Dependability aspects of automotive x-by-wire technologies

Luigi Coppolino[2], Maurizio Di Meglio[3], Nicola Mazzocca[1], Enrico Raffone[1]

[1]Università degli studi di Napoli Federico II, Via Claudio 21 – 80125 Napoli -ITALY
[2]Università degli studi di Napoli Parthenope, Centro Direzionale di Napoli – 80143 Napoli - ITALY
[3]STMicroelectronics Srl - Automotive Product Group - Via Remo De Feo 1– 80022 Arzano (NA) - ITALY
E-mail: nicola.mazzocca@unina.it, luigi.coppolino@uniparthenope.it,
maurizio.di-meglio@st.com, enrico.raffone@raen.it

Abstract:
In the past electronics in automotive was mainly for entertainment and utility applications, today it is going to access safety related functions like in the case of x-by-wire systems. This means that together with technology related issues, practitioners of the fields need to face with safety, time-to-market and cost related requirements. Nevertheless the absence of automotive related standards and best practices has led to plenty of solutions for technologies and specifications. This paper aims at clarifying the state-of-the art in the field of drive-by-wire related applications, identifying areas where electronics is being, where it might be used and what technologies are employed to facilitate the digital experience in automotive industry. At the end of the paper the implementation of a board suitable to develop dependable full by-wire systems is presented. Such board is the first step toward the development of a dependable full brake by-wire system as planned at the STMicroelectronics Automotive Product Group.

INTRODUCTION

By-wire systems are already employed in other domains such as train, airplane and naval fields [1]. In those domains x-by-wire systems have exploited benefits deriving from the replacement of the traditional mechanical-hydraulic devices by electric ones. The need for suitable design criteria with adequate levels of fault tolerance and redundancy, causes a high startup cost which has been justified in markets characterized by noteworthy investments of big private or public societies, while made by-wire not effective in highly cost-sensitive markets like automotive. Nowadays, however, the reduced costs of technologies and the possibility of new business opportunities have determined a distinct scenario characterized by a slow but progressive introduction of by-wire systems in automotive so that in the last years all car makers have turned their interests on research programs about full by-wire applications.
Unfortunately the lack of reference standards for the specific application field has led to the development of a number of proprietary solutions each with its own pros and cons. In literature few attempts to put order in such a mess [2][3] do exist, anyway they are either outdated or limited to technical details of some specific subsystems [6]. Since at the STMicroelectronics working group on automotive technologies is planning the development of a dependable full x-by-wire system, it was necessary the analysis of available technologies from the point of view of their dependability features and this paper tries to report the results of such technologies comparison. While leading our analysis we have focused our attention on a brake-by-wire system, evaluating existing technologies from the point of view of an engineer aiming at developing such a system. At the end of the paper we propose the implementation of a board suitable to develop dependable full brake by-wire systems.

THE REFERENCE SYSTEM

By-wire systems are conceived to replace traditional automotive means as throttle, steer or brake. In this section we try to identify the main subsystems involved in a by-wire system. To focus the attention on a concrete case study without loss of generality, we will refer to a full brake-by-wire. In such a context the main changes relate the transmission linkages substituted by a communication network, and the mechanical actuators substituted by the electric ones. Each actuator, located next to the relative mechanical part (e.g. the brake caliper), is based on a brushless motor and a mechanical transmission. An Electronic Control Unit (ECU) follows predefined strategies to pilot its closest actuator in compliance with the driver's inputs, environmental conditions and the current state of the vehicle. The ECU related to the pedal board transduces brake pedal commands and regulates the feedback on the pedal according to the braking actions and the vehicle current state. At the heart of the system there is the communication network. Since desired characteristics for the communication subsystem will include determinism, fault-tolerance, and reliable messaging, a time-triggered communication is the most natural choice as discussed in next section.

COMMUNICATION SUBSYSTEM

A real-time communication system for automotive x-by-wire applications needs to meet requirements that

exceed usual constraints for communication systems. In automotive such requirements are classified by the SAE (Society of Automotive Engineers) as Class C or D (see Tab. 1), and imply regularity of information transfer and minimized latency jitter or ideally a constant latency. Such requirements can be met by assuring a fail-operational behavior for the communication subsystem. The continuity of the communication service in case of fault is assured by active redundancy. The communication subsystem must be tolerant to electromagnetic interference and the mean time to recover from a "blackout" should exhibit minimal latency. For error detection a consensus on operational nodes and functions, i.e. a membership agreement, is necessary, both at a node level and possibly at the level of control functions. It is important that exits from that membership are detected unanimously and timely by all the remaining participants. The communication protocol should support a proper scheme to guarantee both atomic broadcast and message reception acknowledgement. In a hard real-time environment the network implementation must guarantee, that the worst case execution time of the server is smaller than the maximum response time that is expected by the client.

Table. 1: SAE networks classification

Class A	Low Speed (<10K bits/second) Convenience features (entertainment, audio, trip computer, etc.)
Class B	Medium Speed (10K b/s to 125K b/s) General information transfer (instrument cluster, vehicle speed, legislated emissions data, etc.)
Class C	High Speed (125K b/s to 1Mb/s) Real-time control (powertrain control, vehicle dynamics, x-by-wire, etc.)
Class D	Very High Speed (greater then 1Mb/s) Multimedia and safety-critical applications (Internet, digital TV, x-by-wire, etc.)

The communication system must assure that the contents of the messages are not mutilated and that faults that are specified in the fault hypothesis are properly handled [3].

All these requirements are satisfied by time-triggered communication paradigms, where activities are driven by the progress of time. Further, multi-access protocols based on TDMA provide deterministic access to the medium and thus bounded response times. Hence, the static planning of transmission can be used as the base for detecting the failure of the stations.

Such characteristics let prefer time triggered protocols, and especially TDMA protocols, to event triggered ones (where activities are driven by predefined events) when dealing with x-by-wire applications.

Mainly, there are three TDMA based networks that are candidates for supporting x-by-wire applications, namely: TTP/C from University of Vienna, FlexRay from a consortium of foremost manufacturers and TTCAN from Bosch, that reuses the most important automotive event-triggered protocol hardware, CAN hardware [4].

At the time of writing, FlexRay, which leans on the world's automotive industry, seems to be in a very strong position for becoming the standard in the industry, but from our point of view the focus of this paper is on technologies, that today can be used to make a concrete by-wire system.

Time-Triggered Protocol (TTP/C)

TTP/C protocol is the core of TTA Architecture, that has been designed and extensively studied at the Vienna University of Technology in Austria. Hardware implementations and their related software tools are available and commercialized from many years. TTP/C is the most complete time-triggered protocol at this time and it is already successfully used in aerospace applications. It implements typical dependability related service as bus guardian, a component that prevents a node from transmitting outside its static specification as wrong time or larger frame; membership service, an algorithm that allows to know the set of stations that are properly functioning; support for mode changes, that allows to manage the system in every functioning type.

Concerning the physical layer, the transmission is on redundant channels and each channel transports its own copy of the same message, this is important for EMI problems that might affect the single channel. TTP/C supports both a bus topology and a star topology. In the last version of the protocol the bus guardian is integrated into central star couplers; to avoid the single point of failure the star topology should be doubled. TTP/C is designed to be independent from the physical layer, to this intent the protocol use the Media Independent Interface (MII) standardized by 802.3u, allowing to use also Ethernet as physical layer and hence setting up star configurations by adopting simple Ethernet hubs.

With respect to the MAC layer, TTP/C uses a synchronous TDMA schema, the single node accedes the bus in a static, deterministic, sequential order according to a predefined temporal plan. The constant period during which the station transmits is called TDMA slot. During a single slot a single frame transmission is allowed. A sequence of TDMA slots is called TDMA round; in a round the sequence of stations is always identical. The sequence of two TDMA rounds sets up a 'cluster cycle', that is the basis of communication (Fig. 1). The length of slots in a cluster cycle remains constant for a station while different stations may have slots of different lengths.

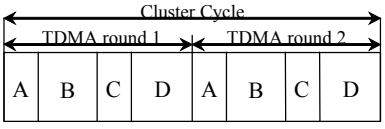

Fig. 1: Example of a TTP/C communication cycle with nodes A, B, C

Consecutive TDMA rounds may differ according to the data transmitted during the slots.
TTP/C implements the main services for fault tolerance and it provides clique avoidance and membership algorithms that have been formally verified ([7], [8]). Cliques are subsets of stations that disagree on the state of the system, for example on the functioning stations at a given time, so communicating exclusively with a part of cluster [7]. The fault hypothesis is precisely stated: two successive faults must occur at least two rounds apart. In such a case this time-triggered protocol solves, at specification level, typical distributed system failure modes as reported in tab. 2, and then situations outside the fault hypothesis are treated using "never give up" strategies, which aim to continue operating in a degraded mode.

Table. 2: Typical distributed system failure modes

Typical Failure Mode	TTP/C	FlexRay
Babbling idiot failures	Yes. Bus Guardian and host in different chips	Yes/No. Bus Guardian but one chip
Masquerading failures	Yes. No ID station	No. ID station in header
Slightly-off-specification (SOS) failures	Yes. Signal renew	No
Crash/Omission (CO) failures	Yes. Membership service	No. Application
Massive transient disturbances	Yes. Membership service	No

FlexRay

The founding FlexRay consortium is composed by important core members as BMW, Bosch, General Motors, Philips, Motorola, Daimler Chrysler, and Volkswagen. The FlexRay specification we refer to is the recently released version 2.1 ([9]).

The protocol enables the transmission on single or double channels, because its employment is thought not only for safety-critical functions. It can be configured as a bus, a star or a multistar and the use of replicated channels or bus guardians is mandatory only for safety-critical applications.
The FlexRay idea of communication is a little different from the one of TTP/C, in fact there is a larger flexible concept according to which at MAC level FlexRay defines a communication cycle as a concatenation of a time-triggered window and an event-triggered one, so in practice there are two protocols applied at the same time. During the event-triggered part of the communication cycle, a Flexible TDMA (FTDMA) is implemented: the time of transmission is divided into minislots, so every station has a given number of minislots, the station can start the transmission of a frame inside each of its own minislots, but if this is not the case there is a loss of bandwidth. The time-triggered window uses a TDMA protocol, the main difference from TTP/C is that, in a time-triggered window one station uses several slots, but the size of single slot is constant (Fig. 2). The structure of FlexRay communication cycle is statically stored in the nodes as TTP, but mode changes aren't supported.

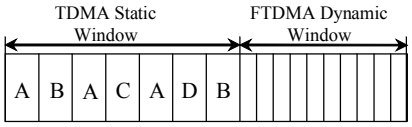

Fig. 2: Example of a FlexRay communication cycle with 4 nodes.

As for the dependability mechanisms, FlexRay defines only bus guardian and clock synchronization algorithms. Membership service and mode management facilities aren't implemented so they will have to be implemented in software or hardware layers on FlexRay. This aspect introduces the problem to implement exactly the services that are needed for a safety-critical distributed application as brake-by-wire.

Time-Triggered CAN (TTCAN)

TTCAN is a communication protocol that try to realize a time-triggered communication on a typical event-triggered protocol, CAN, by adding a software layer. TTCAN uses CAN controllers, but requires that controllers are able to disable automatic retransmission of frames for transmission errors and to provide the upper layers with the point in time at which the first bit of a frame was sent or received ([12]). The communication performances, as frame format, bit rate etc., are the same of CAN protocol. Dependable aspects, as channel redundancy, is possible but not standardized ([11]) and there aren't bus guardians.
TTCAN idea of communication is based on a basic cycle as the concatenation of one or several time-triggered windows and one event-triggered window (Fig. 3). During the event-triggered window the classical CAN protocol is implemented. The sequence of consecutive basic cycles in loops is called system matrix. The master node of the bus, that initiates the basic cycle through the transmission of the 'reference message', represents a single point of failure.
The main issue is the lack of dependability services as bus guardian, membership services etc. so that TTCAN is not suitable for drive-by-wire systems.

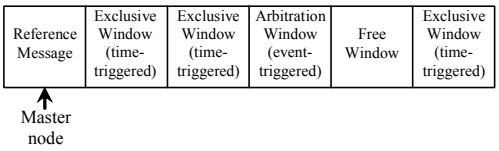

Fig. 3: Example of a TTCAN basic cycle

SENSORS AND ACTUATORS COMMUNICATION SUBSYSTEM

First proposals about x-by-wire systems count that sensors and actuators are directly linked to the stations in the distributed embedded system. Today this has moved towards attempts to substitute traditional connectivity schemes with low cost automotive networks for sensors and actuators. Two possible examples of such networks are LIN and TTP/A. The low cost characteristic is supported by simplicity of communication controllers, but also by limited requirements of microcontrollers driving the communication, e.g. low computational power, low cost oscillators. The global idea is a hierarchical communication architecture with a backbone including a time-triggered architecture ([13]).
LIN and TTP/A are master-slave networks: a master coordinates the communication on the bus and a slave is allowed to send a message only if polled by its master. The master sends a 'command frame' containing the identifier of the message whose transmission is requested and slave answers with the related 'data frame'.

LIN

The LIN protocol born publicly during a press conference at the SAE World Congress in Detroit on March 6, 2000, by a consortium of seven automotive partners: Audi, BMW, DaimlerChrysler, Volvo, Volkswagen, Motorola and VCT. The LIN definition study began in October 1998 and a first specification draft was released in July 1999. The objective of LIN is to provide a standard low-cost sensor network complementary to the CAN functionality, that results in communication costs per node two to three times lower when compared to CAN.
The protocol defines a cluster based on a master node and several slave nodes linked to a common bus. The physical layer is defined as a single wire with a data rate up to 20 Kb/s, that is a precise choice against EMI problems, coherently to the low-cost intention. The master node decides when and which frame has to transmit according to a schedule table, such schedule is the core of communication, it contains a planned list of frames, that have to be transmitted. The defined schedule ensures the determinism of the transmission. LIN, as well as TTP/A, is a serial protocol according to which the master sends a 'command frame' or a 'data frame' and one of the slaves answers with a 'data frame'. The structure of master-slave dialogue is shown in Fig. 4. In LIN the interframe gap is variable, this aspect underlines a different philosophy of protocol design from TTP/A. The temporal predictability of protocol execution is subordinated to the local application tasks, so local temporal properties of the application are considered more important than global temporal properties of the communication protocol, this is confirmed by a significant permitted jitter concerning the point in time when a message must be sent [14].

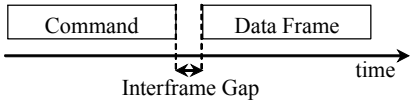

Fig. 4: Master-slave dialogue

TTP/A

TTP/A is a low-cost field-bus protocol concordant with TTP/C bus, which is part of the time-triggered architecture (TTA). It aims at connecting sensors and actuators in embedded real-time systems in different application domains, as automotive, railway etc.. The objective of TTP/A is to provide timely communication, remote on-line diagnostics and plug-and-play capability. In contrast with LIN, which is supported by big industrial sponsors, TTP/A is an academic development of Technical University of Vienna, Austria, was published at the SAE World Congress in 1995 [15]. Few years later a start-up synchronization and an interface file system (IFS) were added to TTP/A protocol [16], now it is commercially available from the TTTech company, but not currently in use in production cars [6].
TTP/A, as well as LIN, is used as SAE Class A network, where the needs in terms of communication does not require the implementation of higher bandwidth such as CAN. TTP/A shares the main design principles of LIN, as example the data rate on a single wire is equal to 20 Kb/s, but other transmission supports enabling higher data rates are possible. The supported communication paradigm is master-slave as Fig. 4 shows but in TTP/A the interframe gap is constant, in accordance with the protocol design idea. In TTP/A, contrary to what happens in LIN, the global timing properties have priority over the local timing properties within a slave, there is a good end-to-end timing and a minimal jitter of distributed transaction, but there is a minor role of local task.
At communication level, TTP/A also supports, other than master-slave rounds, multi-partner rounds and broadcast rounds. The multi-partner round enables several slaves to send a message after a single command frame. A broadcast round is a special master-slave round in which only master send frame. The software development for TTP/A, as well as LIN, is supported by software tools. TTP/A development tools are integrated in the TTA Architecture tools by TTTech.

POWER SUPPLY SUBSYSTEM

The electrical loads of modern cars have increased dramatically over the last 10 or 15 years, especially

luxury cars are huge consumers of electrical power. For x-by-wire systems, beyond the growing problem of loads, there is the need of a power supply that has to be very reliable, because the loss of power means a safety critical situation as loss of brake o steering functions. There are several requirements for power supply subsystems for by-wire systems [17]:

- Reliability: It's important a dual power supply to guarantee the system against a first fault;
- Higher voltages: so that with constant power there is a reduction of current;
- Power management: to provide an automatic management of power supply in case of a lack of power;
- Electronic charge control of the batteries.

In [3] there is a conceptual architecture that include the notion of a dual-redundant power supply, according to which the power supply shall have two outputs, of which at least one shall be fully operational even when there is a fault in the power supply part. The suggested solution is shown in [3] and presents two batteries and one alternator (G). This choice is justified by expensive cost of alternator compared to battery, but especially because the chosen configuration can tolerate all single and double open circuit faults on batteries, alternator and connections among them.

Another key issue of power supply subsystem is the need to change from 12-Volt standard to 42-Volt standard. Such a technology change is necessary for the achievement of a major benefit coming from higher voltage: the reduction of current flows given a specific power consumption value. This leads to wiring bundles as much as 20% smaller than what needed with a traditional power supply. Such a reduction provides in turn the reduction of cable mass and, as a consequence, fuel consumption and emissions. This topic opens new issues about the need of dual 12/42 Volt systems, coming with the commercial risk for car manufacturers, that must swap to 42-Volt technology, and the need of re-designing the major part of all the electronics in the car equipments.

EXPERIMENTAL RESULTS

Based on the previously reported technologies analysis we have prototyped a board for full brake by-wire systems, which is the core for the redundant control of the single braking corner. The main components of that board are the microcontroller host and the communication controller. While choosing such components between existing ones we considered aspects like production technology, availability of reliability data, maturity level of the production process (year of component beginning production), etc..

Concerning the host, our choice fell on microcontrollers of the ST10 family, the STMicroelectronics' industry-standard 16-bit microcontroller family. ST10 is a 16-bit CPU, compatible with Infineon C16x series. Since its introduction, ST has sold more than eighty million chips with the ST10 core, eleven million of which have embedded flash memory. With the DSP-MAC, STMicroelectronics leverages this success, adding cutting-edge DSP possibilities to its ST10 advanced 16-bit MCU. The ST10 architecture is based on an analysis of the real needs of system designers and software engineers in some of the fastest-moving segments of the industry, where high-performance, real-time capabilities and low-power consumption are essential. In this family we have opted for the ST10F269, a microcontroller characterized by production technology of 0.35µm, and year of production, 2000.

About communication controller we have decided for a TTP/C communication controller AS8202NF from Austriamicrosystems, which is an integrated device supporting serial communications according to the TTP specification version 1.1 ([18]). It performs all communication tasks such as reception and transmission of messages in a TTP cluster without interactions with the host CPU. AS8202NF is based on a 16-bit RISC architecture with technology of production 0.35µm.

The chosen architecture, as depicted in Fig. 5, presents doubled boards, hence avoiding the single point of failure.

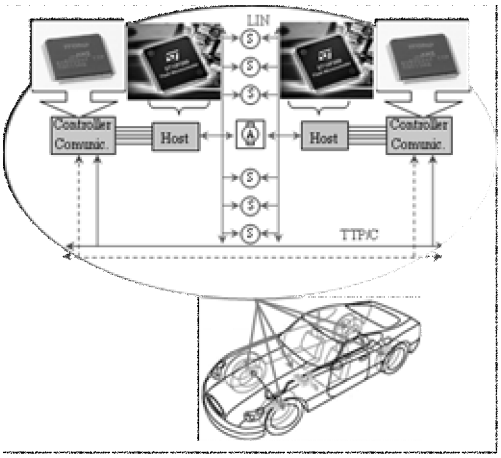

Fig. 5: Concept scheme for architectural proposal

CONCLUSIONS AND FUTURE WORKS

In this paper we have analyzed the most important technologies available for automotive x-by-wire systems. Concerning the communication sub-system we noticed that TTP/C is the reference model for safety-critical applications, it is fast and more developed than other solutions, but non-suitable for

sporadic messages. Contra FlexRay has a more flexible communication idea and the capacity of handling also event-triggered transmissions. Today both protocols are suitable for x-by-wire applications, but the maturity and services favor TTP/C.
About sensors and actuators communication subsystem, the implemented solutions often count on direct links end-to-end to the near ECU, but there is a growing interest in sensor networks. In this paper we have presented LIN and TTP/A as representative of such a kind of solutions. Both networks appears adequate but the adoption of LIN seems to be favored.
In the power supply subsystem section we have given a hint about the main topics in this field: 12/42 Volt swapping and principal requirements for power supply by-wire subsystems.
We have also proposed an architecture of a board for full brake by-wire systems. Starting from the realized board we plan to design and develop a full brake-by-wire system in accordance with the dependability analysis drawn in this work.

REFERENCES

[1] R. Johansson, P. Johannessen, K. Forsberg, H. Sivencrona, and J. Torin, “On Communication Requirements for Control-by-Wire Applications”, in Proceedings of the 21st International System Safety Conference (ISSC 2003), System Safety Society, Ottawa, Canada, August 4-8, 2003, pp 1123-1132.

[2] M. Bertoluzzo, P. Bolognesi, O. Bruno, G. Buja, A. Landi, A. Zuccollo, "Drive-by-wire systems for ground vehicles", 2004 IEEE International Symposium on Industrial Electronics, 4-7 May 2004, Page(s): 711 - 716 vol. 1

[3] X-By-Wire Team, “X-By-Wire: Safety Related Fault Tolerant Systems in Vehicles,” Technical Report XbyWire-DB-6/6-24, November 1998.

[4] Robert Bosch GmbH. (2006) CAN Literature. [Online] http://www.semiconductors.bosch.de/en/20/can/3-literature.asp

[5] E. Pofahl, "The application of IEC 61508 in the automotive industry", Ford Research & Advanced Engineering, D, Summer 2005.

[6] N. Navet, Y. Song, F. Simonot-Lion, C. Wilwert, "Trends in automotive communication systems", Proceedings of the IEEE, Vandoeuvre-les-Nancy, France, June 2005, Page(s): 1204 – 1223 vol. 93.

[7] G. Bauer and M. Paulitsch, “An investigation of membership and clique avoidance in TTP/C,” in Proc. 19th IEEE Symp. Reliable Distributed Systems, 2000, pp. 118–124.

[8] H. Pfeifer, D. Schwier, et al. Formal Verification for Time-Triggered Clock Synchronization. Dependable Computing for Critical Applications 7, IEEE Press, 1999.

[9] FlexRay Consortium, "FlexRay Communication System, Protocol Specification, Version 2.1" [Online]. Available: http://www.flexray.com

[10] T. Fuhrer , B. Muller, W. Dieterle, F. Hartwich, R. Hugel, M. Walther, “Time Triggered Communication on CAN”, 2002, Robert Bosch GmbH

[11] B. Müller, T. Führer, F. Hartwich, R. Hugel, and H. Weiler, “Fault tolerant TTCAN networks,” presented at the 8th Int. CAN Conf. (iCC), Las Vegas, NV, 2002.

[12] Robert Bosch GmbH. (2004) Time Triggered Communication on CAN. [Online] http://www.semiconductors.bosch.de/en/20/ttcan/index.asp

[13] Reilhac P & Bavoux B, "Vehicle E/E Architecture: A New Paradigm for Collaborative Product Creation? A Case Study", SAE Convergence 2002. Transportation Electronics. Detroit, MI. October 21-23. 2002. SAE 2002-21-0006.

[14] H. Kopetz, W. Elmenreich, and C. Mack, "A Comparison of LIN to TTP/A," Research Report 4/2000 Institut fur Technische Informatik, TU Wien, Austria.

[15] H. Kopetz, "TTP/A -- A Time-Triggered Protocol of Body Electronics Using Standard UARTS", Proc. SAE World Congress, Society of Automotive Engineers, SAE Technical Paper 950039. pp. 1-9.

[16] H. Kopetz, M. Holzmann, et al, "A Universal Smart Transducer Interface: TTP/A. Object-Oriented Real-Time Distributed Computing", Newport Beach, Cal. IEEE Press. pp. 16-23.

[17] B. Hedenetz, R. Belschner, "Brake-by-wire without Mechanical Backup by Using a TTP-Communication Network“, SAE International Congress 1998, SAE 981109.

[18] Time-Triggered Protocol TTP/C High-Level Specification Document Protocol Version 1.1 Specification edition 1.4.3 of 19-Nov-2003 Document number D-032-S-10-028