# High-Availability Controller Concept for Steering Systems: The Degradable Safety Controller

J. BOERCSOEK, M. SCHWARZ, E. UGLJESA, P. HOLUB, A. HAYEK
Computer Architecture and System Programming
University of Kassel
Wilhelmshoeher Allee 71, 34121 Kassel
GERMANY
j.boercsoek@uni-kassel.de, m.schwarz@uni-kassel.de, eugljesa@uni-kassel.de, holub@uni-kassel.de,
ali.hayek@uni-kassel.de http://www.rs.eecs-uni-kassel.de

*Abstract:* - A high degree of reliability is a basic necessity for all critical elements of a vehicle. This is particularly true for the systems used to control or steer the vehicle. Numerous *steer by wire (x-by-wire)* concepts were developed over the years, but for a variety of reasons, none were ever implemented. Most of them considered only standard single microcontroller system architectures with a low degree of reliability according to international reliability and safety standards. Given its design, the concept presented in this paper has the potential to fill this gap.

*Key-Words:* - Steer-by-wire, Safety-related systems, High-Availability, on-chip redundancy

## 1 Introduction

A range of electronic steering systems can be found in a variety of modern vehicles. Nonetheless, these systems still do not achieve the desired goals with respect to availability, reliability and functional safety. This is due to the increased effort and the resulting complexity of these control systems, as well as the redundant network technology that would usually be necessary for such a system. Efforts to integrate functional safety into systems with complex structures can now be seen, which should allow these functions to be realized in compact spaces at low weight levels. Changes have also been made to the standards, making these systems appear to be worthy of approval. When considering a complex system such as an electronic steering system with no mechanical coupling between the steering wheel and the controlled wheels, not only the mechanical components, but also the control electronics, sensors and actuators must be taken into account as an overall system. For high-availability systems, requirements to take redundancy as well as systematic and common cause failures into account are particularly important. Other aspects such as the real-time capability under worst case conditions also play an essential role. The structure proposed in this paper not only features high-availability, but also the redundancy levels required for such systems.

## 2 X-By-Wire Survey

One of the latest patents granted by the United States Patent and Trademark Office (USPTO) in the last millennium is owned by Dilger et al. (employees of Robert Bosch GmbH), and titled 'Steer-By-Wire Steering System for Motorized Vehicles' and issued on 29. December 1999 with patent number US 6,219,604 BI [1]. It describes how a force feedback system can use haptic/tactile perception to provide the driver with information about the current road conditions. If the driver does not exhibit predefined reactions, e.g., reducing the speed, or the system detects an imminent danger, the system intervenes by taking appropriate measures.

Many x-by-wire systems are now commonplace. To control or drive vehicles, they all use operating commands that are electrically forwarded to the actuators, e.g., the servo motors. Power need no longer be transmitted mechanically between the operating elements and corresponding actuators.

For a system suitable for use in series production, the functional safety aspects must be given the same consideration as the purely functional aspects. According to the European Product Liability Act, car manufacturers and their suppliers may only use new systems, if they are thoroughly tested and can demonstrate sufficient operational reliability. In the 125 years since Carl Benz' patent motor vehicle number one was first taken for a test drive in and around Mannheim [2], the automotive industry has collected sufficient experience on the mechanical

ISBN: 978-1-61804-056-5

side. In contrast, mechatronic systems, among which the x-by-wire systems are included, have only been in use in the automotive industry for roughly the last 25 years.

There are a variety of safety concepts for the various application areas. The objective is always to ensure that the system enters the safe state whenever a detected dangerous failure occurs. The dominant idea for track-guided transportation systems, such as those used in railways, is the 'fail-safe' concept. If the safety system is demanded or detects a dangerous failure within its logic, the equipment under control (EUC) and the safety system itself are stopped in accordance with the “de-energize to trip principle”. The train stops. Because of the very high safety requirements for railways, the safety systems must be structured redundantly and feature high diagnostic coverage. Accordingly, this also applies to all railways signaling technology [4]. This safety concept would have fatal consequences if used for air traffic! In air traffic, if a safety-critical situation occurs, the aircraft, usually an airplane must be able to continue its flight until the next safe landing is possible. In this case, the 'fail silent' safety concept and all of its fall back levels apply. While a dual modular redundancy is usually sufficient to achieve a safe state in the railway industry, i.e., the EUC and the safety system stop as soon as the safety system detects a discrepancy between the redundant channels; at least a triple modular redundancy is required in the avionics industry. A triple modular redundancy is the minimum requirement since the airplane must continue to fly. With dual modular redundancy, if a failure occurs, the safety system is not able to decide which of the two channels is still operating properly. With triple modular redundancy, if a dangerous failure occurs - but not a common-cause failure, which is a topic of its own - one can assume that this single failure only occurs in one channel. Using a majority voting device (voter), the two channels still operating properly can be identified and the faulty channel can be switched off (fail silent), thus allowing the airplane to continue its flight until the next landing site.

As studies by DaimlerChrysler show [5], if a failure occurs, a 'fail silent' principle used in an automotive steer-by-wire system, with a mechanical fall back level, can endanger the safety of the driver, passengers and other people involved in the traffic. When a failure occurs, the steer-by-wire system is shut down and the driver uses the mechanical control of the vehicle. The driver must therefore have a certain amount of time to be completely in control of the vehicle. The solution to this problem is the combination of the two principles, 'fail silent' and fault tolerance through redundancy. In the EU sponsored research project HAVEit [3], this is implemented by having a secondary system that adopts the function of the primary system if a safety-critical failure occurs [6]. This secondary system operates until the driver is able to completely control the vehicle and acknowledges such to a safety control system, or safety controller (SC), as it is referred to in the following sections. This SC has to demonstrate the 'fail operational' characteristic. At least within the scope of vehicle steering, fail operational means that the SC has to operate safely until the driver has acknowledged safe control of the vehicle. “Fail operational” and “fail safe” are not necessarily the same thing, since 'fail safe' means that a safe state is adopted in the event of a failure, e.g. usually the SC is shut down if the SC itself has a safety-critical failure. Nonetheless, to ensure that the SC is also fail safe, either the redundancy principle, very high diagnostic coverage or a combination of the two methods can be applied to achieve a high safety integrity level in accordance with IEC 61508 [7].

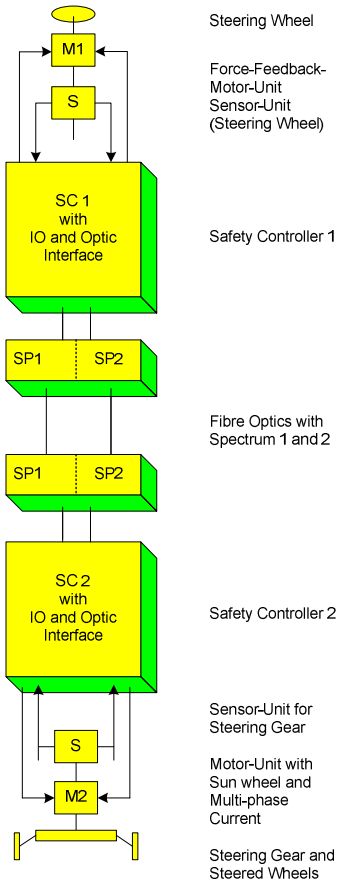


Fig. 1 High availability controller system diagram

This paper describes a safety controller concept that can be integrated into the generic platform used in the HAVEit project [6].

ISBN: 978-1-61804-056-5

This paper proposes a modified platform including the separation of the SC into two parts, the control unit and the actuating unit. Additionally, a redundantly structured fiber-optic connection placed between the two SC units serves for communications and is operated with two different spectra (Fig. 1). Thanks to their degradation levels, the individual SCs themselves have identical a 1oo4 (one-out-of-four) RISC core architecture and comply with both the 'fail operational' and the 'fail safe' principles in a highly effective manner.

## 3 Safety Integrity in Accordance with IEC 61508 and ISO 26262

The IEC 61508 standard is entitled "Functional safety of electrical/ electronic/ programmable electronic safety-related systems". The first edition [8] has been accepted as European standard 2001 by CENELEC. Since May 2010, the second edition of the IEC 61508 is updated and valid [7]. In accordance with the IEC Guide 104 [9], IEC 61508 is to be considered a safety basic standard. As basic standard, it serves as guideline for sector standards that are valid for a specific application area. Specific application requirements can thus be taken into account in practice. The first sector standards based on IEC 61508 are IEC 61511, Functional safety - Safety instrumented systems for the process industry sector [10], IEC 62061, Safety of machinery - Functional safety of electrical, electronic and programmable electronic control systems [11], and IEC 61513, Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems [12]. An additional objective of the IEC 61508 standard is to present to users, whether developers or operators, a general approach on how the various safety aspects can be taken into account throughout the entire safety lifecycle of a safety system. The main concern of the study group responsible for this standard was to provide the various users a consistent, testable procedure. IEC 61508, a test basis that is valid EU-wide and recognized worldwide, can thus be used by notified bodies to test, validate and certify the safety system developed or operated by the user.

The approach presented in the IEC 61508 standard for developing and structuring a safety system is based on a risk analysis performed on a high-risk system. IEC 61508 makes no statements about the methodology for performing the risk analysis. IEC 61508 suggests the qualitative risk graph as a possible method, see [7] Part 1, Section 7.6.2.9, Note. 5. The method of the qualitative risk graph is explained in the informative Section E of Parts 5. The risk analysis allows one to determine the safety integrity level that the system must comply with to minimize the risk resulting from the high-risk system. Defining the safety integrity level (SIL) for a safety system also means that upper and lower failure thresholds are set. IEC 61508 provides four different SILs. A safety system can be operated in two differing modes: in low demand mode, if the safety function of the safety system is seldom demanded (less than once per year) or in high demand mode, if it is often demanded (more than once per year), see [7] Part 4, Section 3.5.16. The IEC 61508 equates the high demand mode with the continuous mode. In this mode of operation, the safety function is integrated in the system's normal operation and maintains the process to be monitored in a safe state, should a failure occur, see [7] Part 4, Section 3.5.16. In the low demand mode, the failure rate is defined as the "the average safety function's probability of failure to perform its design function on demand", see [7] Part 4, Section 3.5.17. In case of high demand or continuous mode of operation, the failure threshold is defined as "the average probability of a dangerous failure" per unit [1/h], see [7] Part 4, Section 3.5.17. The continuous demand mode is to be used for safety functions used within the scope of steer-by-wire. For SIL 3 applications, the maximum mean frequency of a safety function's dangerous failure is less than $10^{-7}$ 1/h, see [7] Part 1, Section 7.6.2.9, Table 3.

ISO 26262 "Road vehicle - Functional Safety" [15] is a sector standard based on IEC 61508, which takes the specific requirements of the automotive sector into account. The current standard state for Parts 1-9 is currently classified as "international standard under publication", which means that the standard has been adopted with respect to its content and is expected to be legally published as international standard within this year. The informative part 10 (Guideline on ISO 26262) is available as draft version. The current scope of ISO 26262 concerns safety-relevant *E/E*-systems (Electrical/Electronic systems) used in passenger cars up to a total weight of 3.5 t for ensuring functional safety. This scope could be extended in the future to utility vehicles [16]. Similarly to IEC 61508, the ISO 26262 also describes the various requirements to the overall product lifecycle, from the development 9f the safety system up to its decommissioning. ISO 26262 provides this description taking a car's lifecycle into account. While IEC 61508 informatively explains the risk graph as method for determining the required SIL,

ISO 26262 is more precise. Part 3 of the standards presents a normative description of the procedure for analyzing risk using the risk graph. The term "risk" is used in different ways depending on the discipline. In engineering sciences as well as in the IEC 61508 and ISO 26262 standards, risk refers to a combination of the probability that the harm occurs and the severity resulting from it [17]. For calculating the risk, IEC 61508 uses the following parameters: *F* = frequency of, and exposure time in, the hazardous zone; *P* = possibility of failing to avoid the hazardous event; *W* = probability of the unwanted occurrence, and C = consequences of the hazardous event. In accordance with ISO 26262, risk can be calculated from the combination of the severity resulting from the harm S, the probability of exposure regarding operational situations *E* and the controllability C. Depending on the valence of the various parameters, the risk can be substantially the same in the most various combinations. In process industry as well as in avionics, an event causing damage has usually a higher severity level than a severe car accident. On the contrary, a car accident is more frequent than an aircraft accident or damage in process industry [18]. The objective is in all these cases, the risk reduction achieved through appropriate safety systems.

In IEC 61508, a safety integrity function (SIF) serves for reducing the risk reduction associated with equipment under control (EUC). The safety integrity function is usually integrated in a safety controller, and the safety controller and the EUC are two independent units. ISO 26262 does not use the term *EUC* but *item.* According to the authors, these differentiation should make it clear that a separation between safety system and equipment under control is not always possible in the automotive industry, e.g., if the safety system itself is a part of the system. This can be illustrated using the example of steer-by-wire: On the one hand, the system is used to during normal operation, and, on the other hand, it serves as safety system if the safety function is demanded due to a system failure. The functional safety of such systems is referred to as functional intrinsic safety.

This example also shows another distinctive feature between IEC 61508 and ISO 26262: The steer-by-wire system must intervene often (in terms of IEC 61508, this means more than once per year) and in possible future cars [21], [22] even continuously to drive the vehicle in the required direction. While IEC 61508 distinguishes between *low demand* and *high demand* or *continuous mode of operation,* ISO 26262 uses the term *operational situation.* A *hazardous event* is described in ISO 26262 as a "combination of a hazard and an operational situation" (Part 1, Section 1.59) in which a "safety operation" (Part 1, Section 1.114) must be performed. This situation appears to correspond to the high demand or continuous mode of operation in accordance with IEC 61508. The safety integrity of a safety integrity function is defined as SIL (Safety Integrity Level) in IEC 61508, and as ASIL (Automotive Safety Integrity Level) in ISO 26262. The common element in the two parameters is that both lower failure thresholds as well as the hardware architecture metric are taken into account. Both standards specify four different integrity levels for a safety function. ISO 26262 introduce an additional level, which is stated as QM (Quality Management). This level means that the function is not a safety function. The requirements for this function are met through the sole implementation of quality management requirements, e.g., in accordance with ISO 9000 [19] or ISO/TS 16949 [20]. The range of values specified in the two standards (see IEC 61508, Part 1, Table 3 and ISO 26262, Part 5, Appendix G, Table G.l) is not identical for all four integrity levels, as shown below in Table 1. In IEC 61508, the hardware architecture metric is determined by the safety parameters *safe failure fraction* (SFF) and *hardware fault tolerance* taking the used component type into account (see IEC 61508, Part2, Table 2 and 3).The SFF express the relation between detected - safe as well as dangerous failures - and all potential failures (detected as well as undetected). The hardware fault tolerance is determined by the redundancy of the architecture in use. For the used components, the difference is made between proven components, for which the failure modes are known and non-proven components.

Table 1. SIL and ASIL according to IEC 61508 and ISO 26262

| IEC 61508 | | ISO 26262 | |
|---|---|---|---|
| SIL | Average frequency of dangerous failure of the safety function PFH [1/hr] | Random hardware failure target values | ASIL |
| 4 | $10^{-9} \le PFH \le 10^{-8}$ | $\le 10^{-8}$ | D |
| 3 | $10^{-8} \le PFH \le 10^{-7}$ | $\le 10^{-8}$ | C |
| | | $\le 10^{-8}$ | B |
| 2 | $10^{-7} \le PFH \le 10^{-6}$ | $\le 10^{-8}$ | A |
| 1 | $10^{-6} \le PFH \le 10^{-5}$ | --- | --- |
| --- | --- | No Safety function | QM |

ISBN: 978-1-61804-056-5

ISO 26262 does not use the terms SFF and hardware fault tolerance. The terms *single point faults metric* and *latent faults metric* are used instead. *Single point fault* (SPF) generally refers to a dangerous failure that is not detected by the safety function. If a redundant safety architecture is used, the SPF can be split in a fraction including a dangerous failure which cannot be detected even by the redundant safety function and once again referred to as *SPF*, and a fraction of a detectable dangerous failure, the so-called *residual fault* (RF). This RF remains undetected in a non-redundant structure and is only detected if redundant safety architecture is used (see [15], Part 5 Annex Band C). In addition of the failure rates SPF and RF, there is also the *multi point faults* (MPF). They include dangerous failures, that can be controlled and are, independently of the architecture, detected by the safety function, so-called MPF, or by the vehicle driver within a given time period, so-called MPF perceived, or as third MPF type, the MPF latent which are controllable but not detectable faults (see [15] Part 1). The common failure rate $\lambda$ of a HW element is composed of all previously described failure type and can be expressed mathematically as follows:

$$\lambda = \lambda_{SPF} + \lambda_{RF} + \lambda_{MPF\_DP} + \lambda_{MPF\_L} + \lambda_S \quad (1)$$

The failure rate $\lambda_{MPF\_DP}$ includes both the *MPF detected* and the *MPF perceived.* $\lambda_{MPF\_L}$ describes the failure rate of MPF latent. The safe failures are included in the failure rate $\lambda_S$. According to IEC 61508, the *SFF* is defined with the following equation:

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda} \quad (2)$$

Where $\lambda_S$ is the failure rate for the safety failure, $\lambda_{DD}$ is the failure rate for the dangerous detected failures and $\lambda$ the total failure rate for all failures. According to ISO 26262, the following equations apply for metrics: For the SPF metric (SPF_M):

$$SPF\_M = 1 - \frac{\sum (\lambda_{SPF} + \lambda_{RF})}{\sum \lambda} = \frac{\sum (\lambda_{MPF} + \lambda_S)}{\sum \lambda} \quad (3)$$

with

$$\lambda_{MPF} = \lambda_{MPF\_DP} + \lambda_{MPF\_L} \quad (4)$$

For the LF metric (LF_M):

$$LF\_M = 1 - \frac{\sum \lambda_{MPF\_L}}{\sum (\lambda - \lambda_{SPF} - \lambda_{RF})} \quad (5)$$

The relation between number of safe failures and dangerous failures will probably turn out to be in favor of safe failures. In terms of metrics, however, this means that every removed failure worsens the metric value see also [23]. This is probably not targeted by the automotive industry since the metric values specified above should make a statement about a safety system's quality, i.e., how safe the system is.

# 4 Safety Controller Concept

A trend in the automotive industry is the requirement for increasingly high quality of the electronic functions. Safety critical functions, previously based on pneumatic, hydraulic or purely mechanic concepts, are noticeably implemented today using programmable safety controllers. And the trend continues to develop in the direction of controller miniaturization. In fact, due to the continuing development of semiconductor structures whole safety controller can be integrated to a single chip. In this context, several research approaches has been published dealing with the implementation auf safety-related architectures with on-chip redundancy. These are usually based on Field Programmable Gate Arrays

## 4.1 Proposed Architecture

Since the proposed controller is planned to be used for steer-by-wire in automotive applications, several dependability requirements have to be considered. On one hand, high availability architecture is required in automotive control systems. On the other hand, such architecture needs to be combined with high safety measures as described in section 2. In this context, the standard IEC 61508 presents a set of system architectures to fulfill dependability requirements based mainly on redundancy and diagnosis. Considering high safety the 1oo2-, 2oo3-, and 1oo3-architecture can be respectively targeted according to the standard. Furthermore, enhanced system architectures can be adopted as the 2oo4- or the 1oo4-architecture. Based on its quadruple redundancy the proposed architecture offers a higher safety. Possible disadvantages of the proposed architecture as the increasing power consumption and systems costs carry less weight while targeting a

one chip solution. In order to insert a higher availability to the propose architecture a concept of degradability is introduced. Once a system failure is detected the failed system component will be excluded and the controller will be degraded to a 1oo3-architecture and so on to a 1oo2-architecture as shown in Fig. 2. Meanwhile, the failed components can be repaired or replaced based on the used technology. This new concept of degradability provides the safety controller with a very high availability. In the following the 1oo4-architecture as well as its on-chip implementation are briefly introduced.

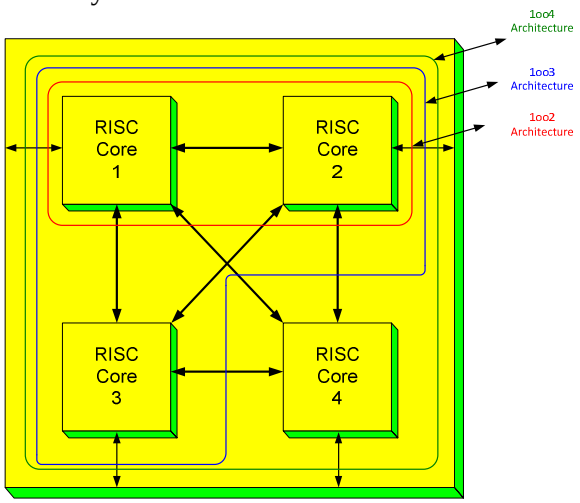


Fig. 2 Degradable safety controller

## 4.2 1oo4 Architecture Calculation

In order to calculate safety and reliability parameters of the proposed degradable controller a sophisticated calculation is needed to be introduced. The calculation of these parameters is mainly based on the parameter of the basic architectures. While the 1oo2- and 1oo3-architectures are described in [7], the calculation of the 1oo4-architecture is briefly described in the following. Extended calculations are given in [25] and [26].

### 4.2.1 Reliability

The calculation of the redundant system reliability can be carried out under the condition that the failures free operational times of the elements are independent random values. The reliability function of the 1oo4-architecture is calculated as follows:

$$R_{1oo4}(t) = \sum_{i=1}^{4} \binom{4}{i} \cdot R^{i}(t) \cdot (1 - R(t))^{4-i}$$
$$R_{1oo4}(t) = 4 \cdot R(t) - 6 \cdot R^{2}(t) + 4 \cdot R^{3}(t) - R^{4}(t) \quad (6)$$

With $R(t)$ is the reliability function for each single element *i*.

### 4.2.2 MTTF-Value

The simplified form of the MTTF-value (Mean Time to Failure) can be deduced from the reliability function as shown below. A detailed calculation of the MTTF-value using Markov models is described in [26].

$$MTTF_{1oo4} = \int_{0}^{\infty} R(t) \cdot dt$$
$$MTTF_{1oo4} = \frac{25}{12} \cdot \lambda \quad (7)$$

Where $\lambda$ is the failure rate for a single element.

### 4.2.3 PFD-Value

An essential value for the calculation of safety-related controller is the average value of probability of failure on demand ( $PFD_{avg}$ ). In the following the simplified form of this value is given. This brief calculation is based on fault-tree analysis and do not conclude common cause failures. Further calculations are based on the mentioned standards and can be found in [26].

$$PFD_{avg} = \frac{{\lambda_D}^4 \cdot T^4}{5} \quad (8)$$

Where $\lambda_D$ is the failure rate for dangerous failure and $T$ is the life time.

## 4.3 On-Chip Implementation

As already mentioned in the introduction the aim of the proposed concept is to integrate a safety controller into a single chip. Therefore four 32-Bit RISC processors in form of Intellectual Properties (IPs) and several needed components as local memories, hardware comparators, communication interfaces are to be implemented on a single chip. In this context, a first approach for on-chip safety-related systems based on a 1oo2-architecture has been presented in [24]. For a start, a high capacity FPGA is going to be targeted as a flexible rapid-prototyping platform. As a future prospect the design of an ASIC is planned. While implementing safety systems with on-chip redundancy, several

requirements and measures are to be taken into account according to the IEC Standard [7]. These requirements vary from modeling according to the V-Model given in [7], using special coding rules and guidelines, as well as using special rules for placement and routing of the system. The chip integration and analysis of the proposed controller will be published in a separated work.

## 5 Fiber-optic Communication

Optic-fiber [27], [28] is used in many consumer telecommunications applications, such as the transmission of telephone and internet communication, and cable television. Due to much lower attenuation and interference, optic-fiber communications has large advantages over existing copper wire in long-distance and high-demand applications. Therefore, using optic-fiber connections in safety-related applications offers several advantages. However, making any communication system safe needs to be modelled according to standards. In this context, an approach of a redundantly structured fiber-optic connection is proposed in this work. These are to be placed between the two SC units and operated with two different spectra as shown in Fig. 3.

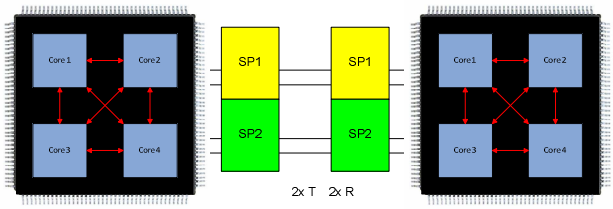


Fig. 3 Schematic of an optical bus system

In [29] several bus architecture models for safety related applications are introduced. In addition, several methods are presented, which deal with qualitative control of faults and transmission errors according to the standard IEC 61508. In the following, a summarized analysis of the data integrity of fiber-optic busses is given. Further calculations are given in [29]. For the needed analysis, the calculation of the probability of undetected error $R_{ue}$ plays an essential role. This is given by the following equation:

$$R_{ue}(p, C) = \sum_{l=1}^{n} A_l \, p^l (1-p)^{n-l} \qquad (9)$$

Where

$C$ = arbitrary linear code
$A_l$ = component of the weight distribution of $C$ = number of code words of weight $l$
$l$ = summation index, representing the number of corrupted bits
$p$ = single bit error probability (bit error ratio, $BER$)
$n$ = block length
$d$ = minimum distance

the weight of a code word being defined as the number of non-zero bits.

Each $A_l$ satisfies the inequality

$$A_l \le \binom{n}{l}$$

from which easily the so-called worst case formula can be deduced:

$$R_{ue}(p, C) = \sum_{l=1}^{n} \binom{n}{l} p^l (1-p)^{n-l} \qquad (10)$$

A linear code $C$ is said to be proper if and only if the probability of undetected error $R_{ue}(p,C)$ is an increasing function of $p$ in the interval [0, 1/2]. In [30] the following estimate has been proven for proper linear codes, where $r$ is the degree of the CRC-polynomial:

$$R_{ue}(p, C) \le \frac{72}{121}\sqrt{2\pi}\,\frac{\sqrt{n}}{2^r}\,\frac{1}{d!}\,n^d\,p^d + 2(\sqrt{2p})^{n-1} \qquad (11)$$

The probability of undetected error $R_{ue}$ is mainly dependent from the probability of bit failure of the used communication media. As shown in Table 2 fiber-optic connections provide smallest values which enforce using them in safety-related applications.

Table 2. Examples of probabilities of bit failures depending of the transmission medium [27]

| **Probability of bit failures *p*** | **Transmission medium** |
|---|---|
| > $10^{-03}$ | Transmission path |
| $10^{-04}$ | Unscreened data line |
| $10^{-05}$ | Screened twisted-pair telephone circuit |
| $10^{-06}$ - $10^{-07}$ | Digital telephone circuit (ISDN) |
| $10^{-08}$ | Coaxial cable in local defined application |
| $10^{-09}$ to $10^{-12}$ | Fiber optic cable |

## 6 Mechanical model

As safety and availability are needed in all the steps of the steer-by-wire process, a safety-related model is also needed at mechanical layer. The proposed model is based on the sun wheel concept, also referred as center gear concept [31]. The latter consists of five gearwheels, four outer (epicyclic gear, also referred to as planetary gear) and one inner (sun gear). The center gear may also incorporate the use of an outer ring gear or annulus, which meshes with the planet gears. A simple construction of a center gear is shown in Fig. 4. Each of the inner gearwheels is forced by a drive while having a position measuring system placed on its shaft measuring the rotational driveway and revolutions per minute (rpm).

By using four independent measuring systems it is possible to detect the actual position of the outer gearwheel. In case of failing of one, two or three measuring systems the actual position of the outer gearwheel is detectable by the other ones. Another advantage by economic respectively environmental means is the use of less powered drives (downsizing) which need less energy in comparison to a big high powered drive. The system is developed for having the capability to run even on three of the four drives with the other drive supporting the others. Even if one drive fails completely the system can run with the other drives without any complications which would not be possible with the system having only one main high powered drive. This increase the availability of the entire system proposed in this work.

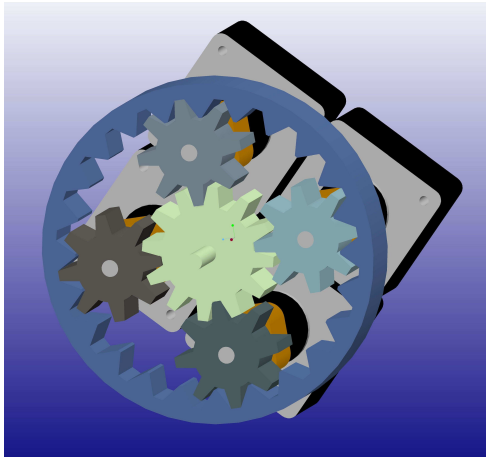

Fig. 4 Center gear concept

## 7 Conclusion and Future Work

The development of a high availability degradable safety controller on a single chip will enhance the steer-by-wire systems by reducing components, power consumption and system costs and increasing system availability, while maintaining the required safety integrity level. The proposed controller will be implemented on an FPGA platform, which serves as an ideal prototyping platform for verification and validation issues. As a long-term plan a safety controller based on ASIC is targeted. Furthermore several software issues need to be solved, such as operating system, synchronization and visualization. A communication approach based on redundant optic-fiber connections in steer-by-wire applications has been presented and needs to be implemented. Therefore, a calculation of the probability of undetected failure was demonstrated. Finally, a concept for enhancing availability at mechanical layer has been presented by using a sun wheel (center gear) concept.

Summarized, the proposed approach covers the system safety and availability at all layers of the steer-by-wire concept.

*References:*


[1] E. Dilger et al., *Steer-By-Wire Steering System for motorized Vehicles*, United States Patent, Patent No.: US 6,219,604Bl, Assignee: Robert Bosch GmbH (DE), Filed: Dec. 28, 1999, Date of Patent: Apr. 17, 2001.

[2] Kaiserliches Patentamt, Patenschrift Nr. 37435, Benz und Co.: Fahrzeug mit Gasmotorantrieb, Mannheim, November 1886

[3] Haveit EU Project, http://www.haveit-eu.org

[4] D. Bahr, R. Saykowski, J. Börcsök, 1. Hölzel, *Speicher- programmierbare Steuerungen - Die Neuausrichtung in der Signaltechnik*, Signal + Draht, Rail Signaling and Telecommunication, Nov. 2008.

[5] R. Freitag et al., *Anforderungen an das Sicherheitskonzept von Lenksystemen mit Steer-by-Wire Funktionalität I Safety concept requirements of steering systems with steer-by-wire functionality*, DaimlerChrysler, Tagung der VDI-Gesellschaft Fahrzeug- und Verkehrstechnik, Baden-Baden, 2001.

[6] J. Schomerus et al., *Ein Steer-by-Wire System für hoch-automatisierte PKW*, Fachtagung Mechatronik, Dresden, 2011.

[7] IEC Commission, *Functional safety of electrical/electronic/programmable electronic safety-related systems*, IEC 61508 Ed. 2, part 1 – 7, CENELEC, Geneve, 2010.

[8] IEC Commission, *Functional safety of electrical/electronic/programmable electronic safety-related systems*, IEC 61508, part 1 – 7, CENELEC, Geneve, 2001.

[9] IEC Commission, *The preparation of safety publications and the use of basic safety publications and group safety publications*, IEC Guide 104, CENELEC, Geneve, 2010.

[10] IEC Commission, *Functional safety - Safety instrumented systems for the process industry sector*, IEC 61511, part 1 - 3, CENELEC, Geneve, 2003

[11] IEC Commission, *Safety of machinery - Functional safety of electrical, electronic and programmable electronic control systems*, IEC 62061, CENELEC, Geneve, 2005.

[12] IEC Commission, *Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems*, IEC 61513, CENELEC, Geneve, 2001.

[13] P. Yih, Steer-by-Wire, *Implications for Vehicle Handling and Safety*, Dissertation, 2005.

[14] W. Gaupp et al., *Sicherheitsbelange aktiver Fahrdynamik-regelungen*, Berichte der Bundesanstalt für Straßenwesen, Heft F 33, Bergisch Gladbach, 2001.

[15] ISO, *Road vehicles - Functional safety*, ISO 26262, part 1 – 10, International standard under publication, Geneva, 2011.

[16] 1.Sauler, *ISO 26262-Die zukünftige Norm zur funktionalen Sicherheit für Straßenfahrzeuge*, Elektronik Praxis, 2009.

[17] ISO, IEC, *Safety aspects - Guidelines for their inclusion in standards*, 2nd ed., Geneva, 1999.

[18] J. Mayer, *Neues Redundanzkonzept für elektrische Antriebs-systeme*, Audi Konferenz Center, Kolloquium und Auftaktveranstaltung der INLUniBw, 2011.

[19] ISO, *Qualitätsmanagementsysteme - Grundlagen und Begriffe*, ISO 9000:2005, Geneve, 2005.

*[20]* ISO, *Qualitätsmanagementsysteme. Besondere Anforderungen bei Anwendung von ISO 9001:2008 für die Serien- und Ersatzteilproduktion in der Automobilindustrie, 3rd ed.*, ISO/TS 16949, VDA, 2009.

[21] B. Damir, *HAVEit project provides different levels of automated driving*, http://www.robaid.com/tech/haveit-project-provides-different-Ievels-of-automated-driving.htm, 30.07.2011.

[22] N. N., *China erprobt fahrerloses Auto*, http://www.car- it.automotiveit.eu/china-erprobt-fahrerloses-auto/id-0028540, 12.08.2011.

[23] I. Sauler, *Alle Fakten zur neuen Sicherheits-Norm für die Autoindustrie*, ISO 26262, Elektronik Praxis, 2010.

[24] J. Börcsök, A. Hayek, B. Machmur, M. Umar, *Design and Implementation of an IP-core Based Safety-related Communication Architecture on FPGA*, ICAT XXII International Symposium, Bosnia, 2009.

[25] J. Börcsök, *Models to Calculate Safety and Reliability Parameters for Embedded Systems, Computer Architecture and System Programming*, ICAT XXII International Symposium, Bosnia, 2009.

[26] M. Al-Bokhaiti, *Design and Implementation of Multi Processor-based Communication Architecture for Safety-Related Applications Using FPGA*, University of Kassel, Master Thesis, 2011

[27] G. P. Agraval, *Fiber-Optic Communication Systems*, 3rd Ed., Wiley, Hoboken, New Jersey, 2002

[28] G. E. Keiser, *Optical Fiber Communications*, 3rd Ed., McGraw-Hill, New York, 2000

[29] J. Börcsök, *Safety Bus Systems*, Fifth International Conference on Networked Sensing Systems, Kanazawa, Japan, 2008

[30] DIN V 19250, *Grundlegende Sicherheits-betrachtungen für MSR-Schutzeinrichtungen*, Beuth Publishing Company, Berlin, 1998

[31] P. Lynwander, *Gear Drive Systems: Design and Application*. Marcel Dekker, New York, 1983