Yes	Yes, but swapping requires breaking network, depending on configuration	Yes	Yes	Yes	Yes, breaks loop in arbitrated loop topology	Yes
Supports Composability (Yes/No)	No	Yes	Yes	Yes	Yes	No	No	No	No	No	No
Designed Specifically for Safety Critical Systems (Yes/No)	Yes	Yes	Yes	Yes	Yes	No	No	No	Yes	No	No
Membership Service	No	No	Yes	No	No	No	No	No	No	No	No
Inherent Redundancy	Dual-redundant bus	Yes	Dual redundant bus, supports replica determinism	Yes for static frames on dual redundant bus, optional for other frames	No	No	No	No	Yes, dual redundant switches and links	No, but AE specified implementations are dual redundant	No
Redundancy Management	Defined at application level	Yes	Yes, inherently dual redundant, supports task and node replication (hardware/software)	No, must be implemented at application level	No	No	No	No	Defined at application level	No	No
Operate in Fault Tolerant (Fail-Op/Fail-Safe) Mode	Yes	Yes	Yes	Yes	No	No	No	No	Yes	Yes, AE specified implementation	No

Feature	MIL–STD–1553	Safebus	TTP/C	FlexRay	TTCAN	IEEE–1394B	SpaceWire	Ethernet 10/100 Base-T	AFDX	Fibre Channel	Gigabit Ethernet
Fault Hypothesis	None published	Guaranteed to tolerate one arbitrary fault, may tolerate multiple faults At most, one component of any pair can fail	Guaranteed to tolerate one arbitrary fault Never give up strategy may allow tolerance to multiple faults for a given application	None published	None published	None published	None published	None published	None publshed	None published	None published
Fault Containment	Yes, if secondary bus can be used to remove or tolerate the fault	Yes, multiple levels of redundancy (pair-of-pairs for all components, fail silent nodes, shadow nodes)	Yes, in hardware, membership, message status, dual-redundant bus	No, FT must be implemented at the application level	Yes, if CAN controller is not faulty	No	No	No	Yes, if fault is confined to one dual-redundant switched network.	No	No
Babbling Idiot Avoidance	Not inherent, defined at application level	Yes, bus guardian	Yes, bus guardian	Uses timeout, no bus guardian	In the case of repeated faulty messages while CAN controller is not faulty, or if the application processor can place transceiver in stand-by	None	None	None	Detected and suppressed by switch	None	None
Message Failure Detection	Yes, status bit	Yes, BIU pairs check transmitted and received data	Yes, message status, global acknowledement	Yes	Yes, by sender and receiver in hardware	No, in isochronous mode Yes, in asychronous mode (hardware)	Yes, parity, invalid destination,credit error, error end of packet	Yes, collision and RX at phy., no acknowlege (TCP, not UDP)	Yes, port detects overflow errors or switch identifies message failure and discards	Yes, link loss, acknowledgement, sequence error, message format	Yes TCP, not UDP
Tolerant to Message Loss	No, retransmit required	Yes, bus is quad redundant	On one channel	For redundant messages	No, retransmit only during arbitration phase	No, retransmit required	No	No, retransmit required	On one dual redundant switch network	No, retransmit required in standard config.	No, retransmit required
Prompt Communication Error Detection And Error Reporting	12 μs timeout for RT response (may be extended to >20 μs)	Yes, error detection is concurrent with message transmission/reception BIU reports error to host via registers	Yes (hardware), message error upon receipt, node fault within two TDMA communication cycles	Yes, message error during transmission and upon receipt	Yes (hardware), message error during transmission and upon receipt	Message receipt errors and acknowledge errors reported at link layer (hardware) Detection of presence of peer node at port	Link disconnect error reported in 1 μs	Collision detection (50-μs, hardware) and RX error at phy. Loss of communication between 2 nodes depends on network size—TCP, not UDP software	Variable, depending on link bandwidth and number of switches	Link errors and frame errors reported to sender through transmission of reject messages after error is detected Class 3 provides no acknowledgement Timing depends on network size and loads	Collision detection (50-μs, hardware) and RX error at phy. Loss of communication between 2 nodes depends on network size—TCP, not UDP software
Node Failure Detection (Controller Hardware Level)	Only for RTs, via response timeout, no other at hardware level	Yes	Yes	No	Yes	Via arbitration timeout or cable bias voltage loss	Only via link disconnect error and failure to reconnect Timeout indicator provided to application.	No	No	May be detected by missing acknowlege at link control facility	No
Node Failure Reported Consistently and With Low-Latency (Yes/No)	Only master knows	Yes, nodes fail silent; others detect by loss of scheduled communication	Yes, all functional nodes aware	No	To local application processor only	No	Yes, in the case of link failure only	No	Only nodes expecting data may be aware at application level	No	No
Tolerant to Node Loss	No, if bus master(s) is (are) lost, otherwise yes, communication still proceeds between remaining nodes	Yes, communication will proceed between remaining nodes	Yes, communication will proceed between remaining nodes	Yes, communication will proceed between remaining nodes	Can tolerate missing or unpowered nodes, but communication may not proceed correctly between remaining nodes in some cases	Depends on topology Only if an unused loop connection exists	Yes, communication will proceed between remaining nodes	Yes, communication can still proceed between remaining nodes	Yes, communication can still proceed between remaining nodes	Yes, communication can still proceed between remaining nodes	Yes, communication can still proceed between remaining nodes

Feature	MIL–STD–1553	Safebus	TTP/C	FlexRay	TTCAN	IEEE–1394B	SpaceWire	Ethernet 10/100 Base-T	AFDX	Fibre Channel	Gigabit Ethernet
Error Handling Approach	Terminal shutdown/ reset	Self-checking buses are used All BIU pairs check and compare all data traffic, BIU pairs must agree BIUs discard bad data and enforce fail silence	Replicated channels manage message loss on one channel; fail silence for protocol errors; FTUs (error masking); restart with self test	Message errors reported to host	Uses CAN message arbitration and fault management Node fails silent after transmitting max. number of error frames FT transceivers can communicate on one wire	Report error message codes from link layer Retransmit on loss of asychronous message	Link, parity, and credit error prompt reset of link and error reporting to application Reports detectable link physical connection faults to application	Retransmit on collision detection (MAC), loss of data (TCP, not UDP)	Switch can detect/ localize failures at the ports and discard bad messages No error/flow control on transmitted data Switch enters quiet mode for catastrophic failure	Retransmit on busy, reject, or lack of acknowlegement, request by recipient	Retransmit on collision detection (MAC), loss of data (TCP, not UDP)
Extensibility (Ease of Expansion)	Depends on implementation	Requires design of new schedule	Requires design of new schedule	Requires design of new schedule for new static slots	Requires design of new system matrix (message patterns)	Easy	Requires routing switch reconfiguration	Easy	Requires design of new switch configuration data table	Easy	Easy
COTS Test Equipment (Yes/No)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Availability of Off-the-Shelf Hardware (Yes/No)	Yes	No	Yes	Yes, consortium only	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RAD-Hard/Tolerant Off the Shelf Parts	Yes	No	Yes, rad-tolerant via FPGA implementation	No	Yes, rad-tolerant via FPGA implementation	No, custom made exist	Yes	Somewhat, via rad-tolerant FPGAs (see FPGA IP entry below)	Somewhat, via rad-tolerant FPGAs (see FPGA IP entry below)	Yes (FC–1 and FC–2) via rad-tolerant FPGA. No rad-tolerant phy.	Somewhat, via rad-tolerant FPGAs (see FPGA IP entry below)
IP Available for ASIC Implementation (Yes/No)	Yes	Yes, but not necessarily to third parties	Yes	Yes, consortium only	Yes	Yes	Yes	Yes	Yes, limited avialability	Yes	Yes
IP Available for FPGA Implementation (Yes/No)	Yes	Yes, but not necessarily to third parties	Yes	Yes, consortium only	Yes	Yes, link layer	Yes	Ethernet MAC	Ethernet MAC via FPGA implementation, no phy. AFDX specific functions are proprietary, limited availability	Yes (FC–1 and FC–2)	1/10G Ethernet MAC and PCS
Software Design Tools	Yes	Reported under development in 1992	Yes, system generation from high-level specs.	Yes, consortium only	Yes	No	No	No	Yes, application programming interface library	No	No
Open Specification	Yes	ARINC 659 is available for purchase by public SAFEBus spec. is proprietary	Yes, but implementation must be licensed	Yes, but implementation requires membership in or an agreement with the consortium	Yes	Yes, but implementation must be licensed	Yes	Yes	AFDX spec. is proprietary, ARINC 664 part 7 is available for purchase by the public	Yes	Yes
Formal Methods Applied	No	Details of assurance process not published	Yes	No	Yes	No	No	No	No	No	No
Notes	Bus must be tested to determine the effect of stubs/couplings	SafeBus is a registered trademark of Honeywell, and is currently the only implementation of ARINC 659		Consortium has expressed no interest in using FlexRay outside automotive applications	Availability of TTCAN level-2 hardware is limited at time of writing TTCAN can be implemented in software.		Space-rated hardware exists for SMCS (IEEE 1355 based) Most SpaceWire compliant hardware currently available as VHDL cores with the exception of router designs	Entries based on 10/100 Base-T using TCP or UDP	AFDX is a trademark of Airbus	Governed by multiple ANSI specifications (52 available from ANSI) Flexible and complicated	Entries based on 10/100 Base-X using TCP or UDP

REFERENCES

1. Rushby, J.A.: "Comparison of Bus Architectures for Safety Critical Embedded Systems," CSL Technical Report, SRI International, 2001.

2. Miner, P.S.; Carreno, V.A.; Malekpour, M.; and Torres, W.: "A Case Study Application of RTCA DO–254: Design Assurance Guidance for Airborne Electronic Hardware," Digital Avionics Systems Conference, October 2000.

3. MIL–STD–1553b: "Aircraft Internal Time Division Command/Response Multiplex Data Bus," September 21, 1978.

4. MIL–STD–1553b Notice 4: "Interface Definition for Digital Time Division Command/Response Multiplex Data Bus," January 15, 1996.

5. MIL–STD–1553: "Protocol Tutorial," Condor Engineering, Santa Barbara, CA, July 16, 2004.

6. Schleicher, S.K.: "Revved-Up 1553 Flavors Boost Performance," COTS Journal, The RTC Group, July 2003.

7. ARINC Specification 659: "Backplane Data Bus," Aeronautical Radio, Inc., Annapolis Maryland, December 27, 1993.

8. Hoyme, K.; and Driscoll, K.: "SAFEbus," Proceedings Digital Avionics Systems Conference, pp. 68–73, Seattle, WA, October 1992.

9. Kopetz, H.; and Bauer, G.: "The Time-Triggered Architecture," Proceedings of the IEEE, Volume 91, Issue 1, pp. 121–126, January 2003.

10. Time-Triggered Protocol TTP/C High-Level Specification Document Protocol Version 1.1, D–032–S–10–028, TTTech Computertechnik, Edition 1.4.3, November 19, 2003.

11. FlexRay Communications System Protocol Version 2.1, FlexRay Consortium, May 12, 2005.

12. FlexRay Communications System Electrical Physical Layer Version 2.1, FlexRay Consortium, May 2005.

13. Fuhrer, T.; Muller, B.; Dieterle, W.; et al.: "Time-Triggered Communication on CAN," Robert Bosch GmbH, Proceedings 7th International CAN Conference (ICC), Amsterdam, The Netherlands, 2000.

14. Hartwich, F.; Muller, B.; Fuhrer, T.; et al.: “CAN Network With Time-Triggered Communication,” Robert Bosch GmbH, Proceedings 7th International CAN (ICC) Conference, Amsterdam, The Netherlands, 2000.

15. Chau, S.N.; Alkalai, L.; Burt, J.B.; and Tai, A.T.: “The Design of a Fault Tolerant COTS-Based Bus Architecture,” Proceedings of 1999 Pacific Rim International Symposium on Dependable Computing (PRDC’99), Hong Kong, China, December 1999.

16. IEEE Standard for a High-Performance Serial Bus—Amendment 2, IEEE Standard 1394b, Institute of Electrical and Electronics Engineers, New York, NY, December 14, 2002.

17. IEEE Standard for Heterogeneous Interconnect (HIC) (Low-Cost, Low-Latency Scalable Serial Interconnect for Parallel System Construction), IEEE Standard 1355–1995, IEEE Computer Society, IEEE, June 1996.

18. IEEE Standard for Low-Voltage Differential Signals (LVDS) for Scalable Coherent Interface (SCI), IEEE Standard 1596.3–1996, IEEE Computer Society, IEEE, July 1996.

19. SpaceWire—Links, Nodes, Routers, and Networks, ECSS–E–50–12A, European Cooperation for Space Standardization, January 24, 2003.

20. IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific requirements, Part 3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, IEEE Computer Society, IEEE, March 8, 2002.

21. Aircraft Data Network Part 7 Avionics Full Duplex Switched Ethernet (AFDX) Network, ARINC Specification 664, Part 7, Aeronautical Radio, Inc., June 27, 2005.

22. AFDX Protocol Tutorial, Condor Engineering, Inc., Santa Barbara, CA, March 1, 2005.

23. Hendricks, S.P.: Exploration of Fibre Channel as an Avionics Interconnect for the 21st Century Military Aircraft, Thesis, Naval Postgraduate School, September 2000.

24. IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements, Part 3 Carrier Sense Multiple Access With Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications, Amendment 1: Media Access Control (MAC) Parameters, Physical Layers, and Management Parameters for 10 GB/s Operation, IEEE Computer Society, IEEE, March 8, 2002.

25. Mattox, R.M.; and White, J.B.: “Space Shuttle Main Engine Controller,” NASA–TP–1932 M–360, November 1, 1981.

26. Carlow, G.D.: “Architecture of the Space Shuttle Primary Avionics Software System,” Communications of the ACM, Volume 27, Number 9, pp. 926–936, September 1984.

27. Adams, C.: “1553:Ever Faster,” *Avionics Magazine*, December 1, 2004. Available online at http://www.aviationtoday.com/cgi/av/show_mag.cgi?pub=av&mon=120

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave Blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	April 2006	Technical Memorandum

4. TITLE AND SUBTITLE

Comparison of Communication Architectures for Spacecraft Modular Avionics Systems

5. FUNDING NUMBERS

6. AUTHORS

D.A. Gwaltney and J.M. Briscoe

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

George C. Marshall Space Flight Center
Marshall Space Flight Center, AL 35812

8. PERFORMING ORGANIZATION REPORT NUMBER

M–

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Aeronautics and Space Administration
Washington, DC 20546–0001

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

NASA/TM—2006–

11. SUPPLEMENTARY NOTES

Prepared

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified-Unlimited
Subject Category 19
Availability: NASA CASI 301–621–0390

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This document is a survey of publicly available information concerning serial communication architectures used, or proposed to be used, in aeronautic and aerospace applications. It focuses on serial communication architectures that are suitable for low-latency or real-time communication between physically distributed nodes in a system. Candidates for the study have either extensive deployment in the field, or appear to be viable for near-term deployment. Eleven different serial communication architectures are considered, and a brief description of each is given with the salient features summarized in a table in appendix A. This survey is a product of the Propulsion High Impact Avionics Technology (PHIAT) Project at NASA Marshall Space Flight Center (MSFC). PHIAT was originally funded under the Next Generation Launch Technology (NGLT) Program to develop avionics technologies for control of next generation reusable rocket engines. After the announcement of the Space Exploration Initiative, the scope of the project was expanded to include vehicle systems control for human and robotics missions. As such, a section is included presenting the rationale used for selection of a time-triggered architecture for implementation of the avionics demonstration hardware developed by the project team.

14. SUBJECT TERMS

digital data bus, serial data bus, serial communications, avionics

15. NUMBER OF PAGES

32

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	Unlimited

National Aeronautics and
Space Administration
IS20
George C. Marshall Space Flight Center
Marshall Space Flight Center, Alabama
35812