



Fault tolerant Automotive CAN Control Embedded System

Balachandra Pattanaik Sathyabama University, Research Schoolar, Electrical and electronics Engineering

Dr S. Chandrasekaran Velammal Engineering college, Anna University, Chennai-600 066, India

ABSTRACT

Control and prevention of failures to reduce failure and improve operations by enhancing performance with system-level analysis partitioning end-to-end functions at design itself. The improvement in the reliability and safety of a system with repairable components with respect to the fault tolerant systems under study correspond to a flexible arrangement of fault tolerant units (FTU's). CAN Controllers are used in automotive for fault tolerant embedded system. The existing reliability enhancement models are emphasizing various redundancy techniques. This leads to defence tetchiness that is coupled from the real functional system. By using CAN Electronic Control Unit (CECU) can be adjusted and specialized according to the needs of the system integrator of recovery time minimization from the affected or degraded states in the automotive systems.

KEYWORDS: FTU's, CECU and Automotive System

I. Introduction

The Controller Area Network (CAN) protocol defines the data link layer and part of the physical layer in the OSI model, which consists of seven layers. The International Standards Organization (ISO) defined a standard, which incorporates the CAN specifications as well as a part of physical layer: the physical signalling, although the controller area network (CAN) protocol was originally introduced for automotive applications. The physical media most commonly used to implement CAN networks are a differentially driven pair of wired with common return. For vehicle body electronics single wire bus lines are also used. Some efforts have been made to develop a solution for the transmission of CAN signals on the same line as the power supply. The parameters of the electrical medium become important when the bus length is increased. Signal propagation, the line resistance and wire cross sections are factors when dimensioning a network. In order to achieve the highest possible bit rate at a given length, a high signal speed is required. For long bus lines the voltage drops over the length of the bus line. The wire cross section necessary is calculated by the permissible voltage drop of the signal level between the two nodes farthest apart in the system and the overall input resistance of all connected receivers. The permissible voltage drop must be such that the signal level can be reliably interpreted at any receiving node. The consideration of electromagnetic compatibility and choice of cables and connectors belongs also to the tasks of a system integrator. It is now widely used in process control and many other industrial areas. In comparison with earlier protocols (and standards such as "RS-485"), CAN is easy to use and provides more hardware support for error detection/recovery.

As a consequence of its popularity and widespread use, most modern microcontroller families now have one or more members with on-chip hardware support for this protocol. This means, in turn, that FT CAN networks can now be implemented at very low cost. These embedded systems are task specific computing or controlling units. These systems are growing in number and complexity with addition of new functionality and features to modern automobiles. Designing and developing such automotive embedded systems requires a structured approach and a very well defined set of guidelines facilitating this process. The remaining nodes, upon receipt of this message, start local timers (each with different values), which upon expiry allow local tasks to be executed and messages to be, transmitted in different timeslots on the network. However this type of "domino" architecture lacks scalability, as the authors note that "a Flex CAN network for a safety-critical system always has to be characterized by a small number of nodes." If we are to develop reliable embedded systems using CAN, then we need to ensure that we can achieve reliable group communications. This means, for example, that when one node transmits a message, all nodes must receive the same message. One deficiency with CAN is that this condition may not always be satisfied, [1][2]. This problem can arise as follows. CAN receivers achieve consensus that the accepted message is valid by processing an error-free sequence of bits up to the sixth bit of the EOF sequence. At this point, the receiving CAN controllers accept the message. The sender, however, validates the transmission at the very last bit of the EOF. If the subset of receivers detects an error

in the sixth bit of the EOF sequence, they will subsequently reject the message and begin transmission of an error flag in the seventh bit of the EOF. The remaining receiver nodes will already have accepted the message; thus, an inconsistent delivery has arisen. Under normal circumstances, the sender will queue the message for retransmission; therefore, the possibility of inconsistent message duplicates (IMDs) or inconsistent message omissions (IMOs) arises. Previous studies have shown that the probability of this situation occurring in normal CAN is highly dependent on the bit rate, the nature of the bus traffic, and the number of nodes connected to the bus. The automobile industry has hitherto witnessed the advent of various electronic control systems that have been developed in pursuit of safety, comfort, pollution prevention, and low cost. These control systems, however, presented a drawback in that since the communication data types, required reliability, etc. differed between each system, they were configured in multiple bus lines [3][4], resulting in increased wire harnesses. Therefore, the need arose for reducing the number of wire harnesses, transferring large amounts of data at high speed and so on. To meet the need, BOSCH, an electrical equipment manufacturer in Germany, developed CAN in 1986 as a communication protocol for automobiles. Thereafter, CAN was standardized in ISO 11898 and ISO 11519, establishing itself as the standard protocol for in-vehicle networking in Europe now. Today, CAN is widely accepted for its high performance and reliability [7], and is used in a broad range of fields from FA devices and ships to medical and industrial equipment. CAN and the other communication protocols developed concurrently made it. Physical layer of CAN being discussed as follows [9].

II Physical Standards Of CAN ECU

In February of 1986, Robert Bosch GmbH introduced the serial bus system Controller Area Network (CAN) at the Society of Automotive Engineers (SAE) congress. It was the hour of birth for one of the most successful network protocols ever. Today, almost every new passenger car manufactured in Europe is equipped with at least one CAN network. Also used in other types of vehicles, from trains to ships, as well as in industrial controls, it describes the bus access unit functions as well as some medium-dependent interface. The high-speed standard specifies a two-wire differential bus whereby the number of nodes is limited by the electrical busload. The characteristic line impedance is 120 Ohm, the common mode voltage ranges from -2V on CAN_L to +7V on CAN_H. The nominal specific propagation delay of the two-wire bus line is 5 ns. In order to achieve physical compatibility all nodes in the network must use the same or a similar bit-timing. For automotive applications the SAE published the SAE J2284 specification. This specification defines the bit-timing for rates of 10 k bit/s to 1 M bit/s. It also provides recommendations for bus lines and for connectors and pin assignment. This standard is mainly used for body electronics in the automotive industry. Since for this specification a short network was assumed, the problem of signal reflection is not as important as for long bus lines. This makes the use of an open bus line possible. This means low bus drivers can be used for networks with very low power consumption and the bus topology is no longer limited to a linear structure. It is possible to transmit data asymmetrically over just one bus line

in case of an electrical failure of one of the bus lines. The common mode voltage ranges between -2V and +7V. The power supply is defined at 5V. Transceiver chips, which support this standard, are available from several companies. The fault-tolerant transceivers support the complete error management including the detection of bus errors and automatic switching to asymmetrical signal transmission.

In February of 1986, Robert Bosch GmbH introduced the serial bus system Controller Area Network (CAN) at the Society of Automotive Engineers (SAE) congress. It was the hour of birth for one of the most successful network protocols ever. Today, almost every new passenger car manufactured in Europe is equipped with at least one CAN network. Also used in other types of vehicles, from trains to ships, as well as in industrial controls, CAN is one of the most dominating bus protocols – maybe even the leading serial bus system worldwide. CAN open networks were used for internal machine communication, especially for drives. CAN open features very high flexibility and configurability. This allows using CAN-based networks for closed-loop control. Also the real-time performance in CAN-based in-vehicle networks increases with the use of TTCAN. In vehicles data traffic must usually be both event-triggered.

III. Implementation Of FTCAN In Automotive

The Fault Tolerant controller area network (FT CAN) protocol was originally introduced for automotive applications but is now also widely used in process control and many other industrial areas. The present requirement a low-cost redundancy-management scheme for replicated FT CAN channels that helps to ensure that clocks (and, hence, tasks) on the distributed nodes remain synchronized in the event of failures in the underlying communication channels, without the need for expensive or proprietary interface electronics. We argue that, when using this framework with duplicated channels, the probability of inconsistent message delivery drops to acceptable levels for a wide range of systems. Through an analysis of the protocol and a case study, we conclude that the creation of reliable, low-cost, distributed embedded systems using FT CAN is a practical possibility. The planned deployment of X-by-Wire technologies is leading the automotive industry in the world of safety-critical applications. More precisely, the design of such systems must take into account the dependability of two kinds of requirements. On the one hand, safety, the absence of catastrophic consequences, for the driver, the passengers and the environment, has to be ensured and on the other hand, the system has to provide reliable service and be available for the solicitations of its users. It consists of Display unit, FT CAN Mother Board, Fault injection Board, Fault Injection Board, Battery, Power supply, Microcontroller(MC 33889) .If there is any fault in the vehicle it will find out the actual fault fault occurred and display it to the person who is driving and also control the accelerator and brake.

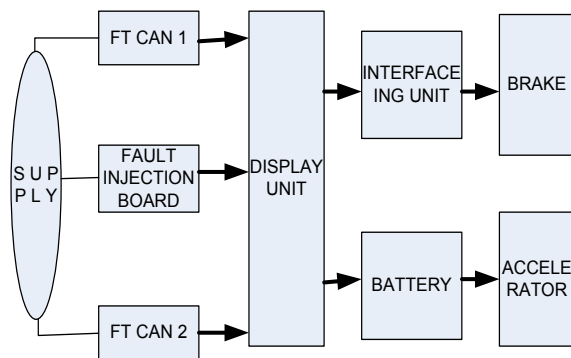


Fig 1. Block Diagram of Automotive Embedded Systems

The block diagram consists of two FT CAN's. The FT CAN 1 is connected with the brake pedal and accelerator pedal. The one end of the FT CAN 2 is connected with the main power supply. The other end of the FT CAN 2 is connected to the display unit and the FT CAN interfacing unit. The interfacing unit is connected to the battery and the battery is connected to the wheel. Both the FT CAN's are connected by the fault injection board in which the faults are being injected. Although CAN was primarily intended to support event-triggered communications between unsynchronized nodes, time triggered communication which has a number of benefits may be enforced, if due care is taken at the system design stage. A number of hardware- and software-based

protocol extensions and modifications have been proposed to enable time-triggered communications on CAN. These tend to rely on the use of a global clock that, in turn, supports a time division multiple access (TDMA) message schedule. For example, Turski describes a distributed clock synchronization methodology with a potential resolution of bit time, 1 using a combination of hardware and software. Pimentel and Fonseca describe a time-triggered system that, although it does not utilize a global clock, controls a cycle of communication via a synchronization message sent by a primary message producer with an accurate clock.

IV. Analysis of Safety communication in Fault tolerant Automotive Systems

CAN on a twisted pair of copper wires become an ISO standard in 1994 in Europe for data transmission in automotive applications, due to its low cost, its robustness and the bounded communication delays. Different modes of communication in fault tolerant in automotive being analysed in technical specifications SFAS (Safety Fault tolerant Automotive Systems) the specific requirements of the different automobile domains have led to the development of a large number of automotive networks. CAN, TTP/C, Flex Ray, media-oriented system transport, one of the important requirements of an automotive communication system is fault-tolerance. The SFAS is followed with following tables assumed true as '1' false as '0' in between as '#'. In automotive CAN (Controller Area Network) is widely used are shown in Table I and II respectively.

Table I. Analysis of usage communication

USAGE	CAN	TTCAN	Flex RAY
Chasis	1	1	0
Airbags	1	0	0
Power train	1	1	#
X-by-wire	#	1	1
Multimedia	0	0	0
Telematics	0	0	0
Diagnostics	1	#	#

Table II. Analysis of Requirement communication

REQUIREMENTS	CAN	TTCAN	Flex RAY
Fault tolerance	#	#	1
Determinism	1	1	1
Bandwidth	#	#	1
Flexibility	1	1	1

CAN possess some fault-confinement mechanisms aimed at identifying permanent failures due to hardware functioning at the level of the micro-controller, communication controller or physical layer. The scheme is based on error counters that are increased and decreased according to particular events. The main drawback is that a node has to diagnose itself, which can lead to the non detection of some critical errors. Without additional fault-tolerance facilities, CAN is not suited for safety-critical applications such as future X-by-Wire systems [5]. For instance, a single node can perturb the functioning of the whole network by sending messages outside their specification (i.e. length and period of the frames). A framework to provide selective fault-tolerance for messages with various fault-tolerance requirements scheduled on CAN is proposed in [6]. The set of messages are analyzed off-line and scheduling attributes are provided that ensures feasible transmission of messages as well as retransmissions upon error occurrences that satisfy the fault-tolerance function operates normally[8]. Both the FT CAN's are connected by the fault injection board in which the faults are being injected. Although CAN was primarily intended to support event-triggered communication as shown in table III. Graph of High speed CAN and the comparison being shown in fig II.

Table III. High speed CAN

Bus Topology	Recessive			Dominant		
	Min	Nom.	Max.	Min.	Nom.	Max
CAN_High(V)	2.0	2.50	3	2.75	3.50	4.50
CAN_Low(V)	2.0	2.50	3	0.50	1.50	2.25
P.D(H-L)(V)	-.05	0	0.05	1.5	2.0	3.0

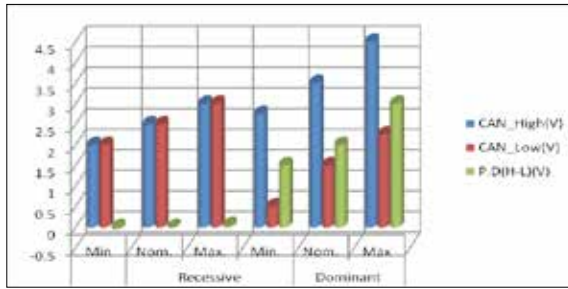


Fig II. Graph of High speed CAN

Conclusion

In the current state of practice, automotive embedded systems make widely use of fault tolerance is used at the wheel angle but seldom at the ECU level because the criticality of the functions does not absolutely impose it. Some future functions, such as brake and accelerator, are likely to require active redundancy in order to comply with the acceptable risk levels and the design guidelines FT CECU. The system will play a central role by providing the services that will simplify the implementation of fault-tolerant applications. Any reliable embedded system will have its failure response carefully built into it. Safety Fault tolerant Automotive Systems are being discussed and future technical enhancement can be done.

REFERENCES

- [1] R. Bosch, CAN Specification 2.0. Postfach, Stuttgart, Germany:Robert Bosch GmbH, 1991. | [2] M. Farsi and M. Barbosa, CANopen Implementation: Applications to Industrial Networks. U.K.: Research Studies Press Ltd., 2000. | [3] K. Pazul, Controller Area Network (CAN) Basics, Microchip Technology Inc., 1999, Preliminary DS00713A, Page 1 AN713. | [4] Philips, P8_592 8-bit Microcontroller with on-Chip CAN Datasheet, Philips Semiconductor, 1996. | [5] N. Navet, F. Simonot-Lion, "A Review of Embedded Automotive Protocols", Technical Report, Nancy Université, 2008. | [6] H. Aysan, A. Thekkilakattil, R. Dobrin, S. Punnekkat, "Fault Tolerant Scheduling on Controller Area Network(CAN)", Proc. of Emerging Technologies and Factory Automation Conference, pp. 1-8, 2010. | [7] T. Nolte, H. Hansson, L.L. Bello, "Automotive Communications - Past, Current and Future", Proc. Of 10th IEEE Conference on Emerging TeFactory Automation, Vol. 1, pp. 985-992,2005. | [8] Freescale Semiconductor, MC33889FS, Inc.2006 | [9] Jittiwut Suwatthikul and Ross McMurran, R. Peter Jones "Automotive Network Diagnostic Systems" 2006, IEEE. |