Physical Architectures of Automotive Systems

T. Forest
GM Research, Warren, MI

A. Ferrari
Parades, Roma, IT

G. Audisio, M. Sabatini
Pirelli Tyre SpA, Milano, IT

A. Sangiovanni-Vincentelli
Univ. of California Berkeley, CA

M. Di Natale
Scuola S. Anna, Pisa, IT

Abstract

This section will provide insight into new developments and advances in electronics automotive architectures. The design of innovative chip architectures, new upcoming standards for high-bandwidth and deterministic communication (FlexRay) and sensors are the domains of interest, with emphasis on reliability and support for advanced active safety functions.

1. Introduction

The trends are clear. The increase of electronic content in a car is a continuing trend that creates opportunities and challenges. The need of reducing energy consumption and pollution has created pressure for car makers to devise better control algorithms for engine and in general power train control. Alongside the appetite for consumer electronics and communication devices that the car buyers are demonstrating, there is also a growing concern about the number of lives that are lost in our roads due to accidents. Both in US and Europe, regulatory pressures on safety are evident. Safety is becoming a major driving force for the auto makers. Safety at a societal goal level aims at zero accident cars, albeit it is clear that this is an ideal situation that is likely never to be reached. Nevertheless it is certainly possible to increase safety of cars by orders of magnitude. These advances can only be achieved with a tight integration of the control function of the car. Control for safety will demand that timing constraints on messages between subsystems to be met, failure to be communicated to the driver but also handled automatically by the car itself to take the driver to a safe location always and that environmental conditions be detected and handled in realtime.

These requirements need that OEMs, Tier 1 suppliers and semiconductor makers cooperate to define software, subsystems and IC components that can be corralled towards the overall safety goals. This session deals with the hardware architecture and component side of the equation. From hardware architecture point of view, there is a trend towards a move from federated architectures where one subsystem corresponds to a function, to an integrated one where functions are distributed across different ECUs. In this move, the interconnect infrastructure in use today that is fundamentally event driven does not offer the guarantees that are needed. Hence, there is a definite trend to move towards a time-triggered dominated architecture where timing guarantees and a degree of fault tolerance can be assured at the subsystem level. The FlexRay bus architecture and protocol will become a pervasive solution in the car of the future. In Section 2, a detailed discussion of the standard and of the design problems it poses will be offered.

The fault tolerance requirements will have to be also addressed at a lower level of abstraction. The pressure from car makers and Tier 1 suppliers on semiconductor makers to provide zero defect parts is mounting. With decrease in feature size, the difficulty of reducing faulty parts is increasing, hence posing fundamental design issues at the chip architecture level. In Section 3, a discussion of novel safety driven standards, of the trends and challenges in designing future chips and chip sets is offered.

To control the effects of the environment on driving conditions, we need a number of intelligent sensors that can measure all kind of environmental conditions that have an effect on the safety of passengers and drivers. The IC technology is offering now sensors with capabilities and prices unthinkable a few years ago. Wireless technology is removing barriers to their layout and to the possibility of retrofits. On the other hand, mastering and using efficiently the massive amount of data produced will be a great challenge in itself. In Section 4, the use of sensors is described to make tires intelligent, in the sense that they can measure using devices inside the tire itself quantities that are directly connected with the stability of the vehicle. The challenges of placing electronic components inside a tire are daunting but the payoffs invaluable. The overall trend is clear: OEMs, Tier 1 and semiconductor makers are bound by imagination and technical ability to put to good use a cornucopia of new

978-3-9810801-3-1/DATE08 © 2008 EDAA

technologies.

2. The Flexray Communication System, Benefits and Challenges

New applications in chassis systems, propulsion system control, driver assistance, and other areas require increasing bandwidth as well as improved determinism and fault tolerance.

Automotive systems have relied heavily on the Controller Area Network (CAN) [1] communication standard for several years. In modern systems, the CAN bus is simply running out of bandwidth. To overcome these issues, recent automotive architectures are complex systems in which several independent CAN links are connected via gateways. However, these systems do not really provide a significant increase in the available bandwidth, and certainly do not enhance determinism. Furthermore, experience has shown that these systems are difficult to design, and quite brittle (not resilient to change).

FlexRay [3] is a new communication protocol that offers substantially increased bandwidth, significantly improved determinism, and built-in support for some types of redundancy and fault tolerance.

We describe some protocol characteristics, including a general description of the time triggered nature of FlexRay, and the partitioning of communication time into static and dynamic segments.

FlexRay offers many benefits, but it also poses a number of challenges to automotive designers. Many characteristics of the protocol are different from CAN, and a number of issues must be considered for FlexRay that never needed to be considered for CAN [4].

General topics to be discussed are:

Physical Layer Issues The 10 Mbit/s electrical physical layer (EPL) is much harder to design if compared with the relatively uncontrolled nature of CAN networks. The FlexRay EPL specification bounds the topology and configuration of networks allowing a large number of nodes, stubs, branches, etc. Practical experience has indicated that the actual working configurations will probably have stricter requirements than the general ones currently in the standard specifications. In order to get the FlexRay EPL to work at 10 Mbit/s the networks must be simplified. EMC will probably require that the total number of nodes per branch is limited to 4 or 5. Passive star connections seems to have significant problems with signal integrity. Stubs in the network also seem to have issues, forcing each branch of the network to be a linear daisy chain. Finally, active stars are practically required to achieve a significant number of nodes, which introduces costs and additional constraints on system design.

The challenges are many. Some groups (JASPAR, for example [6]) are advocating running FlexRay at lower speeds [7], which allows significant additional Flexibility in topology. Reducing the speed, however, also reduces the available communication throughput, one of the primary benefits with respect to CAN.

Selection of termination nodes FlexRay nodes can be either terminating or middle nodes. Each branch of the network must have two terminating nodes, and the rest of the nodes need to be middle nodes. Terminating nodes need to be located at the end of the linear branches, and the two types of nodes use different electrical circuitry (in general, a hardware change is required to switch between node types). The topology of the network determines which type of node is required, and changes in topology (over model years, or for optional content within vehicles or vehicle lines) drive different termination requirements. As a result, it is quite challenging to identify hardware that can be used in a variety of vehicles without requiring modifications.

Cycle design The configuration of the FlexRay protocol is quite complex. There are a large number of parameters that are highly inter-related, with many configuration constraints governing them. Experience has shown that designing a cycle can be quite complex, especially if it needs to accommodate functionality with varying communication requirements. CAN is comparatively very simple, with only a few parameters that control the entire operation. Once standard configurations are identified, the designer can typically stick with them.

Schedule design Communication scheduling is a well studied problem, and coming up with a FlexRay schedule for a single, well defined problem, while not easy, is not exceedingly difficult - scheduling techniques are very well known. The intention of the OEMs, however, is to allow designs to be carried over from one model year to another. This implies that most characteristics of the schedule must remain fixed, and the cycle and schedule design must be put together early in the design phase. Furthermore, the planned configuration must provide enough flexibility to support future communication requirements that are not even dreamed of at the time these system design characteristics need to be finalized. This is a challenging task, involving many tradeoffs.

Selection of Sync and Startup nodes FlexRay requires a specific number of sync and startup nodes in order for the network to start up and keep operating. The location of the sync and startup nodes is important to fault tolerant characteristics. Networks that have active stars (required for sys-

tems with any significant number of nodes) introduce additional fault tolerance issues. For example, if we assign most sync nodes to one branch, the network cannot operate if that branch has a fault, but if we assign sync nodes to individual branches, then if the star temporarily fails the stable networks on the branches evolve independently and cannot be recombined without interfering with each other. Obviously, physical topology, option content, and other factors play a role in this decision, and the additional behavioral requirements of sync/startup force a challenging software problem if the roles are moved from node to node.

Planning for evolution Planning for the evolution of communication is more difficult with FlexRay. Again, assuming that we don't completely redesign the system for each set of features or model year, FlexRay has finite resources (the number of static slots, the number of mini-slots, the total available bandwidth, precedence/order of slots, etc.) and these must be carefully managed. CAN in contrast was quite easy - we simply keep adding messages into the system until analysis (or empirical testing) shows that communications no longer fit on the link. Systems tend to degrade gracefully, gradually missing deadlines, as opposed to the hard misses that happen with FlexRay.

Integration of software with the communication schedule This is a new issue for automotive. Today our software runs unsynchronized to the communication system - we dump message on the link when we are ready, and take them off when we are ready. FlexRay systems can operate in this way as well, but at a substantial penalty in efficiency. Much better efficiency can be achieved by coordinating the applications with the communication schedule, but this poses numerous challenges (mode switching, changes to control algorithms, fault tolerance, etc.). The link also tends to change a local scheduling problem (only having to worry about the tasks in one box) into a much more complicated global problem (need to worry about the scheduling of tasks in all boxes).

3. Designing SOC Architectures for Reliability/Availability and Safety

Car makers are developing cars with increasing performance and safety features. This is made possible by the pervasive use of electronic subsystems exchanging information (inside and outside the vehicle) and closely interacting with mechanical parts and with the surrounding environment. While in the past, the benefits were mainly measured in terms of increased fuel economy and vehicle performance, currently the trend is to increase drastically driving comfort and safety. The latter is the most innovative area for automotive electronics. The objective of safety systems is to increase the safety of the vehicle in case of accidents or critical situations (passive safety) and to help the driver to avoid accidents and/or to reduce its probability (active safety) in adverse driving conditions. Active safety requires a highly integrated approach where several vehicle functions, such as suspension, steering, braking and vehicle stability controls, are receiving information from collision avoidance systems and from sensors related to road, traffic and obstacles to vision. The trend toward an integrated active safety clearly increases the complexity of electronic systems and poses several design challenges. The complexity has to be managed inexpensively (low cost is always the predominant factor in automotive design), on the hardware part, by exploiting silicon technology scaling, even if it must cope with challenging quality (*zero defectivity*) and reliability targets. Moreover, for safety critical sub-systems, the automotive industry is currently applying the standard IEC61508 (2nd edition) [11] and is pursuing the definition of a tailored standard for automotive system (ISO 26262). These standards provide a structured approach to assure that a certain degree of robustness against systematic (inserted accidentally during design) and random (due to hardware) faults is achieved.

Functional Safety The IEC61508 standard defines rules to achieve functional safety and identifies four levels of integrity (robustness) called Safety Integrity Level (SIL) 1 to 4. For each SIL level, the standard constrains the probability that a dangerous failure, i.e. a failure that has an adverse effect on the overall system, might happen. For system that operates in continuous mode of operation, the probability is measured as Failure In Time (FIT): 1 FIT represents a failure every billion of hours (10^9). For SIL2 and SIL3 systems, which are the most typical in automotive, the probability of failure per hour is, respectively, between 10^{-6} and 10^{-7} and between 10^{-8} and 10^{-9}. In addition, the standard constraints, for each SIL level, the capability to detect failures. For SIL2 and SIL3 systems, the ratio between undetected failure rates and all failure rates must be below, respectively, 10% and 1%. Unfortunately, for automotive sub-systems the reliability target allocated to electronic devices is lower than the previously mentioned values by one to even three orders of magnitude. This poses several design challenges for highly integrated system-on-chip solutions where the common silicon substrate limits the capability to achieve the desired level of safety. Another important aspect related to fault tolerant systems is the behavior (called hardware fault tolerance, HFT, by the standard) in case of one or more faults occur. The current automotive systems are fail-safe: when a failure occurs the system must move into a safe state. Example of the safe state for a power-train system is to stop (i.e. shutdown) the generation of torque

(HFT=0). More difficult might be to reach the safe state in other sub-systems, such as electrical steering or braking systems. In these cases, it might not be sufficient to move into a non operational mode to be safe, but the systems must be fault-tolerant (fail-operation) and robust against one (or even more) fault: the system cannot stop the computation of the safety function (HFT>0).

Technology Trends On the silicon technology side, the ITRS roadmap [5] clearly shows an opposite trend when compared to the application targets, in robustness and sensitivity to environmental conditions. While technology scaling allows to accommodate more complex functionality than in the past, the expected failure rate for hard faults, i.e. changes of the physical structure that modify the behavior of the circuits, and for soft errors, i.e. changes of the state of a signal due to (radiation) particles or interference, is constant or is even increasing for circuit unit. For example, in the current technology (130-65nm) the soft error rate is in the order of 1000 FIT/Mbits. As example, a device with 128Kbyte of RAM suffers of about 1000 FIT, which is several orders of magnitude above the desired target (10-0.1FIT). The same applies to flip-flops and, in a reduced form, also to combinatorial logic. For example, a device with 300KFlipFlop suffers of about 300 FIT, which is again above the target. This technology trend could be compensated only by selecting the appropriate architecture that fits both the performance and the safety (or availability) targets.

Architectural Trends Any form of fault-tolerance is based on redundancy that can be spatial, or temporal, or pertaining to information [9, 10, 2]. One of the most important issues is the definition of fault-containment regions (FCRs) i.e. "collection of components that operate correctly regardless of any arbitrary logical or electrical fault outside the region" [8] and whose faults do not cross region boundaries. In general, this requires the use of independent power and clock sources, the electrical isolation of interfaces and may also require physical separation to avoid common-mode failures. These fault-tolerance requirements call for multi-chip/multi-package solutions, at least for fail-operational structures and are apparently clashing with current silicon technology trends. In fact, recent advances in device integration and IC packaging make the implementation of complete systems on a single chip (SoCs) or in a single package (SiPs) not only viable but also cost effective. Indeed, the most hazardous drive-by-wire applications will deploy redundant distributed architectures implementing fail-operational configurations. Nonetheless, single chip fail-operational architectures may be of important value if we account for the occurrence of soft errors. There are several architectures currently in use in automotive. The most traditional one calls for a physical separation (at least at board level) between the main computing device and the checker. The checker receives part of the inputs and uses specific algorithms to check the output and to decide if the computing device is correctly working. This solution requires a significant additional software development and costly hardware for the checker. This architecture is mainly suitable for SIL2, even if could satisfy also SIL3 requirements. Increasing the detection capability of the main device, the external checker could be reduced to detect only catastrophic events of the computing silicon unit, such us mechanical breakdown or power supply failures. Therefore, the device is suitable mainly for fail-safe mode of operation. The detection capability of the computing unit could be achieved with different hardware/software tradeoffs. On the software side, a set of software tests runs concurrently with the application software and detects failures of the hardware blocks (CPUs, DMAs, Memory, etc). On the other side, a set of replicated hardware blocks and/or coprocessors continuously checks the presence of faults into the monitored units. All these solutions are capable of achieving very thigh safety targets (>0.1FIT) with different costs and development effort. While it is not fully proof which solution provides the best trade-off between cost, performance and safety target, the current trend is toward the most hardware oriented solutions, capable of achieving better coverage of soft-errors and being less intrusive respect to the application software.

4. Tyre dynamics sensor: a turnkey technology

The tyre is one of the most important component of the vehicle from many aspects: handling, fuel consumption, comfort, and safety.

While, by now, the major part of the vehicle mechanical components are controlled or monitored by electronics, the tyres still remain one of the last crucial component of the car that is intrinsically passive, apart from tyre-pressure-monitoring system (TPMS) that is going to be a standard in all new cars sold in the US, due to the introduction of regulations to that effect, and in luxury new cars in Europe.

The TPMS is an important system that can quickly alert the driver with respect to air loss from the tyre before it can become dangerous for the driver's and passenger's safety. However, until now there is no other system capable of exploiting the tyre intrinsic behaviour for improving safety and handling. An useful information for these purposes is the availability of the maximum friction level between a tyre and the asphalt that can be reached before sliding occurs. This information can be potentially inferred by extracting the relevant physical parameters from the tyre dynamic behaviour using ad-hoc sensors.

Many technical problems have to be addressed and solved to reach this goal and different experts have to

work together to cover all the necessary background to address them: from sensors' technologies, to microelectronics, packaging, energy management, radio technologies, mechanical engineering, data processing, modelling, control systems, chemical engineering, physics etc.

The company that has the capability of developing a consistent, reliable, miniaturized device able to measure tyre physical parameters, compute, transmit, scavenge energy and extract relevant engineering data, will have an important impact on the way car dynamics and safety are addressed, and, as a fall out, will have developed a number of breakthrough technologies that could be used in many other automotive, industrial and consumer fields.

Those technologies include reliable, short range, low power radio technologies, energy scavenging solutions, miniaturized sensors to name a few.

Some of these technologies will be analyzed in the presentation and some possible industrial applications will be described as well.

References

[1] R. Bosch GmBh, CAN Specification, Version 2.0, Stuttgart, 1991.

[2] F. Cristian. Understanding fault-tolerant distributed systems. *Communications of the ACM*, 34(2):56–78, Feb 1991.

[3] Flexray, Protocol Specification V2.1 Rev. A, available at http://www.flexray.com, 2006.

[4] T. Forest The FlexRay Communication Protocol and Some Implications for Future Applications. *SAE Technical Paper Series*, Paper 2006-21-0031, October 2006.

[5] International Technology Roadmap for Semiconductors. http://www.itrs.net/.

[6] JasPar Consortium web page http://www.jaspar.jp/

[7] H. Kamio Interview: Current State and Future Outlook for Automotive Electronics and Networking *Renesas Edge Vol 19*, available at http://tw.renesas.com/

[8] J. Lala and R. Harper. Architectural principles for safety-critical real-time applications. 82(1):25–40, Jan 1994.

[9] V. Nelson. Fault-tolerant computing: Fundamental concepts. *IEEE Computer*, 23(7):19–25, Jul 1990.

[10] V. Prasad. Fault tolerant digital systems. *IEEE Potentials*, 8(1):17–21, Feb 1989.

[11] CEI International Standard Standard. IEC 61508.