Avionics databus safety criteria and certification

Andrew Kornecki
Embry-Riddle Aeronautical University, Daytona Beach, FL 32114, USA
kornecka@erau.edu

Janusz Zalewski
Florida Gulf Coast University, Fort Myers, FL 33965, USA
zalewski@fgcu.edu

ABSTRACT: The paper considers databuses used in avionics and automotive applications (ARINC 629, ARINC 429, FlexRay, CAN, TTP, SAFEbus, SpaceWire, FireWire and others) and identifies the criteria to evaluate them with respect to safety. The criteria address comprehensive aspects of databus assessment problem, combining mechanical (bus wiring, connectors, pinout, module design and dimensions, etc.), electrical (signal levels, their dynamics to carry information, electromagnetic compatibility, etc.), and logical characteristics, including the protocol of exchanging information between devices over a bus, in all three phases: bus arbitration, data transfer and fault handling. A systematic list of safety-related attributes and their relationships for evaluation of aviation databuses is presented, which would allow building the uniform evaluation criteria for certification purposes. Preliminary simulations and real experiments are aimed at protocol comparison, according to the methodology previously developed by the authors. The study is intended to allow establishing standard and objective criteria for evaluating databus technologies in safety-critical applications.

1 INTRODUCTION

The concern for safety in avionics and automotive applications means that assurance must be provided that computer hardware or software does not contribute to situations, which may cause loss of life, injuries or significant property damage. One aspect of this concern is the design and use of computer buses, called databuses, which provide communication to exchange information among various electronics devices on vehicle. This issue is especially important in a view of certification, when regulatory authorities require vendors to make their products compliant with certain sets of criteria to assure safety.

The authors studied this subject in relation to software tools used in the development of real-time safety-critical applications (Kornecki and Zalewski, 2003). A set of consistent criteria was developed, based on existing software engineering standards related to tool use, that help certification authorities to make respective decisions on compliance. In case of databuses, the process, although essential for modern aircraft, has not been started yet, due to the lack of appropriate, agreed upon, criteria.

The objective of this paper is to present an approach to the databus assessment with respect to safety. First, in Section 2, we discuss three basic aspects of this problem: developing the criteria, hazard analysis and failure mode analysis. Then, in Section 3, we present briefly two case studies taken from literature, one in avionics and one in an automotive application, for which databus design plays an essential role in achieving safety. On this basis, we discuss certification concerns in Section 4, and characterize certain bus designs from the point of view of potential certification, in Section 5. In Section 6, we address evaluation data collection for selected buses, which is followed by conclusion in Section 7.

2 FUNDAMENTAL ASPECTS OF DESIGNING DATABUS FOR SAFETY

Safety is a property of computer systems that relates to the operation of a computer in a certain physical environment. In principle, a computer or its software does not have to fail to contribute to the violation of safety and cause an 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, it is not sufficient to focus only on reliability of computer hardware or software (and that of databus, in particular) to assess its suitability for a safety critical application.

The authors recently conducted a general study on the criteria one can use to evaluate software tools for the development of real-time safety-critical systems, from the viewpoint of prospective qualifica-

tion (Kornecki and Zalewski 2003 and 2004). The study indicated that the selection of the criteria and formulation of respective metrics to assess them has to be a part of the broader effort involving risk assessment with both hazard and failure mode analyses for a specific application.

The same conclusion can be applied to the design and use of databuses in safety critical systems. All three aspects of the risk assessment process: multicriteria-based safety assessment, hazard analysis and failure mode analysis, are briefly reviewed below for avionics and automotive applications.

2.1 *Safety Assessment of Avionics Databuses*

Table 1. Criteria for Avionics Databus Certification.

Criterion	Selected Evaluation Factors
Safety	Availability and reliability Partitioning Failure detection Common cause/mode failures Reconfigurability Bus expansion strategy Redundancy management
Data Integrity	Maximum error rate Error recovery Load analysis Bus capacity Security
Performance	Operating speed Schedulability of messages System interoperability Bus length and max. load Retry capability Bandwidth Data latency Transmission overheads
Electromagnetic Compatibility	Switching speed Pulse rise and fall times Wiring Shielding effectiveness Lightning & radiation immunity
Design Assurance	Compliance with standards (such as DO-254 & DO-178B)
Verification and Validation	Examples: functionality testing, system system testing, other forms of testing, failure management, degraded mode operation, etc.
Configuration Management	Examples: change control, compliance with standards, documentation, interface control, system analysis, etc.
Continued Airworthiness	Lifetime issues, such as physical degradation, in-service modifications and repairs, impact analysis, etc.

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 certification authorities, 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. The suggested criteria are divided into several categories listed in Table 1.

2.2 *Hazard Analysis for Automotive Electronics*

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 2 includes the hazards with highest associated risk (critical) and their possible controls.

Table 2. Preliminary Hazard Analysis for X-by-Wire Systems.

Potential Hazard	Possible Mitigation
Loss of Power	Dual power system (including battery, wires and connectors)
Loss of Communication	Dual communication system
Loss of Steering	Backup system Reduced functionality redundant system Steer by braking active safety system
Loss of Braking	Backup system Reduced functionality redundant system Brake by steering active safety system
Loss of Electronic Throttle	Backup system Reduced functionality redundant system
Loss of Actuators	Backup actuators Reduced performance actuators
Loss of Sensors (recording driver commands)	Backup sensors Reduced performance sensors

2.3 *Failure Mode Analysis for a Space Application*

Chau et al. (1999, 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 3.

Table 3. Failure Modes Typical for a Space Application.

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

3 AVIONICS/AUTOMOTIVE APPLICATIONS

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 selected case studies taken from the available literature, to illustrate the level of complexity any safety analysis of the databus design has to deal with.

3.1 *Avionics Case Study*

Johansson et al. (2003) analyze a flight control system, fly-by-wire, for controlling flying surfaces of a Swedish JAS 39 Gripen combat aircraft, illustrated in Figure 1. The databus runs along the aircraft connecting actuators and sensors at each surface.

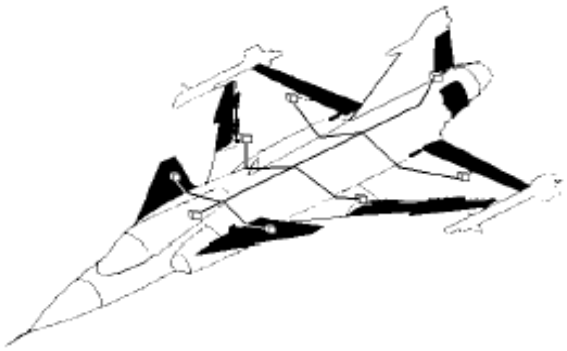

Figure 1. Distributed Flight Control System for JAS 39 Gripen Aircraft (Johansson 2003).

They provide communication bandwidth analysis for these primary control surfaces and engine, as well as for four secondary control surfaces and a variety of sensors, including:

- advanced air data sensors (static pressure, Mach number, altitude, angle of attack, angle of sideslip)
- angular gyro sensors (pitch, roll and yaw)
- acceleration sensors in z and y axles
- cockpit sensors (pilot commands for pitch, roll and pedal), and
- all of the above duplicated.

3.2 *Automotive case study*

Leen and Heffernan (2002) present a more extended application of three databuses coexisting in a single vehicle (Figure 2).

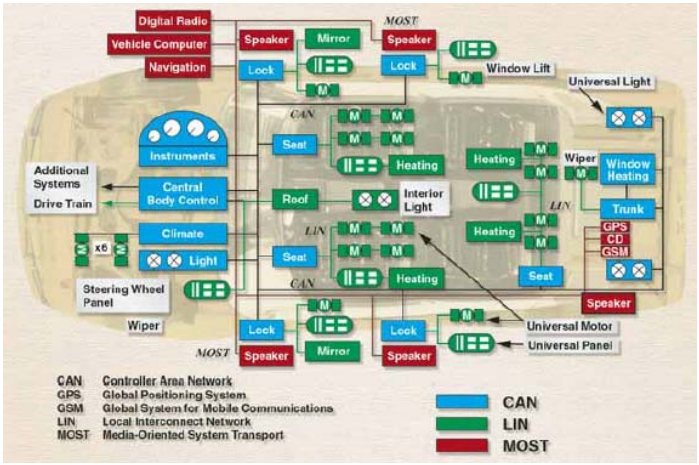

Figure 2. An Example of Modern Vehicle Network (Leen 2002).

Various databuses connect subsystems of various levels of complexity and relation to safety. The high speed MOST (Message Oriented Systems Transport) fiber optics bus connects a variety of entertainment and communication devices. LIN (Local Communication Network) bus, based on a master-slave principle, is used for handling low speed on-off devices, such as seats, door locks, sunroofs, windows, rain sensors, door mirrors, etc. CAN (Controller Area Network) bus is used to connect devices performing more sophisticated functions, such as data communication and control between the instrument cluster, body and climate controllers. On top of it, X-by-wire functions can be connected by a fourth type of bus.

4 CERTIFICATION CONCERNS

To improve the airborne systems, avionics manufacturers consider faster and lighter databuses available on the market. However, in this highly regulated industry, the critical point is to assure the equipment safety. The rigorous certification process following the guidelines of RTCA/DO-178B (1992), for software, and RTCA/DO254 (2000), for hardware, is the base for acceptance of any new or modified computing systems in the aircraft.

RTCA document DO-178B was developed by the avionics industry to establish software considerations for developers, installers, and users, when aircraft equipment design is implemented using software controlled computing devices. RTCA/DO-254 is an evolving industry specification to apply the same rigor as RTCA/DO-178B does for software to

airborne hardware environments. DO-254 was developed by the avionics industry to establish hardware deployment guidelines for developers, installers, and users, when microcomputer hardware, including FPGAs, PLDs and ASICs, are deployed in aircraft equipment designs.

DO254 defines three basic categories of lifecycle processes: planning, development, and CCC (correctness, confidence and control). It also defines the required documents to be produced by an applicant. They include: Plan for Aspects of Certification, Development Process, Verification and Validation Process, Process Assurance, Configuration Management, Status Reporting, Requirements Standards, Coding Standards, and a few others.

DO-178B and DO-254 constitute guidelines for the design/development assurance. For validation and testing there is a need to conform to environmental qualification, as per RTCA/DO-160D (1997), and need for rigorous and complete testing of variety of failure recovery situations. The system safety considerations, due to lack of well-established metrics, are most difficult to evaluate. Two automotive industry standards, SAE ARP 4754 (1996) and SAE ARP 4761 (1996), give additional guidelines to the system safety considerations.

Recognizing that it is critical to establish specific measurable criteria to help in assessment of the databuses, the initial selection of the criteria has been proposed in the CAST Position Paper #16 (2003). The major issues to consider when assessing the bus operation include safety, data integrity, performance, design/development assurance, and validation/testing approaches. Data integrity and performance can be demonstrated by specific array of tests. In the process, the allowed error rate per byte should be defined and means to recover from the errors should be provided. The load analysis and related bus capacity should be also specified. The extreme cases of bus loss, shortening, and opening should be considered in the analyses and tests.

The applicant and certification authority must assure that the evaluation criteria, similar to those listed, are considered. Each specific databus may have details that need to be addressed by a particular method discussed in advance between the applicant and the appropriate certification authority.

Historically, two types of buses, ARINC 429 and 629, have been used in most commercial aircraft. They may not be adequate for the future avionics applications due to the limited speed and bandwidth. Therefore, a number of new databuses currently are being considered. For large transport aircraft, switched Ethernet seems to be the major contender. For general aviation aircraft (business jets and smaller aircraft) a number of different communication technologies are being developed. Some of them include: CAN, ByteFlight, TTP/C, SAFEbus, and others. We consider them in the next section.

5 SELECTED DATABUS DESIGNS

Databus applications and case studies, such as those described in Section 3, as well as others presented in the literature (steer-by-wire, Waern 2003, Wilvert et al. 2003; safe-by-wire system, Boys 2004; car entertainment platform, Lessard 2003), give a broader context for developing databus evaluation criteria with respect to safety. 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 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.

In the following Table 4, we review selected databus characteristics important to safety, addressing the low-level aspects of respective databus designs. Due to a limited space, we only focus on selected issues, leaving out protocol characteristics.

Table 4. Selected Databus Characteristics.

Databus	Type	Archit.	Medium	Rate	Encod.
Arinc 429	serial unidir	single master	2 wires	100kb/s	RTZ bipolar
MIL1553	serial bi-dir.	single master	twisted pairs	1 Mb/s	2phase Manch
Arinc 629	serial bi-dir.	multi-master	twisted pairs	2 Mb/s	Manch ester II
Arinc 659	serial bi-dir.	quad redun.	twisted pairs	30MHz	2phase Manch
FlexRay	serial bi-dir.	fault toler.	optical or wire	10Mb/s	undef.
CAN	serial bi-dir.	multi-master	twisted pairs	1 Mb/s	NRZ + bitstuff
TTP/C	serial bi-dir.	double redun.	twisted pairs	25Mb/s	MFM
IEEE1394	serial	daisy or tree	twisted pairs	400Mb/s	LVDS
Safe-Wire	serial bi-dir.	master-slave	twisted pairs	200 kb/s	3-level
Space-Wire	serial bi-dir.	master-slave	2 wires	Min. 2Mb/s	undef.

6 EXPERIMENTAL DATA COLLECTION

Assuming that the criteria for bus evaluation and certification have been developed, the process still going on and far from completion, one wants to see how would respective buses meet certain requirements that are put on them with safety in mind. To shed some light or bus performance, we conducted two series of experiments: one was plain simulation for well developed databus networked configurations, and another relied on actual data transfer experiments with a modern bus.

6.1 *VMEbus Experiments*

One set of experiments was to conduct simulations designed for a bus well known to the authors from a multitude of industrial applications, VMEbus. Although VMEbus is not currently considered suitable for avionics or automotive applications, we intended to use it as a vehicle for creating a benchmark application for subsequent databus protocol comparisons.

When safety is of major concern in databus design, one wants to have a good hold on databus performance under heavy load conditions. With this in mind, several experiments were designed to understand the behavior of a VMEbus based server under high utilization, and to compare its performance with a circuit-switched interconnect (RACEway) immersed in a bigger network of multiple nodes.

Sample results from a bigger study (Jonnalagadda et al. 2003) are shown in Figure 3. A VMEbus server hooked to an FDDI network shows a significant degradation of performance (measured as access delay) with higher load (channel utilization). Its performance pattern is typical to any other configuration of interconnects, as shown by the shape of respective curves, and demonstrates significant improvement of behavior if newer bus architecture is used (RACEway). In a view of this research the experiments verify the suitability of conducting access delay vs. bus load simulations for determining databus response of specific bus designs.

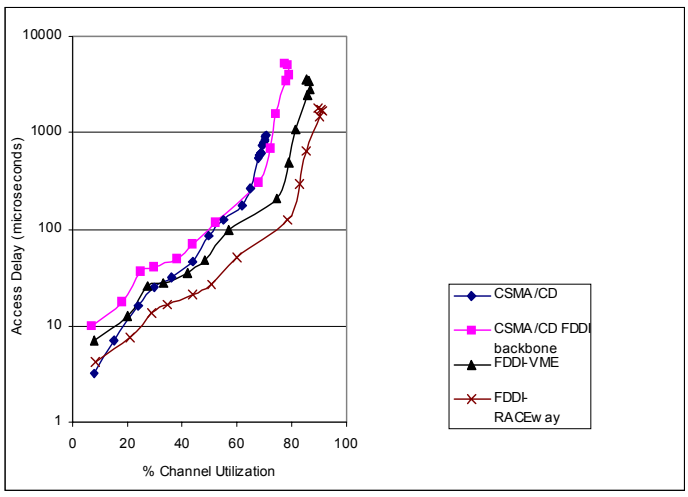

Figure 3. Server Access Delay for 64-byte Packets.

6.2 *IEEE Std 1394 – FireWire Experiments*

Another set of experiments was aimed at conducting actual measurements of data transfers over the bus to see the effect of internal databus properties, such as protocol variations, packet/block size, dependence on software driver properties, etc. Of modern databuses available to the authors, IEEE Std. 1394 (1995), known as FireWire bus, was selected, because of its diversity of configurations that can be experimentally set up and rearranged at the convenience of experimenters.

As a part of a bigger study (Williamsson et al. 2004), we focused on investigating the limits of data transfer speed for two distinctive transmission modes of IEEE Std 1394 databuses: asynchronous and isochronous transmission. An isochronous transmission mode provides reserved bandwidth for real-time data, every 625 microseconds, which is highly relevant for safety-critical applications, because of the message delivery guarantees.

The results of experiments, conducted for PCILynx boards under Linux and a variety of different device drivers, confirmed the superiority of isochronous transmissions over the traditional asynchronous mode, as shown in Figure 4. But at the same time, the experiments revealed significant degradation in the maximum data transfer rate achievable in practice, versus the theoretical one (163 Mb/s as opposed to theoretical 400 Mb/s for IEEE Std 1394 databuses in isochronous transmission mode).

In a view of this research, the experiments proved the necessity of conducting practical measurements of data transfer rates, and other databus parameters, to verify vendor's claims and compliance with standard's specifications. When facing a decision on selecting a specific databus for safety-critical applications, performance data are of high significance with respect to making the right choice. They are also crucial in finding how widely various databus designs differ in meeting application requirements.

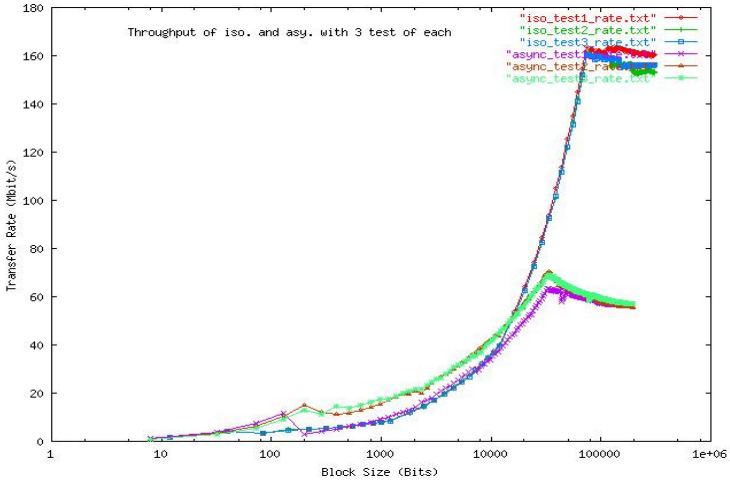

Figure 4. IEEE 1394 Throughput over a Raw Driver for Asynchronous and Isochronous Transmission Modes.

7 CONCLUSION

Because of the risks involved in using computer equipment and software in safety-critical applications, specific industries, such as civil aviation or automotive industries, are highly regulated. As a result, databuses with their hardware and software components need to be certified for use in these critical applications. Therefore an urgent need exists to develop a consistent set of criteria for databus evaluation that can be used by certification authorities and applicants to assess respective bus designs.

In this paper, we described an approach than can be used as a starting point to develop a comprehensive set of criteria and corresponding measurement procedures for databus evaluation. It has to be a part of the overall risk assessment process for a safety-critical application, and include a databus component as an important part of computer hardware and software design. Corresponding hazard analysis and failure mode analysis should be accompanied by the evaluation of safety criteria for a specific application and the databus under consideration.

Specific results of this study include the determination to what extent simulations and experimental data collection can be useful in databus evaluation for safety-related purposes. Simulation experiments, conducted for a variety of bus configurations with network interconnects, confirmed the usefulness of access delay vs. bus load simulations to determine databus response of specific bus designs. On the other hand, practical experiments, conducted for various configurations of IEEE Std 1394/FireWire databus, proved the validity of measuring data transfer rates, and other databus parameters, to verify vendor's claims and compliance with standard's specifications.

When facing a decision on selecting a specific databus for safety-critical applications, performance data, whether obtained via simulation or via practical measurements, are of high significance with respect to making the right choices. They are also crucial in finding how widely various databus designs differ in meeting specific application's requirements.

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. Paper No. 2004-01-0205. Warrendale, PA: Society for Automotive Engineers

CAST Position Paper CAST-16. 2003. *Databus Evaluation Criteria*, URL: http://www.faa.gov/certification/aircraft/avinfo/software/CAST/cast-16.rtf

Chau S.N. et al. 1999. Design of a Fault-Tolerant COTS-Based Bus Architecture, *IEEE Trans. Reliability* 48(4): 351-359.

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*: 35-42. Los Alamitos, Calif: IEEE Computer Society Press.

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. 171-182. Warrendale, PA: Society for Automotive Engineers

IEEE Std 1394. 1995. *High Performance Serial Bus*. New York: IEEE

Johansson R. et al. 2003. On Communication Requirements for Control-by-Wire Applications, *Proc. 21st Int'l System Safety Conference*: 1123-1132. Unionville, VA: System Safety Society

Jonnalagadda V., M. Mathure, A. Kornecki, J. Zalewski, 2003. Considering Local Bus Traffic in Network Performance Simulations, *Proc. CNDS'03 Communication Networks and Distributed Systems Modeling and Simulation Conference*: 109-114. San Diego, Calif.: Society for Modeling and Simulation

Kornecki A., J. Zalewski. 2003. Design Tool Assessment for Safety Critical Software Development, *Proc. 28th NASA/IEEE Software Engineering Workshop*, Greenbelt, MD: 105-113. Los Alamitos, Calif: IEEE Computer Society Press.

Kornecki A., J. Zalewski. 2004. Criteria for Software Tools Evaluation in Safety Critical Real-Time Systems, *Proc. PSAM-7/ESREL'04 Int'l Conf. on Probabilistic Safety Assessment and Management*, Berlin, Germany, June 14-18, 2004

Leen G., D. Heffernan 2002. Expanding Automotive Electronic Systems, *IEEE Computer* 35(1): 88-93

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

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

RTCA/DO-160D. 1997. *Environmental Conditions and Test Procedures for Airborne Equipment*, Washington, DC: RTCA Inc.

RTCA/DO-178B. 1992. *Software Considerations in Airborne Systems and Equipment Certification*. Washington, DC: RTCA Inc.

RTCA/DO-254. 2000. *Design Assurance Guidance for Airborne Electronic Hardware.* Washington, DC: RTCA Inc.

SAE ARP 4754. 1996. *Certification Considerations for Highly-Integrated or Complex Aircraft Systems*. Warrendale, PA: Society of Automotive Engineers.

SAE ARP 4761. 1996. *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*. Warrendale, PA: Society of Automotive Engineers.

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

Williamsson C., D. Williamsson, J. Zalewski. 2004. A Study of Cluster Computing over IEEE 1394, *Proc. SAWAMAS-2004, 2nd Swedish-Amrican Workshop on Modeling and Simulation*: 209-217. Orlando, FL: University of Central Florida

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*, 193-200. Lisbon, Portugal.

Zalewski J., ed. 1995. *Advanced Multimicroprocessor Bus Architectures*, Los Alamitos, Calif.: IEEE Computer Society Press.