Evaluation of numerical bus systems used in rocket engine test facilities

Schmidt, Volker[*] Georgiev, Pavel[†] Horn, Harald[‡]

Neumann, Heike[§] Hätte, Inna[¶] Fricke, Matthias[‖]

1 Introduction

Currently measurement, control and command system (MCC) for rocket engine test facilities use classical connections for measurements and also for control and command systems of the test bench and the engine. At the moment numerical bus systems are mainly used inside the MCC system or to interface stages (MIL STD-1553). In future applications, engine and stage components are interfaced by numerical bus systems instead of direct wiring. In addition the common known MIL-STD-1553 bus system will be compared with modern approaches.

This paper provides an overview of public available information concerning bus systems used in aeropspace applications. The evaluation criteria are chosen with respect to the use in rocket engine test benches and launch vehicles. The questions asked to each bus are focussed on reliability and performance since the data bus network is as safety-critical for the test bench as it is for the launch vehicle.

Beside interfacing the engine or stage avionics, numerical bus systems also allow MCC systems to react more flexible on changed requirements for acquisition, control and health monitoring. Possible extensions and constraints, to include such systems in existing MCC systems, are also shown in this paper.

This study comprises all together seven data bus systems with MIL-STD-1553 serving as a reference for this concept, as it is proven to be reliable and it is the most used data bus system in military avionics and in aerospace in the last thirty years. The following specifications are taken into consideration:

- FC-AE-1553,
- HyPer 1553,
- Time-Triggered Protocol (TTP), SAE AS 6003,
- Time-Triggered Ethernet (TTEthernet), SAE AS 6802,
- SAE AS5643 based on IEEE 1394 (FireWire).

During the course of the study AFDX (implementation of ARINC664 part 7), FlexRay and MIL-1773 were taken into consideration,

[*] Volker.Schmidt@dlr.de
[†] Pavel.Georgiev@dlr.de
[‡] Harald.Horn@dlr.de
[§] Heike.Neumann@dlr.de
[¶] Inna.Haette@dlr.de
[‖] Matthias.Fricke@dlr.de
German Aerospace Center (DLR), Institute of Space Propulsion - Engineering, 74239 Hardthausen, Germany

but they dropped out as options. The functionality of AFDX is completely covered and surpassed by TTEthernet. FlexRay is limited by its reach – it specifies 24 meters as maximal data bus length. MIL-1773 is often given as an example for optical fiber variant of the MIL-1553 bus protocol, but during the course of the study we were not able to find a supplier for it.

2 Test-bench setup

One possible implementation scheme of the bus with two independent paths from MCC to each ES is presented on figure 1. The following basic requirements are to be fulfilled by each of the candidates:

- Reliability requirements shall be met.
- The data bus system shall tolerate MCC failure.
- The data bus shall be able to deliver the command law from MCC to the ES every 10ms.
- End-to-end latency over the bus shall not exceed 1ms.
- A bus length of at least 50m is considered, taking into account the dimensions of P5.
- The data bus shall provide at least 200 kbit/s throughput.

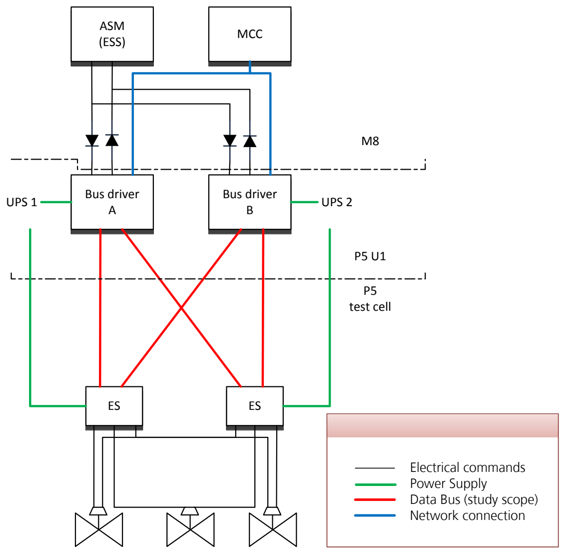

Figure 1: Test Bench bus topology with two independent channels per ES

3 Presentation of data buses

In order to make the presentation simple and clear the STANAG 3910 and HyPer 1553 buses are grouped together, since they approach augmentation of MIL-STD-1553 in incremental steps and preserve its basic features.

Due to possible slight differences in the definitions the basic properties and features of data bus systems, a terminology definition list is presented The definitions presented there are uniform with the definitions given in the documents describing the Time-Triggered Architecture and AS5643.

The short data bus overviews attempt to present the basic elements of the systems, the operation principle and possible advantages or drawbacks. The table should ease comparison of specific features

3.1 MIL-STD-1553 - Time-division command-response multiplex data bus

The MIL-STD-1553 standard establishes requirements for digital, command-response, time division multiplexing data bus. It encompasses the data bus line and its interface electronics and also defines the concept of operation and information flow on the multiplex data bus and the electrical and functional formats to be employed.

The main elements of the system are Bus Controller (BC), Remote Terminal (RT) and

Bus Monitor (BM). BC is assigned the task of initiating information transfers on the data bus.BM is a terminal, assigned the task of receiving bus traffic and extracting selected information to be used in a later time. RTs are all terminals not operating as the BC or as a BM.

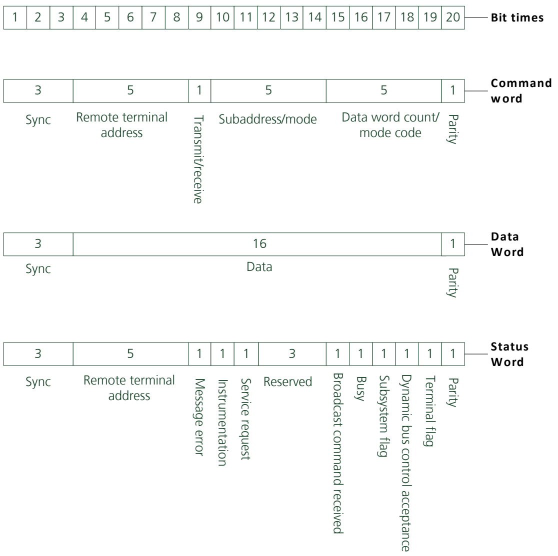

Figure 2: MIL-STD-1553 Data Word Formats

Operation is asynchronous, which mean every terminal (BC, RT and BM) uses independent clock source – at reception clock information can be derived from the message. Each message is formed by three types of words – command word, data word and status word. The format of the words in MIL-STD-1553 is given in figure 2.

Redundancy issue: Transmission is allowed only on one of the data buses (redundant data bus is quiet). If a BC fault is detected, the control can be offered to the redundant BC. BM or redundant BC can be used to monitor the health status of the BC. The data transportation media consists of shielded twisted pair cables, bus-stub coupling and termination resistors in the end of the bus line. Basic information is given in

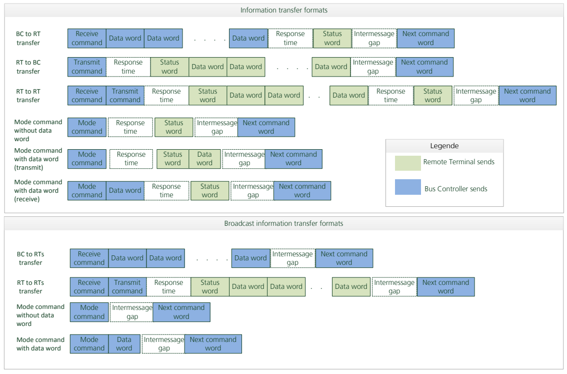

Figure 3: MIL-STD-1553 Messaging Sequences

table 1. Detailed information for the stub coupling and recommendations can be found in [1]

Table 1: MIL-STD-1553 Hardware characteristics

Characteristics	Description
Cable	Twisted pair (12 twists per meter), shielded
Capacitance wire-to-wire	100pF/m
Characteristic impedance (Z_0)	70 to 85 Ω (at 1MHz frequency)
Cable attenuation	5 dB/100m
Cable termination resistors	($Z_0 \pm 2\%$) Ω
Transformer coupled stubs (preferred)	Up to 6m length, galvanic isolated
Direct coupled stubs	Up to 30cm length

The topology of the bus is multidrop (fig. 4) with a maximum length of 100m.

3.2 HyPer-1553

The high-performance 1553 operates on the same physical layer with enhanced transceivers, which allows the system to achieve 200 Mbit/s throughput. It is a dual-rate, which means that the 1 Mbit/s transmission operates concurrently with the

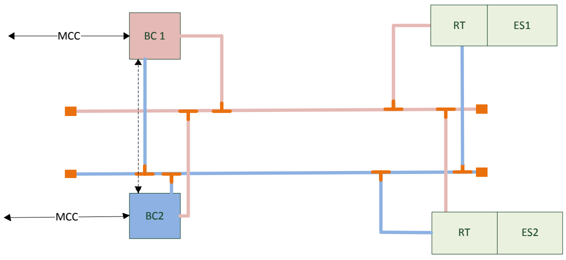

Figure 4: Example topology implementation of MIL-STD-1553

200 Mbit/s transmission. It is not available to purchase yet, it is not feasible to be available in the next 2 years, says the supplier. Successful try with HyPer-1553 running on flying aircraft fighter F-15 were made. There is Turbo-1553 [2] offered by the same supplier (DDC), it offers 5Mbit/s on the same physical layer.

3.3 FC-AE-1553

Fibre Channel was developed originally as storage area network. It provides throughput in the Gbit/s range (from 1 Gbit/s to 10 Gbit/s) over optical fiber or cable as physical layer. The Fibre Channel FC-AE-1553 uses MIL-1553 as upper layer protocol, but it is substantially different. The protocol is quite flexible and complex - there are 52 Fibre Channel specifications defining different aspects or uses, connecting computer systems, storage and other peripheral devices. The specifications are publicly available through American National Standards Institute (ANSI). The protocol stack (Figure 5) is similar to the OSI model, where the highest level allows mapping of another protocol (Upper layer protocol) over the Fibre Channel network. FC-AE-1553 is mapping of MIL-1553 bus protocol over Fibre Channel with physical layer adequate to use in avionics environment.

Using optical fiber introduces certain advantages and disadvantages [3]:

- the reduced EMI/EMC concerns;
- much shorter process of installing the system, since the procedure does not require as many measurements with system on and off as in electrical system;
- Less weight;

There is a drawback using optical fiber in radiation environment, namely due to proton single effects on the receiver, bit error rate is higher, hence message replication is needed and throughput is halved

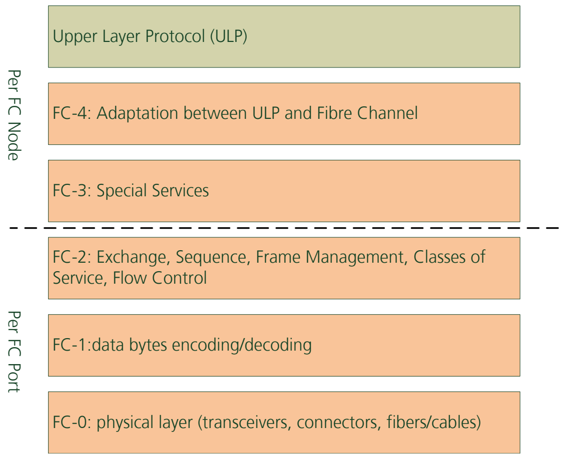

Figure 5: Protocol Stack of Fibre Channel

The elements of MIL-STD-1553 and FC-AE-1553 executing identical function have different names – the analogy is shown in Figure 6. Mapping MIL-1553 protocol means that FC-AE-1553 executes the logic shown in Figure 3.

In the hierarchy of Fibre Channel Messaging: Exchanges consist of Sequences, Sequences consist of Frames, Frames consist of Transmission Words, Transmission Words consist of Transmission Characters. Each Transmission Character represents 1 byte data encoded into 10bits. Detailed information about each element can be found in [4].

Depending on physical layer the length of the data bus can reach >100m using optical

MIL-STD-1553	FC-AE-1553
Bus Controller (BC)	Network Controller (NC)
Remote Terminal	Network Terminal
RT Address	Network Terminal Adress
RT Subaddress	NT Subaddress (NT_SA)
MIL-STD-1553 Message	FC-AE-1553 Exchange
Command Word	Command Sequence
Status Word	Status Sequence

Figure 6: Terminology equivalence between MIL-STD-1553 and FC-AE-1553

fiber or 30m using copper cable. Latency is in μs range.

The system can work as full-duplex, which means it can employ two Network Controllers in parallel use. In conclusion FC-AE-1553 offers an excellent throughput and a decent latency, but it has still reliability issues. In spite of the reports [5] of using successfully Fibre Channel on military aircraft, the technology might need still time to mature – multi redundant Fibre Channel network was used as control system of unmanned flying vehicles at DLR Braunschweig and has shown very high failure rate, due to sensitivity towards vibration.

3.4 AS5643

AS5643 is a modification of the popular IEEE1394 (FireWire), it is suitable for real-time, deterministic communication. This type of network is used as control system for latest generation military missiles and jet fighter aircraft (e.g. ICBM and F-35).

The network provides throughput in the range between 100 Mbit/s and 3,2 Gbit/s where 100 Mbit/s is the base rate and any higher rate is the base rate multiplied by power of 2 (2, 4, 8, 16, 32). End-to-end latency is under 3 μs. It has a tree topology, with specified limit between the distance of 2 nodes of 4,5 meter. A supplier claims that 20 m would not affect negatively the network, however the distance limit and the resulting need of repeater nodes is main disadvantage of AS5643. A possible topology implementation is presented in Figure 7. The maximal span of the bus is 72 m (a data frame sent is limited to 16 hops over node).

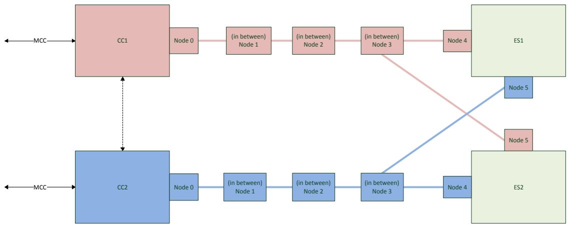

Figure 7: Topology of AS5643

The payload information over the network is carried through asynchronous stream packets (Figure 8). The asynchronous streams includes various mechanisms for error and fault detection:

- Vertical Parity Check (VPC), applied on the data payload;
- CRC;
- Health status word. It signals packet error, subsystem error, node error. It gives STOF offset acknowledgement and status of each port of a node (connected, receiving OK, beta mode and the negotiated data rate);
- Heartbeat word. Guarantees that the control computer software creates fresh data.

The Asynchronous Streams packets have integrated the FC-AE-ASM (Anonymous subscriber messaging) as an upper layer protocol. ASM is a protocol, in which, a Remote Node on the network can subscribe to each message that it requires. The ASM software in the Remote Node will forward only the messages to which the Remote Node has subscribed. ASM is an upper layer protocol tailored for the demands of highly modular embedded real time systems operating under a "data push" paradigm. ASM is designed to be independent of lower level protocols and, as such, does not utilize the IEEE 1394 header to transport ASM-peculiar information. ASM is 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.

In order to decrease failure probability the AS5643 system can be implemented with dual or triple redundancy, where there are two levels of redundancy:

- Two CCs are controlling two replicated channels.
- CC can control the network of the neighbor CC through its physical layer (with data link and controller powered off).

Downside of the AS5643 is that it does not allow hot swap, at the moment. There are other weaknesses which need to be considered regarding its vulnerability to babbling nodes, unexpected node detachment, CC not producing STOF, etc., which are described in [6].

3.5 TTP - Time Triggered Protocol

TTP was developed 20 years ago as a concept for Time-Triggered Architecture. TTP does not specify physical layer, still there are two current attempts to make a standard its use with MIL-STD-1553 physical layer (SAE AS6003/1) and with RS-485 (SAE AS6003/2). It is limited to 64 nodes, 100 m length (MIL-STD-1553 physical layer), 240 bytes maximal length word of (which 4 bytes are CRC), it gives a relatively low latency (under 20 μs). The topology of the TTP network is flexible, it can be star or multidrop bus (similar to MIL-STD-1553). Possible topology implementation with central bus guardian is shown in Figure 9.

The basic element of a TTP network is a node with a TTP controller. The media access is TDMA, in each node a personalized message descriptor list is stored (MEDL), that specifies at which instant a data transmission must be performed or accepted by the node. The TDMA principle employed in TTP can be seen in fig 8

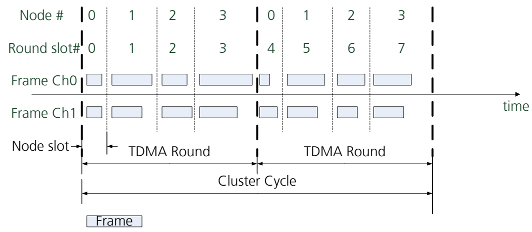

Figure 8: Time Triggered Protocol TDMA access method

Each node is permitted to use the full capacity of the network during its assigned node slot. The periodic sequence of node slots is called TDMA round. The length of node slot the sending sequence does not change – from this point of view TDMA rounds are equal. A node can send frames with different length and type in different TDMA rounds. The pattern of periodically recurring TDMA rounds is called Cluster Cycle. Frame Ch0 and Frame Ch1 are two redundant channels. Note, that the frames sent over the redundant channels are not obligatory having the same content and type.

Another element of a TTP network is the bus guardian. The bus guardian is an autonomous subsystem that protects the communication channels from temporal transmission failures. The temporal firewall serves as well to protect the bus against transmissions that are apt to lead to ambiguous results at the receivers ("slightly-off-specification" faults). The system needs bus guardian for each node, which makes star topology more attractive, having two central bus guardians, serving all the nodes.

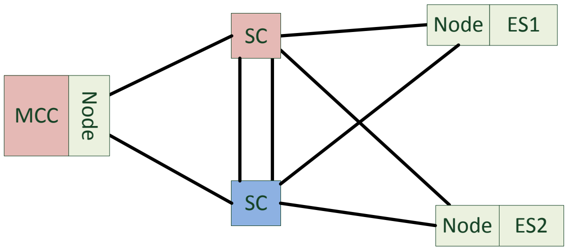

Figure 9: Topology of TTP with central bus guardian

The TTP system is built on global time base. The clock synchronization includes the following steps: Every clock reads the time values of a well-defined ensemble of clocks. Every clock calculates a correction term for its clock using a clock synchronization algorithm. Every clock applies the correction term to its local clock to bring the clock into better agreement with the ensemble. At least 4 clocks must participate in the cluster in order to prevent Byzantine faults. This results in a requirement of at least 4 nodes in one network. As an option it is acceptable to use clock synchronization external to the system, or external clock correction term.

The Time-Triggered Protocol provides membership service – the TTP controller informs its host computer about the state of every other computer in the cluster with a latency of less than two TDMA rounds. The membership service employs a distributed agreement algorithm to determine, in case of failure, whether the outgoing link of the sender or the incoming link of the receiver has failed. Additionally the protocol states a fault tolerance hypothesis – it can tolerate any single hardware failure if it is properly configured. Membership service and fault tolerance hypothesis are distinctive for the Time Triggered Architecture and they make the TTP a suitable solution for safety critical tasks.

The protocol is used as a control system for Full Authority Digital Engine Control (FADEC) in military jet fighter F-16 and in the cockpit of Airbus A380.

Opposed to theThe TTP has the disadvantage that it is not scalable. If a network needs to be expanded over 64 nodes the TTP can't support it. Even though it is stated that "throughput is limited only by the physical layer", in practice TTP can't provide more than 5 Mbit/s with a physical layer suitable for aerospace applications.

3.6 TTEthernet

TTEthernet was created after an unsatisfying attempt to use the TTP over Gigabit Ethernet. It was selected as data bus system in the Orion spacecraft. It enjoys both the high reliability, fault-tolerance standards of the Time-Triggered Architecture and the large experience gathered from Ethernet - the most deployed Local Area Network by now. A TTEthernet is compliant with DO-254 (Design Assurance Guidance for Airborne Electronic Hardware) and DO-178 (Software Considerations in Airborne Systems and Equipment Certification). It provides a throughput in the range of 100 Mbit/s to 1 Gbit/s, the maximal bus length can reach hundreds of meters, particularly if fiber optic harness is used.

The basic physical elements of TTEthernet are End Systems (at each connected device) and Switches. The work principle is similar to TTP – a global time base is established and each End System can use the whole capacity of the bus for a certain time slot.

TTEthernet provides three traffic types (see Figure 10) – best effort traffic (BE), rate-constrained (RT) traffic and Time-Triggered

(TT) traffic. The bandwidth of the system can be configured on demand with various fractions of traffic type, depending on the applications. The BE traffic is standard Ethernet (IEEE802.3), the media access is CSMA (Carrier Sense Multiple Access), not suitable for real-time application, but for any other. The BE gives the advantage, that TTEthernet network can be directly connected to an Ethernet LAN network without need of translation. The RT traffic represents the specified in ARINC664 part7 Ethernet traffic, it is suitable for real-time communication, it provides bounded delay + jitter of a frame up to 500 ï¿$\frac{1}{2}\mu$s. The TTEthernet RT traffic technology is identical with the AFDX used in civil aircraft (Airbus). The TT traffic makes use of the global-time base of the system, it gives acceptable for hard real-time applications with delays and jitter of few μs depending on configuration.

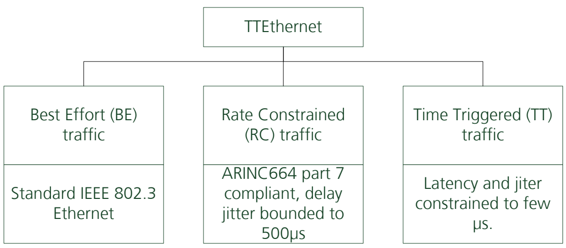

Figure 10: Optional traffic types for Time-Triggered Ethernet

TTEthernet uses standard Ethernet frames, they provide standard MAC addressing and error detection through CRC. Clock synchronization is "transparent clock" through exchange of Protocol Control Frames between the End Systems. The protocol allows the integration of IEEE1588 Precision Time Protocol mixed with the TTEthernet technology in case a device using IEEE1588 is included in the TTEthernet network.

The topology of the system is switched (star), presented on Figure 11. Similar to TTP, the TTEthernet uses a function called Bus Guardian, which provides a temporal firewall for every node of the system. This contains faults as "babbling" node and malicious software failures. A bus guardian is a compulsory functional part in between any two nodes of the TTEthernet system, the example given is a star topology with two central Bus Guardians (note, that guardian represents merely a function, not a separate device).

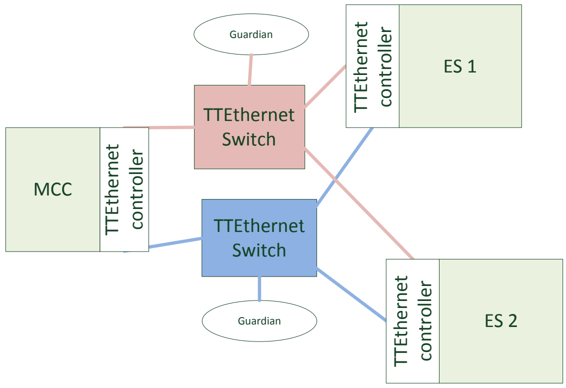

Figure 11: TTEthernet topology

Similar to TTP, TTEthernet provides a membership service and fault-tolerance hypothesis. Membership service means that the network end system gives information to its host processor for the health status of each node in the system. The fault-tolerance hypothesis allows one (or two, depending on implementation [7]) arbitrary hardware failure.

4 Conculsion

The engine test bench functional specification requires the probability of catastrophic event not to exceed 10^{-6}. The probability of failure for certified avionics data network system is not allowed to exceed 10^{-9}, since it is assumed this is a catastrophic failure condition. Assuming that the probability of catastrophic failure condition is equally distributed and the number of different catastrophic failure conditions is not more than one thousand implies that the avionics systems are capable of meeting the reliability requirement of the test bench. For launch-vehicle borne environment where there can be additional mechanical, EMI and radiation hazards, an additional safety assessment needs to be made.

Most of the systems presented are capable of addressing the "crossing" implementation since they are designed to be redundant per se. In this context TTP and TTEthernet have the advantage of being "replica deterministic". Replica determinism means that with active replication, fault-free replicated components are required to deliver identical outputs in an identical order within a specified time interval.

When considering the possible replacement for MIL-STD-1553 in future engine test benches it is assumed that adding large throughout capacity is not primary concern.

AS 5643 and FC-AE-1553 have both excellent throughput and latency parameter, but TTP and TTEthernet are step forward in terms of reliability and fault-tolerance, due to the membership service, the fault-tolerance hypothesis and the compliance with the DO-178 and DO-254.

Assuming reliability and safety are priority in the task to control SCoRE-D, we would recommend TTP with MIL-1553 physical layer (SAE AS 6003/1) and TTEthernet (SAE AS6802) as appropriate choices to replace MIL-STD-1553. Between TTP and TTEthernet, the latter has the advantage of being scalable, hence more suitable if more network members and higher transmission rates would be necessary in the future.

5 Definition of terms

ASM is the emergency stop system of engine test benches in Lampoldshausen (automate de sécurité manuel);

Asynchronous (1) pertaining to a transmission technique that does not require a common clock between the communicating devices. Timing signals are derived from special characters in the data stream itself. (2) not synchronous, not occurring or existing at the same time or having the same period or phase;

BER Bit error rate is 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;

Composable system (composability) A system is composable when its elements keep their properties after integration. In other words an element keeps at least its performance and features on a level prior to integration;

CRC cyclic redundancy check;

Error an unintended part of a state within a system that may lead to a future failure;

Failure a service of a system deviates from its specification;

Fault is the cause of the error;

Isochronous Uniform in time (having equal duration) and recurring at regular intervals. A form of data transmission that guarantees to provide a certain minimum data rate, as required for time dependent data such as video or audio. Isochronous transmission transmits asynchronous data over a synchronous data link so that individual characters are only separated by a integer number of bit-length intervals. This is in contrast to asynchronous transmission, in which the characters may be separated by arbitrary intervals, and with synchronous transmission.

Robust partitioning no failure in a function (or in hardware unique to a single function) can cause another function to fail. It refers to critical and non-critical functions sharing the same hardware.

Space partitioning protection of program, data and dedicated I/O and registers

Time partitioning protection of the processor and communications bandwidth assigned to a function

Transmission latency the duration starting with the sending trigger of a frame until the reception of the frame at a receiver; Also called end-to-end latency

Transmission jitter the maximum variation in the transmission latency;

References

[1] Interface standard for digital time division command/response multiplex data bus. Ministry of Defense, 1978.

[2] Mil-std-1553 evolves with the times. Data Device Corporation, 2010.

[3] K. A. LaBel, C. J. Marshall, P. W. Marshall, P. J. Luers, and R. A. Reed. On the suitability of fiber optic data links in the space radiation environment: a historical and scaling technology perspectivev. In *Aerospace Conference, 1998 IEEE*, volume 4, 1998.

[4] Robert Nixon. Fibre channel framing and signaling -3 (fc-fs-3). Project T11/1861-D Rev 0.90, 2009.

[5] G. Warden and B. Fleissner. Fibre channel testing for avionics applications. In *AUTOTESTCON 2004. Proceedings*, pages 583 – 589, 2004.

[6] Haowei Bai. Analysis of a sae as5643 mil-1394b based high-speed avionics network architecture for space and defense applications. In *Aerospace Conference, 2007 IEEE*, 2007.

[7] Hermann Kopetz, Astrit Ademaj, Petr Grillinger, and Klaus Steinhammer. The time-triggered ethernet (tte) design. In *8th IEEE International Symposium on Object-oriented Real-time distributed Computing (ISORC), Seattle, Washington*, 2005.

[8] D.A. Gwaltney and J.M. Briscoe. Comparison of communication architectures for spacecraft modular avionics systems. Technical Report NASA/TM—2006–214431, Marshall Space Flight Center, Marshall Space Flight Center, Alabama, 2006.

[9] D. Jameux W. Steiner, G. Bauer. Ethernet for space applications: Ttethernet. In *International SpaceWire Conference 2008*, 2008.

[10] H. Kopetz. Fault containment and error detection in the time-triggered architecture. In *The Sixth International Symposium on Autonomous Decentralized Systems*. ISADS, 2003.