Journal of Traffic and Transportation Engineering 6 (2018) 176-182
doi: 10.17265/2328-2142/2018.04.003

# Functional Safety for Automotive Ethernet Networks

Luc van Dijk[1] and Günter Sporer[2]

*1. NXP Semiconductors Netherlands BV, Nijmegen, 6534 AE, the Netherlands*

*2. NXP Semiconductors Germany GmbH, München, 81829, Germany*

**Abstract:** In this paper, the need for functional safety in automotive Ethernet is investigated. For this the ISO26262 standard is used but also a comparison with legacy IVN (in-vehicle-networking) is made. In addition, an outlook of future automotive networks is considered and investigated if this brings a further need for safety in automotive Ethernet. From these efforts, it was found that there are several drivers for safety in automotive Ethernet that especially hold for switches.

**Key words:** Automotive, Ethernet, functional safety, fail operational, ISO26262, network, PMHF.

## 1. Introduction

The automotive industry is driven by the mega trends on connectivity, electrification and autonomy. Connectivity is following the demand of being connected and on-line inside the vehicle. Electrification is driven by governments worldwide, setting regulations on emissions. Similarly, the targets of governments worldwide to reduce fatalities, e.g. halving the number of fatalities by 2020 as a target set by the European Commission, are driving the automotive industry towards autonomous vehicles. In these vehicles there will be a significantly higher demand for electronics and semiconductors, in order to equip the vehicle in particular with more sensors and processing power. As a matter of fact, the semiconductor value per car will be more than double in the next 10 years. These architectures demand more bandwidth inside the vehicle, and functional safety will play an increasing role in these vehicles.

It clearly follows from these trends that automotive Ethernet as well as functional safety will be inevitably part of modern and future vehicles. The need for functional safety inside Ethernet (in particular switches and PHYs) has not been explored though, and that is the main objective of this paper.

In this paper we will first introduce functional safety and then investigate the need for functional safety in automotive Ethernet, amongst others by comparison with legacy IVN (in-vehicle-networking) protocols like CAN (controller area network) and FlexRay. A further need for safety is then identified via an exploration of future networks, finally this paper ends with conclusions.

## 2. Introduction to Functional Safety

Originally, for example for Anti-Lock Braking Systems, the automotive industry was proving functional safety compliance via the IEC61508 standard [1]. However, this standard is written as an umbrella standard in order to allow individual industries (like the nuclear power industry and mechanical engineering) to derive their specific standards from it. In the automotive industry it was also quickly realized that specific needs were to be taken into account. The “catastrophic events” are not applicable, also it would not be possible to distinguish between events with one or more fatalities as per IEC61508. Furthermore, the SILs (safety integrity levels) as defined in the IEC61508 needed adjustment it turned out that automotive systems often needed a classification between SIL2 and SIL3. For those main reasons the automotive industry defined an automotive specific safety standard, originally targeting passenger

**Corresponding author:** Luc van Dijk, M.Sc.; research field: electrical engineering.

cars and light utility vehicles. The standard is called ISO26262 and the first revision was released in November 2011 [2].

This year, there will be a new revision of the standard released that has now road vehicles in scope (except mopeds) but trucks, busses and (semi)trailers are no covered as well. In addition, there is a guideline added for semiconductors [3].

In the ISO26262 so called ASILs (automotive safety integrity levels) are defined, ranging from ASIL A to ASIL D, with ASIL D being the highest safety level. The meaning of an ASIL is essentially how much residual risk remains in a particular automotive system. The risk reduction, required to achieve the required ASIL, is achieved by the reduction of random and systematic failures. Systematic failures are caused by human errors and can be prevented by a proper design process. Random failures can for example be caused by thermal wear-out or aging. These failures can be detected by implementation of appropriate safety measures like self-tests, redundancy or monitoring. It is further noted that hardware related failures can be random or systematic, while software related failures will always be systematic.

In the development of an ISO26262 compliant system two main phases are defined, the Concept Phase, and the Product Development Phase. In the Concept Phase, the first step is to perform the item definition, which describes the system and its environment, but also includes the agent (driver). After that the hazard analysis and risk assessment is performed which identifies and analyses hazardous situations. Safety goals are now defined as well, to prevent damage from hazardous events. An ASIL will now be set for each individual safety goal, following for the level of the parameters: severity, exposure and controllability. It is also possible that a QM (quality management) level results from the assessment, in that case safety requirements do not hold. Finally, in the Concept Phase, a functional safety concept is created, which contains the functional safety requirements but also criteria for functional safety validation. The functional safety requirements defined in the Concept Phase are on an architectural, i.e. independent of hardware and software. In the product development phase, which is the next main phase in the development of ISO26262 compliant systems, technical safety requirements are generated. Hardware and software are now also introduced in the architecture. When system design and validation is completed, hardware and software safety requirements are defined. After that, hardware and software design and validation is performed [4].

### *2.1 Vehicle Safety*

In modern automotive systems, security is playing a crucial role, and the significance of security will only grow for future connected (autonomous) vehicles. Nevertheless, safety and security are sometimes still mixed-up. We define overall vehicle safety as compromised of the pillars, functional safety, security and reliability, refer to Fig. 1. Please note that functional safety and security are linked and can sometimes even be in tradeoff. For example, if we associate (an Ethernet) message authenticity with security as the main requirement and message latency as the essential safety related requirement then if we add more security (e.g. pairwise key distribution instead of single key distribution), this requires more resources and causes delays. Another example, in the scope of IEEE802.1 TSN (time sensitive networking) we can consider message availability as the main requirement for safety while message integrity can be considered as the main requirement for security. Frame replication and elimination will enhance availability but it increases the risk for a frame to get manipulated by a hacker [5].

A further link to be discussed and shown in Fig. 1 is between functional safety and reliability. Device reliability is dependent on the intrinsic technology failure rate and this, together with other parameters like a.o. package failure rate and mission profile is used to calculate the HW failure rate. The hardware

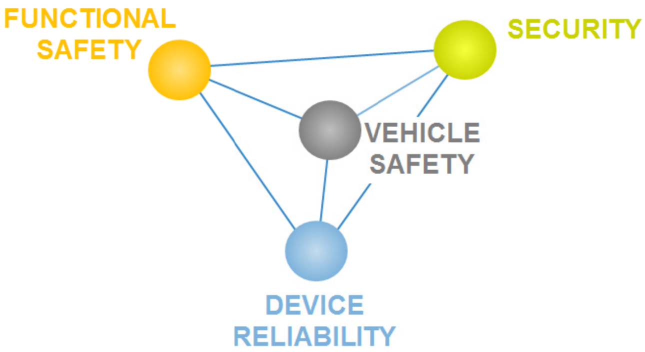

**Fig. 1 Aspects of vehicle safety.**

**Table 1 Ethernet versus legacy IVN.**

| | CAN transceiver | FlexRay transceiver | Ethernet switch |
|---|---|---|---|
| Topology | Bus | Bus, star, mixed | Point-to-point |
| Bitrate | 1 Mbps | 10 Mbps | 100 Mbps, Gbps upcoming |
| Technology | High voltage BCD | High voltage BCD | CMOS |
| Feature size | Around 1 μm | Around 1 μm | (Deep) sub micron |
| Processing | Not included | Not included | Included |
| Digital density | Minor | Minor | Significant |
| configuration | Not applicable[a,b] | Not applicable[a] | Significant |
| Memory | Not included | Not included | Both volatile and non-volatile |
| L2 protection | Included, but not in transceiver | Included, but not in transceiver | (Partially) included in switch |
| Redundancy | Not included | Included, two channels | No, can be included by link replication |

[a]: Configuration in microcontroller; [b]: Except for partial networking.

failure rate is an input to the failure mode effect and diagnostic analysis as specified in the ISO26262.

## 3. Functional Safety in Automotive Ethernet

In this section we want to identify the need for safety in automotive Ethernet, for this we start with a comparison with legacy IVN. The main protocols in legacy IVN are CAN, LIN (local interconnect network), FlexRay and MOST (media oriented systems transport). In Table 1 we compare Ethernet with CAN and FlexRay, since LIN and MOST are generally not applied in safety critical applications.

### *3.1 Transient Faults*

Transient faults are faults that occur and subsequently disappear. Transient faults can be caused by transient disturbances (e.g. as specified in ISO7637) or by EMC (electromagnetic compatibility) or ESD (electrostatic discharge) events. Since Ethernet is running on a significantly higher data rate as legacy IVN the sensitivity to transient faults will be larger in Ethernet. Another type of transient faults are soft errors. Soft errors are caused by alpha particles (device package related) as well as cosmic ray from space [6]. Since this is a transient and fast effect it is especially applicable to latches and SRAM (static random access memory), it can not only cause single event upsets but also multiple bit upsets. As shown in Table 1, Ethernet is implemented in CMOS (complementary metal-oxide-semiconductor) technology with very small feature size, but legacy IVN is implemented in high-voltage bipolar CMOS DMOS (double-diffused metal-oxide-semiconductor) technology with fairly large feature size [7, 8]. Furthermore, in Ethernet switches there is significant digital processing as well as volatile memory. All this makes that the soft error rate must be considered (including safety mechanisms) for Ethernet but not for CAN and FlexRay.

### *3.2 PMHF Budget Assignment*

In the ISO26262 standard an item is specified as an array or an array of systems to implement a function at vehicle level. Let us link this definition to a vehicle architecture based on several domains, connected via a central gateway. It is clear that for many ADAS (advanced driver assistance functions), like emergency braking or adaptive cruise control, an overall implementation will be both in the ADAS domain, containing sensors like RADAR, and/or LiDAR and cameras as well in the powertrain domain containing the braking system. This interconnection will contain multiple Ethernet switches.

Similarly, the safety goals are defined on vehicle level as well, and each safety goal has an associated PMHF (probabilistic metric for hardware failure). This PMHF can be calculated by taking the sum of the individual systems as shown in Fig. 2.

It follows that it in order to meet the PMHF requirement for a safety goal, the PMHF of the IVN ($PMHF_b$), i.e. especially including the Ethernet Switches must meet,

$$PMHF_b \le PMHF_{SG} - PMHF_a - PMHF_c \quad (1)$$

where $PMHF_{SG}$ is the PMHF of the safety goal and $PMHF_a$ and $PMHF_c$ are the PMHF of the sensor fusion and processing and of the actuators respectively.

### *3.3 Layer 2 Protection*

In legacy IVN protocols like CAN and FlexRay, there are safety measures implemented in L2 (layer 2) of the OSI model [9, 10]. In CAN the following L2 error mechanisms are implemented; CRC (cyclic redundancy check), bit stuffing errors, bit errors, ACK (acknowledge) delimiter error, CRC delimiter error, ACK slot error. In Ethernet this is not included, expect for CRC. Let us now consider an example system of four ECUs (electronic control units) that are connected to a fusion ECU where the data of the individual sensors are merged. This is shown in Fig. 3, on the left-hand side based on a CAN bus, and on the right-hand side based on an Ethernet implementation.

In the ISO26262 standard a latent fault is a fault that itself will not result in a violation of a safety goal, but together with another fault (e.g. a bit flip on the bus) this might be the case. An example of a latent fault can be a failure in the CRC module of ECU 1, as indicated with the red crosses is Fig. 3. In case of a CAN-based system, a further error, like a bit-flip on the bus, will now

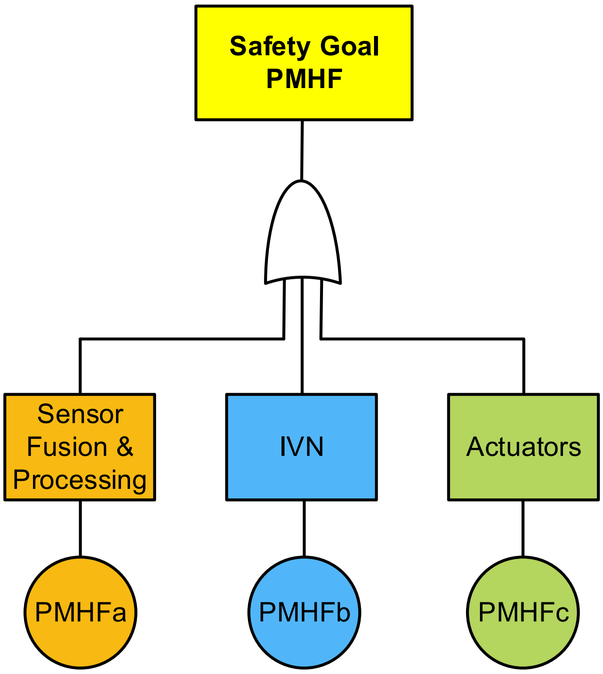

**Fig. 2 PMHF budget assignment.**

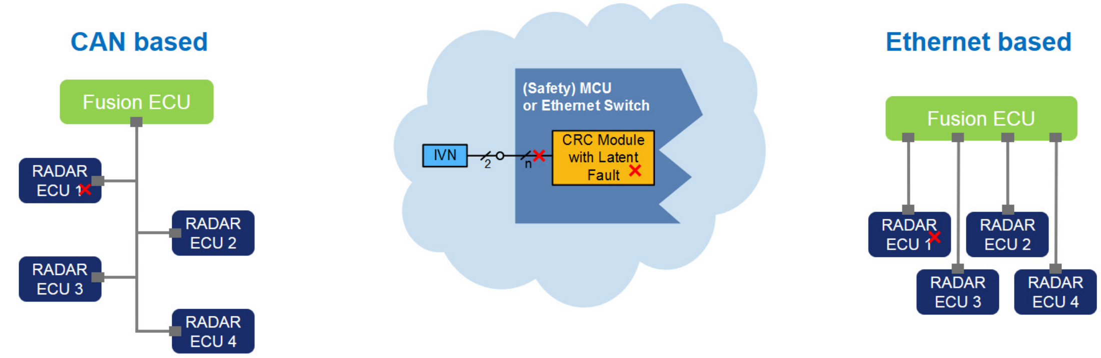

**Fig. 3 CRC in CAN and Ethernet.**

still be detected by the CRC modules in the other ECUs and error frames will be sent by those ECUs, such that the fusion ECU is notified about the bit-flip. However, in case of the Ethernet based implementation, when a bit flip occurs on the connection between ECU 1 and the fusion ECU, this will not be detected by the radar ECU and the fusion ECU will not be notified. Another case is depicted in the middle of Fig. 3, the next failure is now a failure in the ECU itself (rather than a bit flip on the bus). This failure will now neither be detected by other nodes/ECUs in the CAN based implementation, nor will it be detected by other nodes in the Ethernet based system. It follows that safety measures are needed for latent faults in the CRC module, this is normally the case for CAN based implementations since the CRC module is then implemented in a microcontroller featuring sufficient safety measures, however, this might not automatically be the case in an Ethernet based system where the CRC module might be implemented in the switch.

## 4. Future Networks

The automotive industry is heading towards autonomous driving. The SAE has defined six automation levels, ranging from “no assistance” to “no driver” [11].

This will be a major further driving factor for functional safety. The automotive systems associated with the lower levels of automation will still have the driver as a backup in case of an issue, however this will not hold for the highest level of automation. For those vehicles it will therefore be important to have redundancy in place. In this section we will review this especially for automotive Ethernet.

### *4.1 Seamless Redundancy*

Standard Ethernet does not feature seamless redundancy. As an example, the RSTP (rapid spanning tree protocol) may take up to a few seconds for reconfiguration [12].

For seamless redundancy, two main principles exist, the first one is a PRP (parallel redundancy protocol) where the redundancy is in the network topology, the traffic is duplicated in two networks. The other main principle is HSR (high-availability seamless redundancy) which is based on a ring protocol, traffic is sent in two directions. We will review the HSR principle first and then the PRP.

### *4.2 TSN (Time Sensitive Networking)*

Time sensitive networking is a collection of standards, this is the continuation (and renaming) of the work originally done in the Audio and Video Bridging Group [13]. One standard of TSN is the IEEE802.1CB and the topology is shown in Fig. 4.

There is a talker that transmits a frame which is duplicated in the left-hand side switch and sent in two directions, according to the green and blue path in Fig. 4 to a switch on the right-hand side, the frames contain a sequence number. In the switch on the right-hand

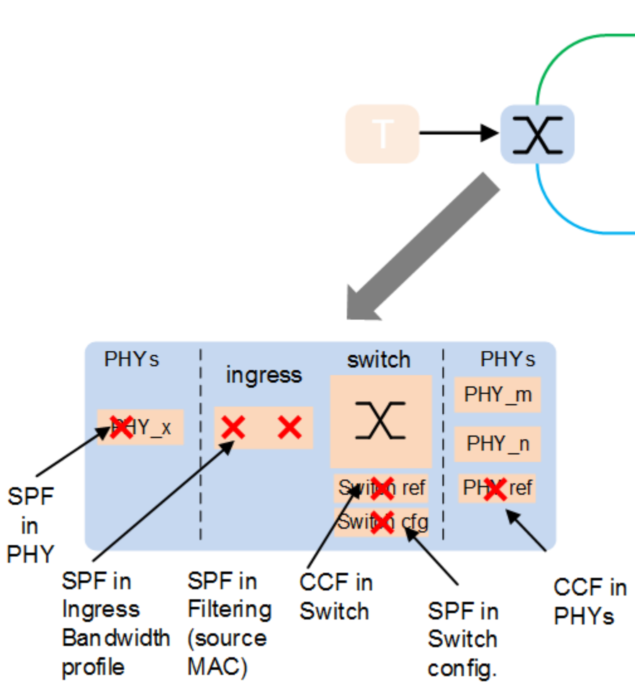

**Fig. 4 Seamless redundancy.**

side the duplicate is eliminated and the sequence tag removed.

This protocol can be handled in the switches, there is no extra hardware or software needed in the end-nodes. From a functional safety perspective this additional functionality (larger memory and processing power) does impact the safety metrics and needs to be taken into account.

In addition, failures in the switches can result in failure of the protocol. This is also illustrated in Fig. 4. It follows that SPF (single point failures) amongst others, the PHY or ingress bandwidth profile or in the filtering (of the source MAC) can cause failure of the protocol. Similarly, a common cause failure in the switch or in the outgoing PHYs may also cause failure of the protocol. Similar examples can be identified for the switch on the right-hand side in Fig. 4. One could also implement the replication and elimination at the talker (sender) and listener (receiver) respectively, but this will not solve all the potential safety issues we just identified.

In summary, implementation of the seamless redundancy protocol in switches has a big consequence for functional safety and requires safety measures in the switches.

### *4.3 Parallel Redundancy Protocol*

In case of a PRP implementation, the hardware is (partially) doubled.

This will not result in issues as discussed in the previous section but it might be a more expensive system solution.

## 5. Conclusions

Automotive Ethernet is the technology of choice for future vehicle architectures, this must include functional safety. Functional safety is all about risk reduction, for this, both product measures as well as an appropriate development process need to be in place.

It was shown that device reliability, functional safety and security are linked, all these contribute to vehicle safety. In particular functional safety and security will play an increasing role in future vehicle architectures, they are linked and sometimes even in a tradeoff.

In order to understand the need for functional safety in Ethernet better, a comparison was made between legacy IVN and Ethernet, it was found that automotive Ethernet, especially the switches, is fundamentally different from legacy IVN in particular w.r.t. technology and topology. This has direct consequences for functional safety for example in order to handle the SER. The larger digital content and memory content will require further functional safety measures.

It was further shown that Ethernet will be part of an item, it will consume part of the PMHF associated with safety goals and therefore forces a low PMHF on Ethernet devices as shown via a PHMF budget assignment.

We also discussed and reviewed if L2 E2E protection in a comparable manner as featured in CAN may be included in Ethernet, but showed that this needs careful assessment (example shown with LPF) for implementation in e.g. switch.

Finally, we discussed and reviewed future networks, especially including fault tolerance, and found that either redundant hardware is required but explained that in case of HSR special safety measures will be required in switches.

## References

[1] International Electrotechnical Commission. 2010. “IEC/TR61508-0, ed1.0&2.0:2005&2010.” Accessed March 29, 2018. http://www.iec.ch/functionalsafety.

[2] International Organization for Standardization. 2011. “Road Vehicles—Functional Safety.” (Part 1 to 9). Accessed March 29, 2018. http://www.iso.org.

[3] International Organization for Standardization. 2018. “Road Vehicles—Functional Safety.” (2nd ed.). Accessed March 29, 2018. http://www.iso.org.

[4] NXP. n.d. “Functional Safety for ISO 26262 and IEC 61508.” Accessed March 29, 2018. http://www.nxp.com/functionalsafety.

[5] Lin, C. W., and Yu, H. F. 2016. “Invited: Cooperation or Competition? Coexistence of Safety and Security in Next-Generation Ethernet-Based Automotive Networks.” In *Proceedings of ACM/EDAC/IEEE Design Automation Conference (DAC)*, 1-6.

[6] Chavali, K. M. 2017. “SER Scaling and Trends in Planar Submicron Technology Nodes.” In *Proceedings of Technical Papers on IEEE Electron Devices Technology and Manufacturing Conference*, 206-8.

[7] Wessels, P., Swanenberg, M., Claes, J., and Ooms, E. R. 2006. “Advanced 100V, 0.13 µm BCD Process for Next Generation Automotive Applications.” In *Proceedings of* IEEE International Symposium on Power Semiconductor Devices and IC’s, 1-4.

[8] Rudolf, R., Wagner, C. O’Riain, L., Gebhardt, K.-H., Kuhn-Heinricht, B., von Ehrenwall, B., von Ehrenwall, A., Strasser, M., Stecher, M., Glaser, U., Aresu, S., Kuepper, P., and Mayerhofer, A. 2011. “Automotive 130 Nm Smart-Power-Technology Including Embedded Flash Functionality.” In *Proceedings of IEEE 23rd International Symposium on Power Semiconductor Devices and ICs*, 20-3.

[9] ISO/IEC 7498-1. Accessed March 30, 2018. https://www.iso.org/standard/20269.html

[10] Aboubacar Diarra, Robert Bosch GmbH. 2013. “OSI Layers in Automotive Networks.” IEEE 802.1 Plenary Meeting, Orlando.

[11] Society of Automotive Engineers. n.d. Levels of driving automation. Accessed March 30, 2018. https://web.archive.org/web/20170903105244/https://www.sae.org/misc/pdfs/automated_driving.pdf.

[12] IEEE802.1w. Rapid Reconfiguration of Spanning Tree from IEEE 802.1: 802.1w.

[13] Institute of Electricaland Electronics Engineers. n.d. Time-Sensitive Networking Task Group. IEEE802.1. Accessed March 30, 2018. http://www.ieee802.org/1/pages/tsn.html.