EVS30 Symposium
Stuttgart, Germany, October 9 - 11, 2017

Fail-operational Safety Architecture for Domain-ECUs with Multicore Processors

Bülent Sari[1], Prof. Dr.-Ing. Hans-Christian Reuss[2]

[1]*ZF Friedrichshafen AG, Friedrichshafen, Germany, buelent.sari@zf.com*

[2] *Forschungsinstitut für Kraftfahrwesen und Fahrzeugmotoren Stuttgart (FKFS), Stuttgart, Germany, Hans-Christian.Reuss@fkfs.de*

Abstract

This paper discusses the possible fail-operational solutions to show how the safety concepts and safety architecture for domain ECUs with multicore processors can be created efficiently in order to fulfill the ASIL-D safety requirements and increase the system availability with fail-operational. Additionally, the ASIL-D safety concepts with decomposition approach are investigated for Domain ECUs. Finally, the developed concepts will be evaluated with use-cases.

Keywords: ISO 26262; multicore processors; fail-operational; Domain ECU; safety architecture; ASIL-Decomposition; ASIL-D

1 Introduction

Nowadays, it has become necessary to use the multicore processors in the automotive industry because of more processing power, more memory and higher safety requirements. The application of multicore processors is increased with the E-mobility and autonomous driving. In particular, the new vehicle systems through electrification of power train and autonomous driving have become more safety-critical. Safety is becoming more and more important with the ever increasing level of safety related E/E Systems built into the cars such as driver assistance systems, which bring new challenges to be tackled with the innovative solutions. Therefore it is necessary to investigate the safety solutions particularly for ASIL-D-Systems. The single core processors cannot fulfill ASIL-D requirements, because ISO 26262 requires a very high diagnostic coverage and hardware independency for the systems. In order to fulfill these requirements, either an additional processor should be used or multicore processors should be applied from the safety point of view. Because solutions with additional processor are expensive, the dual core processors or multicore processors with independent cores are used currently for ASIL-D-Systems. But the currently applied multicore processors will not be sufficient to fulfill the requirements in the near future, because the powerful functions of the vehicle systems increase and the OEMs aim to reduce the control units in vehicles. Therefore the microcontroller manufacturers currently develop the multicore processors with more, currently up to six independent cores, which makes it possible to combine different control units in a domain ECU with multicore processors, for example ADAS Platform from TTTech [3]. Additionally, the system availability is very important for autonomous driving and should be increased with fail operational architectures. This brings additional challenges for the software and safety architecture. For that reason, it is necessary to investigate fail-operational safety architectures for domain ECUs. The independence of the software functions and systems must not be violated in safety critical applications, for that freedom from interference needs to be assured.

According ISO 26262-1, functional safety is absence of unreasonable risk due to hazards caused by malfunctioning behaviour E/E systems and must ensure that, in case of a failure, the system itself will be in a safe-state. This means that in case of a fault, the system either has to be switched off or has to be driven with an (emergency) operation. There is a need for fault tolerant systems for two main reasons:

- It is necessary to keep the system active in the case of an error, if a system shutdown such as steering is not possible in case of an error
- The fault tolerant systems are essential for autonomous driving

2 Safety Architecture Mechanisms

It is necessary to keep the system active in case of an error, if a system shutdown such as brake is not possible in case of an error. A system failure can be minimized or avoided within risk minimization. On the one hand, the achievement of risk minimization is ensured by reducing either the operating time or the failure rate. On the other hand, risk minimization can be achieved within properly developed system safety architecture mechanisms such as fail-safe architectures or fail-operational architectures.

2.1 Fail-Safe Safety Architecture

Fig. 1 shows a typical fail-safe architecture. The main principle is that the system is monitored with its main components, such as the sensor, control unit and actuator, by means of different diagnostic functions and is switched off in the case of an error.

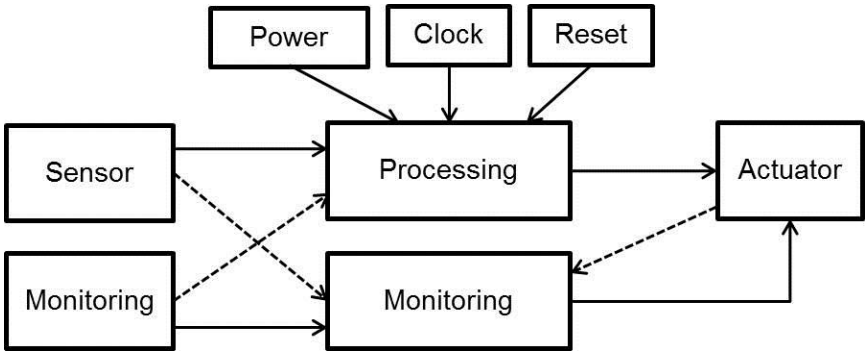


Figure1: Fail-safe architecture [1]

2.2 Fail-Operational Safety Architecture

As mentioned before it is not always possible to shut down the system in case of a failure.

Fail-operational safety architecture can be realized as diversity or redundancy regarding necessary system architecture requirements. Diversity is achieved within two or more different hardware and software application, which are developed from different companies or teams. In a redundant system, the hardware such as processor is developed from the same company and same development teams. The software is done by two or more equal instances. In the following subsection, a short overview of possible realization approaches for fail-operational systems is described.

2.2.1 1-out-of-3 Safety Architecture

The 1-out-of-3 system approach with one voter is derived from 2-out-of-3 system approach. This approach is not suitable for fail-operational safety architecture, because system cannot continue after failing of two units. There are no remaining reference units anymore to check the correctness of the remaining unit.

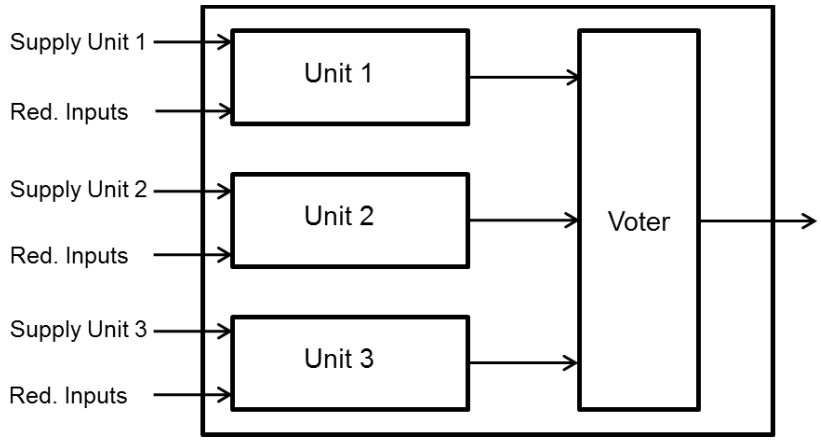


Figure2: 1oo3

2.2.2 2-out-of-3 Safety Architecture

The 2-out-of-3 safety architecture is well-known fail-operational architecture. This approach is also known as Triple Modular Redundancy (TMR) and is used widely in avionic domains as reference architecture for safety critical fail-operational systems. In this approach, three units are calculated redundantly and also independently from each other. It is very important to use the different input signals and also power supply by the calculation of functions. Afterwards, the results are compared and if at least two of the calculated units have the same result, the output is true.

If one of the units fails, the system can continue with the remaining two units. So it is still possible to compare these units regarding the correctness and the system is still fail-operational.

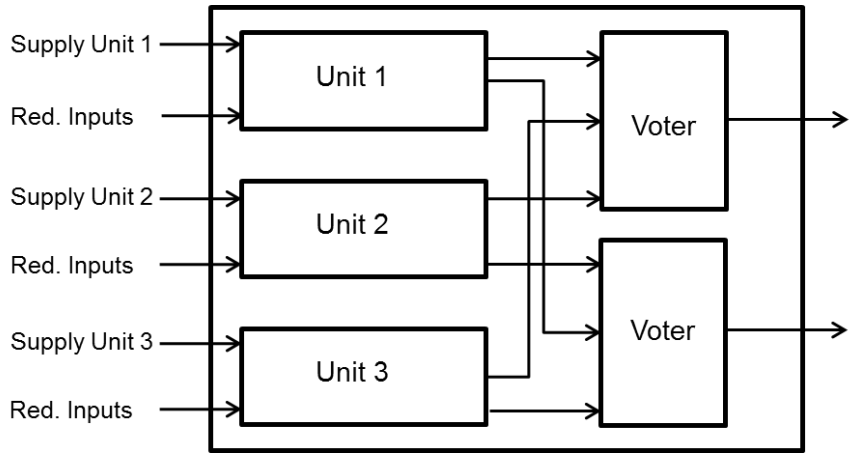


Figure3: 2oo3

This approach is very useful regarding fail-operational. But there are also some disadvantages such as necessity for more ECUs, more power consumption. Therefor it is difficult to implement the 2oo3 safety architecture due to costs issues for automotive projects.

2.2.3 2-out-of-2 Safety Architecture

In comparison to 2oo3 architecture the realization of 2oo2 system is easier. If one of two components fails in one of two channels, the system is further available with one remain channel. But in this case the system is not more fail-operational. It is not good to perform a safety critical system only with one channel, but it is applicable for a certain period of time.

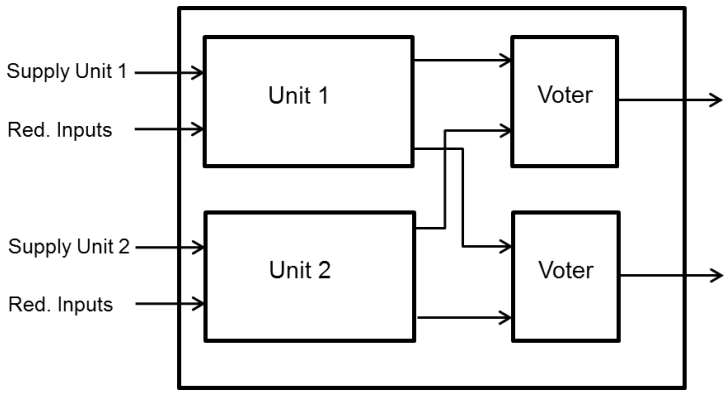


Figure4: 2oo2

2.2.4 2-out-of-2 PD Safety Architecture

The technical paper [4] describes 2-out-of-2 (2oo2) DFS architecture which can be consists of either two equal or diverse subsystems. In this architecture concept, each subsystem uses its own monitoring concept and is designed as fail-safe system to detect its own errors (Fail-Safe (FS)). The disadvantage of 2oo2 DFS is to spend unnecessary processing power because of the cyclic monitoring of units.

The Fig. 5 shows the new developed fail-operational safety architecture 2-out-of-2 Performance Diagnosis (2oo2 PD). In this approach, the redundant or diversity redundant units are compared to each other. If the results are equal, it will be used directly for the control of actuators. But if the results are unequal, then the units will be monitored from the monitoring functions in order to find out and isolate the defective unit. The fault unit will be disabled and the system will be controlled from the correct unit and thus the system remains fail-operational.

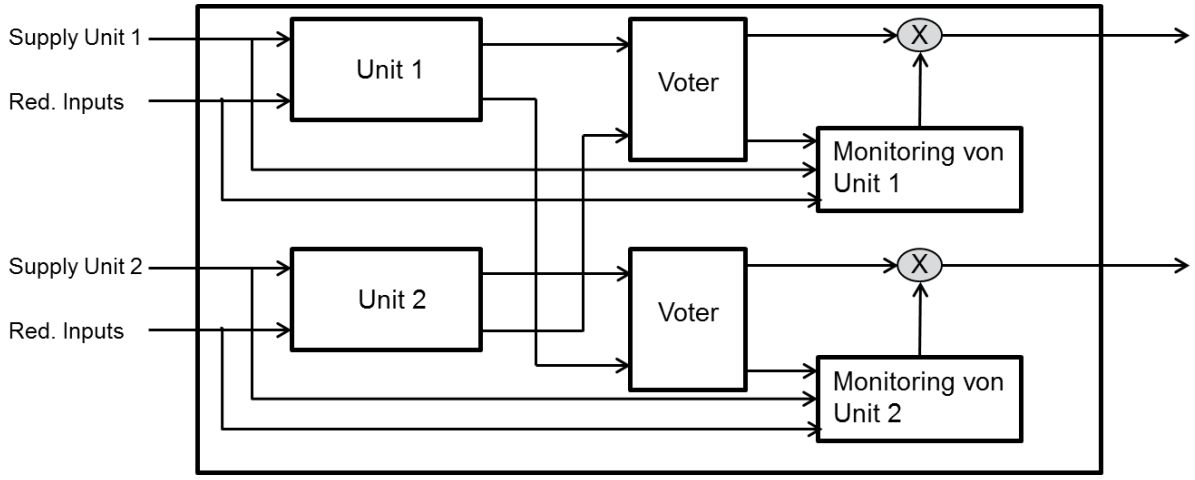


Figure5: 2-out-of-2 Performance Diagnosis (2oo2PD)

3 Fail-Operational Safety Architectures for Domain ECUs with Multicore Processors

If the shutdown of a system is dangerous, because one or more safety goals are interrupted by its shutdown, fault tolerant measures must be developed for such systems, which in the case of a failure, at least enable emergency operation. Such systems are called fail-operational systems and are investigated with the related works [2].

Typical fail-operational systems are 2oo3 systems, which are used very widely in the field of avionics as mentioned before. Such systems provide very high availability through their redundant architecture structure. They consist of three fully independent redundant elements from the sensor to the actuator. These three different paths are plausibly checked against one another, and thus it is possible to find and isolate the defective path in the case of a failure. In an error, the system can be maintained with the other two remaining systems. However, such systems cannot be used in the automotive sector because of cost reasons.

3.1 The developed Fail-Operational Safety Architecture

In the meantime, the application of multicore processors is increased with the E-mobility and autonomous driving. In addition, the OEMs and system providers seek to reduce the number of ECUs in the vehicle. In this context, it is investigated whether the fault tolerant systems can be realized with domain ECUs within multicore processors. Fig. 6 shows the developed solution for fail-operational architecture. The main feature of this approach is the usage of the second processor as back up for the faulty processor or arithmetic core. The safety-critical functions are calculated redundantly in each processor and compared with each other. If the results do not match, then these results are compared with the result from the other processor to find the fault path. The system can then actively work with the remaining paths.

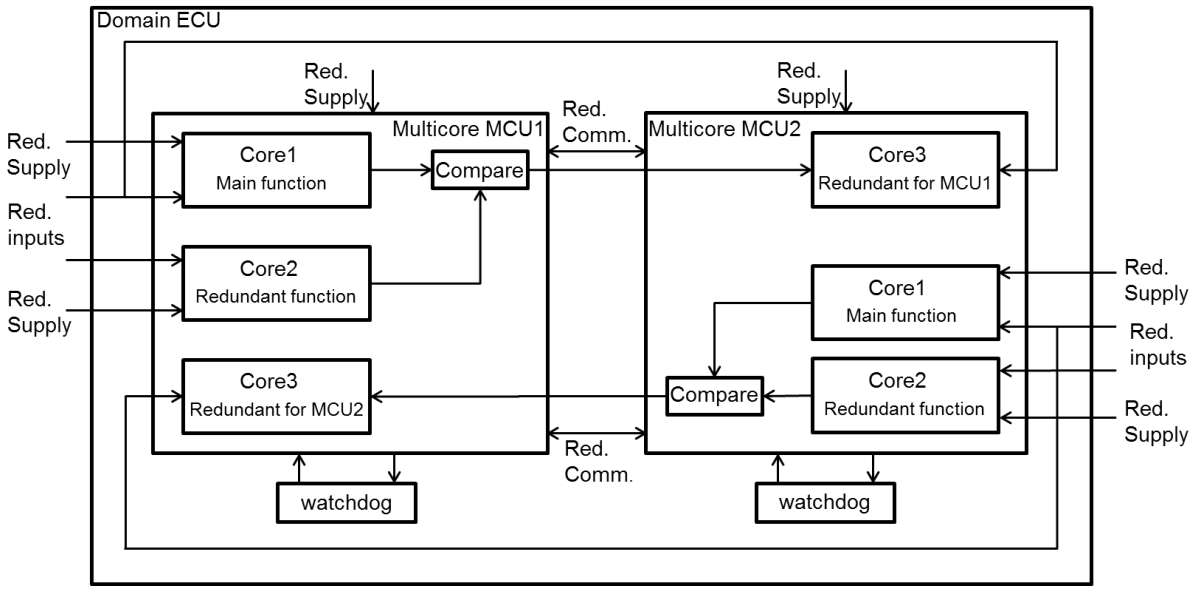


Figure6: Fail-operational architecture for domain ECUs within multicore processors

The benefit of this approach is the increasing of system availability regarding the fail operational architecture within the redundant cores.

3.2 ASIL Decomposition – Sufficient Independence of Decomposed Parts

As mentioned before, the new vehicle systems through electrification of power train and autonomous driving have become more safety-critical. ISO 26262 provides the possibility to apply decomposition approach for the development of safety critical systems, particularly ASIL-D rated safety systems. An appropriate decomposition has the advantage to reduce the ASIL rating of the top events. But the application of ASIL decomposition requires redundancy of safety requirements, which should be allocated to sufficiently independent architectural elements.

ISO 26262 mentions the following requirements to the decomposition approach [5]:

"As a basic rule, the application of ASIL decomposition requires redundancy of safety requirements allocated to architectural elements that are sufficiently independent."

"If the architectural elements are not sufficiently independent, then the redundant requirements and the architectural elements inherit the initial ASIL."

"In the case of use of homogenous redundancy (e.g. by duplicated device or duplicated software) and with respect to systematic failures of hardware and software, the ASIL cannot be reduced unless an analysis of dependent failures (see clause 7) provides evidence that sufficient independence (see ISO 26262-1:2018,1.74) exists or that the potential common causes lead to a safe state. Therefore, homogenous redundancy is in general not sufficient for reducing ASIL due to the lack of independence between the elements."

As shown in Fig 7, the ASIL of safety goal is inherited by corresponding safety requirements and safety functions. The graphic shows additionally, that the decomposed functions of sufficiently independent architectural elements inherit the original ASIL information in the brackets.

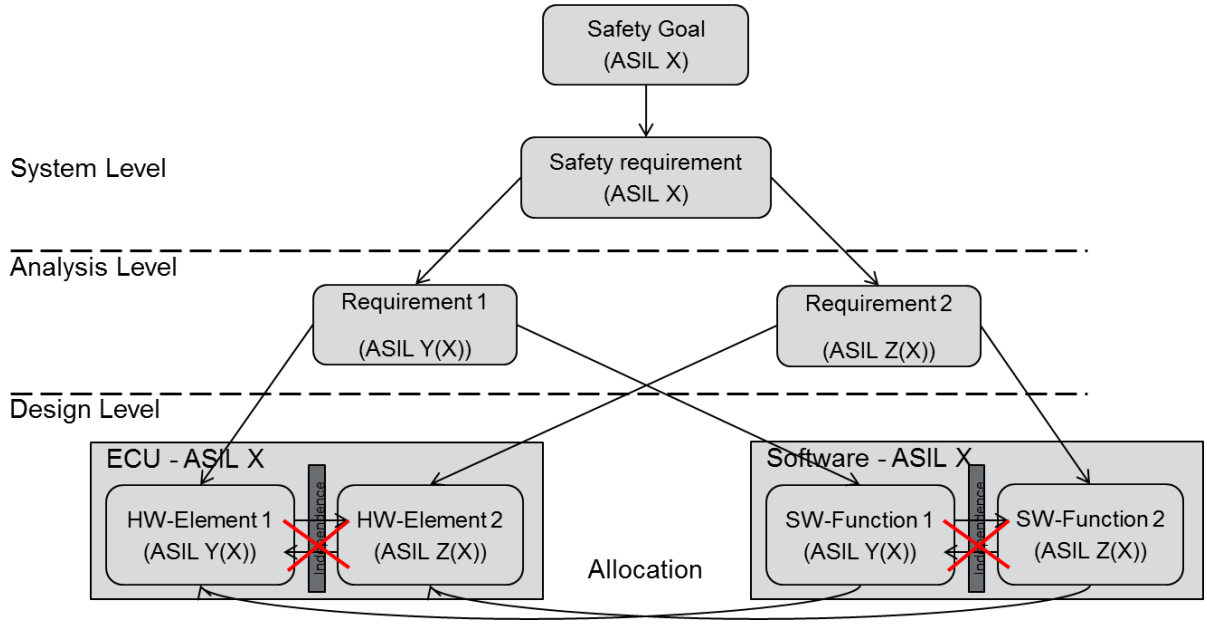


Figure7: ASIL Decomposition

The invented fail-operational architecture is also suitable to apply the decomposition approach for ASIL-D systems according ISO 26262-9 as shown in Fig. 8, because the Domain ECUs offer within developed architecture concept the requested sufficiently independent architectural elements.

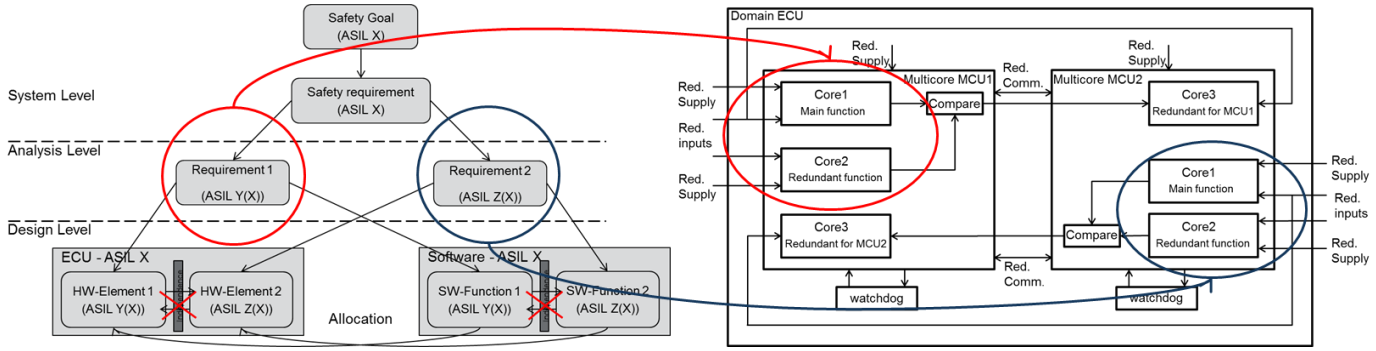


Figure8: Independent distribution of decomposed parts

4 Use-Cases

4.1 Fail-Operational Powertrain Domain

The developed fail-operational safety architecture concept for domain ECUs can be applied as shown in Fig. 9 by power train domain. The transmission control ECU and electric machine and inverter ECU can be integrated to a power train domain ECU which consists of two independent and diversity multicore processor. It is important to use two different multicore processors in order to reduce systematic errors from the semiconductor supplier. Each processor has own redundant power supply and redundant signals for the performing of the software. Each processor is also monitored from the different independent watchdog. If one of the processor has any failure, then the safety critical functions of this processor will be performed by the backup core of the other processor. So the system remains fail-operational as long as the backup core is able to perform the software correctly.

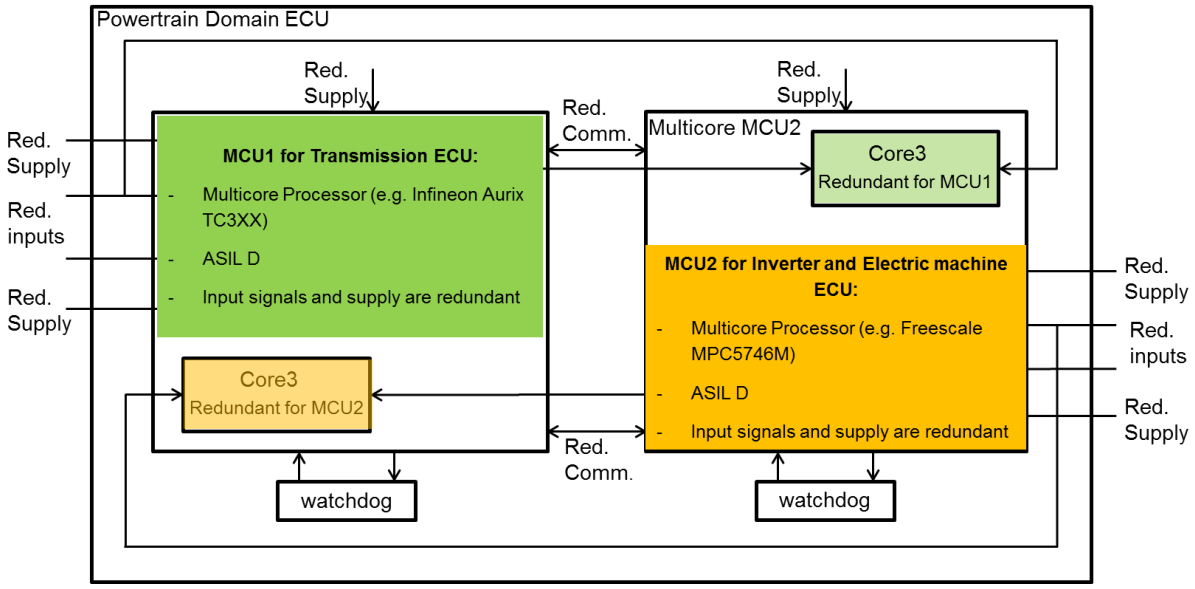


Figure9: Power train domain – Fail-operational

4.2 Decomposition

The decomposition example from ISO DIS 26262-10.1_(2Ed)_BL04 is extended further as shown in Fig. 10 in order to show the suitability of the developed fail-operational safety architecture within the domain ECU for applying of decomposition approach.

Fig. 10 shows the extended example for a system with an actuator that is triggered on demand by the driver to open the door using a dashboard switch.

For the purpose of this example, the architecture of the item is extended as follows:

- The driver`s request is read by actuator control ECU, which powers the actuator through a dedicated power line.
- The vehicle speed information is provided from VS ECU via CAN-Communication and is compliant with ASIL C.
- The second vehicle speed information is provided directly from the speed sensor and is compliant with ASIL A.

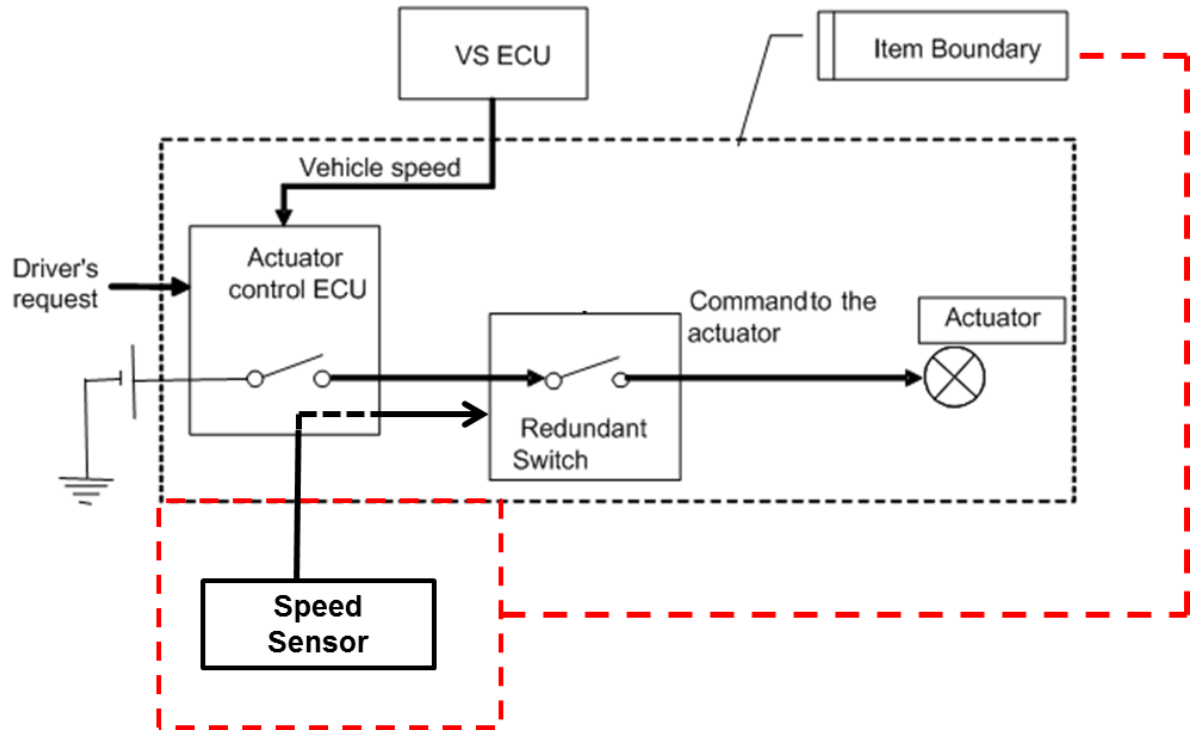


Figure10: Extended decomposition example

The **hazardous event** considered in the analysis is the opening the vehicle door due to the activation of the actuator while driving at a vehicle speed above 15 km/h, with or without a driver request.

For the purpose of the example, the ASIL associated to this hazardous event is classified as ASIL D.

The associated **safety goal** is “Avoid opening the door due to the activating the actuator while the vehicle speed is greater than 15 km/h” and classified with ASIL D.

The defined safety goal can be fulfilled within the implementation of the following decomposed requirements:

- Requirement 1: the actuator control ECU does not power the actuator if the **vehicle speed from the VS ECU** is greater than 15 km/h => ASIL C (D).

- Requirement 2: The Redundant Switch is in an open state if the **vehicle speed from the speed sensor** is greater than 15 km/h. => ASIL A (D).

As shown in Fig. 8 by chapter 3.2, the **safety goal** "Avoid opening the door due to the activating the actuator while the vehicle speed is greater than 15 km/h" can be realized within the application of ASIL decomposition. The developed fail-operational safety architecture enables the possibility that the decomposed safety requirements allocated to architectural elements are sufficiently independent.

5 Conclusion

This paper shows the possible fail-operational safety architectures for domain ECUs within multicore processors. The developed approach enables to apply the ASIL-D safety requirements and increases the system availability with fail-operational. The developed approach is evaluated with the application of hybrid vehicle powertrain in order to show the advantages. The main advantage of the concept is to realize the powertrain fail-operational. The second advantage is to implement the decomposition approach for safety critical systems and to prove easily that the decomposed safety requirements allocated to architectural elements are sufficiently independent.

References

[1] C. Temple and A. Vilela, *Fehlertolerante Systeme im Fahrzeug Von Fail Safe zu Fail Operational*, Elekroniknet, July 2014

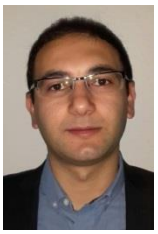
[2] A. Kohn, M. Käßmeyer, R. Schneider, A. Roger, C. Stellwag, A. Herkersdorf, *Fail-operational in safety-related automotive multi-core systems*, Industrial Embedded Systems (SIES), 2015 10th IEEE International Symposium

[3] M. Lawng, *Fail-Operational ADAS-Plattform*, HANSER automotive 9 / 2015

[4] A. Kohn, R. Schneider, A. Vilela, A. Roger, et al., *Architectural Concepts for Fail-Operational Automotive Systems*, SAE Technical Paper 2016-01-0131, 2016, doi:10.4271/2016-01-0131.

[5] ISO 26262 – Part 9 ''Requirements decomposition with respect to ASIL tailoring'', 2011.

Authors



I got my Master’s degree in Electrical Engineering and Information Technology at the Technical University of Munich (TUM).

I have been working since 2010 at ZF Friedrichshafen AG.

At first I worked at the functional development department for passenger car automatic transmissions. I had dealt with the model-based software development and was responsible for the development of safety-critical functions.

Since 2014, I have been working as safety manager and I am responsible for functional safety of automatic transmission projects and also for functional safety of ADAS projects. I am also team member of the VDA (German Association of the Automotive Industry) AK (working team) SOTIF.

Additionally, I do my PhD at the University of Stuttgart on the topic "Functional safety of vehicle systems using multicore processors and applying new design methods in electronics development".