

# Markov Chain-based Reliability Analysis for Automotive Fail-Operational Systems

Andre Kohn and Rolf Schneider  
AUDI AG

Antonio Vilela and Udo Dannebaum  
Infineon Technologies AG

Andreas Herkersdorf  
Technical University of Munich

## ABSTRACT

A main challenge when developing next generation architectures for automated driving ECUs is to guarantee reliable functionality. Today's fail safe systems will not be able to handle electronic failures due to the missing "mechanical" fallback or the intervening driver. This means, fail operational based on redundancy is an essential part for improving the functional safety, especially in safety-related braking and steering systems. The 2-out-of-2 Diagnostic Fail Safe (2oo2DFS) system is a promising approach to realize redundancy with manageable costs. In this contribution, we evaluate the reliability of this concept for a symmetric and an asymmetric Electronic Power Steering (EPS) ECU. For this, we use a Markov chain model as a typical method for analyzing the reliability and Mean Time To Failure (MTTF) in majority redundancy approaches. As a basis, the failure rates of the used components and the microcontroller are considered. The comparison to a non-redundant system shows a significantly higher reliability and MTTF of the redundant approaches.

**CITATION:** Kohn, A., Schneider, R., Vilela, A., Dannebaum, U. et al., "Markov Chain-based Reliability Analysis for Automotive Fail-Operational Systems," *SAE Int. J. Trans. Safety* 5(1):2017, doi:10.4271/2017-01-0052.

## INTRODUCTION

One of the main aspects when developing safety-related automotive systems is fulfilling the requirements of the ISO 26262 standard for functional safety. Today, automotive Electronic Control Units (ECUs) are able to detect a misbehavior and as a consequence shutdown or reboot the device. The corresponding fail-safe architectures are realized in current single-core or multi-core control units.

Due to the more complex algorithms, Driving Assistance Systems (DAS) can already overtake several tasks which are up to now handled by the driver. This will be much more intensified in the future by extensive automation. But the system shutdown of a fail-safe architecture in a fully-automated vehicle will cause an uncontrollable behavior of the car. Hence, a redesign of the safety architecture, including the replacement of fail-safe systems by fail operational approaches, is an important step for coming E/E architectures.

In our contribution we present a system design approach for a fail operational Electronic Power Steering (EPS) ECU which uses two subsystems based on a dual-core lockstep CPU each. We define a

corresponding Markov chain and identify several failure use cases to derive the reliability of the EPS ECU. Furthermore, we compare the results to a non-fail operational system with respect to the general automotive life cycle.

## RELATED WORK

Fail-operational is up to now not widely-spread in automotive industry although it is not a completely new topic. An overview about today's microcontroller safety architectures is given in previous publications [1], [2]. Furthermore, the authors present the 2-out-of-2 Diagnostic Fail Safe (2oo2DFS) architecture as an approach for fail-operational in future automotive multicore systems. These contributions are the basis for our work in this paper.

In this context, researchers from Tsinghua University of Beijing analyzed different M out of N decisions concerning safety and reliability [3]. However, this work is a more generic approach and does not consider automotive systems.

A comparison of a lock-step pair, the traditional Triple Modular Redundancy (TMR)-spare scheme and a Duplication with Temporary TMR and Reconfiguration (DTTR) scheme can be found in [4]. The results show a reliability improvement of their DTTR scheme for multicore ECUs.

The focus of another related work was an approach for a flexible microcontroller architecture which can be applied for fail-safe and also fail-operational. This concept addresses semiconductor vendors for developing new hardware architectures considering functional safety issues [5].

A review of fault-tolerant architectures focusing on industrial applications is given in [6]. The authors propose a cost effective lockstep platform implemented as a fail-operational or two fail-silent systems.

The challenges when replacing fail-safe by fail-operational in automotive ECUs is also addressed in [7]. For this, common fail-operational approaches such as TMR, a duo-duplex and a hybrid concept are presented.

## RELIABILITY BASICS

Generally, a technical system consists of several units which must not fail for a certain time to improve the reliability. The reliability defines the unit's trustworthiness relating to a continuous functionality for a specified time. Hence, the reliability  $R$  of a technical unit defines the probability of functionality within the interval  $(0, t]$ . Another value in this context is the failure rate  $\lambda$ . This means the time-dependent reliability  $R(t)$  is defined as:

$$R(t) = e^{-\int_0^t \lambda(\tau) d\tau}$$

Electronic components mostly have an exponential distribution for the fault rate which is represented by the so called *Bathtub Curve*.

This curve consists of three phases while the first phase the fault rate is much higher. The reason for this are early failures in the start-up at  $t = 0$  due to manufacturing errors. The second phase represents the useful life of the component with a constant failure rate while in the end the probability for a failure is again higher due to component aging (Figure 1).

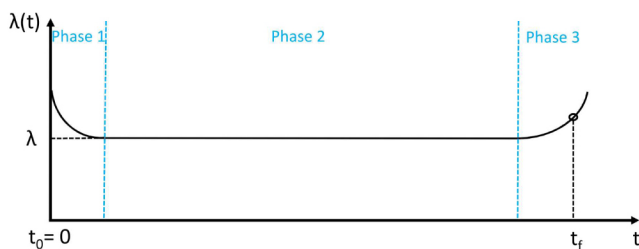


Figure 1. Typical course for the failure rate of a technical unit

The assumptions of a system analysis often includes a faultless system at start-up which means  $R(0) = 1$ . With this prerequisite the following reliability function can be applied:

$$R(t) = e^{-\lambda t}$$

Generally, the reliability  $R(t)$  is a degree for the continuous functionality of an irreparable technical unit. Hence, in the failure case it cannot be moved to an operating state.

A further factor for reliability analysis is the mean durability of a system which is represented by the *Mean Time To Failure (MTTF)* and which is defined by the integral on the reliability:

$$MTTF = \int_0^{\infty} R(t) dt$$

## SAFETY-RELATED AUTOMOTIVE SYSTEMS

The reliability of safety-related system is an essential part when developing ECU architectures. This means, the car must always be controllable to avoid hazards which might injure the passengers or traffic participants. Hence, the availability of basic vehicle functions which control the vehicle, namely braking and steering, must be guaranteed. But the trend towards more intelligent Driving Assistance Systems (DAS) and automated driving complicate this concern due to the fact that more driving tasks are handled by the vehicle instead of the driver. This is also confirmed by the SAE standard J3016 which defines five levels of driving automation [14]. The highest level implies a fully automated car which provides a full-time performance by an automated driving system even without driver. Hence, a mechanical fallback for braking and steering, e.g. the driver, is not available. As a consequence, these levels require a redesign of the automotive E/E and ECU architectures to achieve the fault tolerance required for realizing a fail-operational function. Typical use cases are systems as steer-by-wire and brake-by-wire which use a second control electronic instance so that functionality can temporally be guaranteed even in case of a failure.

Generally, safety-related automotive systems must comply with the requirements of the ISO 26262 which defines four risk classes, namely ASIL-A, ASIL-B, ASIL-C and ASIL-D. Moreover, the standard uses the Failures in Time (FIT) as a measure of the failure rate and as a measure of the probability of failure per hour. This includes the calculation of the failure amount in  $10^9$  hours. In this context, the ASILs require different FIT rates which are listed in Table 1.

Table 1. ASIL FIT rate requirements [7]

| ASIL | Failure Rate                           |
|------|----------------------------------------|
| D    | $< 10^{-8} h^{-1} = 10 \text{ FIT}$    |
| C    | $< 10^{-7} h^{-1} = 100 \text{ FIT}$   |
| B    | $< 10^{-6} h^{-1} = 1000 \text{ FIT}$  |
| A    | $< 10^{-5} h^{-1} = 10000 \text{ FIT}$ |

## HOMOGENEOUS AND DIVERSE REDUNDANCY

Fail operational systems are the main challenge of future E/E and ECU architectures to comply with safety requirements in automated cars. A key aspect for realizing fail operational is the implementation of either homogeneous or diverse redundancy.

Homogeneous redundancy means an application of two identical calculation instances. The advantage is a reduced development effort due to the same components. But the usage of this approach is often limited by the complexity to control dependent failures, especially the ones originating from systematic faults. This means, a systematic error affects all parts of a homogeneous system.

Diverse redundancy contains two or more heterogeneous components which do either the same or different calculations to achieve equivalent functionality. Hence, different algorithms or sub-architectures can be applied. Typically, in avionics there is homogeneous redundancy to improve the reliability and diversity to achieve functional safety. An advantage of this approach is that components can be developed by different suppliers. Furthermore, diverse hardware with different failure rates helps to reduce common cause faults which lead to system failure.

### Majority Redundancy

A popular approach in redundant circuits is the so called Majority Redundancy which is based on an M out of N (MooN) decision. This means the functionality of a system with  $N$  components can be guaranteed if  $M$  components are faultless. A voter as a central unit decides which calculating units provide correct values. Generally, all elements are implemented to guarantee the same functionality so that each of them has the same failure rate at runtime (*hot redundancy*). A special case of a MooN redundancy is a series connection ( $M = N$ ) so that all elements must be faultless. In a system with two components this also means a higher failure rate and hence a lower availability. However, compared to a one-component system, the second communication channel improves the system's integrity. A disadvantage is that in case of different outputs if one channel fails, the correct value cannot be identified and the system must be shut down or transferred to the safe state.

An alternative approach for a fail operational architecture in automotive systems is the 2-out-of-2 Diagnostic Fail Safe (2oo2DFS) architecture realized by two 1-out-of-1 (1oo1) channels with diagnostics (1oo1D). The monitoring function of each 1oo1D channel is capable to detect a misbehavior and shut down the channel thus achieving a fail silent property. The 2oo2DFS can be enhanced with a cross-communication between the two channels enabling one of the channels to diagnose the state of the other channel and by that takeover some of the functionality of the failing channel. This is of interest in the presence of an asymmetric software architecture where one channel comprises safety-critical functions and comfort functions and the second channel safety-critical functions and partial comfort functions in a hot standby mode. After a detected failure of the first

channel, the second channel can take over partial functionality of the comfort functions. The same principle could be applied to safety critical functions at the cost of a more complex software architecture. An example for the 2oo2DFS architecture can be found in [Figure 2](#).

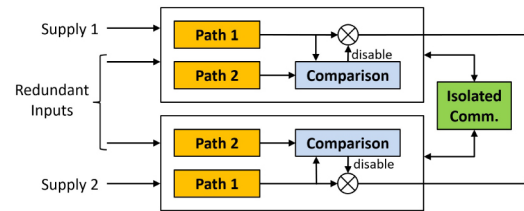


Figure 2. Example for a 2oo2DFS architecture

Safety-related microcontrollers of the automotive industry often use Lockstep cores for redundant calculations in order to achieve the necessary level safety integrity. This feature allows realizing the fail safe part of the 2oo2DFS architecture. In our contribution we apply the 2oo2DFS to a close-to-production automotive function while we analyze the reliability of a symmetric and an asymmetric 2oo2DFS system.

### Redundancy as a Basis for Fail-Operational in Cars

Generally, redundancy respectively MooN decisions require a safety analysis on different implementation levels. Distributed redundancy on E/E architecture level means an implementation of software components on different ECUs which can be located in different vehicle domains. For example, a steering control function can be computed in an Electronic Power Steering (EPS) ECU and in a central DAS ECU in parallel. This means, the ECUs provide redundant outputs from different domains.

An implementation example for diverse redundancy on E/E level is illustrated in [Figure 3](#).

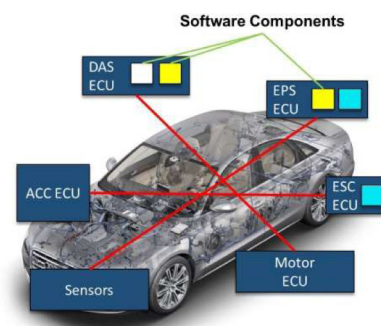


Figure 3. Example for distributed redundancy on E/E architecture level

As an alternative, homogeneous redundancy can be realized by using two identical ECUs, either in different domains or within the same domain. While diverse redundancy can apply existing ECUs, the homogeneous approach doubles the ECU costs, packaging, weight and necessary bandwidth of the communication bus.