Vehicle Safety Beyond ISO and ASIL: How Ethernet Networking Components Enhance the Safety of Self-Driving Cars

Steffen Lorenz, Jochen Schyma
Automotive Ethernet Solutions
NXP Semiconductors Germany GmbH
Hamburg/Munich, Germany
steffen.lorenz@nxp.com

Claude R. Gauthier, Ph.D.
Automotive Ethernet Solutions
NXP Semiconductors, Inc.
San Jose, USA
claude.gauthier@nxp.com

Abstract

The prospect of a fully autonomous car is a game changer in many ways, especially in terms of vehicle safety. Today, safety goals are achieved by end-to-end "concepts," with the driver as the ultimate fall back. However, once the computer takes control, the availability of communication paths becomes crucial to allow fail operational systems. Vehicle safety then requires a combination of functional safety and reliability.

In this context, the role of Ethernet ICs is changing. While current car networks usually do not impose safety requirements on these connectivity ICs, IC vendors are starting to see an increase in demand for products with a certain safety requirement and ASIL level. Beyond marketing figures and ticking off feature lists, there is more needed to compare the value of integrated safety features.

This paper will explain the system context of functional safety in networking ICs, examples and outlook on how the network will eventually support failure prevention. Finally, the paper will provide background to methods of implementing the ISO 26262.

I. INTRODUCTION

The automotive industry is following three megatrends: autonomous driving, electrification and service oriented, user-defined HMI. All those trends accelerate the transition toward zonal E/E architectures in the vehicles. This transition, in combination with up and coming vehicles with full or partially autonomous driving capabilities, is having an impact on the functional safety requirement for in-vehicle networking.

The ISO 26262 [1] generally defines the development steps required to bring the inherent risk of hazards caused by malfunction of an E/E system to an acceptable level. Depending on the potential severity, the exposure to such a situation and the controllability of the system in case of a failure, each system gets assigned to an Automotive Safety Integrity Level (ASIL), which goes from A (lowest) to D (highest). Different parts of the system inherit these requirements. This paper will focus on the Safety Element out of Context development, as typically used for the development of standard ICs.

II. SAFETY ELEMENT OUT OF CONTEXT

The process as described in the ISO 26262 is a top-down approach, inheriting requirements from system level to sub parts. As an exception to this, a process called "Safety Element out of Context" (SEooC) development is defined. ICs are often developed as SEooC, as the development starts much before the actual system development and is typically not intended specifically for one dedicated car. During the development of the IC, assumptions of the later context need to be made. The assumed context is also defining the ASIL for this SEooC development.

When a SEooC is used in a safety-related system, the system integrator must verify the assumptions of the SEooC development with the safety requirements of the actual context, i.e., the development of this specific function (see Figure 1). Only with all assumptions fulfilled, the ASIL of the SEooC becomes valid. As an example, the SEooC development might have assumed an external safety measure for some of the internal failure modes. This measure must be available in the actual system. Thus, the ASIL classification of an IC is useless without the knowledge of the used context.

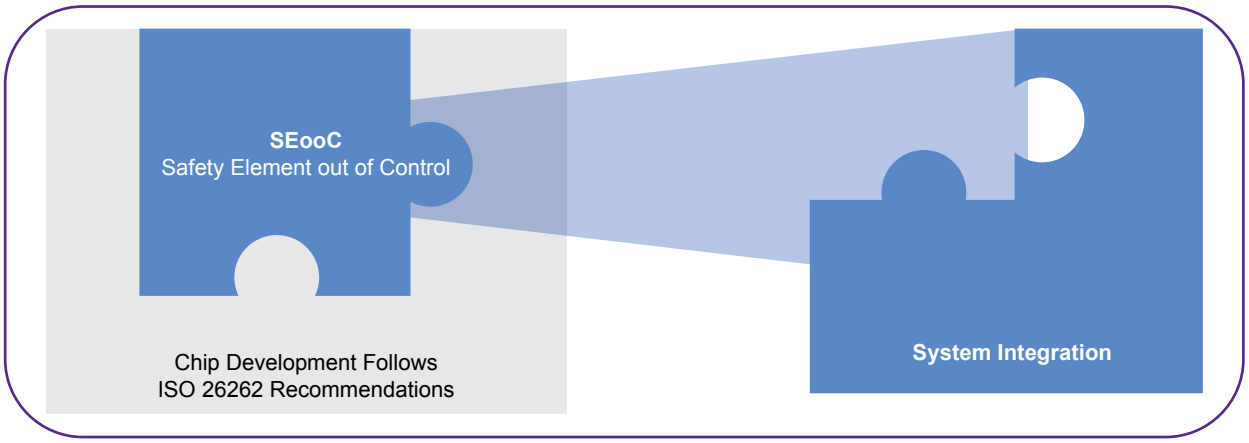


Figure 1: Integration of SEooC

III. FUNCTIONAL SAFETY IN THE ROBOT CAR

Typically, there are several functional safety measures that cover all kinds of failures and are available in end-to-end protected systems. These safety measures can detect if data is corrupted, too late, sent multiple times or even missing. In short, today's in-vehicle networks are relatively safe. We could almost say that our work here it done.

The reason for this lies in the not-too-distant future. Nevertheless, let's start with the current common approach. Let's assume a vehicle uses sensor data to realize a driver assistance system, e.g., automatic distance control. The end-to-end protection ensures correct data, and if the network is corrupted, the system detects that no valid sensor data is available anymore. The system will be switched off and the driver will get a notification to take over full control. The car remains operational.

Now assume the same situation for an autonomous car. There is no driver to take over; consequently, the system would have to stop the car (see Figure 2). The absence of a driver, or at least one who can immediately react, causes the safe state to have a direct impact on the availability of the vehicle service.

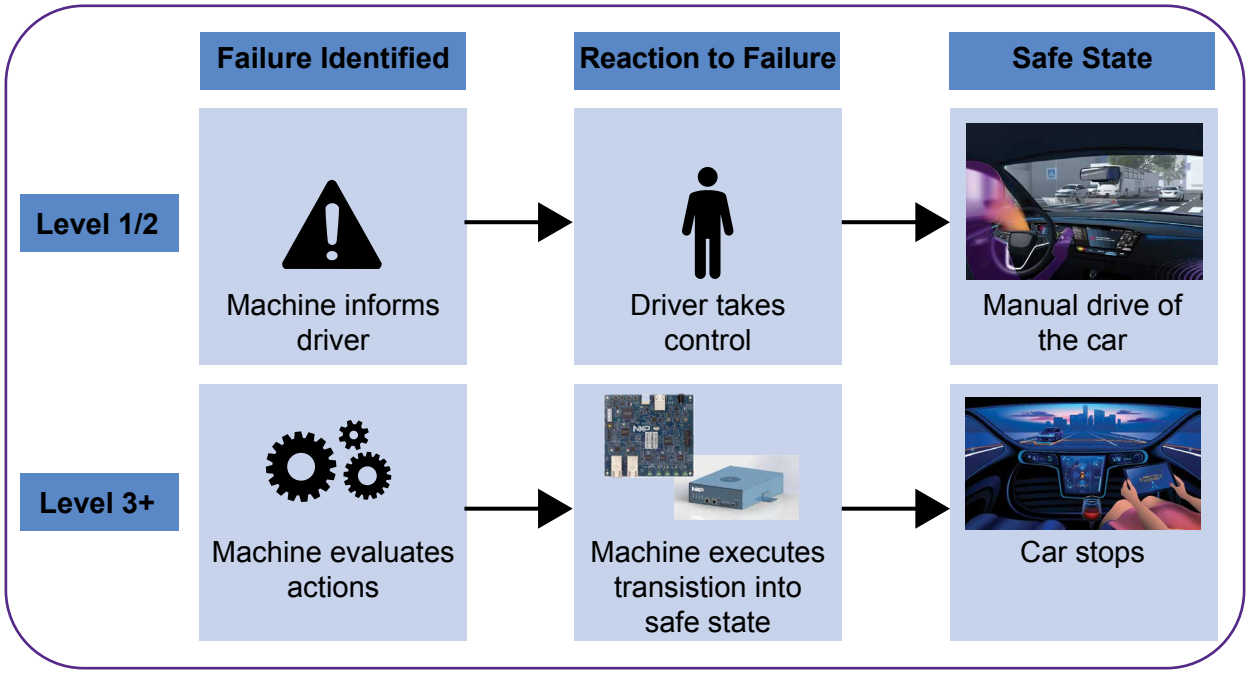
IV. HOW THE NETWORK IC KEEPS YOUR CAR DRIVING

We described the situation in rather black and white terms, and there will be many cases which will not directly cause the car to stop. Nevertheless, it is worth a closer look to see how measures taken to increase vehicle service availability on the network ICs may improve performance.

Vehicle service availability can be improved by ensuring the availability of communication services in the vehicle by:

- Preventing failures
- Predicting failures
- Reacting to failures

The reliability of components in the signal path determines communication availability. It starts with the right process during development, including a safety culture in the organization, and ends with true automotive quality measures during manufacturing, such as technology screening based on qualification data and field return. The interplay of these measures ensure the lowest failure rates. Weak devices that might have a higher failure probability are sorted out during testing already. This results in low failure probability in the field and would cause the system to enter a safe state.



1

Figure 2: System reaction on failure depening on autonoumous level

Another aspect is the predictability of a failure. From a pure functional safety point-of-view, this aspect is not relevant, as the ISO 26262 process focuses on detection of failures and reliable transition into a safe state. A stopped car is a safe car. Taking availability into account, however, it makes sense spend some effort on detecting failures before they actually occur. In the case of a temperature increase, it is possible to switch off unnecessary parts of the system but still keep the essential parts alive. For an Ethernet network, some infotainment connections may be switched off while the back-bone communication stays on. The signal quality indicator of an Ethernet PHY is an example for the detection of degrading link quality due to environmental conditions.

Finally, there will be failures that happen without prior notice. There is no way to prevent this completely. In many cases this will be covered by end-to-end detection on the system level; thus, adding detection on a lower level does not increase the diagnostic coverage nor the safety of the system. There is, however, another aspect that explains why it makes sense to detect the failure where it happens. The closer the detection is to the failure source, the higher the probability that the system can react on this failure and prevent impact to the overall system. An Ethernet switch with ECC-protected memory is able to correct the wrong memory cell so the date can transmit correctly, despite the failure. A network might be using IEEE 802.1CB [2] Ethernet stream replication/ elimination) to build redundant channels to increase the availability in case of cable or connector failures, even though it is not a full redundancy in terms of functional safety.

V. CONCLUSION

Functional safety development for networking components, specifically Ethernet ICs, makes sense, but it is necessary to challenge the plain ASILx rating in the datasheet. Only by knowing about the detailed context is it possible to judge the value of the safety measures.

A mature development process and high manufacturing quality are the basis for increasing the availability of service for future cars by keeping the safety on the same high level. The right measures for preventing, predicting and reacting to failure scenarios complete the package for highly reliable future car networks.

REFERENCES

1 ISO 26262:2018 Road Vehicles – Functional Safety, 2nd Edition.

2 IEEE 802.1CB:2017, IEEE Standard for Local and Metropolitan Area Networks – Frame Replication and Elimination for Reliability

How to Reach Us:

Home Page: **www.nxp.com**
Web Support: **www.nxp.com/support**

USA/Europe or Locations Not Listed:
NXP Semiconductors USA, Inc.
Technical Information Center, EL516
2100 East Elliot Road
Tempe, Arizona 85284
+1-800-521-6274 or +1-480-768-2130
www.nxp.com/support

Europe, Middle East, and Africa:
NXP Semiconductors Germany GmbH
Technical Information Center
Schatzbogen 7
81829 Muenchen, Germany
+44 1296 380 456 (English)
+46 8 52200080 (English)
+49 89 92103 559 (German)
+33 1 69 35 48 48 (French)
www.nxp.com/support

Japan:
NXP Japan Ltd.
Yebisu Garden Place Tower 24F,
4-20-3, Ebisu, Shibuya-ku,
Tokyo 150-6024, Japan
0120 950 032 (Domestic Toll Free)
https://www.nxp.jp/
https://www.nxp.com/support/support:SUPPORTHOME

Asia/Pacific:
NXP Semiconductors Hong Kong Ltd.
Technical Information Center
2 Dai King Street
Tai Po Industrial Estate
Tai Po, N.T., Hong Kong
+800 2666 8080
support.asia@nxp.com

www.nxp.com and imxcommunity.org

Document Number: ETHNETVEHSAFWPA4 REV 0