SAFETY ISSUES IN AVIONICS AND AUTOMOTIVE DATABUSES

Janusz Zalewski [1], Dawid Trawczyński [2], Janusz Sosnowski [2], Andrew Kornecki [3], Marek Śnieżek [4]

[1] *Computer Science Department, Florida Gulf Coast University*
Fort Myers, FL 33928, USA, zalewski@fgcu.edu
[2] *Institute of Computer Science, Warsaw University of Technology*
Nowowiejska 15/19, 00-665 Warsaw, Poland, d.trawczynski@ii.pw.edu.pl jss@ii.pw.edu.pl
[3] *Dept. of Computer & Software Engineering, Embry-Riddle Aeronautical University*
*Daytona Beach, FL 32114, USA,*kornecka@erau.edu
[4] *Dept. of Control & Computer Engineering, Rzeszów University of Technology*
35-959 Rzeszów, Poland, sniezekm@prz.rzeszow.pl

Abstract: In avionics and automotive applications of computing, special care must be taken of issues related to safety. Assurance must be provided that computer hardware or software does not contribute to situations, which may cause loss of life or significant property damage. One aspect of this concern is the design of databuses, which provide a medium to exchange information among various electronics devices in a vehicle. Unfortunately, only a few aspects of bus design have been sufficiently covered in the research studying system safety. This paper reviews and compares available information on bus specifications. Databuses are discussed regarding their properties, such as signal characteristics and bus protocols, with respect to safety.

Keywords: Safety-Critical Systems, Databus, Avionics, CAN, TTP, FlexRay, IEEE-1394.

1. INTRODUCTION

In avionics and automotive applications of computing special care must be taken of issues related to safety. Assurance must be provided that computer hardware or software does not contribute to situations, which may cause loss of life or significant property damage. One aspect of this concern is the design of databuses, which provide communication medium to exchange information among various electronics devices controlling the vehicle. However, current recommendations, such as *Guide to Avionics Databuses* (1995) in the UK or *Principles of Avionics Data Buses* (1995) in the US, are a decade old and do not provide sufficient guidance on the design and usage of buses that take advantage of the latest technologies.

This paper reviews safety issues in relation to databus design and presents an overview of several databus technologies that are currently used in avionics and automotive applications.

2. SAFETY ASPECTS OF DATABUSES

Safety is a property of computer systems that relates to the operation of a computer in a certain physical environment. It is commonly assumed that safety can be evaluated only in the entire system, of which computer is a part. Computer hardware and software is not safe or unsafe by itself, unless it is used in certain application. Only then, one can assess how improper computer operation may inadvertently affect the external environment and potentially contribute to the loss of life, injuries, or large financial losses.

In principle, a computer or its software does not have to fail to contribute to the accident. Its operation may be perfectly well adhering to specifications, but the chain of unanticipated external events may cause the entire system (of which a computer is a part) to enter some unpredictable state, for which the computer was not designed. In this view, safety aspects of a databus have to be considered in the context of an overall risk evaluation process. This normally involves three separate aspects: hazard analysis, failure mode analysis, and safety assessment based on a set of specific criteria.

In this section, we review three above mentioned components of risk evaluation process and present some case studies, that could be used as baselines against which safety critical computer applications should be analyzed.

2.1 Aspects of Risk Analysis

Because of the risks involved in using computer equipment in safety critical applications, specific industries are highly regulated. For instance, in civil aviation in the US, several standards exist that

address various aspects of airborne system certification, both for software (DO-178B) and for hardware (DO-254). As a result, databuses with their hardware and software components need to be embedded into specific project and a specific vendor needs to provide appropriate data to make arguments for meeting the certification objectives.

Hazard analysis for complex automotive systems involving electronic communication devices (such as databuses) has been done recently by Debouk et el. (2003). They present a list of potential hazards that need to be taken into account at the beginning of safety analysis of X-by-wire systems, consisting of steer-by-wire, brake-by-wire, electronic throttle, and active safety systems. They divide associated risks according to critical, moderate and low consequences. Table 1 includes the hazards with highest associated risk and their possible controls.

Table 1. Hazard Analysis for an X-by-Wire System

Potential Hazard	Possible Mitigation
Loss of Power	Dual power system
Loss of Commun.	Dual communication system
Loss of Steering	Backup system Reduced functionality Steer by braking active safety system
Loss of Braking	Backup system Reduced functionality Brake by steering active safety system
Loss of Electronic Throttle	Backup system Reduced functionality
Loss of Actuators	Backup actuators Reduced performance actuator
Loss of Sensors	Backup sensors Reduced performance sensor

Chau et al. (2001) describe and discuss typical failure modes for a highly reliable bus architecture for space applications. Their study is related to the use of commercial-off-the-shelf products, such as those compliant with IEEE Std 1394 and SpaceWire, to be used in high availability avionics systems. They identified those failure modes that are fairly frequent or critical to the survival of the spacecraft. A summary of the discussion is presented in Table 2 below.

Table 2. Failure Modes for a Space Application

Failure Mode	Description
Invalid Messages	Messages sent across the bus contain invalid data
Non-Responsive	An anticipated response to a message does not occur or return in time
Babbling	Communication among nodes is blocked or interrupted by uncontrolled data stream
Conflict of Node Address	More than one node has the same identification

In addition to hazard analysis and failure mode analysis, multicriteria-based safety assessment is used in the risk assessment process in aviation and automotive industries for evaluating databuses. Rierson and Lewis (2003) provide a set of preliminary criteria to certify avionics databuses on civil aircraft. Their analysis, although not an official position of the FAA, is aimed at providing aircraft manufacturers with some initial data on the ways to approach the certification process, when developing, selecting, integrating or approving a databus technology in the context of a civil aircraft project. Some of the suggested criteria, divided into several categories, are listed in Table 3.

Table 3. Criteria for Avionics Databus Certification

Criterion	Selected Evaluation Factors
Safety	Availability and reliability, Partitioning, Failure detection, Common cause/mode failures, Bus expansion strategy, Redundancy management
Data Integrity	Maximum error rate, Error recovery, Load analysis Bus capacity, Security
Performance	Operating speed, Bandwidth, Schedulability of messages, Bus length and max. load, Retry capability, Data latency
Electromagnetic Compatibility	Switching speed, Wiring, Pulse rise and fall times, Lightning & radiation immunity
Design Assurance	Compliance with standards (such as DO-254 & DO-178B)
Configuration Management	Change control, compliance with standards, documentation, interface control, etc.
Continued Airworthiness	Physical degradation, in-service modifications and repairs, impact analysis, etc.

2.2 Automotive and Avionics Case Studies

The theoretical and engineering methodologies and tools, such as those described in previous section, have to be applied to practical cases before any credible safety assessment of a databus design can be made. Below, we briefly present two case studies taken from the available literature, to illustrate the level of complexity any safety analysis of the databus design has to deal with.

Waern (2003) studied a system for steer-by-wire application, as an example of X-by-wire system, illustrated in Fig. 1. All its individual components are connected electronically via a databus and include an array of sensors (steering wheel sensors, wheel angle sensors, environment sensors, etc.) and respective actuators (steering actuators, driver feedback actuators, etc.). All X-by-wire systems, where X stands for brake, steer, shift, throttle, etc., are extremely demanding, since their functions are extremely critical for safety.

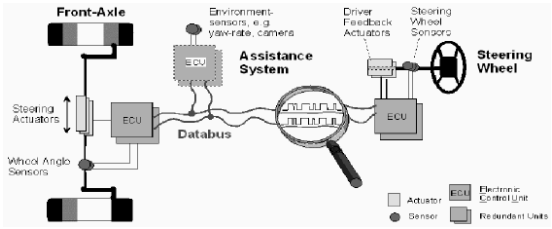

Fig. 1. Steer-by-Wire System (Waern 2003)

Similar case studies have been presented in the literature for aircraft. Yeh (1998) analyzes a flight control system, fly-by-wire, for controlling flying surfaces of Boeing 777 commercial aircraft (Fig. 2). Around a dozen of ARINC 629 buses glue together multiple systems consisting of sensors, transducers, actuators, alerts and warnings, electrical and hydraulic power control, information management system, interfaces and other digital electronics.

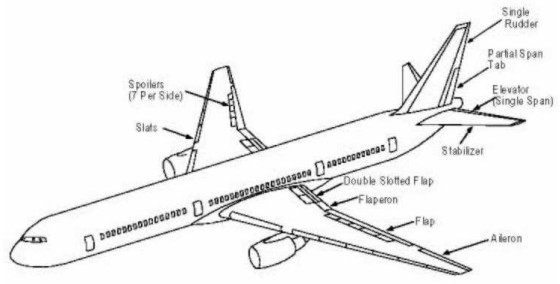

Fig. 2. Boeing 777 Flight Control Surfaces (Yeh 1998)

For this system, a comprehensive safety analysis was performed to assess all potential, significant failures of the fly-by-wire system, including single failures, latent failures, and failure combinations. In the analysis, system separation, partitioning and redundancy were addressed in particular,

3. DATABUS DESIGNS

Case studies presented above, as well as others described in the literature (steer-by-wire, Wilvert et al. 2003; safe-by-wire system, Boys 2004; car entertainment platform, Lessard 2003), give a broader context for studying databus design with respect to safety. There are essentially three types of applications that require the use of buses on vehicles:

- entertainment
- traditional, under the hood, and
- safety related.

For each of those categories different databus solutions have been proposed and developed. In this study, we concentrate on databuses designed for safety related applications, giving only a limited consideration to other kinds of buses.

Essential characteristics of databus description from the safety standpoint do not differ much from conventional bus specifications, which must include mechanical, electrical and logical elements of the bus design (Zalewski 1995):

- *mechanical* properties concern bus wiring, connectors, pinout, module design and dimensions,
- *electrical (or optical)* properties are related to signal levels and their dynamics to carry information, including electromagnetic characteristics, and
- *logical* properties concern the protocol of exchanging information over a bus.

Specifics of the bus protocol must include separate descriptions of the three phases of bus operation:

- bus arbitration (competing for bus access)
- data transfer, how devices exchange data once they obtain bus access, and
- fault handling (dealing with bus errors).

Bus protocols are typically described in terms of a layered approach, defining various aspects of bus operation according to the respective layers of the ISO/OSI Reference Model, especially Physical, Data Link and Application layers.

Some, but not all of these elements, have been included in databus comparisons published thus far in the literature. Our purpose in this paper is not so much to compare existing bus technologies, but to review them with respect to specific characteristics important for safety. In the following sections we are addressing the most important aspects of respective databus designs. Due to a limited space, we only focus on selected issues.

3.1 Traditional Avionics Databuses

This is the oldest category of databuses, well documented and researched, with a multitude of applications worldwide, on both military and civilian aircraft (Newport 1995).

ARINC 429 - general purpose avionics databus, the most used databus in commercial aviation:

- data rate: 1 Mb/s or 12-14.5 kb/s with 1% tolerance
- type: serial, unidirectional (two buses needed for bi-directional operation), point-to-point
- medium: two signal wires, wired transformer coupling
- bit encoding: Return-To-Zero bipolar, 10V, trilevel
- architecture: serial point-to-point one way protocol with only one transmitter on a wire pair and one to twenty receivers
- protocol: Williamsburg "bit oriented" and Numeric Data, Discrete Data, File Data
- frame length: 32 bit sequential words separated by at least four bit times of zero voltage (NULL) eliminating the need for a separate clock signal wire (self-clocking)
- frame format: typically includes five primary fields – one Parity bit, SSM, SDI, and 8-bit System Address Label, leaving 18-20 bits for payload data
- max. length or electrical load: 20 receivers
- fault tolerance features: only parity bit.

MIL-STD-1553B/1773 - Aircraft Internal Time-Division Command/Response Multiplex Data Bus, in use since 1973, widely applied in military avionic:

- data rate: 1 Mb/s (20 Mb/s for MIL-STD 1773)
- type: serial, bi-directional, self synchronized

- medium: twisted-shielded pairs of wires (a second path for bus traffic should one of the buses be damaged); fiber for MIL-STD-1773
- bit encoding: biphase Manchester II; logic one is transmitted as a positive pulse followed by a negative pulse; logic zero is a negative pulse followed by a positive pulse; serial digital pulse code modulation
- architecture: single master (bus controller), the only device that can initiate communication; three functional modes of terminals allowed on the data bus: the bus controller, the bus monitor, and the remote terminal (only one controller may be active at a time)
- protocol: serial digital multiplex data bus system shall function asynchronously in a command/response mode, and transmission occurs in a half-duplex manner
- frame length: 20 bits (16 bits command data and status, 3-bit sync, 1 bit parity)
- frame format: twenty 1.0-microsecond bit times allocated for each word (3 bit-time sync pattern, a 16-bit data field specified differently for each word type, and 1 parity check bit); three types of words: command, status, and data
- max. length or nodes: 32 (master + 31)
- fault tolerance features: (a) accuracy and long-term stability of +/- 0.1% (short-term stability is less than 0.01%); (b) nominal characteristic impedance of the cable (Z_0) within the range of 70.0 to 85.0 ohms at a sinusoidal frequency of 1.0 MHz; may be transformer coupled

ARINC 629 - upgrade and modification of 429, used only on 777:
- data rate: 2 Mb/s
- type: serial, bidirectional, distributed control, without the need for a bus controller (avoiding single-point failure mode)
- medium: two signal wires (twisted pair)
- bit encoding: Manchester II
- architecture: multi-master, autonomous terminal
- protocol: digital autonomous terminal access control (collision avoidance); Basic protocol and Combined protocol (for periodic and non-periodic traffic, with priority)
- frame length: 16 bits of data, 1 parity bit and 3 sync bits
- frame format: inherited from MIL-STD-1553
- max. load: up to 120 terminals
- fault tolerant features: (a) each terminal monitors its own transmissions; (b) non-intrusive, inductive coupling.

ARINC 659/SAFEBUS - Backplane Data Bus for Integrated Modular Avionics, developed by Honeywell, installed only on the Boeing 777:
- data rate: 60 Mb/s (with clock rate 30 MHz)
- type: serial unidirectional tightly coupled synchronous backplane bus
- medium: 2 data lines and one clock per bus (12 lines total on a backplane)
- bit encoding: uses backplane transceiver logic
- architecture: quad-redundant
- protocols: physical and data link layers; Table Driven Proportional Access for medium access
- frame length: 32 bits
- frame format: compatible with ARINC 629; Frame Description Language
- max length: up to 42 inches
- fault-tolerant features: fault detection, fault containment and redundancy.

3.2 FlexRay (Fuehrer 2003)

Designed for future generation high-speed control applications in vehicles, as a replacement of CAN, TTCAN, TTP/C:
- data rate: 10 Mb/s
- type: serial, bi-directional, half-duplex transmit
- medium: differential pair, 2-channel redundancy
- bit encoding: NRZ8N1 & Frame Start Sequence
- architecture: multi-master, fault tolerant, single/dual channel, bus/star or mixed topology; collision-free arbitration via unique ID and slot counting (during startup collisions may happen)
- protocol: time-triggered and event-triggered supported by static (TDMA) and dynamic slots
- frame length: 264 bytes
- frame format: 5B header, 254B data, 3B CRC
- max. length 24 m; max. nodes 22 (or 64???)
- fault tolerant features: (a) frame recognition with 11b frame ID; (b) error detection/data validation with 11b header CRC and 24b frame CRC; (c) clock synch: offset and rate correction (fault tolerance midpoint)
- bus highlights: two independent physical layer channels; recurring communication cycle in guaranteed time; static segment for polling and dynamic for temporal events.

3.3 CAN and TT-CAN (Leteinturier 2003)

World standard in automotive electronic control, wide component manufacturing and support bases; typical application involves 2-10 control units with soft real-time requirements:
- data rate: 10 kb/s to 1 Mb/s
- type: serial, bi-directional, multi-master
- medium: differential twisted pair, single wire, optical fiber
- bit encoding: NRZ with bit stuffing, 5V/50mA transceivers
- architecture: multi-master bus, bitwise priority arbitration, event-triggered with no clock synchronization, multicast transmission with message filtering
- protocol: Physical Layer + Data Link Layer (Logical Link Control + Media Access Control = Object + Transfer Layers)
- frame length: varies by frame type, for data 107-bit (max. 64 data bits, 11 bits address id, 15 bit CRC, 6 bit control field)
- frame types: data, remote, overload, error
- max length: 40 m for 1 Mb/s, 100 m for 500 kb/s, 200 m for 250 kb/s, 500 m for 125 kb/s, 6 km for 10 kb/s; max 2048 nodes theoretically for CAN 2.0A - average nodes: 2-10 nodes per network

- fault tolerant features: (a) frame recognition determined by polarity of the RTR bit, data and remote frames separated by interframe spacing; (b) error detection: stuff, bit timing, data, 15 bit CRC, format and message acknowledgement error detection
- bus highlights: immediate message retransmission, low message latency for small traffic loads, wide support network of manufactures and suppliers, highly tested.

TT-CAN - adds session layer on top of CAN, uses TDMA as medium access protocol, disables retransmission and provides global clock synchronization via master reference message, with 1-8B of data per frame. Bus highlights include: support for deterministic messages and fault handling, low jitter transmission, 25-35% typical data efficiency, error detection and redundancy management; improved bus utilization for higher traffic loads as compared to CAN.

3.4 TTP/C (Maier et al. 2002)

Designed for avionic flight control (Airbus) and automotive control (drive-by wire, steer-by wire, chassis and body control):
- data rate: 25 Mb/s over Ethernet, 5 Mb/s over optical fiber and twisted pair RS-485, 2 Mb/s over twisted pair ISO 11892-2
- bus type: serial, bi-directional, with bus-guardians
- medium: twisted pair, optical, Ethernet
- bit encoding: Modified Frequency Modulation
- architecture: time triggered (TTA) for fault tolerance, replica determinism, fail-silence, composability; topologies include active star, passive bus, combinations with bus guardians; three communication modes - startup, dowload, normal
- protocol: Physical Layer + Data Link Layer + Protocol Service Layer + FT-COM Layer; strict TDMA slotting by means of rounding, with ET traffic possible if scheduled statically
- frame length: 4-8 bit header, 240B total data length, 24-bit CRC
- frame types: I-frame (initial synchronization), N-frame (application data)
- bus length: depends on medium; max. nodes 64; average 4-32 nodes with high safety requirements
- fault tolerant features: (a) redundancy with two separate channels (duplicated nodes and buses); (b) error detection: 24 bit CRC, with clique detection for all asymmetric communication faults, different dividing polynomial seeds for dual channel operation; (c) distributed clock synchronization with offset correction in microseconds range; (d) frame recognition via Frame Type Identifier.
- bus highlights: fault tolerance, replica determinism, fail silence, error containment by bus guardian, guaranteed message latency and jitter, dual redundant TT messages, consistent membership and clique detection, high data efficiency 60-80%, effective long propagation delay handling; static scheduling implying safe bandwidth utilization through the MEDL data structure.

3.5 IEEE 1394/FireWire (Teener 1995)

Designed for high-speed entertainment applications:
- data rate: up to 400 Mb/s
- type: serial, asynchronous and isochronous
- medium: two shielded twisted pairs, two power conductors (entire cable shielded)
- bit encoding: IEEE Std 1569 LVDS (Low Level Differential Signaling)
- architecture: milti-master, daisy-chain or tree
- protocol: physical, link and transaction layer
- frame length: 16B for isochronous transmission
- frame (packet) format: ???
- max. nodes: 63 on a segment
- fault tolerant features: (a) data and header packet CRC; (b) timeout conditions; (c) error code in the acknowledgement and response packets; (d) enabling/disabling individual ports for reconfiguration; (e) isochronous transmission guaranteeing message delivery
- bus highlights: asynchronous transmission for reliable message delivery; multicast isochronous transmission; tree topology.

3.6 Safe-by-Wire (Boys 2004)

Application in automotive passenger restraint system for deployable devices and for sensors:
- data rate: variable between 20..200 kb/s
- type: serial, bi-directional with integrated power distribution
- medium: unshielded differential pair
- bit encoding/signaling: three data levels (0, 3, and 6 V) and power level (11/30 V)
- architecture: master-slave (multi-master optional); bus, tree, ring, or mixed topology; fast polling with interrupt possibilities, asymmetrical or symmetrical daisy-chain configuration (shut-down individual bus sections)
- protocol: physical, data link & application layer
- frame length: 30 bits including command, addresses, data, CRC, and one error bit
- frame format: 4b command, 6b address
- max. length 25-40m; max. nodes: 64 (3 reserve)
- fault tolerance features: (a) shorts of bus wire, open circuits, and shorts between the bus wires; (b) immunity to “babbling idiots”; (c) multilevel protection against inadvertent deployment; (d) CRC and bit error data validation
- bus highlights: sensor can interrupt current message for exclusive communication of time-critical data; switches in the slaves can split bus into sections; recovery from short made by software and hardware; special D-frame to collect one-bit data from several slaves (30 bits only); latency time for interrupts from smart sensors: 2 bit times at low speed + 1 bit time at high speed ($\cong$ 105 μs).

3.7 Others

There is a multitude of other databuses used in avionics and automotive applications, but due to a limited space it is impossible to describe them all. Only some of them can be mentioned here:

- ROBUS (Reliable Optical BUS) is a fault tolerant bus being developed at NASA as a part of a SPIDER project for high-reliability space missions (Miner et al. 2002)
- SpaceWire is a serial, point-to-point, full-duplex bus based on IEEE Std 1355, modified for space applications, with minimum data rate of 2 Mb/s (no maximum), and predetermined jitter (Chau et al. 2001)
- Byteflight has been designed by BMW to support both event and time driven messaging in passive safety systems; it has been essentially incorporated into FlexRay's dynamic protocol segment (Homer 2002)
- Bluetooth and its derivative, ZigBee, are wireless short-range (< 100 m) networks that may play an important role in the future, because of their natural built-in ability of quick reconfiguration (Trawczynski 2005).

4. CONCLUSION

There is no single databus that could be selected as the best for safety related applications. When a decision is to be made, which bus to use, safety related factors have to be considered involving hazard analysis and failure mode analysis to estimate risks for a specific bus design.

Buses and protocols like FlexRay, TTP/C etc., that have been designed specifically to provide high level of fault tolerance may become the best solution but at higher cost. Therefore a tradeoff analysis has to be also done. Further work is ongoing on a more detailed bus comparison by using simulation and fault injection.

REFERENCES

Boys R. (2004). Safe-by-Wire: The Leading Edge in Vehicle Airbag Control, *In-Vehicle networks and software, electrical wiring harnesses, and electronics and systems reliability*, SP-1852, Society for Automotive Engineers, Warrendale, Penn., Paper No. 2004-01-0205

Chau S.N. et al. (2001). *A Design-Diversity Based Fault-Tolerant COTS Avionics Bus Network*, Proc. 8th Pacific Rim Int'l Symp. On Distributed Computing, IEEE CS Press, Los Alamitos, Calif., pp. 35-42

Debouk R., T. Fuhrman, J. Wysocki (2003). Architecture of By-Wire Systems: Design Elements and Comparative Methodology. *In-Vehicle Networks, Safety Critical Systems, Accelerated Testing, Reliability*, SP-1783, Society for Automotive Engineers, Warrendale, Penn., pp. 171-182

Fuehrer T. et al. (2003). FlexRay – The Communication System for Future Control Systems in Vehicles, *In-Vehicle Networks, Safety Critical Systems, Accelerated Testing, Reliability*, SP-1783, Society for Automotive Engineers, Warrendale, Penn., pp. 35-41

Homer M. (2002). Handling Event Driven Messaging in Distributed Flight Critical Systems, *Proc. DASC'02, 21st Digital Avionics Systems Conf.*, Irvine, Calif., October 27-31, 2002, Vol. 2, pp. 13.C.4-1/6

Lessard M. (2003). *IDB-1304 Automotive Reference Platform – Enabling In-vehicle Entertainment*, Mindready Solutions, Research Triangle Park, NC

Leteinturier P., N.A. Kelling, U. Kelling (2003). TTCAN from Applications to Products in Automotive Systems, *In-Vehicle Networks, Safety Critical Systems, Accelerated Testing, Reliability*, SP-1783, Society for Automotive Engineers, Warrendale, Penn., pp. 75-84

Maier R. et al. (2002). Time-Triggered Architecture: A Consistent Computing Platform, *IEEE Micro*, Vol. 22, No. 4, pp. 2-11

Miner P.S., M. Malekpour, W. Torres (2002). A Conceptual Design for a Reliable Optical Bus, *Proc. DASC'02, 21st Digital Avionics Systems Conf.*, Irvine, Calif., October 27-31, 2002, Vol. 2, pp. 13D3-1/11

Newport J. (1995). *Avionic System Design.* CRC Press, Boca Raton, Fla.

Rierson L., J. Lewis (2003). Criteria for Certifying Databuses on Civil Aircraft, *Proc. DASC'03, 22nd Digital Avionics Systems Conference*, Indianapolis, Ind., October 12-16, 2003, Vol. 1, pp. 1.A.2-1/9

Teener M. (1995), A Bus on a Diet: The Serial Bus Alternative: An Introduction to the P1394 High Perf-ormance Serial Bus. In (Zalewski 1995), pp. 180-194

Trawczynski D., J. Sosnowski, J. Zalewski (2005). A Study of Routing for the Bluetooth Scatternet, *Proc. PDS2004 IFAC Workshop on Programmable Devices and Systems*, Krakow, Poland, November 18-19, 2004, pp. 473-478

Waern M. (2003). *Real-Time Communication: Evaluation of Protocols for Automotive Systems*, Master Thesis, Royal Institute of Technology, Stockholm, Sweden

Wilvert C. et al. (2003). Evaluating Quality of Service and Behavioral Reliability of Steer-by-Wire Systems, *Proc. ETFA 2003 IEEE Conf. on Emerging Technologies and Factory Automation*, Lisbon, Portugal, Sept. 16-19, 2003, pp. 193-200

Yeh Y.C. (1998), Design Considerations in Boeing 777 Fly-By-Wire Computers, *Proc. Third IEEE Int'l High-Assurance Systems Engineering Symp*. Washington, DC, November 13-14, 1998, pp. 64-72

Zalewski J., ed. (1995). *Advanced Multi-microprocessor Bus Architectures*, IEEE CS Press, Los Alamitos, Calif.