Stephan Reinhofer, BSc.

Fail-operational architectures for electric propulsion systems

MASTER'S THESIS

to achieve the university degree of

Master of Science

Master's degree programme: Electrical Engineering

submitted to

Graz University of Technology

Supervisors:

Dipl.-Ing. Dr.techn. Jürgen Fabian

Institute of Automotive Engineering

Adam Schnellbach, MSc.

MAGNA Powertrain Gmbh & Co KG

Graz, November 2015

Affidavit

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbstständig verfasst, andere als die angegebenen Quellen/Hilfsmittel nicht benutzt, und die den benutzten Quellen wörtlich und inhaltlich entnommenen Stellen als solche kenntlich gemacht habe. Das in TUGRAZonline hochgeladene Textdokument ist mit der vorliegenden Masterarbeit identisch.

Datum Unterschrift

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitly marked all material which has been quoted either literally or by content from the sources used. The text document uploaded to TUGRAZonline is identical to the present master‘s thesis dissertation.

Date Signature

Acknowledgement

I would like to thank my supervisors Jürgen Fabian and Adam Schnellbach for the professional support, feedback and assistance during the whole time.

Also i want to give a big thank you to my university colleagues and friends who always supported, motivated and entertained me, not only during working on my master thesis, but at my entire time at the university.

A special thanks goes to my significant other, Lisa Haselgraber, who had to deal with me in stressful situations and always supported me when needed.

Abstract

The ascending electrification in automotive engineering enabled an increase of driver safety through implementation of passive and active safety systems. These systems protect the vehicle occupants in case of an accident or preliminary prevent accidents in critical situations thanks to driving assistance systems. However the increasing use of mechatronic components also yield to a totally different fault behaviour of an road vehicle, making new approaches for the functional safety urgently needed. Today's state of the art in automotive engineering causes safety relevant items and functions to move to a passive state in case of a fault to not disturb the remaining architecture. If there is no mechanical backup system, this inevitably leads to loss of functionality, which is not acceptable for some cases as for instance the service brake or steering.

Because of huge economizing potential in cost- and space reduction due to omission of mechanical backups, a great interest lies on increasing safety of E/E-Systems to be capable of dropping the mechanical backups as next step without lowering the current safety level. For this matter, techniques for the implementation of fault tolerance in electric and electronic systems can be adapted from other branches as for instance from railway, avionic or agricultural. After a theoretical introduction about the terminology and common fault tolerant structures and their usage in automotive architectures, a propulsion system of an electric vehicle is investigated as practical example. Firstly the operating behaviour and the error modes of the architecture are analysed to secondly convert the system to a fail-operational architecture in order to prevent safety relevant consequences caused by malfunctions or total loss.

Kurzfassung

Die ansteigende Elektrifizierung in der Automobilbranche ermöglichte in der Vergangenheit eine Erhöhung der Fahrsicherheit durch Implementierung passiver und aktiver Sicherheitssysteme. Während passive Sicherheitssysteme darauf augelegt sind den Fahrer im Falle eines Unfalls zu schützen, leiten aktive Sicherheitssysteme wie Fahrassistenzsysteme in kritischen Situationen Gegenmaßnahmen ein um einen Unfall bereits im Vorfeld abzuwenden. Die vermehrte Verwendung von mechatronischen Komponenten führte aber auch zu einem völlig neuen Fehlerverhalten des Fahrzeugs, welches neue Ansätze für die Funktionale Sicherheit notwendig macht. Der heutige Stand der Technik im Automobil sorgt dafür das sicherheitsrelevante Komponenten und Funktionen im Fehlerfall einen passiven Zustand einnehmen um die verbleibende Architektur nicht zu stören. Falls keine mechanische Rückfallebene vorhanden ist, führt dies unweigerlich zu einer Reduktion der Funktionalität, was in manchen Fällen wie beispielsweise der Betriebsbremse oder der Lenkung nicht akzeptiert werden kann.

Da ein großes Kosten- und Platzpotential in der Einsparung mechanischer Rückfallebenen liegt, besteht das Interesse die sicherheitsrelevanten E/E-Systeme entsprechend abzusichern um im nächsten Schritt die mechanischen Rückfallebenen zu entfernen, ohne eine Absenkung des Sicherheitsniveau zu erleiden. Techniken zur Implementierung dieser Fehlertoleranz in elektrischen und elektronischen Systemen können hierzu aus anderen Branchen wie der Bahnfahrt, Avionik und auch der Agrarwirtschaft übernommen werden. Nach einer theoretischen Einführung in die Begrifflichkeiten und den gebräuchlichen fehlertoleranten Strukturen bzw. deren Anwendung in automotiven Architekturen, wird als praktisches Beispiel der Antriebsstrang eines rein elektrisch betriebenen Fahrzeugs untersucht. Zuerst wird eine Analyse des Betriebsverhaltens und der Fehlermodi durchgeführt, um im Anschluß das System auf eine fehlertolerante Architektur überzuleiten, dass die sicherheitskritischen Auswirkungen von Fehlfunktionen oder eines Komplettausfalls verhindert.

Abbreviations

ADC	Analogue-digital converter
AMR	Anisotropic magnetoresistance
ARMA	Auto-regressive moving average
ASC	Active Short Circuit
ASIL	Automotive Safety Integrity Level
BMS	Battery Managment System
C	Controllability
CAN	Controller Area Network
CCF	Common cause failure
CRC	Cyclic redundancy check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DAS	Driver assistance system
DG	Differential gear
E	Exposure
E/E	Electric/Electronic
ECU	Electronic Control Unit
EMB	Electro-mechanical brake
EMF	Electromotive force
EPB	Electronic Parking Brake
FIT	Failure in Time
FO	Fail-operational
FOU	Fail-operational unit
FRA	Full redundancy architecture
FS	Fail-safe
FSU	Fail-safe unit
FTA	Fault tree analysis
FTDMA	Flexible Time Division Multiple Access
GMR	Giant magnetoresistance
HARA	Hazard Analysis and Risk Assessment
HV	High voltage
IGBT	Insulated-gate bipolar transistor
INFORM	Indirekte Flussermittlung durch On-line Reaktanz Messung
LIN	Local Interconnect Network
MOST	Media Oriented Systems Transport
MTTF	Mean time to failure
PE	Programmable electronic
PIM	Power Inverter and Motronic
PSM	Permanentmagnet excited synchronous machine
PWM	Pulse-width modulation
QM	Quality Management

RESS	Rechargeable Energy Storage System
S	Severity
SC	Star Coupler
SIL	Safety Integrity Level
SNR	Signal-to-noise ratio
SoC	State of Charge
SoH	State of Health
SRA	Shared redundancy architecture
TDM	Time-division multiplexing
TDMA	Time Division Multiple Access
TMR	Triple modular redundancy

Contents

1 Introduction

Fail-operational architectures are used in safety-critical systems and provide the application with functionality even when an error occurs. Varying on the requirements of an application, the architecture may be designed to deal with more than one failure of the same type.

The origin of fail-operational architectures lies in the aeronautic engineering. Aviation needed technical implementations which provide functionality during the whole flight. Different from other industry sectors, failure in safety critical functions might lead to devastating accidents bringing many lives to death. Precautions had to be made in order to reduce the remaining risk of losing essential functions to an acceptable low level. Lines of business which could cope with downtimes of safety related functions have a different approach than aviation in Airbuses. If an occurring downtime of a safety related function isn't triggering any hazard event, moving the function to a passive safe state is sufficient. This technique is called *Fail Silent* and signifies that an error leads to silencing the concerning function in order to exclude any interferences with other functions or rather the whole system.

The generic term *Functional Safety* summarize all applied strategies which are used to lower unacceptable risks in a system. Varying on the safety goals of a component or system, different techniques are applied. Mandatory requirements for functional safety are determined in various standards for different branches, all derived from the IEC 61508. Coming from the process technology, the IEC 61508 is the mother standard for safety related functions which are controlled with either electric, electronic or programmable electronic units. Since the standard was too generic for some branches, sub-standards were derived which focus on the specific sectors. For instance, railway, avionic, agriculture have their own safety standards, and also automotive build their own, which is the ISO 26262: Functional Safety for road vehicles.

The goal of this thesis is an investigation on fault tolerance measures and tailor an architecture which is capable of giving electric systems in the automotive sector a sufficient fail-operational ability on an economic cost level. This is achieved through assessment and adaptation of existing architectures and techniques of other branches. An altering of existing architectures to the needs of the automotive branch might be the most effective way of finding a suitable architecture.

2 Fundamentals

Defects in electronic components cause either minor faults which doesn't invoke hazardous system failures or major faults which generate dangerous situations for the user. Examples for minor faults in a car are faults in non-safety related systems as air-conditioning or an error in the entertainment system. Any error leading to unintended steering, accelerating or braking during driving can be considered as a major failure.

The objective of safety mechanisms is mitigating major faults by reducing the risk of their occurrence. Safety strategies are applied to ensure that functions fulfil what they are designed for and do not disturb their environment when failing. In order to explain common safety strategies, general terms are explained for a good understanding [1], [2].

2.1 Definition of Terms

Following terms are repeatedly stated in various safety related resources and will be important in later chapters and for a better understanding. This master thesis aims for compliance with the definitions of the ISO 26262, but only takes selected terms as fundamentals. There are only minor differences between definitions in safety related standards since they are all derived from the IEC 61508, however in case of discrepancy, the definitions in the ISO 26262 were preferred [3].

Availability

Describes the capability of a product to be in a expected state and execute its function as intended. As long as the required external resources are available, the product must provide its function in a determined time interval.

Safety and unreasonable risk

In the ISO 26262, safety is defined as the absence of unreasonable risk. Unreasonable risk stands for those situational outcomes where personal or property damage happens to an extend which cannot be tolerated. Safety measures in charge to reduce the risk to an acceptable level, though a total absence of risk is not possible.

Functional safety

The term functional safety describes the absence of unreasonable risk due to a malfunction of an Electrical/Electronic-System. Functional safety is therefore the ability to maintain a safe system state or transit it into a safe state in the presence of malfunctioning behaviour of E/E-components [3].

Component

According to the standard, a component is a low level element which is technically and logically separable and is comprised of more than one hardware or software parts [3]. In Fig. 2.1 the HV-Battery, consisting out of several battery packs, builds a component.

Element

An element can be a system or part of a system including components, hardware, software or hardware parts [3]. In Fig. 2.1 the power electronics or the fuel cell system are for instance elements according to the ISO 26262.

Item

An item can be a system or an array of systems which implement a function at vehicle level [3]. In Fig. 2.1 the whole powertrain of an electric car is declared as an item with propulsion as its main function on vehicle level.

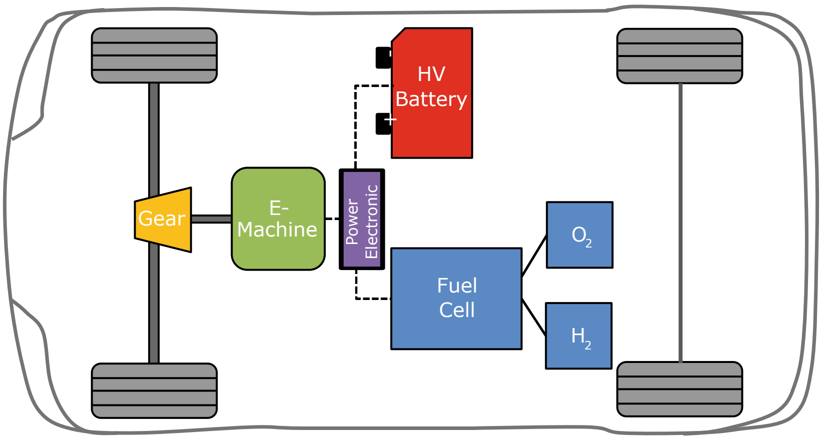


Figure 2.1: A powertrain of an electric car equipped with a fuel cell as range extender according to [4].

Fault

The cause of an error is called fault. A fault can cause an element or an item to fail. Not all faults will lead to an error of an item, but every error has a fault as root cause [5], [3].

Error

An incorrect or not intended computed, observed or measured value or condition is called an error. An error which negatively influences an element or item can lead to a failure of the system [5], [3].

Failure

The term failure describes the deviation of an element behaviour from its specifications and intended functions making the element unable to perform the function as required. Failures are visible for the environment and can have an impact on the system [5], [3].

Common Cause Failure

All failures of two or more elements or items which have a common root as trigger.

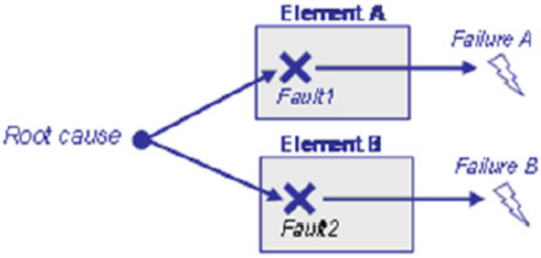


Figure 2.2: Common Cause Failure [3].

ASIL - Automotive Safety Integrity Level

Within the item definition procedure of the ISO 26262, interfaces, constraints, dependencies and interactions with other items are declared among other things. Items are assigned with an appropriate ASIL to evaluate their importance in failure scenarios. A higher level signifies higher safety requirements for the specific item. The level is determined on three factors: Severity, Exposure and Controllability. Dependent on their impact, different classes are assigned during a hazard analysis [3].

Severity

The severity is an estimation of the extent of harm to one or more individuals in a potentially hazardous situation. The classification needs to consider each person potentially at risk including possible injuries dealt to the driver, passengers and even cyclists, pedestrians or persons in other vehicles [3].

Table 2.1: Classes of Severity defined by ISO 26262 [3].

	Class			
	S0	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe and life threatening injuries with probable survival	Life-threatening injuries with uncertain survival, fatal injuries

Exposure

The exposure describes the time span in which an individual remains in a certain operational situation. Situations are either classified by their relative value in % with respect to the vehicle operation time or by their occurring frequency. The environment of the vehicle and performed driving manoeuvres must be considered to determine the exposure [3].

Table 2.2: Classes of Severity defined by ISO 26262 [3].

	Class				
	E0	E1	E2	E3	E4
Classification by duration	Unusual or incredible	Not specified	<1% of average operating time	1-10% of average operating time	>10% of average operating time
Classification by frequency	Unusual or incredible	Occurs less often than once a year	Occurs a few times a year	Occurs once a month or more often	Occurs during almost every drive

Controllability

Controllability defines the ability of affected persons to avoid a specified harm through their timely reactions. Persons involved include the driver, passengers or persons in the vicinity of the vehicle's exterior. While reactions of other individuals than the driver are hard to classify, a representative driver is assumed with the help of driver profiles. Hazards which are difficult or not controllable for the representative driver are classified with a high level. Situations which demand good reaction of more than one person to avoid the harm also lead to a higher controllability class [3].

Table 2.3: Classes of Controllability defined by ISO 26262 [3].

	Class			
	C0	C1	C2	C3
Description	Controllable in general	99% or more of all drivers or other participants are usually able to avoid the harm	90% or more of all drivers or other participants are usually able to avoid the harm	Less than 90% of all drivers or other participants are usually able, or barely able to avoid the harm

Risk and Harm

Risk is defined as the probability of occurrence of harm combined with its severity. The standard for functional safety in road vehicles limits the term harm to personal injury or damage to the health of persons. Dependent on amount and severity, the risk can either be acceptable or unreasonable high, in case of the latter safety mechanisms have to lower the risk [3].

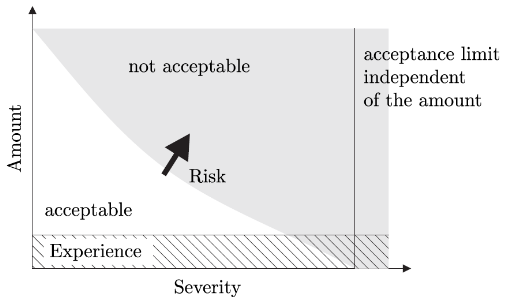


Figure 2.3: Graphical description of acceptable and non unreasonable risk, according to [5].

Safe state

A safe state represents a condition of an item without unreasonable risk radiating from it. This state can either be operational or passive [3].

2.2 Safety vs. Availability

Beside the definition of safety and availability listed in the previous section, a further examination gives a good understanding about the difference of these two, sometimes mistaken, factors. Safety and availability do not necessarily rely on each other: There are systems which are safe but unreliable and system which are highly reliable but unsafe. In many cases these both terms even stand in conflict to each other, where increasing one does result in decreasing the other.

Reliable but unsafe systems are characterized that their components generally work as specified and fulfil their assigned tasks. For instance, a chemical plant manufacturing chemicals has a leakage releasing toxic substances to the environment but still continues on working is a reliable, but unsafe system. The safety could be increased by stopping the procedure as soon as any leakage is detected, which would lower the overall availability of the plant.

Safe but unreliable systems are characterized that their components do not provide the functions they were designed for but at least do not deal any harm to its surrounding environment. For instance a vehicle which doesn't start at all if any part components of its architecture failed is safe but highly unreliable. To increase the availability, one could allow to start the vehicle even when some serious defects might influence the proper functionality. This would lead to an increased operating time of the vehicle by lowering the overall safety of the system. Further practical examples concerning the conflict between safety and availability can be found in [6].

2.3 Failure attributes and allocation

An investigation about the behaviour, attributes and scene of faults will help developing strategies against them. In general the injection form can be divided into two categories: *Systematic* and *random failures*.

2.3.1 Systematic failures

Systematic failures can be injected during every phase of a product life cycle. This includes conceptional failures in the development, variance of material in the production, incorrect repair/maintenance work or not properly decommissioning of a component. To minimize systematic failures, most safety related standards propose life-cycle strategies and models to identify and eliminate mistakes in each stage [7].

Software failure

Software assumes the correct code execution by the hardware, hence it is not directly exposed to random failures and only vulnerable to systematic failures. Incomplete specifications, coding errors or logic mistakes may lead to unknown system states that undermine the intended sequence of the program. Neglected interactions between items or their time schedule are also a serious root of systematic software faults [8],[6].

Systematic hardware failure

Systematic failures can be added to a component unintentionally in different stages of its life cycle as explained before. For systematic hardware failures, a further distinction by means of duration of the fault leads to two systematic sub types of hardware faults:

- **Permanent**
  Permanent hardware faults may be injected by design errors or material impurity in the production process. For electronic hardware, a material impurity can result in a lower conductivity, which accelerate material transport by electromigration. Electromigration is a progressive act which affect the width of circuit paths thus also the resistance. The fault remains in the element and reduces the life span [7].
- **Intermittent**
  Intermittent hardware faults result from external influences by the item environment. The most significant influences are varying temperatures and stress of mechanical contacts. The life time of an electric component is significantly decreased when driven in higher temperatures, because of that, reliable tests use fluctuating heating as a simulation of the ageing process. Intermittent faults often convert to permanent faults over time [7].

2.3.2 Random failures

Random failures occur non-periodic, thus are not reproduceable during tests or in the field. A failure rate is introduced to describe the occurrence of failures per time of a system or component, and is often measured with the unit FIT (Failure In Time), where one FIT stands for one failure during 10^9 hours. As systems consist out of several subsystems which again are composed out of components, the total failure rate of a system is approximated by summarizing all single failure rates of the components. This approximation is only accurate for small partial failure rates [2], [1].

$$\lambda_{total} = \sum_{i=1}^{N} \lambda_i \tag{2.1}$$

The amplitude of the failure rate varies over time and has a graphical characteristic of a bathtub curve (Fig. 2.4.): A high failure rate at the beginning caused by material variations, an almost constant failure-rate during life time with randomly distributed errors, and an increasing failure-rate over time due to ageing effects of the material.

The main obstacle within this treatment is the acquiring of component or hardware unit failure rates. Through documentation in the production process, the failure rate in the infant mortality area can be recorded, however is not of interest. To determine the failure rate for the life time of the product, artificial ageing processes are applied to capture the length of the useful life area and the average failure rate. As soon as the failure rate increases significantly, the end of life of the product is reached.

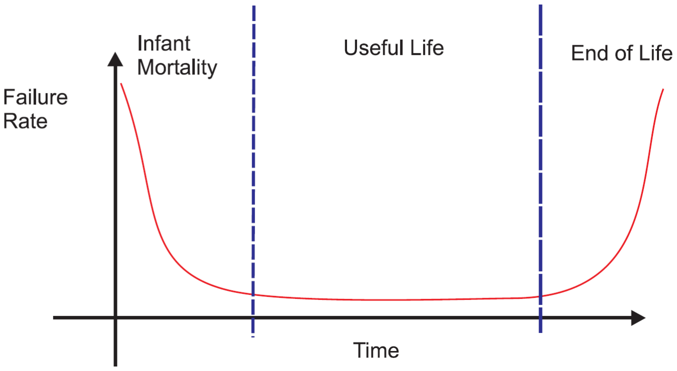


Figure 2.4: Failure rate of electronic components shows a bathtub characteristic according to [2]

For an almost constant failure rate as given during life time, the average time until the first failure occurs can be calculated by building the reciprocal of the failure rate.

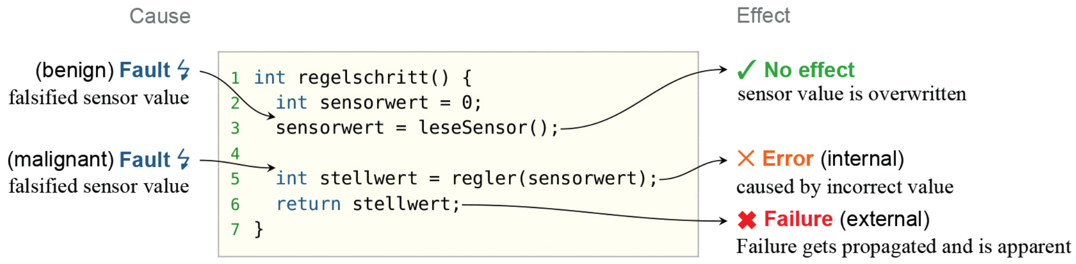
$$MTTF = \frac{1}{\lambda} \tag{2.2}$$

The reciprocal is named *Mean Time to Failure* and is often listed in data sheets of electric components and hardware units.

Random Hardware failure

Random hardware failures become manifest on hardware units of the low level layer like memory, arithmetic elements or bus connections. They occur as a bit error and have a temporary influence on the hardware and software. The primary cause of random hardware failures is ionizing through neuron or alpha radiation. The radiation leads to a charge displacement in a semiconductor, and if high enough, resulting in an inversion of a logic state. Another source for bit errors are alternating electromagnetic fields which cause disturbing pulses on the communication lines of a system. When a bit error occurs in a critical phase of a component, the error can spread through the architecture creating an element or item to fail. While disturbance by electromagnetic fields is suppressed by shielding of the communication paths, cosmic rays are an omnipresent source for the ionization process increasing proportional with the altitude [7].

A hardware solution against ionization particles is done by increasing the required charge to perform a logic state change. This hardening process is realised by either the use of bigger capacitors or appropriate devices which still work correct under the influence of a charge drift. Because of the higher costs and latencies in a hardened circuit, this method is mostly used in difficult environments as aeronautic and space engineering [7]. The effects of random hardware errors on software relies on their time of occurrence and is explained with a coding example below in Fig. 2.5.



```
int regelschritt() {
  int sensorwert = 0;
  sensorwert = leseSensor();

  int stellwert = regler(sensorwert);
  return stellwert;
}
```

Figure 2.5: Impact of transient hardware faults to software according to [7].

If a failure occurs right after the initialisation of sensorwert, but before the return value of leseSensor() is written on it, the defect is removed by the overwriting. If it occurs right after the assignment, sensorwert is corrupted and is now a source for progressive failures. In the example, the functions regler uses sensorwert as transfer parameter what distributes the failure on stellwert. Once the value of stellwert is returned, the fault gets visible due to a wrong actuating [7].

3 Fault tolerant structures

Fault tolerant structures are used to protect safety related systems against faults which trigger the loss of essential functions needed in hazardous situations. Dependent on the importance of an item and its role in the architecture, a certain tolerance against faults can be necessary. The required time to move a system, or more specific a vehicle, into a safe state is the most important factor for determining the required level of fault tolerance. If it is not possible to move the system immediately to a safe state as it is the case with aircrafts, vital functions must be kept available during operation time even under faulty conditions. For manual controlled road vehicles the situation is not as strict, as a full halt of the vehicle is considered as a safe state which is reachable within seconds. With the utilization of autonomous driving, automated control functions must stay operational until the vehicle is under control of the driver.

3.1 Degrees of fault tolerance

To tailor fault tolerance to the needs of a specific application, different levels are introduced. Occurring faults then lead to a transition to lower degrees of fault tolerance with a safe state as last option. By this method, an item always stays in a known state and the remaining architecture is aware of that condition. The intended flow and the properties of these levels are as following:

Fail-operational – FO

Elements or items on a fail-operational level can cope with one internal component failure and remain either fully operational or with degraded functionality. After the first failure, the system loses its fail-operational behaviour and degrades to a fail-safe system. A second failure of a related component cannot be covered making a transition to a safe state necessary. Although through adding redundancy, the fail-operational behaviour is enhanced with multiple FO-layers – usually one per additional component. Adding several fail-operational layers through redundancy is a typical technique in aeronautic engineering, but not reasonable in automotive due to the increasing costs, weight and space per added component. Also the probability that two redundant components fail within a short time span is very low, excluding common cause failures [9].

Fail-safe – FS

Fail-Safe systems are moved to a safe state as soon as one or more failures take place. When the system directly reaches its safe state without external help, it is declared as passive fail-safe, if interactions with other architecture parts are necessary to move a component into its safe state, it is named active fail-safe [9].

Fail-silent

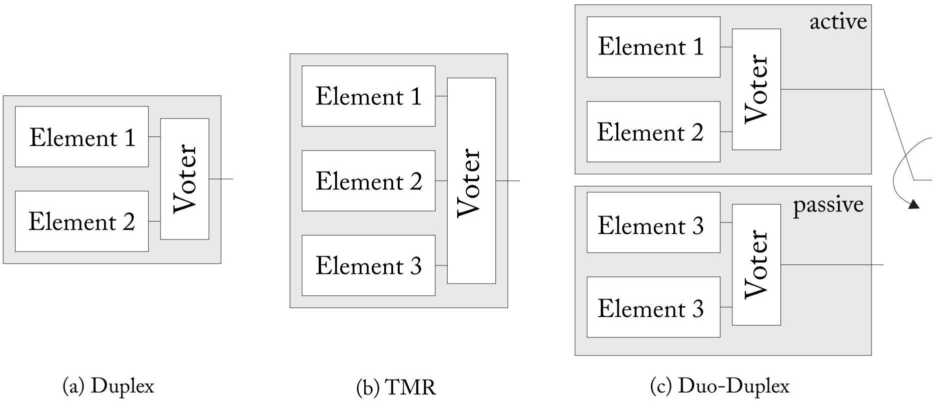
Fail-silent components shut down after one ore more occurring failures and quit their functionality. They appear passive and don't send any output to avoid disturbance of the remaining system [9].

3.2 Measures against hardware failures

3.2.1 Static redundancy with majority voting (M-n systems)

Fault-tolerant architectures usually rely on redundancy to prevent consequences from hardware failures. The most widespread hardware structure is static redundancy combined with a majority voting, also called M-n-Systems. Within this structure, critical elements of a safety related item are multiplied. They are fed with the same inputs and provide, if functionally correct, the same output. To determine if an output is correct or not, all outputs from the elements are fed to a voter. The voter then compares the outputs of the multiplied elements and assumes that the output given by the majority is the correct one. Only the result of the majority voting is forwarded to the output of the item. Possible wrong outputs are suppressed as long as not the majority of the elements deliver the same wrong output values at the same time.

On the basis of majority voting, an element has to be at least tripled to build a 2 out of 3 system. In principle, any amount of elements and majority limit is possible in M-n-Systems, where **m** describes the limit needed for the majority, and **n** the amount of elements used. The minimum set for majority voting, a 2 out of 3 system, is also called *Triple Modular Redundancy* (TMR) and can still operate after one element fails. After one failing element, TMR degrades to a *Duplex System* where the voter simply compares the outputs of the elements instead of a majority voting. The Duplex system needs to shut down when the output of the elements differ, since there is no way in discriminating which element delivers now the correct values and which the wrong ones. A weak spot of M-n systems is the voter: The majority voting or comparison is also realised with an electronic component which might fail as well. However, failures of the voter are not very common, thanks to their simple internal architecture that makes them very reliable. To exclude any impacts of voter failures, either a *Duo-Duplex system* with dynamic reconfiguration can be used instead, or a tripling of the voter clears the structure from single point failures.



(a) Duplex (b) TMR (c) Duo-Duplex

Figure 3.1: Structures with Majority Voting: (a) Duplex System, shuts down when one element fails (b) Triple Modular Redundancy, allows full performance after one failure (c) Duo-Duplex System, has cold standby which is activated when any part (Element or Voter) fails according to [5].

Built with the same elements, M-n systems give protection against random hardware failures. With an installation of similar elements of different manufacturers instead of multiplying one type, a diversity concept is accomplished that protects against common cause failures caused by design or specification mistakes. The disadvantages of M-n systems are the higher costs, power consumption and weight which goes hand in hand with an increasing amount of elements [8], [5].

3.2.2 Dynamic redundancy with hot or cold standby

The idea behind dynamic redundancy is a reconfiguration process triggered by a fault detection routine. As with static redundancy, further elements are added to the basic structure as backup solution, but instead of a parallel operation of primary and backup elements, the reconfiguration process switches between the elements. There are two different approaches concerning the state of the backup element:

- **Hot standby**
  The secondary element is running simultaneously with the primary one, having the same state and performing the same actions, but its output is not connected to the system output.
- **Cold standby**
  The secondary element stays offline while the primary one is working correctly. In case of a failure the reconfiguration process must wake up the backup element and initiate it to a former state of the primary element. To do so, the state of the primary element must be saved as an image on a periodic basis.

A main benefit of hot standby is the short exchange time between elements which comes at the expense of wearing out the backup element to the same extent as the primary one. Cold standby solves the wear and tear with passivated backup, which then leads to higher exchange times due to initialisation routines. For micro controllers with comprehensive software, the state recovery might lead to an information loss dependent on the immediacy of the image.

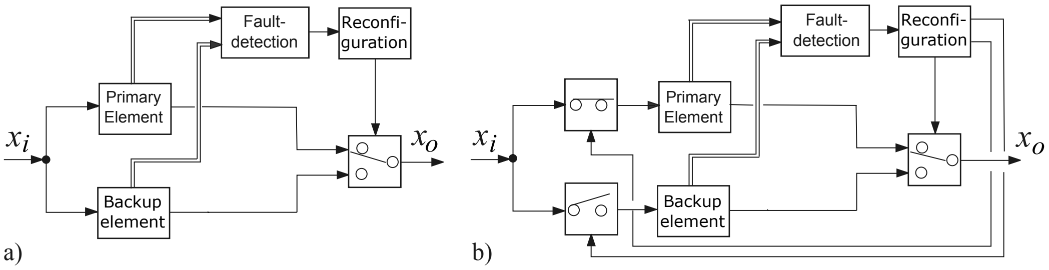


Figure 3.2: Dynamic Redundancy: a) with hot standy and b) with cold standby according to [8].

For dynamic redundancy a reliable fault detection is the most essential part as it initializes the reconfiguration process: The dynamic redundancy is only as good as its fault detection routine. An easy distinction between faulty and correct elements is applicable when fail-silent elements are used: These elements do not send any output when they fail, thus the reconfiguration block is triggered as soon as no data is retrieved from the primary element. Still fault detection is not omitted with this method, but moved to the interior of the fail-silent element [8].

3.2.3 Graceful degradation

Systems with inherent fail-operational behaviour degrade to lower fault tolerance levels when failures occur. An overview of the amount of tolerated failures and the fault behaviour of static and dynamic hardware redundancy strategies is summarized in the table below.

Table 3.1: Behaviour and degradation of static and dynamic hardware redundancy according to [9].

		Static redundancy		**Dynamic redundancy**	
Structures	Number of elements	Tolerated failures	Degradation	Tolerated failures	Degradation
Duplex	2	0	FS	1	FO – FS
TMR	3	1	FO – FS	2	FO – FO – FS
Duo-Duplex	4	1	FO – FS	–	–

Dynamic redundancy on one hand can tolerate more failures with the same amount of elements, but on the other hand requires a solid failure detection which presuppose a detailed knowledge of the element behaviour. With static redundancy, the fault detection is conducted by the voter and relies on discrepancy of the output signals only. This keeps the fault detection at a simple level with low requirements on resources. As disadvantage, if one element remains, the voter cannot tell if the output coming from it is correct or not, thus needs to terminate the output forwarding [8], [9].

3.3 Measures against software failures

3.3.1 Static Redundancy through repeated Execution

A straightforward implementation of fault tolerance into software systems is rerunning the same software several times. Transient faults coming from the hardware won't affect all cycles in the same way, thus this method protects against unintended state changes caused by random hardware failures. Systematic failures cannot be tolerated with this strategy since they lead to the same output after every run.

3.3.2 Static Redundancy by N-version programming

The n-version programming approach uses the same technique in software as M-n systems use in hardware. Several alternatives are programmed independently for the same specification. The main and the alternative software is executed simultaneously, their outputs are compared, and only a correct value is forwarded.

To ensure independence, different programming teams, software languages and compilers are used. This increases the costs, often complicates documentation and the servicing of the item. Analogous to the hardware, the diversity concept protects the software from systematic failures. Only failures inside the specifications are not covered [10], [8].

3.3.3 Dynamic Redundancy with Recovery Blocks

Recovery blocks are a dynamic redundancy concept realised in software. Within this concept, an item contains several alternatives to the main code, as with n-version programming. Instead of running all alternatives simultaneously, only one at a time is executed and its result is checked afterwards by an acceptance test. If the acceptance test detects an error, the previous state is restored and the next code alternative is chosen. When there are no more alternatives left, the whole software item fails. Problems may arise through intercommunication of a running alternative with other processes followed by a failed acceptance test. Other processes need to be informed about the corrupted state of their received data, otherwise consequential failures may be distributed within the system [10].

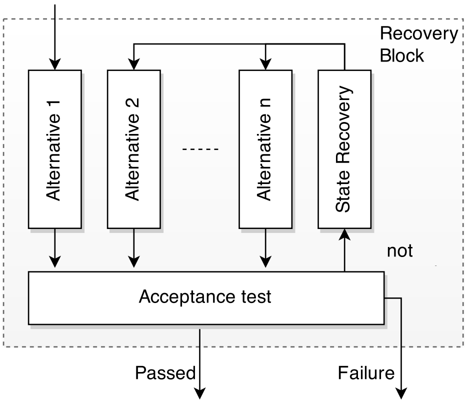


Figure 3.3: Recovery blocks as dynamic software redundancy [10].

3.4 Fault detection methods

The importance of fault detection for dynamic structures were highlighted in the concerning sections 3.2.2 and 3.3.3. Few techniques are now briefly described to give an methodical insight, a detailed description would go beyond the scope of this thesis.

3.4.1 Threshold monitoring

Output signals of a device are monitored and compared to defined threshold values. As long as no given thresholds are reached, no malfunction is detected [8].

3.4.2 Plausibility checks

Plausibility checks try to confirm the correct state of a component by feeding a test signal to the input which shall cause a certain output signal. If the acquired output matches with the expected template, the component is assumed to work correct [8].

3.4.3 Signal analysis

Signal analysis methods are applied on periodic or stochastic signals which are measured directly. Signal models are build with the help of correlation functions, frequency spectra or ARMA (Auto-regressive Moving Average) models. The goal is an extraction of characteristic values out of the measured signals which then are used to judge if an error is present or not. Characteristic values are for instance variances, amplitudes or frequencies [8], [11].

3.4.4 Process analysis

Process analysis may be used if there are at least two or more signals which are related to each other. A mathematical process model is build that mimics the behaviour of the original system. With the help of this model, methods for parameter estimation, state estimation, state observers or parity equations are performed. Again characteristic values are synthesized, as for instance parameters, state variable or residuals [8], [11].

4 Physical and logical components of an architecture

In this chapter generic components and elements of an electric architecture are presented and the topologies and connection strategies are discussed. Few systems that provide control functions are build without computers nowadays and as the implementation of specific functions is realised by software, the hardware components and their interactions are mostly the same. In vehicles, the task of the electric system architecture is the implementation of high level functions which are controllable by the driver. These high level functions are for instance steering, accelerating or braking. The architecture must be sensitive to the demands of the driver and also to environmental circumstances to maintain a high level of availability and safety.

4.1 Sensors

Sensors detect environmental quantities by using physical or chemical effects. Measurement principles are based inter alia on mechanic, inductive, capacitive, magnetic, piezoelectric, optical or thermoelectric effects. By adopting a measurement principle, a quantity is converted into an electric signal which then is usually amplified to prevent information loss due to low signal-to-noise ratio (SNR) and adjusted to the interface restrictions of connected components. In case of smart sensors an amplifier increases the level of the detected signal and a micro-controller in the sensor interior extracts the information out of the signal, digitize it, and sends it to connected components using a declared communication protocol. Simple sensors only forward the analogue signal to their outputs, the postprocessing, and with some measurment principles also the level adjustment, is then carried out by external connected components.

The correctness of gathered information is critical in safety related systems to avoid wrong controlling based on false values. The diagnostic coverage of fault detection mechanisms must be correspondingly high to ensure fail-silent behaviour with no forwarding of corrupted data. Sensor failures are either detected by build-in self-diagnosis or by using a duplex structure as seen on page 13. If a system heavily relies on the measured input quantity, fail-silent behaviour is not sufficient and further redundancy is implemented to ensure the availability of the sensor signal, as for instance with a TMR [12], [13].

4.2 Electronic Control Unit

Electronic control units build the bridge between the measured data from sensors and the desired outputs on the actuators. Their resources vary with the required functionality, but the internal structure is mostly the same for all types of control units. While prior units relied on hard wired analogue circuits, all present units are equipped with computer cores and their functionality is determined by the processed code. Program code and state describing values are stored in non-volatile flash memory, intermediate results and variables are stored either in volatile or non-volatile memory. Microcontrollers usually are monitored by simple hardware components called watch-dogs which can initiate a software reset. States and simple calculations of the microcontroller are monitored, but only to a low extent due to the simple construction of this components. Signal sequences of inputs are also verifiable in software with plausibility checks when their physical behaviour is known [2], [1].

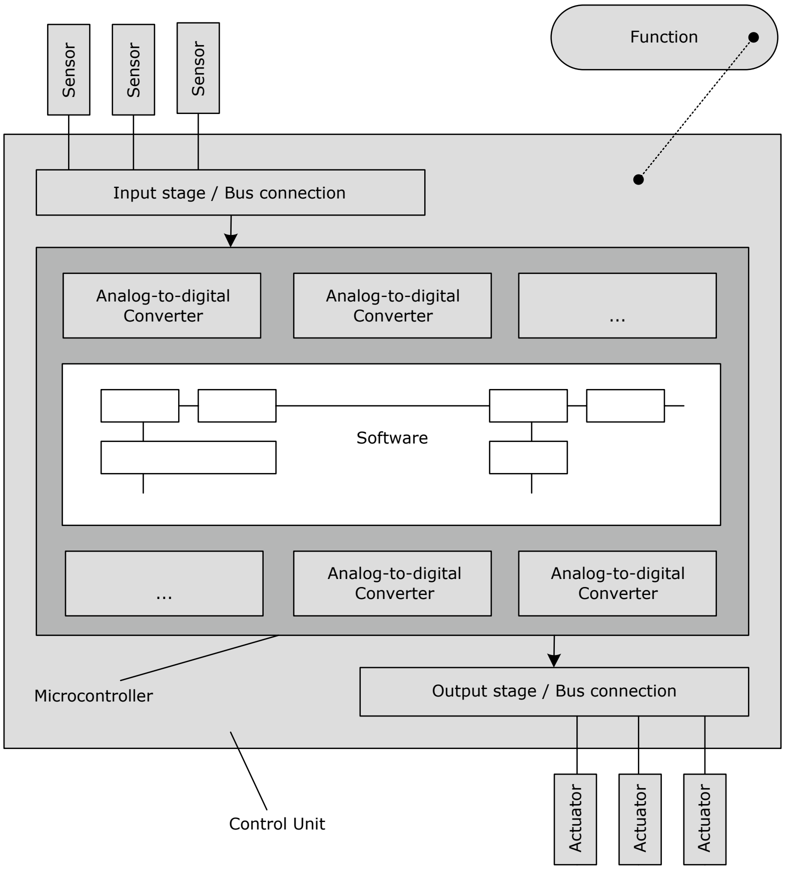

Sensor
Sensor
Sensor
Function
Input stage / Bus connection
Analog-to-digital Converter
Analog-to-digital Converter
...
Software
...
Analog-to-digital Converter
Analog-to-digital Converter
Microcontroller
Output stage / Bus connection
Control Unit
Actuator
Actuator
Actuator

Figure 4.1: A simplified view of an electronic control unit according to [1].

4.3 Actuators

Actuators are the back end of an architecture, finally executing computed functions based on the inputs of the sensors. The functionality of actuators is as crucial as the one of sensors, and due to the mechanical components inside the actuator, they are more at risk to fail. When several actuators are assigned to the same high level function, as for instance four electro-mechanical brakes (EMB) for the braking system, that alignment already supply fault tolerance with reduced performance after one single point of failure. But not all actuators are electro-mechanical, for instance a Light Emitting Diode (LED) displaying a warning signal for the driver is also classified as actuator.

For functions with no intrinsic redundancy inside the architecture, fail-operational behaviour is achieved by dynamic redundancy. Tripling of electro-mechanical actuators is avoided in automotive due to the increasing weight and costs, thats why TMR structures are not applicable and Duplex structures with fault detection mechanisms are preferred. For the fault detection, sensors typically monitor current, force, torque or motion of an actuator to determine its current state. Extending only the least reliable parts of an actuator with redundancy is also a possibility to achieve a low level of fail-operational behaviour [9], [12].

4.4 Physical system arrangement

The communication and energy supply for sensors, actuators and their control units must be provided by an infrastructure. In vehicles, the physical connection is realised with a cable harness: cable runs are bundled and only separated for a short distance at their end point to the component [2]. Communication and energy lines are both wired within the same cable harness, the logical connection between architecture components is divided into three design types.

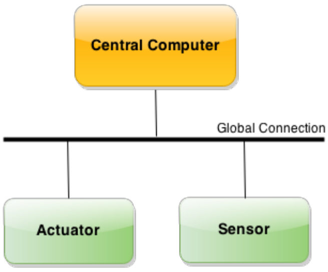


Figure 4.2: Centralised architecture according to [12].

4.4.1 Centralized Architectures

In centralized architectures, computing resources as processing units, memory and IO-peripherals are gathered and placed closely. Functions provided by software are implemented on the central computer which then controls sensors and actuators over communication lines. The advantages of this alignment is the overall reduction of redundancy along the architecture. The amount of sensors and actuators is not affected, but their control units are summarized into one redundant central computer. The susceptibility of this architecture is the central computer, as failing of the same relieves the architecture without data processing [14].

4.4.2 Distributed Architectures

In distributed architectures, every sensor and actuator is equipped with an independent computing node providing functions instead of a centralised software. The computing nodes are interconnected over a bus system which allows data sharing and communication. An adoption of functions by a neighboured micro-controller in case of failure is possible if the nodes are provided with sufficient performance or less important functions are deactivated. In matter of overall size and weight, distributed architectures claim more resources than centralised ones [14], [15]. The available bandwidth of the communication system is shared between all computing nodes, thus is limiting the amount of linkable computing nodes within the architecture. Real-time criteria might not be met at a certain amount of connected nodes.

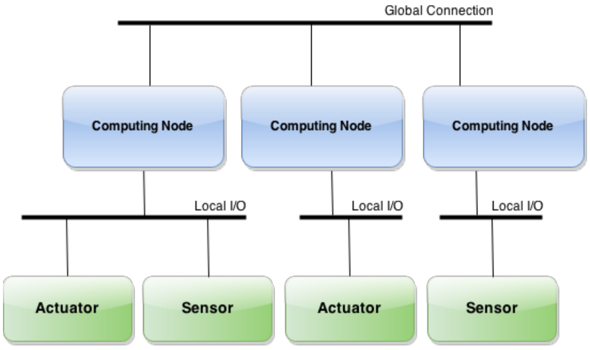


Figure 4.3: Distributed architecture according to [14] and [12].

4.4.3 Hybrid architecture

The hybrid architecture is a combination of a distributed and a centralised architecture. The architecture is partitioned in sub-systems where each follow different functional objectives. Each sub-system has its own computing resources and is connected to required sensors and actuators to perform their functions. A centralised computer system is needed to coordinate the sub-systems effectively and to preclude commands on units that order contrary states or outputs [14].

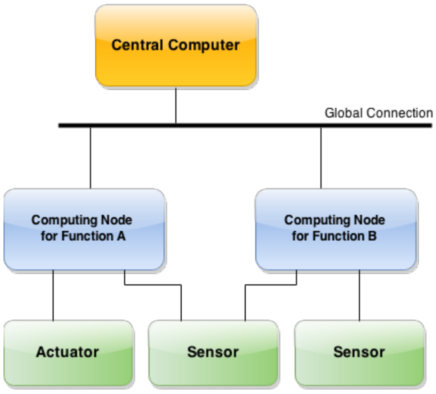


Figure 4.4: Hybrid architecture according to [14].

4.5 Energy system

In vehicles driven by combustion engines the electric energy is provided by two components: a battery and a generator which is also named alternator. The alternator was firstly included to produce electricity for the lights of the vehicle and was realised as DC generator. Meanwhile a three phase synchronous generator (claw pole generator) is used due to its higher efficiency and broader speed range. The generator is connected to the combustion engine and branches off kinetic energy via a v-belt in order to convert it into electricity. Through gearing, the speed of the combustion engine is translated to higher speed for the generator to supply the energy system even when the combustion engine is on idle speed. Nowadays the alternator does not only provide electricity for light but for an increasing amount of electric components [13].

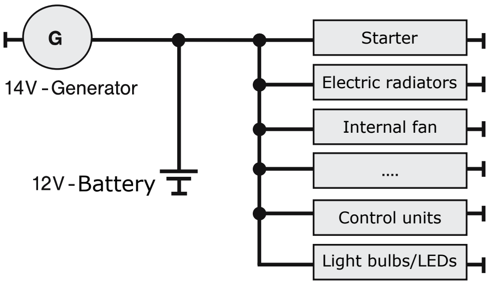


Figure 4.5: Generic electric network with one voltage level for vehicles driven by combustion engines according to [13].

In hybrid vehicles the 14 V architecture is upgraded with a second voltage layer. With the degree of hybridization, the voltage level of the second layer increases, even up to several hundreds of volts if a sole electric driving is intended. Usually both layers are connected over a DC/DC converter which allows a power exchange between the layers. With the DC/DC converter as connection, the generator for the low level layer is omitted as the low level system is powered through the high voltage system. In Fig. 4.6 an electric network of a plug-in hybrid with range extender is displayed. By removing the range extender from this architecture, the energy system in Fig. 4.6 also represents an architecture of an electric car.

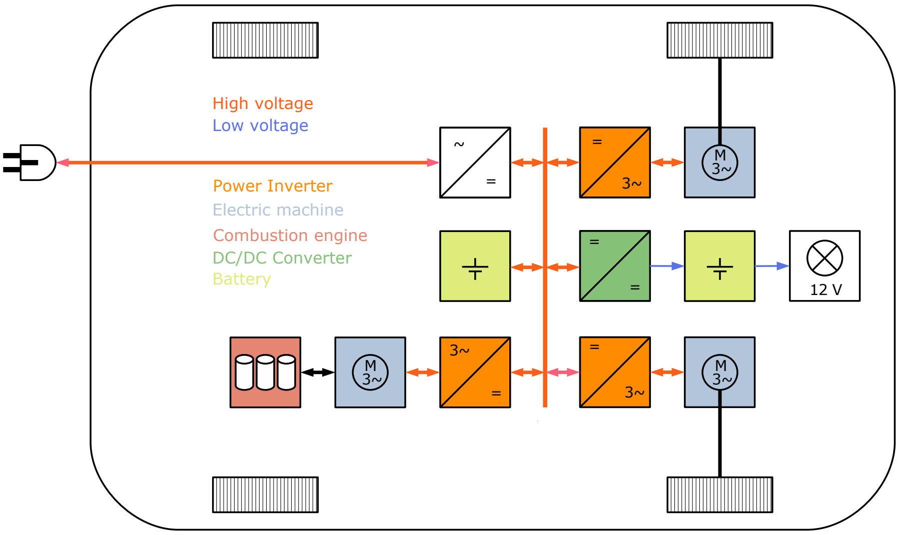


Figure 4.6: Example of an electric network of a hybrid plug-in vehicle with a combustion engine as range extender according to [4].

In terms of functional safety, the presented hybrid architecture provides a redundant supply of electric energy by either the high voltage battery or the combustion engine. Also the low voltage level layer is supplied redundantly by the DC/DC converter and the 12 V battery. If the range extender is removed, the remaining architecture portrays a pure electric vehicle. The energy supply from the combustion engine is then lost, but the fail-operational power supply behaviour not necessarily with it. Modern high voltage batteries are equipped with an intelligent Battery Management System (BMS) that monitors the state of single battery cells. Cell temperature and voltages are often used as indicator to determine the State of Charge (SoC) and the State of Health (SoH) of the battery cells. Furthermore, the BMS performs a charge balancing between cells to avoid overloading or deep discharging of single cells. If a cell or group of cells is assumed to be defect by the BMS, it is isolated from the battery and is not used for energy storage any more. This mechanism corresponds to a graceful degradation of the overall voltage level of the battery, leaving the remaining architecture with decreased but not without power supply [4].

As comparison to energy systems in automotive, the generic structure of an electric network in an aircraft is displayed in Fig. 4.7. In avionics, elements and items are assigned, dependent on their importance, to three priorities: vital, essential and non-essential. Vital or essential systems provide important functions during and after emergency landing respectively, non-essentials supply comfort. Dependent on their priority and their power consumption, loads are grouped and connected to an appropriated layer. The layers are divided into an AC- and a DC-net and are connected via rectifiers and inverters that allow a power exchange during healthy state. Circuit breakers are implemented between every layer to offer an isolation of faulty network parts. For instance if there is a lack of energy due to a generator fault, non-essential functions are disconnected to ensure a supply of the most important functions.

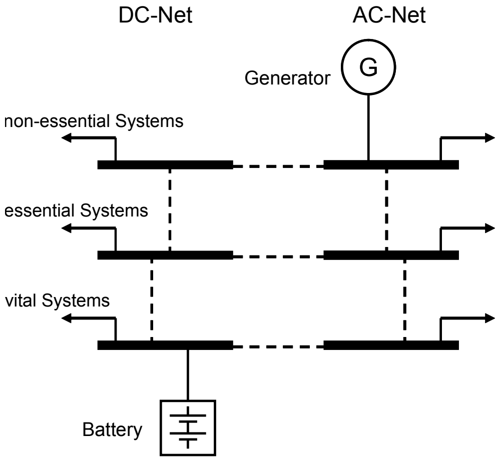


Figure 4.7: Basic hierarchical electric network in aircrafts according to [14].

Between all electroconductive compartments of the aircraft an equipotential bonding must be placed to avoid high potential differences between compartments and systems caused by static charging or lightning. This requires the layers of the electric network to have the same ground potential in all switching scenarios [14].

4.6 Communication System

Bus systems provide communication between several members which are connected over the same physical wires. Strategies which manage syntax, information packaging, channel coding, detection of transmission errors and media access control on the shared communication resource are called bus protocols. Bus systems are widely spread as communication tool and there are many protocols around, each specialized on specific applications. Established protocols in the automotive branch and their qualities are displayed in Table 4.1. In terms of functional safety, deterministic behaviour for meeting real time criteria and robustness against external disturbances are the most important objectives. The strategy how a bus member retrieves access to the bus has a major impact on the latency time between transmitter and receiver which should be ideally as low as possible [2].

Time-triggered vs. event-triggered

Communication activities on a bus system are either initiated by events or by time. In case of event-triggered protocols, an upcoming event as for instance a change in a measured value, initiates the sensor to transmit the new value to an ECU inside the bus system. Secondary communication might then be triggered by the ECU to adjust an actuator. Event-triggered protocols are probabilistic which means that the exact time of the bus usage and the delay time can not be foreseen. In case of multiple requests for bus writing access, the member with the highest priority receives access.

Table 4.1: An overview of different bus protocols used in automotive [16].

	LIN	CAN	FlexRay	MOST
Application	Low-level communication systems	Soft real-time systems	Hard real-time systems	Multimedia
Triggering	time-triggered	event-triggered	time-triggered (nested event)	time or event
Bus Access	Polling	CSMA/CA	TDMA /FTDMA	TDM/CSMA
Control	Single master	Multiple master	Multiple master	Timing master
Bandwidth	19.6 kbps	500 kbps	10 Mbps	24.8 Mbps

Time-triggered protocols are deterministic i.e. the time it takes to send and receive a message over the bus is identifiable. Deterministic behaviour is essential for hard real time applications, where belatedly received informations lead to a failing of the system. Time-triggered protocols reserve time slices for each member in the communication system. Each member retrieve a time slice where it periodically has control of the bus. The period length increases with the amount of members connected to the bus thus with increasing amount of members, a higher data rate is needed to get the same period length between time slices [16], [17].

Due to the urge of deterministic behaviour in safety critical systems, the FlexRay protocol is the most promising. FlexRay can deal with optical and electrical mediums and is decoupled of the network topology: It supports bus, star, cascaded star and hybrid network topologies. However the most used topology for safety related applications is a bus topology with dual-channel setup. The second channel simultaneously transmit the same data to achieve a fault tolerant communication system.

To support event-triggering in FlexRay, a dynamic segment is optionally added to the time period which works with Flexible Time Division Multiple Access (FTDMA) instead of TDMA as bus access method. With FTDMA, every bus member retrieves a mini slot in the dynamic segment which is extended by several slots if the member claims the bus access during his slot. Mini slots of other bus members inside the dynamic segment are then delayed. On one hand the dynamic segment provides FlexRay with the possibility of asynchronous data transfer, which allows increased data throughput or wrapping of event-triggered frames in the dynamic segment. On the other hand the overall time interval is raised which leads to higher waiting time for each bus member until bus access is granted [16], [17].

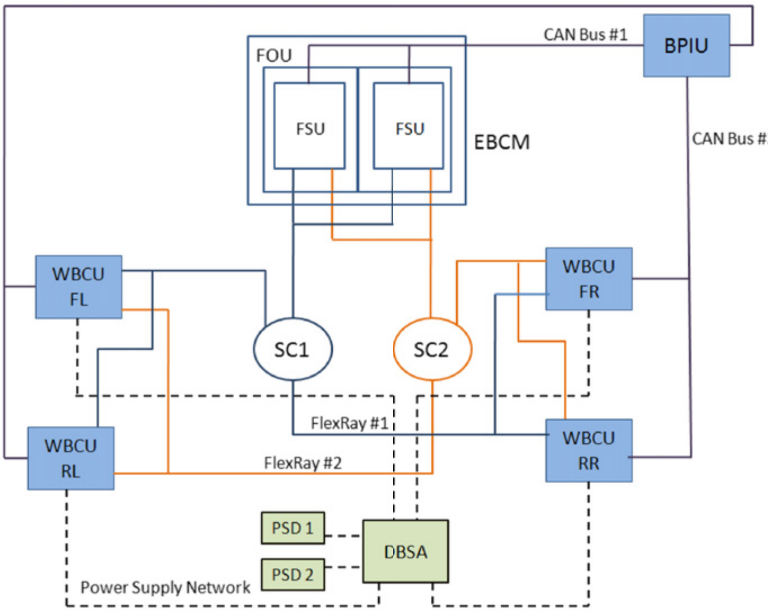
5 Fault tolerant architectures

This chapter exhibits and analyses fault tolerant architectures proposed by various authors in order to show the state of the art and typical usage of this technique.

5.1 Fail-operational brake-by-wire systems

With the introduction of x-by-wire systems as next step towards autonomous driving and further electrification of main vehicle functions, the reliability and safety are essential, as mechanical or hydraulic backup systems are removed within these concepts. Fault-tolerant architectures are the key technology to implement steer-by-wire, brake-by-wire or drive-by-wire systems with a high level of safety.

In [18], a fail-operational architecture for a brake-by-wire system is developed along with the ISO 26262 as guideline for evaluating hazardous situations. In their preliminary hazard analysis, they identified a total loss of braking and vehicle instability due to loss of braking as the most severe cases.



BPIU - Brake pedal interface unit
EBCM - Electronic brake control module
WBCU - Wheel brake control unit

SC - Star coupler (FlexRay)
DBSA - Diode bridge switch arrangement
PSD - Power signal distribution

Figure 5.1: Proposed fail-operational brake-by-wire architecture in [18].

The BPIU builds the human machine interface, sensing the brake request of the driver and forward this to all four brakes (WBCU) over CAN bus #2 and #3 and to both Fail Silent units of the EBCM via CAN Bus #1. The WBCU is a FS unit applying either correct brake force or none with two wheel speed sensors, including an ECU and a brake actuator in its interior. All WBCUs are connected with two Flexray Star Couplers (SC) that enable them to share and vote on all signals and data of the wheel speed sensors and commands from the EBCM. The EBCM builds the central control unit of the architecture, using dynamic redundancy with hot standby of two FS units to ensure fail-operational behaviour. It retrieves input values of the speed sensors and uses that information to determine relevant variables of the vehicle dynamic to alter the drivers brake demand to maintain stability. The energy supply of the architecture is divided into front and rear for the WBCUs, where PSD 1 supplies the front and one FSU of the EBCM, and PSD 2 supplies the rear and the second FSU. To avoid single point failures due to PSD faults, the DBSA distributes the power of the remaining PSD to the entire vehicle in case of an error. The reliability block diagram in Fig. 5.2 shows how the component reliabilities contributes to the system reliability, by accepting that a diagonally pair of WBCUs are necessary to decelerate without loss of stability.

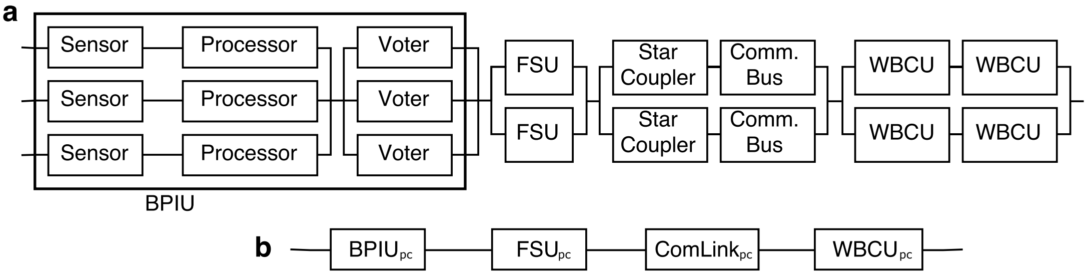


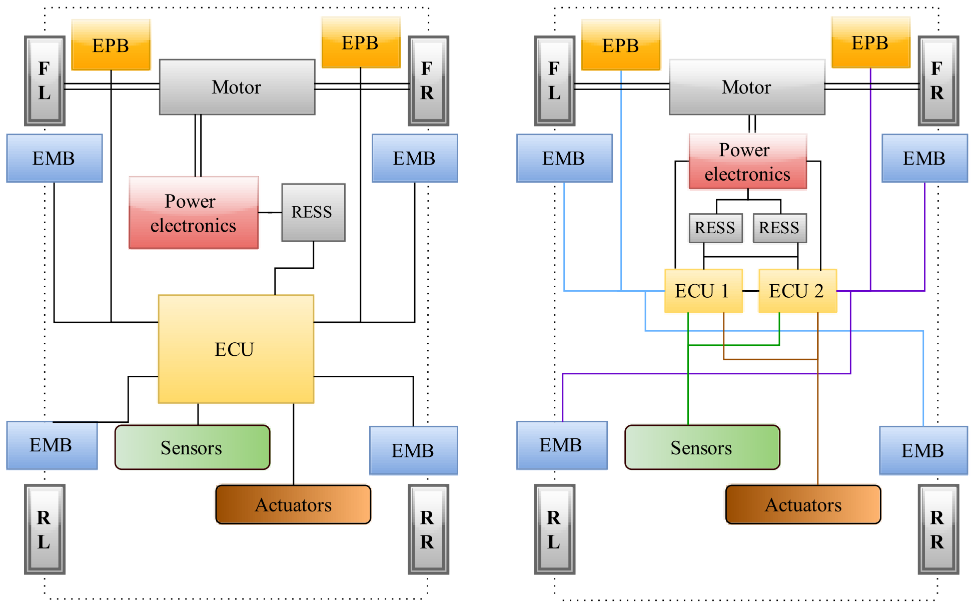
Figure 5.2: Reliability block diagram of the proposed brake-by-wire system with a.) system components and b.) pseudo components to model each subsystem [18].

In [19], the authors investigated the safety risks of an electric vehicle with a generic architecture. Failures of the propulsion system as well as the brake-by-wire and park-by-wire systems were assigned with an ASIL D. The fault analysis marked the energy supply, the communication system, sensors, braking actuators and their controlling units as sources for single point failures of the braking function. Therefore, following adaptations have been made:

- The Electronic Control Unit (ECU) is doubled and two diagonally placed Electromechanical Brake (EMB) actuators are assigned to each ECU respectively. The diagonally assignment of the actuators assures more stability in case of one failing ECU.
- The Electronic Parking Brakes (EPB) are separately connected to the ECUs to avoid a loss of the parking brakes due to one failing ECU.

- A second Rechargeable Energy Storage System (RESS) is added to avoid a loss of braking functions caused by a lack of energy.
- Critical sensors are realised in TMR architecture and the communication bus between sensors and ECUs is implemented as a fault tolerant dual-channel FlexRay bus connected to both ECUs.

Besides the braking function, unintended acceleration caused by a failure in the power electronics or by the motor controller, are also able to cause a severe accident. To suppress driving scenarios where unintended acceleration cause hazardous situations for the driver and its environment, the propulsion system was realised as a fail-safe architecture. With the ECUs managing the vehicle motion control and the energy management, the proposed system is classified as a centralized architecture.



Basic electric vehicle architecture

Advanced electric vehicle architecture

EPB - Electric Parking Brake
EMB - Electro-mechanical Brake
RESS - Rechargeable Energy Storage System
ECU - Electronic Control Unit

FL - Front left tyre
FR - Front right tyre
RL - Rear left tyre
RR - Rear right tyre

Figure 5.3: Architectures of an electric vehicle according to [19].

5.2 Fault-tolerant drive architectures

In [20], an examination of an electric powertrain is carried out with the focus on certain power inverter faults and their impact on permanent excited drives. Three architectures are presented and compared in this paper, including a dual-winding machine with doubled inverter and two arrangements with a redundant inverter leg.

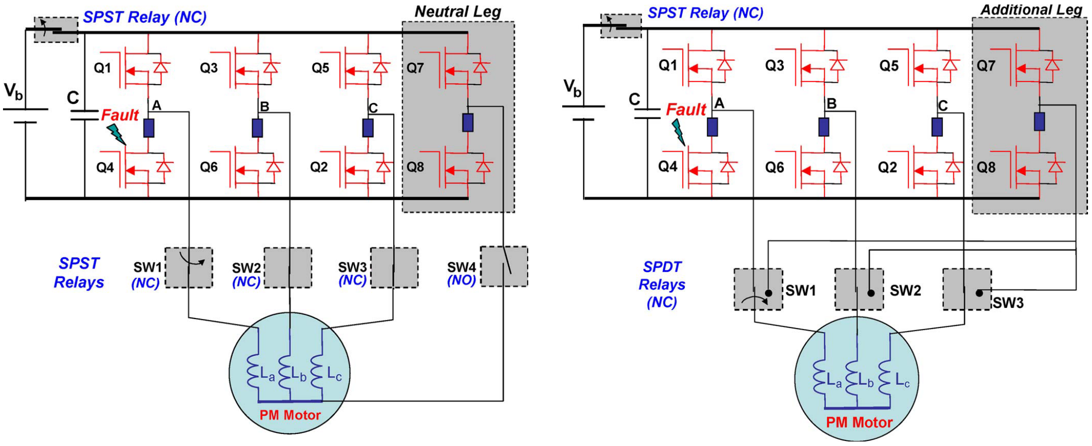


Figure 5.4: Fail-operational inverter architectures for one failure inverter leg [20].

The idea behind the extra leg is adding only a small amount of redundancy instead of doubling the whole item in order to reduce the costs. Fuses and electromechanical relays manage the reconfiguration process in case of shoot throughs, continuously opened or short-circuited switches or open leg failures. No matter which failure takes place, the concerning relay isolates the faulty leg and either connects the extra leg with the neutral of the machine (Fig. 5.4, left) or replaces the phase with the additional leg (Fig. 5.4, right). During the 100 ms of the reconfiguration process, both topologies experience the same torque ripples and current peaks, only determined by the fault type. As soon as the reconfiguration process is finished, the additional leg architecture is capable of providing rated output torque as before, where the neutral leg configuration can only provide the same output if the currents are increased by the factor $\sqrt{3}$.

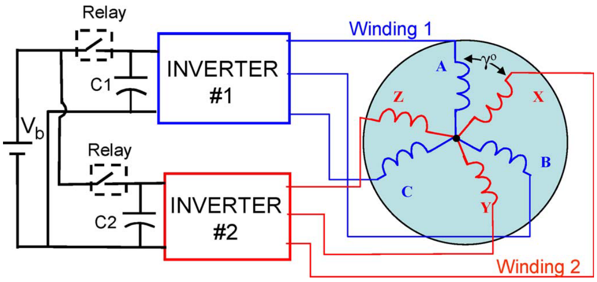


Figure 5.5: A fail-operational six-phase dual winding machine with two independent inverters [20].

The architecture in Fig. 5.5 shows a six phase machine with two independent three phase sub systems. Unlike the additional leg configuration, the inverter is doubled and each sub-system is assigned to one inverter. By this means, not only inverter failures are covered but also short-circuit or open phase faults of the machine only cause a shut down of one subsystem which lead to a degraded performance. A closer investigation of this machine type can be found in [21] and [22].

The authors of [20] proposed among other variables a cost factor and a post-fault performance factor in order to evaluate the merit compared to a conventional power inverter and machine setup. They were defined as follows:

$$\text{CF} = \frac{\text{Cost of the fault-tolerant inverter}}{\text{Cost of the standard inverter}} \tag{5.1}$$

$$\text{PFPF} = \frac{\text{Post fault inverter output power}}{\text{Rated output power of the standard inverter}} \tag{5.2}$$

While doubling the inverter appears to be a cost increase, the cost evaluation in [20] resulted that the dual winding topology only has 59% higher costs, followed by the additional leg configuration with 74% and the neutral leg with 84% as long as the degraded performance is accepted and the inverter must not be able to deliver higher currents by the factor of $\sqrt{3}$. Without overrating the inverter, the PFPF of proposed architectures were 50% for the dual winding, 100% for the additional leg and 67% for the neutral leg solution. If full performance is essential for the application, the additional leg portrays the most cost effective variant as long as other safety measures are not required for the PSM.

5.3 Shared redundancy concept for by-wire systems

In [23] schemes for fail-operational by wire systems are analysed. The authors investigated by-wire systems on system level, firstly introducing a full redundant architecture (FRA) which builds a fail-operational by-wire systems out of two fail-silent architectures. Afterwards a distributed architecture is presented, basing on a shared redundancy concept which relies on fast fault detection and reconfiguration processes. The shared redundancy architecture (SRA) intends to run main and backup processes on all electronic devices in order to share the available hardware instead of adding redundant hardware components.

The most obvious benefit of the SRA are less components: The SRA given in [23] only uses two processors to compute all functions required for all three by-wire systems. This drastic approach was used to place the SRA on the low end of the redundancy scale, in order to achieve a maximum contrast to the FRA. Of course the amount of redundancy can be altered to create a hybrid solution between these two extreme examples.

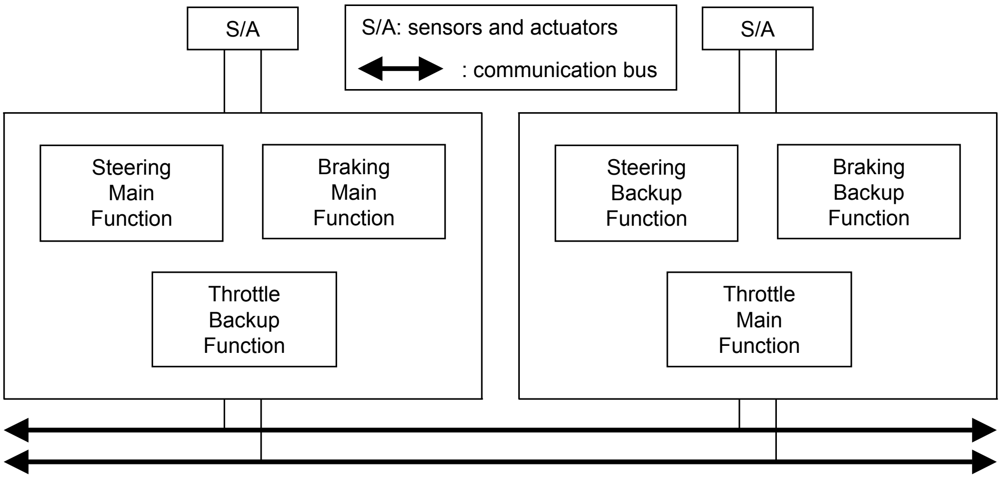


Figure 5.6: A shared redundancy architecture, hosting three by-wire systems on the same hardware [23].

In the SRA, sensors and actuators are either directly connected with single wires or use a redundant bus system as for instance Intellibus. If a doubling of these should be omitted, a mutual bus topology is more promising to supply both by-wire systems with the same sensors and actuators. The communication system between both processors must offer at least two channels and a deterministic time-triggered protocol.

Pros and Cons of the shared redundancy concept

+ SRA is cheaper due to less hardware costs. Also software costs are reduced if the backup control functions provide less functionality

– FRA reconfigurates faster due to its fail-silent subsystems

– FRA can technically cope with more failures and the driver won't realise any internal errors as items fail silent

– Additional engineering effort and expertise is required at the beginning to implement multiple high level functions on the same hardware, in particular if the by-wire systems are from different suppliers.

Summarizing this aspects, the SRA gives a good opportunity to build fail-operational by-wire systems at an economical level, but will consume more resources at the beginning compared to the FRA [23].

6 Propulsion system of an electric car

6.1 Basic architecture

As practical example for applying fault tolerance to an architectures in automotive engineering, a propulsion system of an electric car with rear-wheel drive is investigated. The architecture is reduced to the propulsion system to keep the focus on the essential components. The assumed propulsion architecture is depicted in Fig. 6.1 followed by a component description in following chapter 6.1.1.

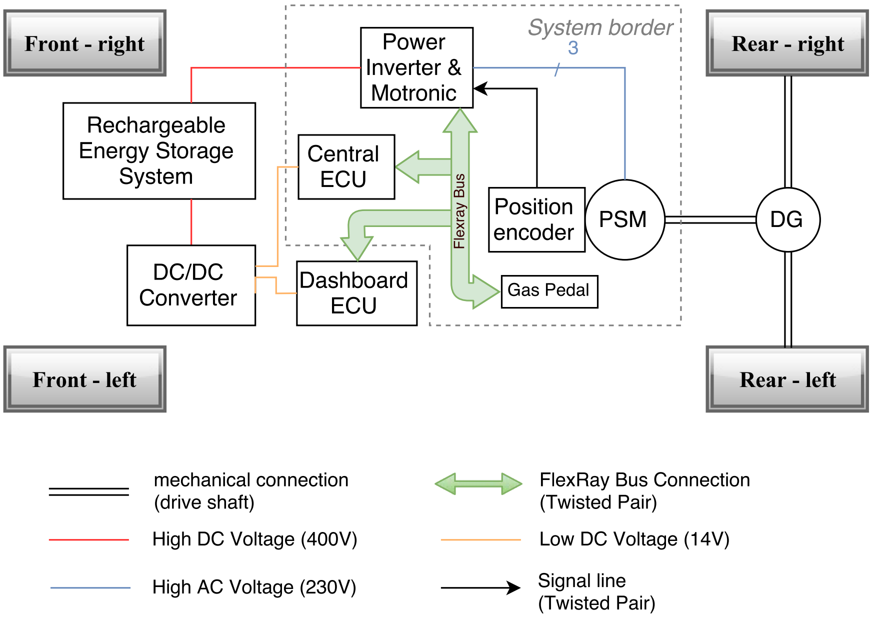


Figure 6.1: Assumed propulsion architecture of an electric vehicle with rear-wheel drive.

The system border marks the investigated parts of the system: The differential gear, as mechanical connection between the output shaft of the PSM and the rear tyres, are excluded from further examinations. The Rechargeable Energy Storage System (RESS), the DC/DC converter and the Dashboard ECU are also excluded from detailed investigations, but are briefly tackled.

6.1.1 Components of the Basic Architecture

Rechargeable Energy Storage System

The core of the RESS is a high voltage traction battery at 400 V which supplies the architecture and is controlled by a Battery Management System (BMS). To validate the State of Charge (SoC) and State of Health (SoH) of the traction battery, the BMS monitors voltage, current and temperature of the battery cells. Depending on the integrity of the BMS, either every single cell is monitored or neighboured cells are grouped and monitored. In order to disconnect the battery from the wiring system, in case of i.e. overheating or a crash, disconnecter units are implemented to prevent damage to the battery cells or the risk of electric shock by improper electric connections to the chassis. An implementation of capacitors with a high capacity (”Supercap”) into the RESS work as a buffer between the wiring system and the battery and therefore increases the efficiency of recuperation while heavy breaking [24], [4].

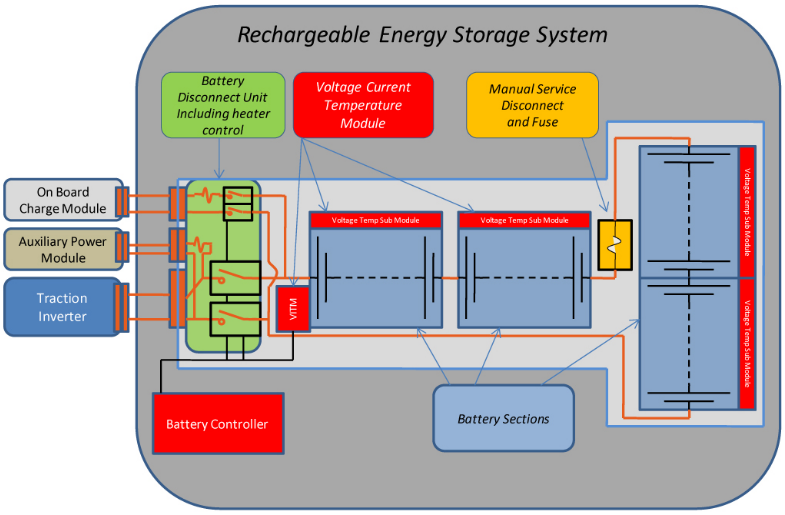


Figure 6.2: Integral parts of a RESS with grouped monitoring [24].

DC/DC converter

The DC/DC converter connects the low voltage wiring system of the electric car with the traction battery. A buck conversion to a board voltage of 14 V ensures that E/E-components of conventional cars can be implemented without an adaptation. As the recuperation is fulfilled by the inverter, a DC/DC converter supporting only one power flow direction from the battery to the low power wiring system is sufficient.

Dashboard ECU

The dashboard ECU builds the connection between the architecture and the driver. It is a low level electronic system which controls warning LEDs that are displayed in the dashboard of the vehicle. The ECU is connected to the Flexray bus and follows the traffic by reading all transmitted data. If a bus member doesn't transmit any valid data during several duty cycles, a fault of the same is assumed and corresponding warning LEDs are set. Also fault detection mechanisms of elements or neighboured elements can inform the Dashboard ECU. For the propulsion system, a red LED is intended to inform the driver that no torque is producible to avoid an initialisation of driving manoeuvres which highly rely on propulsion.

Accelerator Pedal

The accelerator pedal builds the human-machine interface to provide the architecture with the torque demand of the driver. An electronic accelerator pedal converts the angle of the pushed pedal into a voltage signal. In case of smart sensors, a percentage with regard to the maximum angle is given as digital output instead of an analogue voltage signal. Primarily potentiometric or hall sensors are used to detect the position of the accelerator pedal.

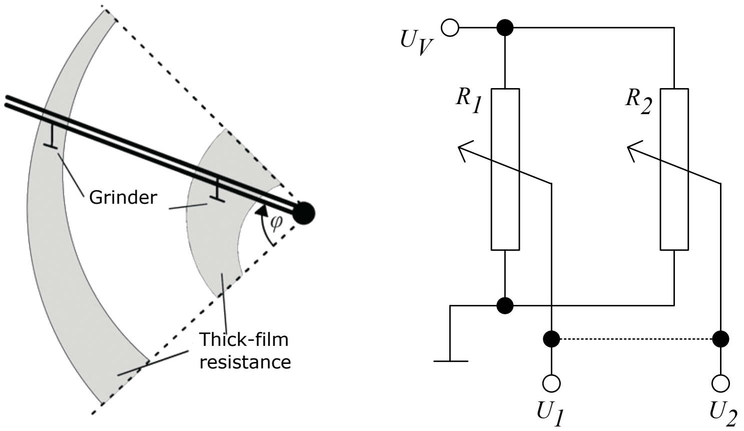


Figure 6.3: Measurement principle of a potentiometric sensor according to [1].

Potentiometric sensors consist out of a thick-film resistance path with grinding connectors moved together with the pedal. The resistance value is therefore proportional to the pedal angle and influences the amplitude of the output signal. To detect faulty output values, a second thick-film resistance path and grinder always sustains the half of the primary voltage [25].

Contact-less pedal sensors (Fig. 6.4) base on hall elements that measure the movement of a permanent magnet mounted on the rotary part of the pedal (Fig. 6.4, A1). With a measuring arrangement of four hall elements shifted by 90°, x- and y- components of the magnetic field are selectively detected (Fig. 6.4, B4 and B5) and lead to two decoupled sinusoidal voltage signals (Fig. 6.4, C). The voltage signals are phase-shifted by 90° and contain the angle information of the pedal [25], [26].

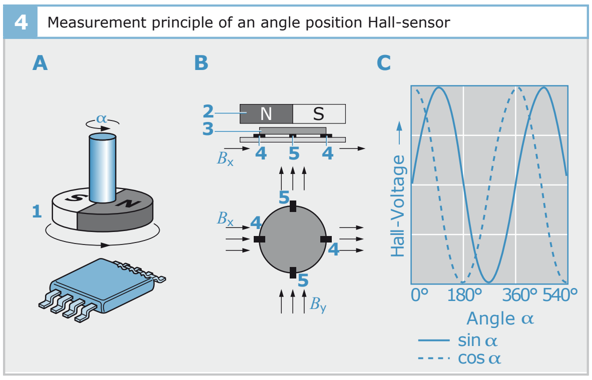


Figure 6.4: Measurement principle of a hall sensor based on four hall elements according to [25].

The hall sensor was chosen as accelerator pedal in the basic architecture due to its insensitivity to fluctuation of the magnetic field, ageing effects and temperature influences. Furthermore, the integrated circuit of the hall sensor provides on-board digitalisation and a communication interface for the Flexray bus.

Central ECU

The Central ECU represents a high level microcontroller connected to the bus system that retrieves the torque demand of the driver and determines the set torque for the Motronic & Power Inverter. Driver Assistance Systems (DAS) communicate with the Central ECU and can alter the torque value if its necessary from a safety point of view. Dependent on the sensor type of the accelerator pedal, different signal processing steps take place in the controller. Analogue sensors deliver their raw data to the controller interface which then extracts the information out of the signal, smart sensors directly digitize the measured value and forward it to the controller. The potentiometric sensor in Fig. 6.3 belongs to the category of analogue sensors: A voltage divider applies a constant voltage to the interface of the ECU which then uses a characteristic curve (Fig. 6.5) to convert the voltage level to the accelerator pedal position [25].

The hall sensor in Fig. 6.4 is combined with a post processing electronic on a single IC which allows a close amplification of the detected signal. First the voltage levels are optimized to the range of the on-board Analogue-Digital Converter (ADC) which then digitize the signals. By applying following equation, the angle information is extracted.

$$\varphi = arctan\left(\frac{U_{sin}}{U_{cos}}\right) \tag{6.1}$$

As the hall sensor is capable to perform this operation already on chip and owns a communication controller that allows integration to a bus system, the Central ECU only

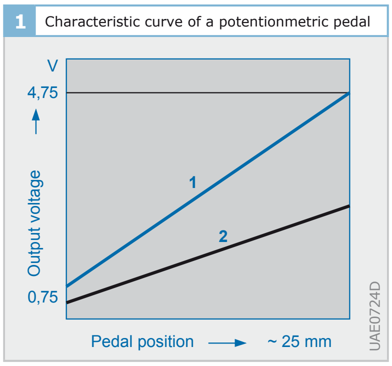


Figure 6.5: Characteristic curve of a potentiometric pedal sensor according to [25].

needs to know the possible minimum and maximum angles of the accelerator pedal to translate the relative angle to desirable torque values [25], [26].

Position encoder

The position encoder detects the actual rotor position and forwards it to the Power Inverter & Motronic. The accuracy of the sensor determines the efficiency of the controlling as small measurement deviations already cause a decrease in torque [27]. In areas with high amount of pollution, sensor principles which make use of magnetic coupling are preferred due to their low vulnerability to soiling. The most common position encoder sensor types are as follows:

- A resolver consists out of two separated coils which are placed with an angle of 90° in between. The changing flux of the rotor induces a sinus voltage in one coil and a cosinus voltage in the other. With the arctangent function, the rotor position angle can be extracted out of the signal ouputs from the sensor. Resolvers are passive sensors with no electronic components what makes them very robust. The amplitude of the analogue output ranges between mV and tens of volts, what requires a range conversion before digitalisation [13], [25].
- Hall sensors using one or more hall elements combined with an integrated circuit to detect the speed or position of the rotor. For position encoding, the sensor consists out of one hall element surrounded by two static half cylinders with a high permeability and a movable circular permanent magnet. A wheel mounted on the machine shaft modulates the magnetic flux in accordance with the rotary position, which is then converted into an electrical signal by an integrated circuit. The integrated circuit includes among other things an amplifier and a DAC which offers a digital interface [1], [2].
- A resistance bridge with anisotropic magneto-resistance (AMR) or giant magnetic-resistance (GMR) components senses magnetic fields through a lowering of their resistance values in presence of a field. The bridge configuration ensures a ratio-

metric measurement of the rotary angle that excludes environmental influences as temperature, ageing or variation of the air gap between sensor and rotor [25].

A resolver was chosen for the use in the basic architecture as it has proven to be very reliable due to its simple structure with no integrated circuits.

Power Inverter & Motronic

The power inverter & Motronic block builds a closed loop control for the permanent excited synchronous machine. Field-oriented controlling is the industry standard for controlling PSM as it offers high efficiency and a dynamic torque controlling. This controlling method uses α/β and d/q transformations to separate the stator currents into a field building current i_d and a torque building current i_q with angular orientation of the rotor. The output torque of the PSM is directly proportional to i_q, thus controlling of a stator current to a maximised i_q will maximise the torque. As the excitation of the PSM is performed by permanent magnets, i_d is regulated to zero as long as the impressed stator voltages of the PSM are below the maximum output voltage of the inverter. As soon as the inverter output is on full value, field weakening with a negative i_d is applied to achieve higher rotational speed. With increasing mechanical rotor frequency, higher field weakening is necessary which yield to a declining of the output torque [28], [4].

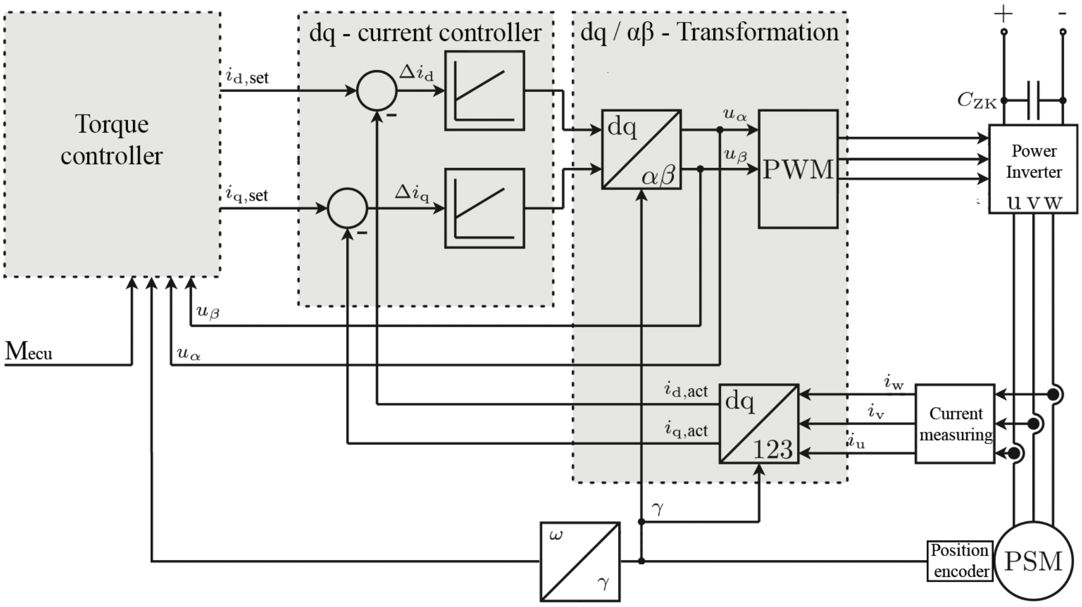


Figure 6.6: Field orientated torque controlling for a PSM according to [28].

The controlling of the power inverter and data acquisition is performed by the motronic and consists of following steps:

- Measurement of the stator currents i_w, i_v, i_w and transformation to rotor current components $i_{d,act}$ and $i_{q,act}$.
- Calculating the angular velocity out of the detected angle by the position encoder.
- Determining a set value for the torque, taking system variables and the proposed value by the central ECU into account.
- Minimizing deviation between desired and actual current values Δi_d and Δi_q.
- Reverse transformation and Pulse Width Modulation (PWM) of the controller output voltages which then are forwarded to the three legs of the power inverter.

Permanentmagnet synchronous machine - PSM

To provide an electric car with a reliable and high-power machine, induction machines are the main choice. Especially asynchronous and permanent excited synchronous machines offer a low-maintenance structure due to omission of outwearing sliding contacts to the rotary parts of the machine. Because of their high efficiency and good dynamic controlling capabilities, a PSM with field oriented controlling has been chosen as drive unit for the architecture [4], [27]. For the hazard analysis of the architecture, a high performance machine is assumed.

6.2 Behaviour during healthy state

The signal flow of the basic architecture, with no present faults, is now analysed to complete the basic architecture description.

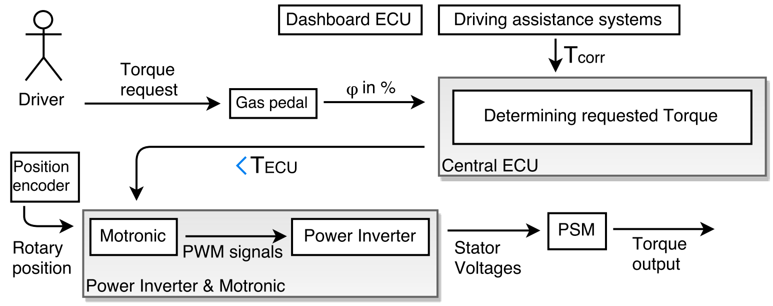


Figure 6.7: Signal flow through the basic architecture when no faults occur.

The torque request of the driver is the starting point of the investigation and is sensed by the accelerator pedal. The accelerator pedal first converts the pedal way into a voltage which is dependent on the angle of the pedal. Secondly the angle information is extracted by the smart sensor and transmitted to the Central ECU over the Flexray bus. The ECU then uses the angle information to calculate the torque demand of the driver and varies it by the inputs of driver assistance systems. As output, T_{ECU} is forwarded over the Flexray bus to the Motronic. The Motronic determines the set values for i_d

and i_q out of the torque request from the ECU, the angular velocity of the rotor and internal voltages for decoupling the d- and q-system. The current controller receives the actual current values $i_{d,set}$ and $i_{q,set}$ by the current measuring and transformation and adjust their output voltages to minimize the deviation between set and real values. The voltages are encoded with a PWM and transferred to the gate inputs of the IGBTs. The power inverter then supplies the PSM with voltages modulated by the switching of the IGBTs. The stator voltages impress the control variables i_d and i_q on the machine to create the desired torque output.

In principal, every failing component in the system chain in Fig. 6.7 can lead to a loss or undesirable amount of propulsion. To ensure that no hazardous vehicle state results out of a failing element or interactions between a faulty element with the remaining architecture, every element is transited to a safe state in case of an error and the driver is informed about the defect. Following table gives an overview about the safe states to which the elements are transited to after a fault in case of a fail-silent architecture.

Table 6.1: Overview of safe states of each component to achieve Fail safe behaviour of the architecture.

Element	Function	Safe State
Accelerator pedal	Sense torque request of the driver	No output
Bus System	Transfer angle information and torque request	No output
ECU	Calculation of a set torque value	No output
Position Encoder	Measuring the rotor angle	No output
Motronic	Controlling of the power inverter	No output
Power inverter	Impressing target values via stator voltages	Active short circuit
PSM	Creating torque output	Active short circuit

The conventional presumption of a safe state for propulsion systems is no torque output, what sooner or later must lead to a standstill of the vehicle. This presumption is implemented straight forward by fail-silent behaviour of all architecture parts of the propulsion system, except for the machine and inverter block.

Active Short Circuit – ASC

Fail-silent behaviour of the power inverter results in termination of all gate signals for the power inverter in order to leave the IGBTs non-conductive, which is critical if the PSM operates at high rotary speeds. While operating in field weakening mode, the power inverter uses the field component of the current i_d to hold the phase voltage of the machine below the voltage output of the inverter. If the inverter is then silenced, the output voltage of the inverter lowers, but the rotor of the PSM still induces a voltage (the back electromotive force) into the phases of the stator. As the stator phase voltage is now above the potential of the inverter, the current flows over the free wheeling diodes of the power switches and uncontrollable charges the HV battery or the DC capacitor if the circuit breakers of the battery already opened.

Therefore silencing the inverter is no safe state, and in order to avoid a damaging of the inverter or the battery, an Active Short Circuit (ASC) is performed instead which permanently conducts the upper or lower half bridge of the power inverter. The Motronic is responsible to trigger and maintain the ASC and the phase windings of the PSM must withstand the continuous short circuit. The high braking torque caused by the ASC is acceptable from a safety point of view as the effect is strongest at slow speed and decreases rapidly at higher rotation speed [27], [29].

6.3 Behaviour under faulty conditions

The signal flow for each single point failure is now observed to give a better insight into the behaviour of the basic architecture.

Accelerator pedal failure

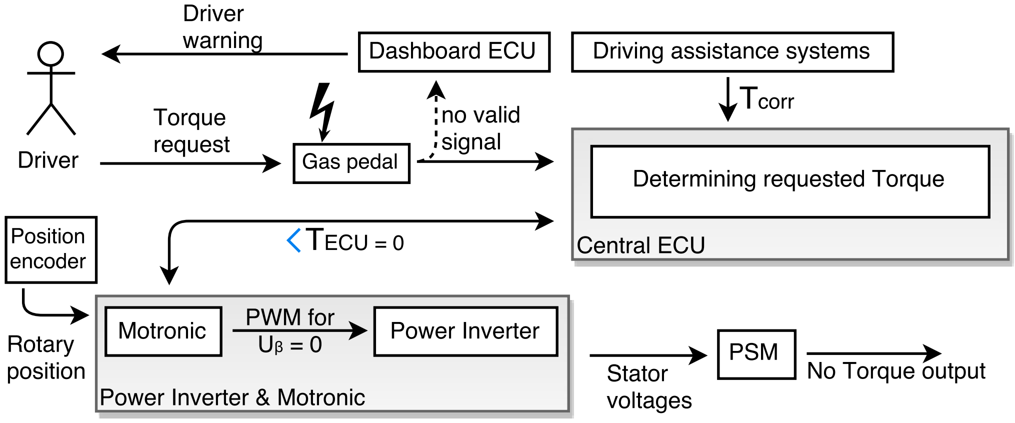


Figure 6.8: Signal flow through the basic architecture when the accelerator pedal fails.

If a malfunction takes place in the accelerator pedal, no output of the pedal is forwarded via the bus to avoid wrong input values to the controlling. When the central ECU detects no or an angle value out of range, the forwarded torque request to the Motronic is set to $T_{ECU} = 0$. The Dashboard ECU also monitors the output values from the accelerator pedal and informs the driver that an upcoming torque request cannot be supported. If the Motronic doesn't receive a torque request by the ECU or it equals zero, the torque related current i_q is controlled to zero, which leads to no output torque by the PSM.

Bus System failure

A failing of the bus system affects the signal paths between accelerator pedal and the central ECU aswell as between ECU and Power Inverter & Motronic. As a result, no set torque can be transmitted to the Motronic which then assumes a set value of $T_{ECU} = 0$. Again no output torque is produced by the PSM.

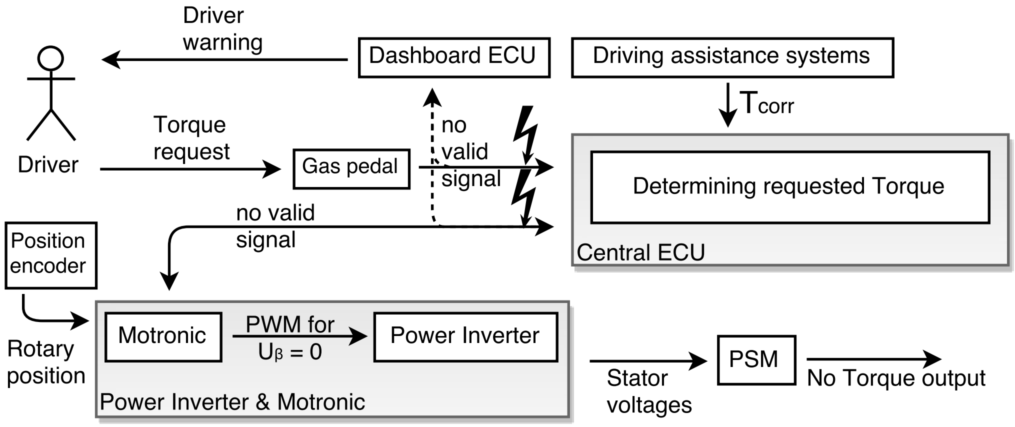


Figure 6.9: Signal flow through the basic architecture after loss of the bus system.

Central ECU failure

If the central ECU fails, the angle value coming from the accelerator pedal cannot be processed and converted into a set torque. Furthermore, inputs from driver assistance systems are neglected. The central ECU is realised as fail-safe unit, so no output signals are forwarded in case of a failure. As soon as the Motronic detects that no set values are send from the ECU, a set value equal zero is assumed.

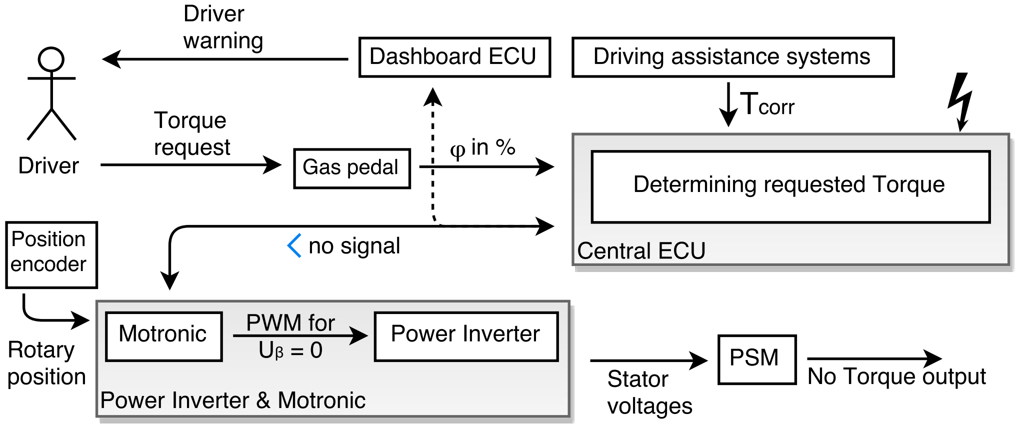


Figure 6.10: Signal flow through the basic architecture when the central ECU fails.

Position encoder failure

The position encoder provides the field orientated controlling with the actual rotary position. Without this information, coordinate transformations from stator to rotor related coordinates and vice versa are not possible. This means that a failing of the position encoder automatically leads to a failing of the field orientated controlling. In case of a resolver, no electronic is present at the sensor thus the fault detection needs to be covered by the Motronic.

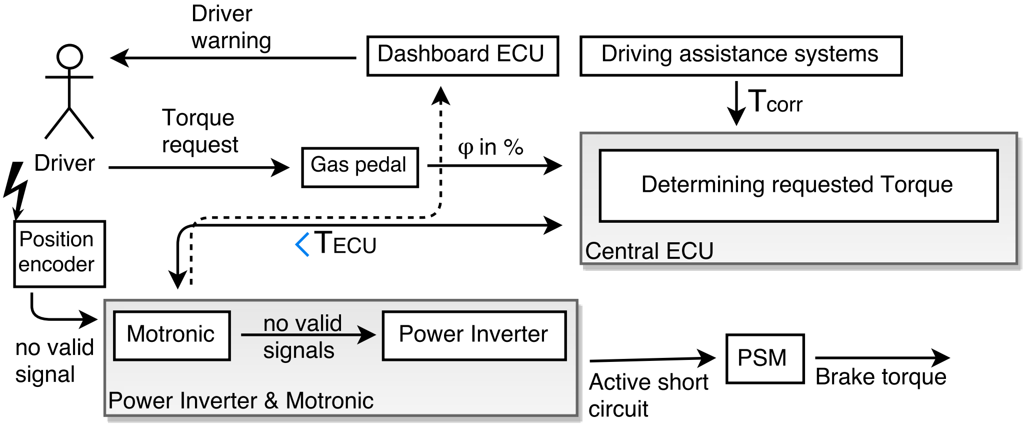


Figure 6.11: Signal flow through the basic architecture after loss of the position encoder.

Differential hall sensors include an electronic circuit for signal processing which can also implement a fault detection to provide fail-silent behaviour. For both cases, no PWM signal is produced for the power inverter, which then performs an active short circuit of the higher or lower IGBT half bridge. The active short circuit protects the IGBTs from destructive back EMF of the PSM in case of high rotary speed but also results in a undesired strong engine brake at low speed.

Motronic failure

Failing of the Motronic itself has roughly the same consequences as losing the position encoder, in both cases no field orientated controlling is possible. Again the power inverter performs an active short circuit to secure its electronic components.

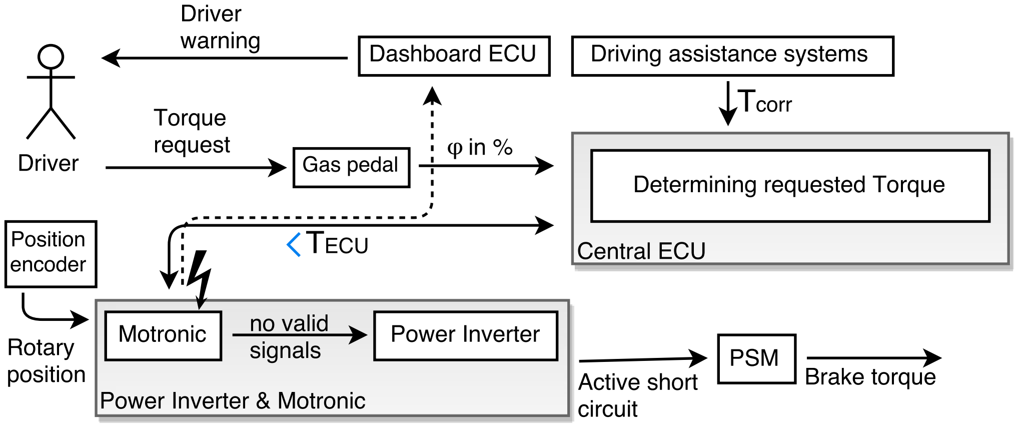


Figure 6.12: Signal flow through the basic architecture after loss of the Motronic.

Power Inverter failure

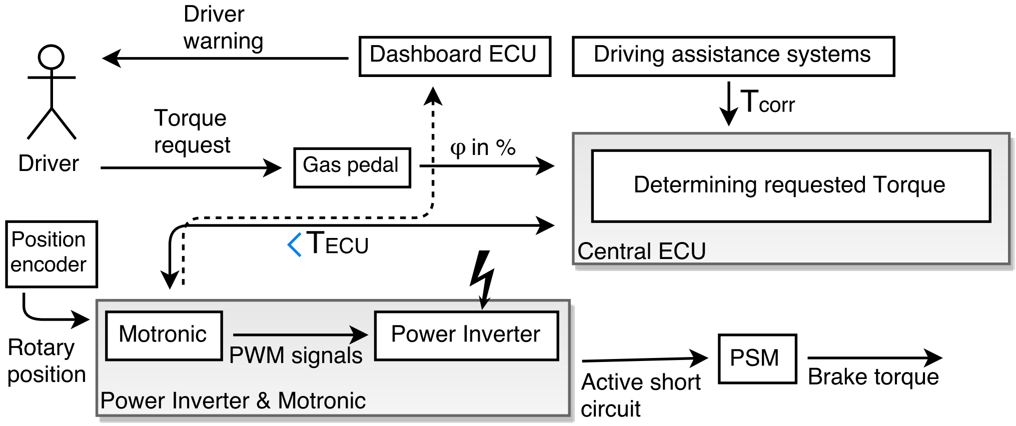


Figure 6.13: Signal flow through the basic architecture after loss of the power inverter.

A loss of one phase of the power inverter already leads to a strong torque ripple due to the missing phase. As this ripple has a strong impact on the controllability of the vehicle, an active short circuit (ASC) is performed for one half bridge of the inverter. Depending on the internal position of the defect, the functional remaining half bridge is preferred to perform the ASC. The high currents during an ASC can lead to demagnetization of the permanent magnets.

PSM failure

Short circuit or open phase failures of the PSM have a strong impact on the torque output on the shaft. A disconnection of all phases by circuit breakers is not practical as it causes a high break torque when driving at high speed and unnecessarily increases the costs of the architecture. Instead, an ASC is considered as safe procedure for the architecture and the driver, as it only causes a high braking torque at low vehicle speeds. The ASC is initiated by the Power Inverter & Motronic block, which can detect a defective phase by the measured stator current inputs.

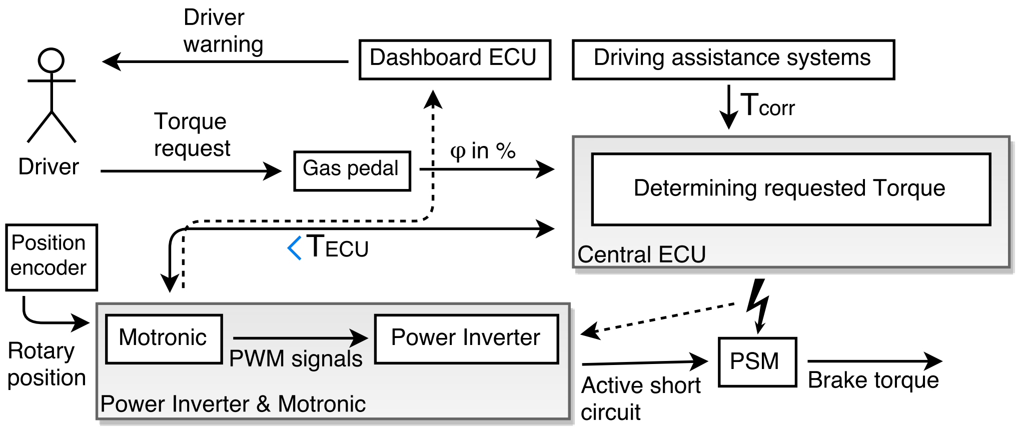


Figure 6.14: Signal flow through the basic architecture after a failure of the PSM.

6.4 Hazard Analysis and Risk Assessment

The Hazard Analysis and Risk Assessment (HARA) is an established method in quality engineering to identify potential mishap scenarios where a system failure can lead to a sever accident. The used methodology was proposed in the ISO 26262:2011 and serves for identifying hazards in the automotive branch and evaluate their inherent risk. Potential scenarios need to be discovered and are assessed with the parameters Exposure, Severity and Controllability. For exposure and controllability, average driving cycles and average driving skills build the basis of the estimation. Based on these parameter values, an ASIL is assigned to a scenario or if the risk is acceptable low, regular Quality Management methods are sufficient and methods of the ISO 26262 are not applied. The scenario is then flagged as Quality Management (QM) instead of receiving an ASIL. A briefly description of the parameter classes can be found in chapter2.1, a more detailed explanation and example values for specific driving scenarios can be found in the standard ISO 26262.

The HARA only evaluates discovered scenarios and their inherent risk, but does not consider detailed technical solutions. Hazardous scenarios which can occur in the basic architecture need to be filtered and if assigned with an ASIL, countermeasures must be applied to reduce the risk. Impacts of propulsion system failures on the vehicle safety were analysed and driving scenarios for complete loss of propulsion, to low/high propulsion and to low/high braking torque have been assessed in upcoming Tables 6.2, 6.3 and 6.4. Only failures of the propulsion system were taken into account. For the analysis, a rear driven vehicle with a strong electric machine is assumed.

Table 6.2: HARA results for a loss of the propulsion system.

Loss of Propulsion	Mishap potential	S	E	C	ASIL
Overtaking	Frontal crash with oncoming traffic	S3	E2	C2	ASIL A
Parking maneuver on hill	Property damage	S0	E2	C2	QM
Lane changing in city traffic	Rear impact crash by another car	S1	E4	C1	QM
Turning at intersection with no traffic light regulation	Side crash by another car	S3	E2	C2	ASIL A
Driving through a Tunnel	Rear impact crash by another car	S3	E2	C1	QM

Loss of braking torque	Mishap potential	S	E	C	ASIL
Driving downhill	unintended acceleration and possibly overload of brakes	S3	E2	C1	QM

In Tab. 6.2, overtaking at country roads and intersections with no traffic light regulation were found as critical situations. For the first scenario the driver must realise early enough that the propulsion is lost and that he has to terminate the overtaking procedure to avoid a frontal crash with oncoming traffic. In the second ASIL rated scenario, the turning cannot be completed and the car remains on the intersection. The driver itself cannot put the vehicle out of danger as its propulsion is lost, but other participating driver can avoid an accident by braking on time.

Table 6.3: HARA results for too low/high propulsion.

Too low propulsion	Mishap potential	S	E	C	ASIL
Heavy Traffic	Rear crash by a car behind	S1	E3	C2	QM
Overtaking	Frontal crash with oncoming traffic	S3	E2	C2	ASIL A

Too high propulsion	Mishap potential	S	E	C	ASIL
Starting on an intersection (first position)	Crash with a pedestrian	S3	E3	C2	ASIL B
Starting on an intersection	Crash with car in front	S1	E3	C2	QM
Leaving at highway exit	Stability loss in curve leading to crash	S3	E4	C2	ASIL C
Parking	Crash with parking car	S0	E4	C2	QM
Heavy traffic	Crash with car in front	S1	E3	C2	QM
Driving at high speed (dry surface)	Loss of stability	S3	E4	C3	ASIL D
Driving at medium speed (snow surface)	Loss of stability	S3	E2	C3	ASIL B

In Tab. 6.3, again the overtaking scenario is rated with an ASIL A and could even be worse than a complete loss as it is less apparent to the driver, however the countermeasure remains the same. The cases for too high propulsion affected more scenarios as it leads to an unintended acceleration of the vehicle. The first entry concerning a vehicle stop at the top position at an intersection: Pedestrians passing by on a crosswalk in front of the car can be hit when there is a non-expected acceleration instead of standstill. The other entries describe the risk of a stability loss under several circumstances with different ratings dependent on their scene. Driving with high speed at dry surface was assigned with the highest ASIL as it has the most common surface condition during almost every driving cycle.

Table 6.4: HARA results for too low/high brake torque.

Too low brake torque	Mishap potential	S	E	C	ASIL
Heavy Traffic	Crash with car in front	S1	E3	C2	QM
Leaving at highway exit	Crash with another car in front	S1	E4	C2	ASIL A
Driving downhill	unintended acceleration and possibly overload of brakes	S3	E2	C1	QM
Unexpected pedestrians on the street	Accident with pedestrian	S3	E2	C2	ASIL A

Too high brake torque	Mishap potential	S	E	C	ASIL
Heavy traffic	Rear crash by a car behind	S1	E3	C2	QM
Locking of one or more tyres	Loss of stability	S3	E2	C3	ASIL B
Wet/snow-covered streets	Loss of stability	S3	E2	C3	ASIL B
Driving trough tight bends	Swerving of the rear	S2	E2	C3	ASIL A
Driving at high speed (dry surface)	Loss of stability	S3	E4	C3	ASIL D

As seen in Table 6.4, unexpected high braking torque is a critical factor in various situations as it has an impact on the vehicle stability. Too low braking torque most likely will lead to a misjudging of the braking distance, but can be balanced with stronger use of the regular braking actuators. Too high braking torque is more severe as it has an impact on the stability of the vehicle: A swerving of the rear or skidding is not controllable by most of the drivers and can lead to serious injuries dependent on the speed and scene.

To overcome the threat of hazardous scenarios inflicted by failures in the propulsion system, functional safety measures must be performed to lower the risk of these scenarios to an acceptable low level.

6.5 Fault Tree Analysis of the basic architecture

To determine the roots of propulsion system failures, a Fault Tree Analysis (FTA) was performed and the result is portrayed in Fig. 6.15. A FTA is a top-down analysis method with the investigated failure mode on top, in this case loss of propulsion, followed by subordinated elements or components causing this system failure. The level of detail is increased with every layer and can be processed until determining single failures of hardware or software parts.

The required amount of time to perform the analysis increases with further degree of detail and gained information might not be relevant as most times components are treated as a whole and rarely single parts are exchanged. For the sake of clarity and to highlight dependencies of subsystems, a systematic level of detail was chosen.

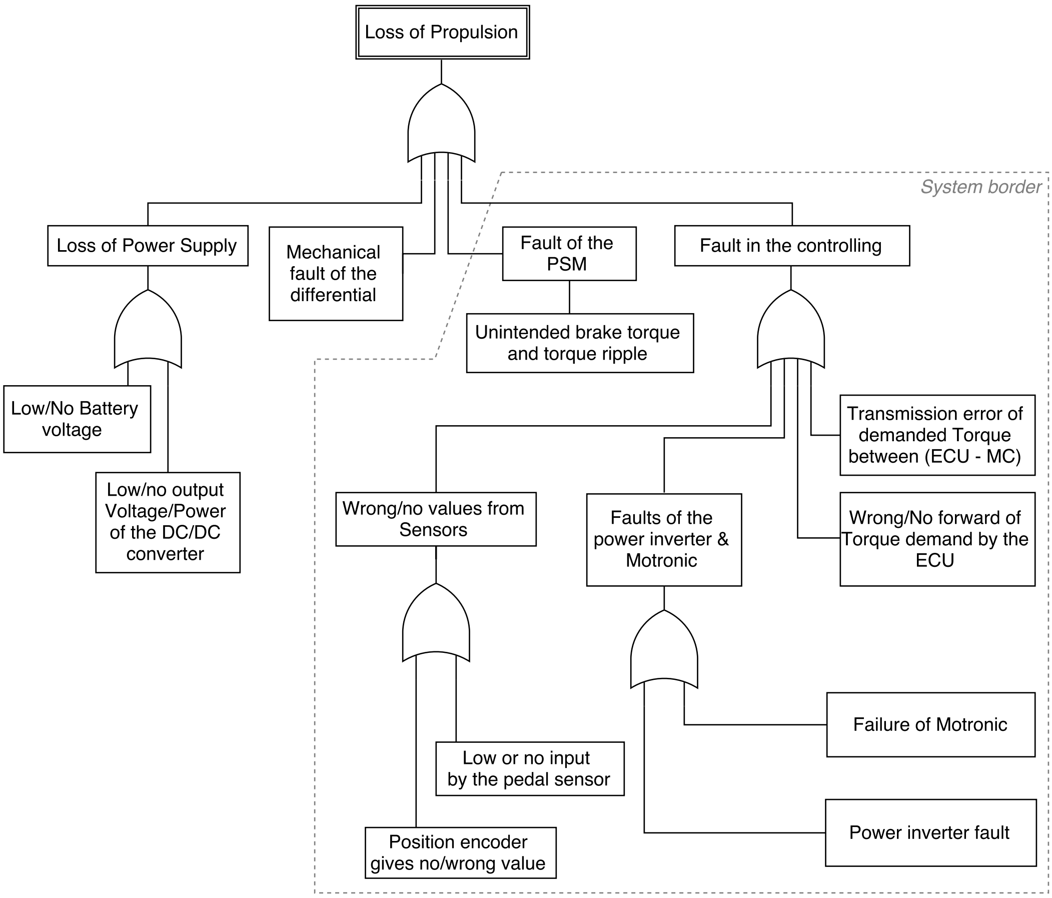

Loss of Propulsion
System border
Loss of Power Supply
Mechanical fault of the differential
Fault of the PSM
Fault in the controlling
Unintended brake torque and torque ripple
Low/No Battery voltage
Low/no output Voltage/Power of the DC/DC converter
Transmission error of demanded Torque between (ECU - MC)
Wrong/no values from Sensors
Faults of the power inverter & Motronic
Wrong/No forward of Torque demand by the ECU
Failure of Motronic
Low or no input by the pedal sensor
Power inverter fault
Position encoder gives no/wrong value

Figure 6.15: Fault tree analysis of the basic architecture for the hazard loss of propulsion.

7 Fail-operational propulsion system for electric vehicles

The importance of an operational propulsion system in some driving scenarios were discovered in the hazard analysis and critical architecture elements were identified within the FTA. In order to rebuild the basic architecture to a fail-operational one, all root causes given by the FTA were remodelled and affected components and their interactions with the remaining architecture were considered. A conversion concept is presented at first followed by a description of the behaviour of the fail-operational architecture in healthy state and during hazard, analogue as with the basic architecture.

7.1 Conversion concept of the basic architecture

Isolation fault of one phase of the PSM

To avoid a single point failure by an error of the PSM, the machine type is exchanged to a 6 phase machine which offers fail-operational behaviour. The slots of the stator are divided equally into two 30° shifted three phase systems which are fed by two independent inverters (Fig. 7.1).

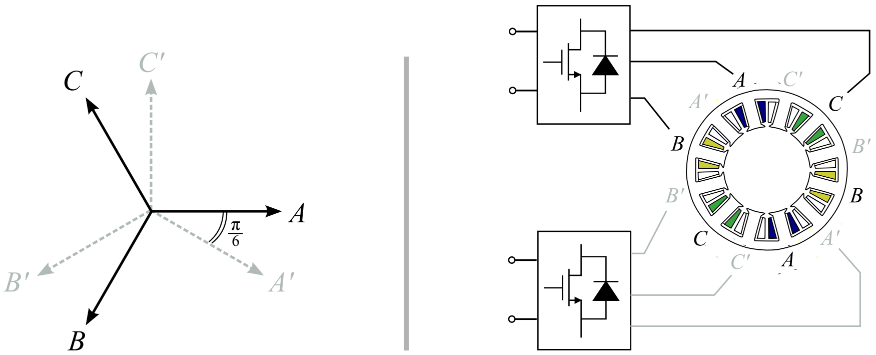


Figure 7.1: The vector diagrams of the two subsystems are displayed on the left and the inverter topology of a 12-slot 10-pole machine is displayed on the right. Only the phases of one subsystem are coloured to emphasize the alternate winding scheme according to [22], [21].

A 12-slot 10-pole machine with non overlapped coils and an interior permanent magnet (IPM) rotor was chosen as proposed in [22]. The benefits of this machine arrangement are the physical separation of the phase windings which lower the fault propagation, high self-inductance to limit the short circuit current and a low torque ripple due to the alternate winding structure. If the voltage values of one phase appear erroneous, the associated inverter performs an ASC for the sub-system degrading the dual winding machine to a 3 phase machine. The short-circuited sub-system produces a resistive torque with dependency on the speed, leaving the performance of the remaining machine with about 40% of nominal torque [21].

Faults of the Power Inverter & Motronic

With the exchange of the electric machine, two conventional power inverters are necessary for the controlling, what also makes the architecture immune to single point failures from the Power inverter & Motronic block. Common failure modes of this block are for instance steadily opened or closed IGBTs because of a hardware defect or due to wrong controlling by the Motronic [30]. Defects will affect voltage and current values of the related phase of the PSM and decrease the overall torque output, and in case of an asymmetric fault distribution, add a torque ripple to the machine output. To prevent the driver from this alternating torque, an ASC is performed as soon as one leg is affected to outrule asymmetric phase errors [29].

Position encoder gives no/wrong value

Differences between the actual and the measured rotor angle lead to miscalculation in the Motronic followed by a reduction of the output torque due to wrong controlling. Enormous angle faults above ±90° force a sign change of the torque which results in strong torque ripples and a controlling inability [26]. A redundancy strategy with two position encoders or a sensorless controlling as alternative is necessary to maintain the propulsion system operational. For diversity reasons, a sensorless controlling is applied as a backup system in this architecture, which is capable of calculating the rotor position out of stator values in case of a position encoder failure.

Low or no input by the accelerator sensor

The torque demand of the driver is a crucial input for the whole propulsion system, what requires a reliable structure to sustain the controlling with data. Because of the superior degree of Diagnostic Coverage (DC) of static M-n-Systems, a static TMR structure for the pedal sensor was implemented. In case of one sensor defect, the TMR degrades to a duplex structure thus the voter functionality changes from majority voting to comparison of the two remaining sensor outputs. The duplex system is capable of detecting a second sensor defect if the output values of the sensors slightly differ, but without enhanced fault detection mechanisms, it cannot identify the correct value out of two given. To avoid a fault propagation based on wrong input values, the pedal sensor is passivated as soon as a second defect is detected.

Transmission error of demanded torque

The communication system of the architecture is realized as a bus system and transmits, among other signals, essential values for the controlling. To avoid a single point failure by the communication system, a dual-channel Flexray system was chosen as it is deterministic protocol and offers fail-operational behaviour. This structure requires a second twisted pair connection (second channel) which simultaneously transmits the same information as the primary one. All bus members need to be connected to both channels in order to obtain system information in case of a channel fault.

Wrong/no forward of torque demand by the ECU

The central ECU determines a torque demand proportional to the accelerator pedal input and forwards it to the Power Inverter & Motronic block. It also builds an interface for high level functions as driving assistance systems which can modulate the torque set value if required. In order to avoid the loss of computing functions, a secondary ECU is implemented as hot standby unit that always performs the same actions as the primary one but does not forward its results to the output.

Over a simple connection line, each ECU communicates its status to the other in order to react on status changes. Both ECUs are fail silent, thus do not send any output when an internal error occurs. When no valid status is transmitted over the communication line, immediately the output of the other ECU is connected to the Flexray bus. To keep the reconfiguration time as low as possible, cold standby is not applicable here as the initialisation of the backup ECU would consume too much time.

7.2 Fail-operational Architecture

The conversion concept is now applied to the basic architecture to achieve fail-operational behaviour. The altered architecture is displayed below in Fig. 7.2.

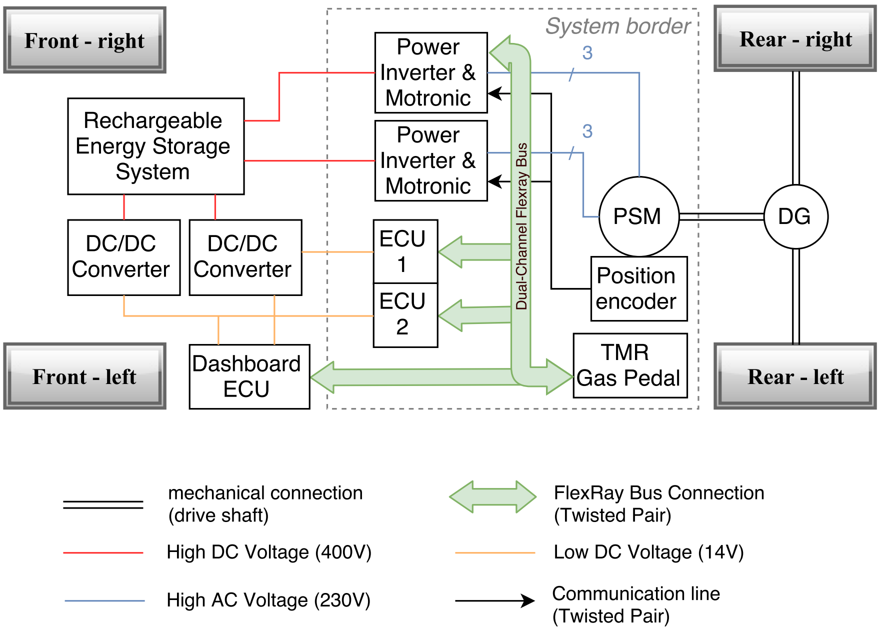


Figure 7.2: Extension of the basic architecture to perform fail-operational behaviour.

7.2.1 Behaviour during healthy state

The signal flow of the fail-operational architecture during healthy state can be seen in Fig. 7.3 and is also initiated by the torque request of the driver.

The TMR pedal sensor detects the pedal movement and converts it into an digital signal that contains the angle information. All three sensors simultaneously detect and forward the request to the voter which then performs a majority voting. The voter assumes a correct function of the sensors as long as their outputs contain only slightly deviations. The two closest values win the majority voting followed by an averaging and forwarding it to the output of the TMR pedal. The central ECU, now replaced by two separated units ECU 1 and ECU 2, retrieves the angle information from the bus and both ECUs post process the information to obtain a set value for the PIM. As long as the ECUs update the status to their redundant partner, only the primary ECU 1 transmits its results to the bus. Both Power Inverter & Motronic blocks then retrieve the set value T_{ECU} from the bus and the rotary position by the encoder and perform the controlling. The stator voltages are applied to the PSM which lead to the desired output torque.

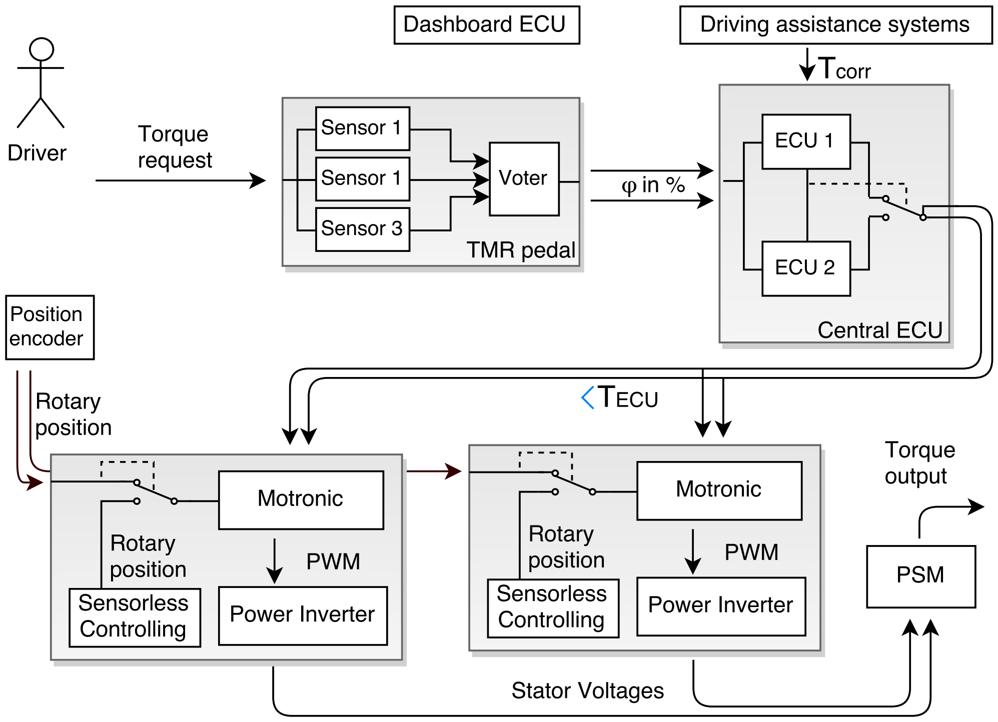


Figure 7.3: Signal flow through the fail-operational architecture when no faults occur.

7.2.2 Behaviour if a failure occurs

Analogue to section 6.2, all single point failures and their impacts on the architecture shall be described. Defect components, detection paths, driver information and effects on outputs are highlighted in blue for clarity.

Failure of one sensor of the accelerator pedal

In this error scenario, one of the sensors used inside the TMR fails and sends no or corrupted data to the voter. The voter, still comparing all outputs of the sensors, detects the strong deviation and only forwards the average of the two remaining sensors. If the error is not transient and appears several times to the voter, the concerning sensor outputs are ignored and the voter reconfigures its decision strategy from majority voting to comparison. The dashboard ECU is then informed about the degradation to a fail silent accelerator sensor through the bus system. With the dashboard ECU as communication interface between the architecture and the driver, the driver is warned about internal errors even if they do not have an effect on functionality yet. A detailed explanation about the driver warning system can be found in chapter 7.5.

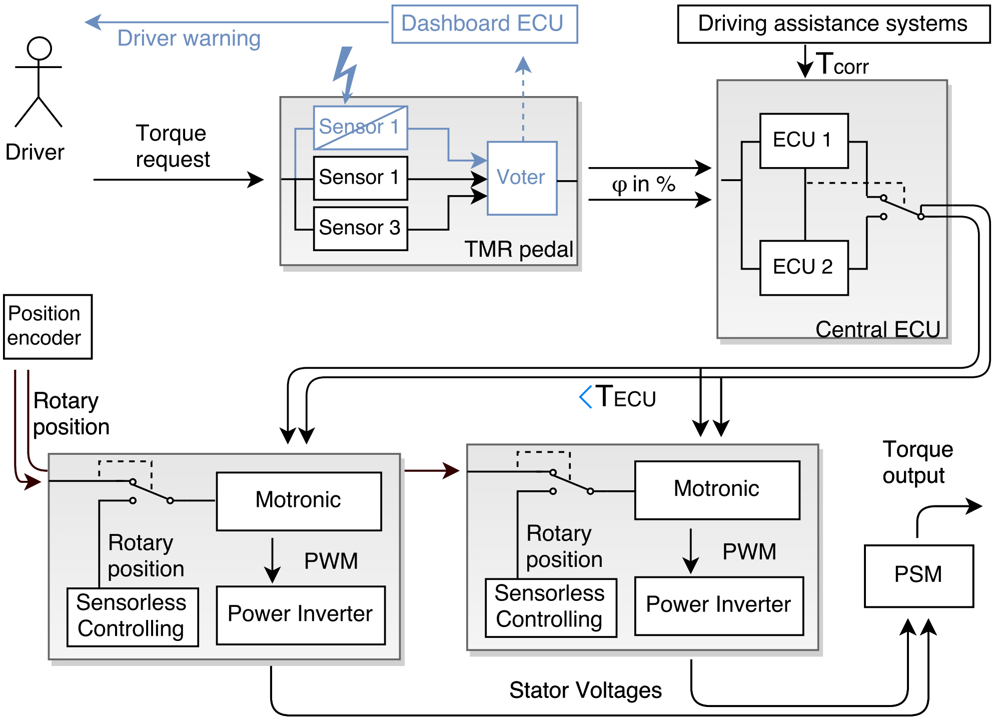


Figure 7.4: Signal flow through the fail-operational architecture after a failure of one sensor inside the TMR pedal sensor.

Failure of one channel of the Bus System

Minor faults of the bus system as information loss is reproduceable at the receiver side with information redundancy and error detecting code as for instance cyclic redundancy check (CRC). To avoid communication problems caused by a erroneous sender giving signals to the bus outside of his time frame, the Flexray protocol proposes the use of a Bus Guardian. The Bus Guardian represents an additional unit between the bus and the communication controller of the bus members and doesn't forward controller signals when outside their timing frames. A loss of one channel of the communication channel by one erroneous and continuously sending member (babbling idiot failure) can be controlled with this strategy [17].

If one communication channel is lost due to other reasons, all vital components participating on both channels can detect the error. The dashboard ECU, also connected to both channels of the bus system, forwards a degradation warning to the driver.

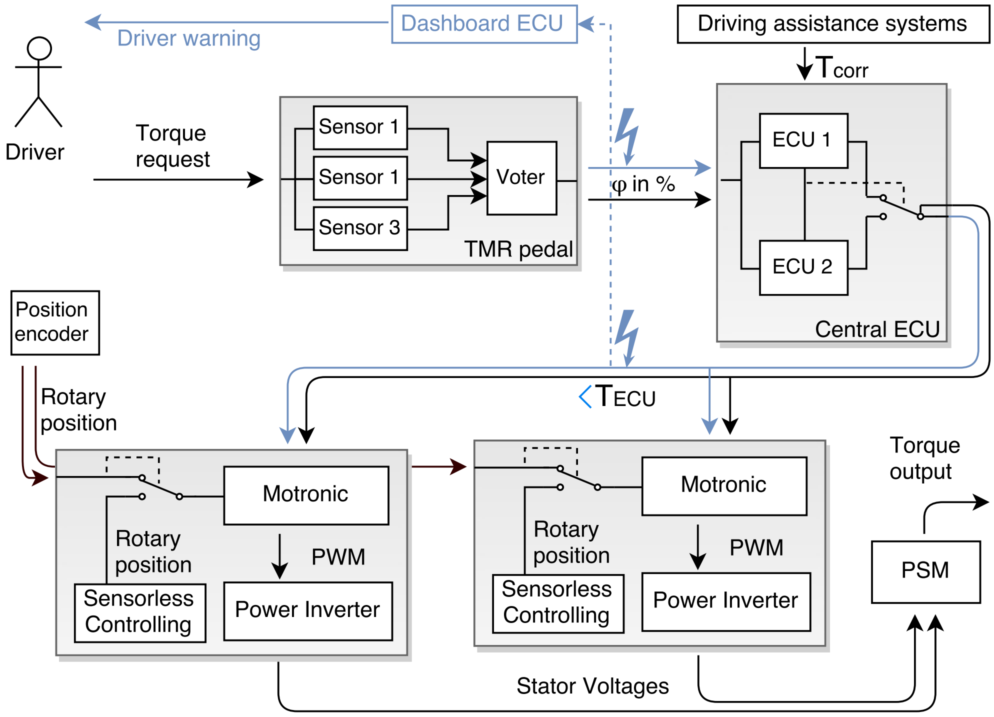


Figure 7.5: Signal flow through the fail-operational architecture after a failure of one channel of the bus system.

Failure of one ECU

The central ECU was extended with a second control unit and a fault detection mechanism which is known as fail-operational through the combination of two fail silent elements. ECU 1 and ECU 2 both retrieve input signals from the bus system, post-process the data and calculate set values for the torque. A communication line with simple mutual status messages between ECU 1 & 2 informs both units about the status of their partner. As soon as no healthy status message is retrieved from the partner, the remaining ECU is now allowed to forward its output to the bus and informs the dashboard ECU about the degradation. The displayed switch in Figure 7.6 is not a logic hardware switch, but implemented in software as intelligent switch.

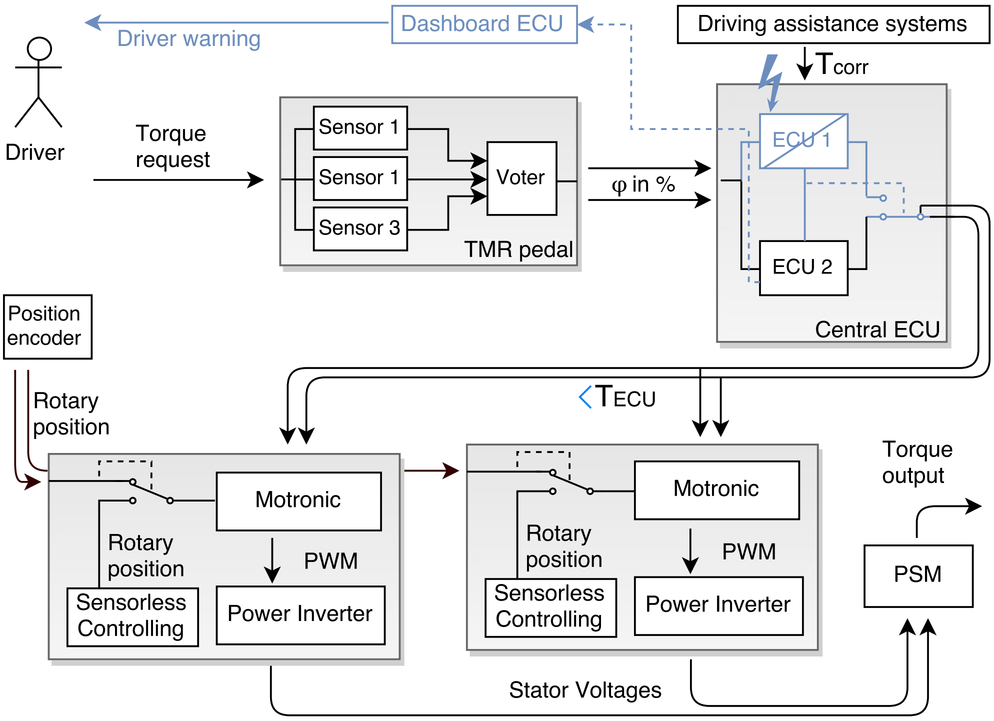


Figure 7.6: Signal flow through the fail-operational architecture after a loss of one ECU.

Failure of the position encoder

A defect of the position encoder leaves both PIM blocks without angle information of the machine. An intelligent switch inside the PIM blocks switches to sensorless controlling which calculates the rotary position out of stator voltages. To perform this estimation, the INFORM-method is used for low rotary speeds and an EMF model is used for high rotary speeds [28]. Signals from the position encoder are now ignored to avoid any influence on the controlling.

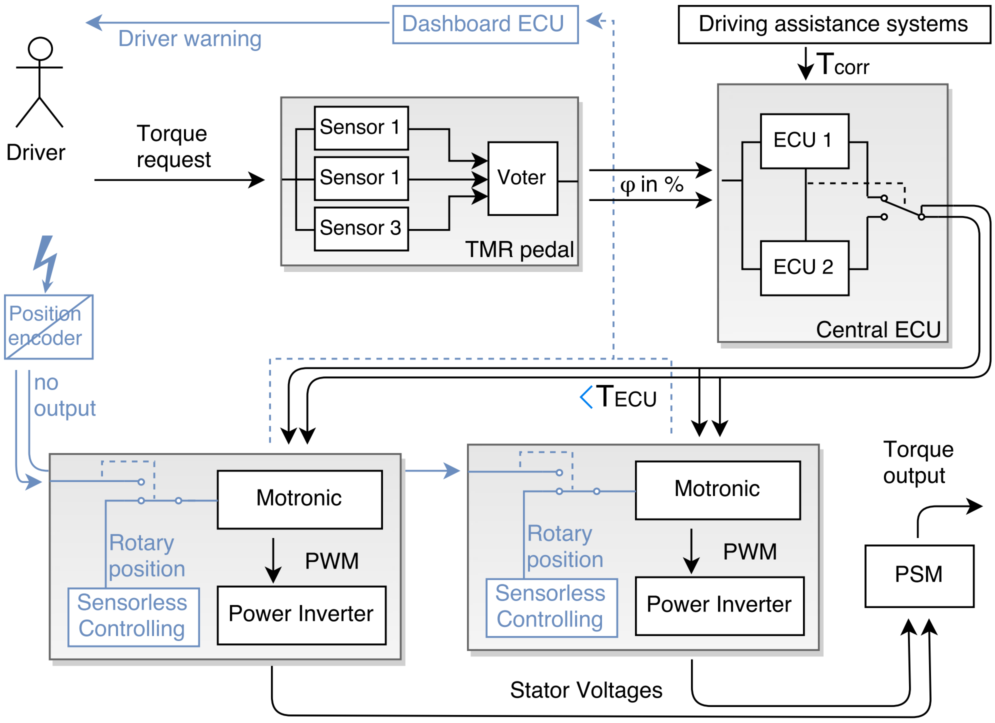


Figure 7.7: Signal flow through the fail-operational architecture after loss of the position encoder.

Failure of one Motronic & Power Inverter

A failing of a PIM block is either caused by an internal fail of the Motronic or the Power Inverter, however both faults require an active short circuit of the inverter to reach a safe state of the PIM block. A single defect of the Motronic is visible to other bus members when no more valid signals are transmitted by the Motronic. If only the inverter compartment fails, the Motronic selects a healthy half bridge to perform the ASC and provides the dashboard ECU with information that one power inverter failed which leads to a lowering of the torque output to 40%. As long as the Motronic is operational, it can perform the ASC, if the Motronic fails as well, the inverter must be able to perform the ASC by itself with a separated logic.

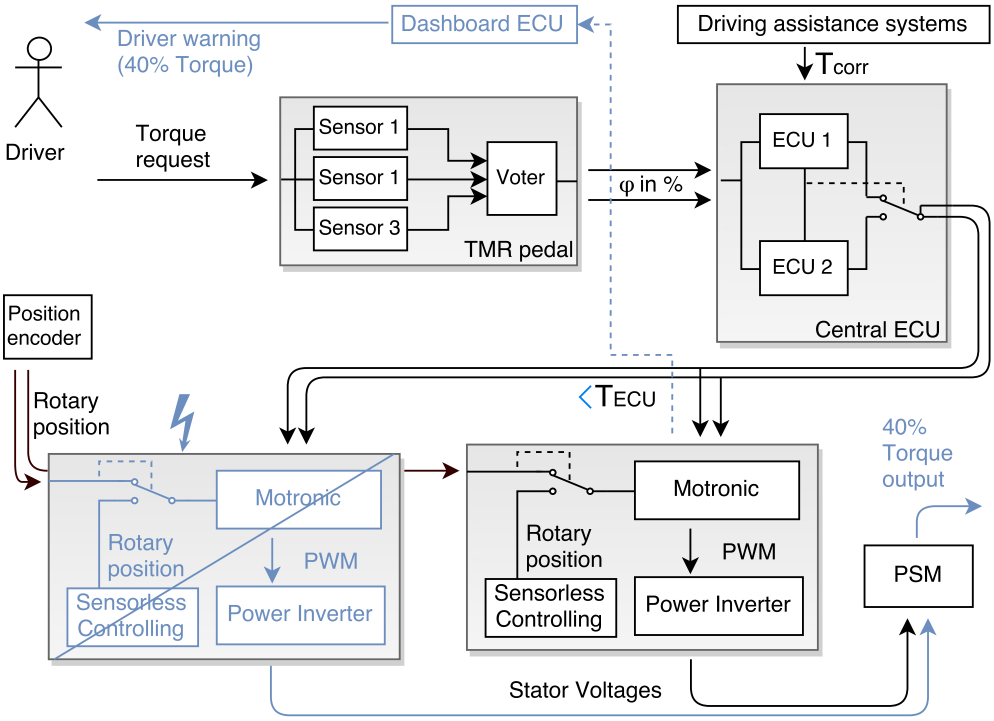


Figure 7.8: Signal flow through the fail-operational architecture after a failure of one Power Inverter & Motronic block.

Failure of one subsystem of the PSM

In case of an open phase or short circuit of one phase, the associated PIM block must transfer to the safe state. Conspicuous values of the stator voltages and currents allow the concerning PIM of the 3 phase subsystem to detect the fault. An ASC is performed and the Motronic of the related PIM informs the dashboard ECU over the bus about the hazard. The dashboard ECU in return gives a warning to the driver that the available propulsion is only on 40%.

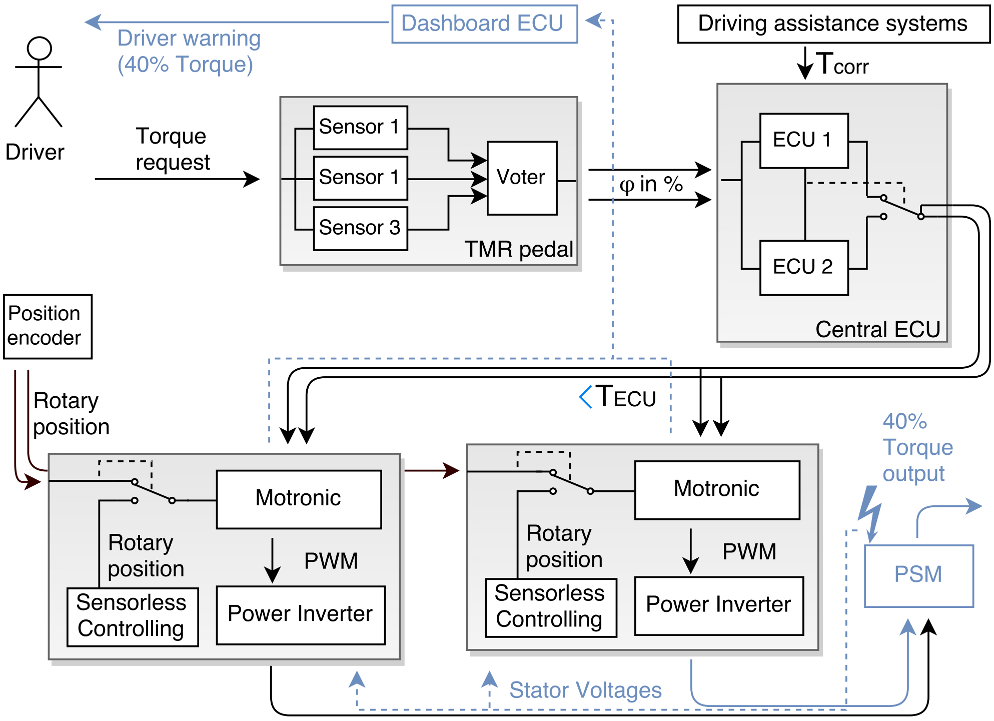


Figure 7.9: Signal flow through the fail-operational architecture after a failure of one 3-phase subsystem of the dual winding PSM.

7.3 Hazard Analysis and Risk Assessment of the fail-operational architecture

Analogue to the basic architecture, a HARA was conducted for the fail-operational architecture to highlight the impact of fail-operational behaviour on the driver safety. The scenarios from the previous HARA were adopted and re-evaluated, considering the fail-operational behaviour and the driver warning system. Assuming the healthy state as starting point for the HARA would not be effective as any first failure is omitted when no CCFs are occurring, instead a degraded state of the fail-operational architecture was chosen as starting point. For the following investigations, it is assumed that one fault already took place which caused the propulsion system to degrade to a maximum of 40 % output performance, any reconfiguration processes are finished, the driver got warned by a dashboard symbol about the situation and is aware about its meaning. The probability of the vehicle being in a degraded state is not used as argumentation to lower the Exposure of the hazard scenarios. Cases assigned with a QM level within the HARA of the basic architecture were not considered.

Table 7.1: HARA results for a loss of the propulsion system.

Loss of propulsion	Mishap potential	S	E	C	ASIL	former ASIL
Overtaking	Frontal crash with oncoming traffic	S3	E2	C1	QM	ASIL A
Turning at intersection with no traffic light regulation	Side crash by another car	S3	E2	C1	QM	ASIL A

A loss of the propulsion system takes place after a second failure of the same component inside the architecture. With the opportunity to warn the driver after the first fault, the awareness of the same increases, especially in the state of degraded performance, improving the controllability for both cases in Tab. 7.1. Moreover, a warned driver will not initiate time critical manoeuvres which require high propulsion, thus a second fault of the same item type only occurs in less critical situations. Both hazards for loss of propulsion are moved from ASIL A to QM because of the improved values of the controllability.

Table 7.2: HARA results for too low propulsion.

Too low propulsion	Mishap potential	S	E	C	ASIL	former ASIL
Overtaking	Frontal crash with oncoming traffic	S3	E1	C2	QM	ASIL A

The same argumentation as in the case of loss of propulsion is applied for too low propulsion while overtaking. Drivers which are aware of the degraded system with lower performance will not start a narrow overtaking manoeuvre which again improves the controllability of the exhibited hazard scenario.

Table 7.3: HARA results for too high propulsion.

Too high propulsion	Mishap potential	S	E	C	ASIL	former ASIL
Starting on an intersection	Crash with a pedestrian	S2	E3	C1	QM	ASIL B
Leaving at highway exit	Stability loss in curve leading to crash	S1	E3	C2	QM	ASIL A
Driving on dry road surface (country road)	Loss of stability	S3	E3	C2	ASIL B	ASIL D
Driving at medium speed (snow surface)	Loss of stability	S3	E2	C3	ASIL A	ASIL B

The risk of too high propulsion from standstill or at low speed is already lowered by the ASC of the faulty motor part. If the remaining healthy motor subsystem also encounters a defect, the second subsystem is short circuited, leading instantly to an even higher braking torque. Also, too high control values are omitted by the TMR structure of the pedal sensor and the hot standby of the ECUs which only forward correct values or none. In consequence, the first entry in Tab. 7.3 retrieves a better controllability and a lower severity, moving its assignment to QM. The second entry, leaving at highway exit, profits from the driver warning system and the reduced performance of the vehicle: Both factors lead to a lower driving speed in general, making a swerving of the rear due to too high propulsion less likely. The same applies for the hazard in the third row of Tab. 7.3, moving the safety level from ASIL D to ASIL B. Also a loss of stability while driving at snow surface is less likely due to the weaker acceleration, but cannot be completely eliminated.

Table 7.4: HARA results for too low brake torque.

Too low brake torque	Mishap potential	S	E	C	ASIL	former ASIL
Leaving at highway exit	Crash with another car in front	S1	E3	C2	QM	ASIL A
Unexpected pedestrians on the street	Accident with pedestrian	S3	E1	C1	QM	ASIL A

As mentioned before, the ASC of the defect sub-system yields to a resistive torque that overlaps with the remaining drive torque of the healthy system, reducing the maximum output power to about 40%. The hazard scenarios for too low brake torque profit from this effect as an shortage of torque is not likely: the braking torque is even higher than regular, especially at low speeds of the vehicle, what lowers the exposure of too low braking torque. Following this consideration, a crash with another car in front while leaving the highway exit is less likely due to the increased braking torque. On one hand, the threat of unexpected pedestrians on city streets is better controlled as the ASC will help to perform a full halt while on low speed. But on the other, pedestrians on country roads define a more severe case as sudden braking from high speed can cause a loss of stability of the vehicle. In general a higher amount of people is encountered during city drive than at country roads or highways, what legitimate the ASC as it suits the more probabilistic case.

Table 7.5: HARA results for too high brake torque.

Too high brake torque	Mishap potential	S	E	C	ASIL	former ASIL
Locking of one or more tyres (below 15km/h)	Loss of stability	S1	E2	C1	QM	ASIL B
Locking of one or more tyres (above 15km/h)	Loss of stability	S3	E2	C2	ASIL A	ASIL B
Wet/snow-covered streets (below 15km/h)	Loss of stability	S2	E2	C3	ASIL A	ASIL B
Wet/snow-covered streets (above 15km/h)	Loss of stability	S3	E2	C3	ASIL B	ASIL B
Driving trough tight bends (below 15km/h)	Swerving of the rear	S1	E2	C2	QM	ASIL A
Driving trough tight bends (above 15km/h)	Swerving of the rear	S2	E2	C2	QM	ASIL A
Driving on dry road (below 15km/h)	Loss of stability	S1	E4	C1	QM	ASIL D
Driving on dry road (above 15km/h)	Loss of stability	S2	E4	C2	ASIL B	ASIL D

The last part of the HARA covers the cases for too high brake torque of the degraded system. As the ASC has a different impact on the vehicle dependent on its speed, all cases were divided into two groups, using 15km/h as borderline between low and medium/high speed. For all cases in Tab. 7.5 below 15km/h, the hazard is lowered as an instant halt will rather take place in case of additional braking torque than a loss of stability. All cases related to higher velocity suffer from instant peak torques, caused by current peaks at the beginning of an short-circuit due to transient effects of the electric machine. While the six phase machine still owns the same short-circuit behaviour of permanent excited synchronous machines, the fractional coil winding technique decouples the subsystems magnetically from each other leading to a distributed flux linkage on the subsystems. The division of the flux leads to lower short circuit peaks, lowering the instantly caused brake torque at the beginning of the ASC. Concerning the HARA, the lower transient braking torque compared to a regular 3-phase machine and the general lower vehicle speed provided by the driver warning and the reduced performance, all cases related to a velocity over 15km/h retrieve a lower ASIL thanks to an improved controllability.

7.4 Fault Tree Analysis of the fail-operational architecture

In this chapter the results of the FTA of the fail-operational architecture are displayed. With the upgrade of all considered weak points against single point failures, the probability of the case *loss of propulsion* is further reduced. The doubling of the DC/DC-Inverter and increased wiring were not taken into account for the revised FTA.

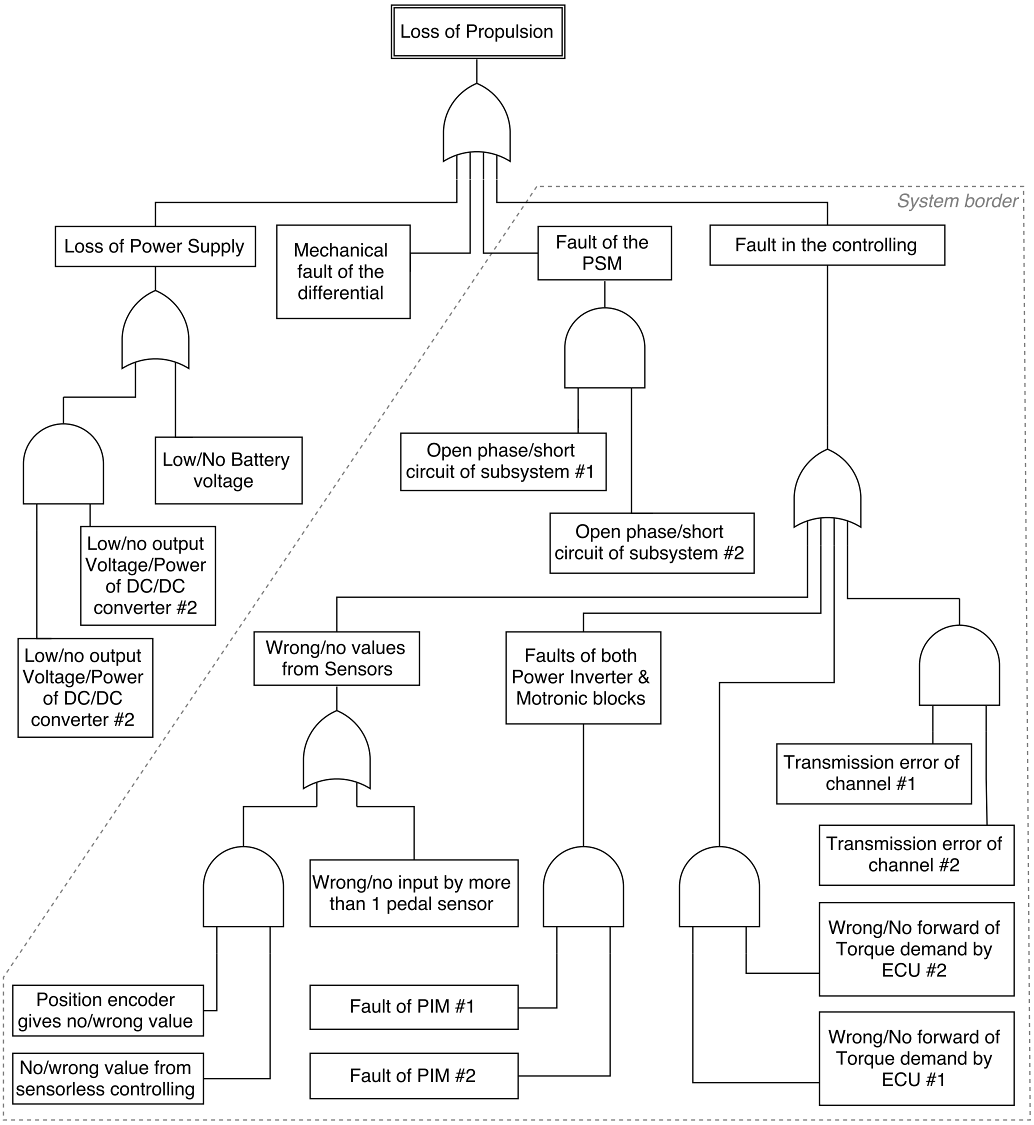

Loss of Propulsion
System border
Loss of Power Supply
Mechanical fault of the differential
Fault of the PSM
Fault in the controlling
Low/No Battery voltage
Open phase/short circuit of subsystem #1
Open phase/short circuit of subsystem #2
Low/no output Voltage/Power of DC/DC converter #2
Low/no output Voltage/Power of DC/DC converter #2
Wrong/no values from Sensors
Faults of both Power Inverter & Motronic blocks
Transmission error of channel #1
Transmission error of channel #2
Wrong/no input by more than 1 pedal sensor
Wrong/No forward of Torque demand by ECU #2
Position encoder gives no/wrong value
Fault of PIM #1
No/wrong value from sensorless controlling
Fault of PIM #2
Wrong/No forward of Torque demand by ECU #1

Figure 7.10: Fault tree analysis of the fault tolerant architecture for the hazard loss of propulsion.

7.5 Warning concept for the Driver

The dashboard ECU provides the architecture with a possibility of warning the driver if any relevant errors occur. In conventional cars, warning lamps for the battery, brakes or the motor exist among others in order to inform the driver if an error occurred. Which particular component failed inside the vehicle is not essential for the driver, but the possible functionality loss or degradation caused by the component fault must be communicated. Also the actions a driver needs to perform as soon as he recognises a warning lamp must be specified and explained in the manual. As unofficial color code in automotive, yellow symbols usually refer to failures which allow a continuing of the driving, sometimes with some restrictions, and red symbols refer to serious faults of the system asking the driver to halt the vehicle as soon as possible. In compliance with this code, two warning signs are intended as driver warning system:

- A yellow symbol (Fig. 7.11, left) which informs the driver that an error occurred which has yet no impact on the output torque but leads to a degradation to a fail silent system, loosing its function with the next failure.
- A yellow or red symbol (Fig. 7.11, right) which is activated in case of a reduction of the output torque, shining in yellow after a degradation to 40 % torque or shining in red in case of a total loss of the output torque.

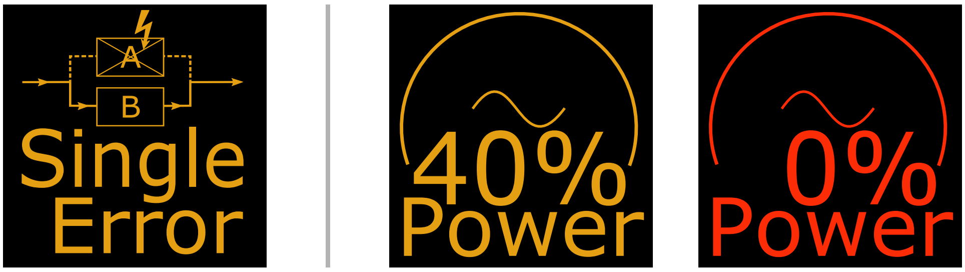


Figure 7.11: Proposed warning symbols displayed at the dashboard for driver information.

In upcoming Table 7.6, the error scenarios from the fail operational section are listed and extended with second failure cases of the same item, plus the warning symbols shown to the driver are displayed. Afterwards the driver behaviour is investigated when exposed to the symbols with or without knowing about their meaning. For an estimation of vehicle trips before a repair is conducted, proposed values of the ISO 26262 part 5 are used:

> Example of assumptions on the average time to vehicle repair, depending on the fault type:
>
> - 200 vehicle trips for reduction of comfort features;
> - 50 vehicle trips for reduction of driving support features;

- 20 vehicle trips for amber warning lights or impacts on driving behaviour;
- one vehicle trip for red warning lights [3]

Following this assumption, the Single Error and the Yellow 40% Power symbol on one hand will lead to an average of 20 vehicle trips before the issue is fixed in a car repair shop. The red 0% Power on the other hand ends the trip and requires reparation before starting over another driving cycle.

Table 7.6: Overview of displayed warning symbols for each single point of failure.

Failing component	**Displayed warning symbols**
One sensor of the TMR pedal	Single Error
Second sensor of the TMR pedal	0% Power
One bus channel	Single Error
Both bus channels	0% Power
One ECU	Single Error
Both ECUs	0% Power
Position encoder or Sensorless controlling	Single Error
Position encoder and Sensorless controlling	0% Power
One Power Inverter & Motronic block	Single Error 40% Power
Both Power Inverter & Motronic blocks	0% Power
One subsystem of the PSM	Single Error 40% Power
Both subsystems of the PSM	0% Power

The proposed warning symbols and their appearance were explained, but are not effective if the driver is not aware of what actions have to be made. The desired reaction of the driver must be specified and noted in the vehicle manual but also driver behaviour must be taken into account in case the human is not familiar with the meaning of the symbols.

Expected driver behaviour when familiar with symbols

First of all we will assume that the driver knowns the meaning of the symbols and recognises them as soon as they appear in the dashboard.

- **Single Error**
  The propulsion system is still working without any flaws in torque, but with higher risk of losing the same. There is no certain prediction possible when a second failure occurs in the affected unit, thus increased attention and awareness of the driver is necessary that the propulsion system might be lost immediately. The driver can continue the current and upcoming driving cycles without any drawbacks in functionality, but in safety. A visit to a car workshop within the next 20 driving cycles is suggested. By successfully warning the driver, the reaction time is shortened if finally propulsion is lowered or lost due to a second fault.
- **Yellow 40% Power**
  The driver is informed that an internal error caused a lowering of the available propulsion to 40%. Driving manoeuvres which rely on propulsion and only have a small time frame to be accomplished should now be avoided. The ongoing driving cycle can be completed and the car remains usable for following cycles, but with reduced performance. Again, a visit to a car workshop within the next 20 driving cycles is suggested and is more likely due to the lower performance. The Single Error symbol is also shown in the dashboard to emphasize the increased probability of propulsion loss.
- **Red 0% Power**
  The propulsion system is now completely lost and moved to a safe state which causes a braking torque in relation of the vehicle speed. The driver must terminate manoeuvres which require propulsion and must try to reach a safe spot with the remaining vehicle speed and finally halt the vehicle. The journey cannot be continued and a breakdown service must be ordered.

Expected driver behaviour when symbols are unknown

As second step, it is assumed that the driver has no knowledge about any meaning of the warning symbols and required countermeasures. The reaction of the driver is difficult to determine as it varies with the experience and state of the driver but nevertheless is carried out below.

- **Single Error**
  The Single Error symbol could create some caution at first, but as it has no impact on the regular vehicle behaviour, it probably is neglected by the driver after some

driving cycles. Some drivers might be curious about the sign and look it up in the manual but the majority won't be bothered too much since it has no influence on functionality. From a safety point of view, it would be reasonable to limit the amount of driving cycles which can be performed after the first appearance of the Single Error symbol. Though this action must be somehow communicated to the driver to avoid a surprisingly non-functional state of the vehicle, which also lowers the availability of the vehicle.

- **Yellow 40% Power**
  A fault followed by degradation of the output torque will be recognised by the driver as soon as he requires acceleration. Keeping the vehicle on a stable speed requires only low torque what makes the impact only slightly noticeable and probably leave it unrecognised at first if there is no warning signal. As soon as the driver recognises the warning symbol, he will be aware of that something is wrong and by reading the 40 % Power probably have the right guess on the degraded propulsion.

- **Red 0% Power**
  A red signal which regularly isn't displayed in the dashboard will cause high caution of the driver, no matter if the meaning is known or not. As the effect of no propulsion combined with a braking torque is directly perceptible, the driver will try to reach a safe spot for the vehicle, no matter if he can identify the propulsion system as root cause or not.

8 Conclusion and Outlook

In the present thesis, the state of the art of fault tolerance methods were analysed in order to pick suitable methods for the automotive engineering sector. Due to the increasing costs, weight and space with every added element, redundant structures exceeding TMR are not applicable. Furthermore, an over excessive use of TMR follows the same rule, why it is only applied to essential input and output variables, elsewhere dynamic methods with hot or cold standby are preferred.

The proposed structure dealt with the impact of loss or malfunction of the vehicles powertrain and what effects are drawn on the driver safety. In order to show the effects of fault tolerant structures, a basic architecture of an electric vehicle was taken and upgraded to a fail-operational one. With the exchange of a conventional 3 phase machine to a 6 phase machine, the architecture is even immune to single drive failures. All root sources for single point failures were identified with a Fault Tree Analysis and countermeasures were set. A HARA was conducted to show the necessity of an adoption and to reveal the influences on exposure, severity and controllability, and with those, on the ASIL. With the FO behaviour of the architecture, the opportunity of early driver warning became possible. A design and concept for the driver warning was presented and expected behaviour of the driver was analysed in the last chapter of the thesis.

As further investigation and development of the architecture, the economic factor of the adoption can be analysed. With tailoring of the level of performance after a failure, investment costs can be reduced on the redundant components. This implies a precise definition about the required length of fault tolerance in order to dimension element performances.

A combination of the propulsion architecture with other high level vehicle functions, as braking and steering, can allow an overall reduction of redundant elements when the resources are shared. The mutual influences of the subsystems must be considered carefully to avoid a decrease of safety due to unexpected situations. Besides an isolated examination of the architectural behaviour of the other systems like it was performed within this thesis for the propulsion system, communication strategies and priorities inside the composed architecture must be defined.

Bibliography

[1] Reif, Konrad: *Automobilelektronik - Eine Einführung für Ingenieure.* 5. Springer Vieweg, 2014. – ISBN 978–3–658–05047–4

[2] Borgeest, Kai: *Elektronik in der Fahrzeugtechnik. Hardware, Software, Systeme und Projektmanagement.* 3. Springer Vieweg, 2014. – ISBN 978–3–8348–1642–9

[3] ISO/FDIS: *ISO 26262: Road vehicles - Functional Safety.* 2011

[4] Tschöke, Helmut: *Die Elektrifizierung des Antriebsstrangs.* 1. Springer Vieweg, 2014. – ISBN 978–3–658–04643–9

[5] Nenninger, Philipp: *Vernetzung verteilter sicherheitsrelevanter Systeme im Kraftfahrzeug*, Universtität Karlsruhe, Diss., 2007

[6] Leveson, Nancy G.: *Engineering a Safer World.* 1. The MIT Press, 2007. – ISBN 7978–3–658–02419–2

[7] Ulbrich, Peter M.: *Ganzheitliche Fehlertoleranz in eingebetteten Softwaresystemen*, Friedrich-Alexander-Universität Erlangen-Nürnberg, Diss., 2014

[8] Isermann, Rolf: *Mechatronische Systeme.* 2. Springer, 2008. – ISBN 978–3–540–32336–5

[9] Isermann, Rolf ; Schwarz, R. ; Stolzl, S.: Fault-tolerant drive-by-wire systems. In: *Control Systems, IEEE* 22 (2002), Oct, Nr. 5, S. 64–81. `http://dx.doi.org/10.1109/MCS.2002.1035218`. – DOI 10.1109/MCS.2002.1035218. – ISSN 1066–033X

[10] Klöber, Thomas ; Spinczyk, Olaf: *Fehlertoleranz in eingebetteten Systemen.* University Lecture, 2006

[11] Isermann, Rolf: *Fahrdynamik-Regelung.* 1. Vieweg, 2006. – ISBN 978–3–8348–0109–8

[12] Manzone, A. ; Pincetti, A. ; De Costantini, D.: Fault tolerant automotive systems: an overview. In: *On-Line Testing Workshop, 2001. Proceedings. Seventh International*, 2001, S. 117–121

[13] Wallentowitz, Henning ; Reif, Konrad: *Handbuch Kraftfahrzeugelektronik.* 1. Vieweg, 2006. – ISBN 978–3–528–03971–4

[14] Flühr, Holger: *Avionik und Flugsicherungstechnik.* Springer, 2010. – ISBN 978–3–642–01611–0

[15] Joahnsson, Roger: A fault tolerant architecture for brake-by-wire in railway cars / Department of Electrical and Computer Engineering, Chalmers Lindholmen University College. 2003. – Forschungsbericht

[16] Kimm, H. ; Ham, Ho-sang: Integrated Fault Tolerant System for Automotive Bus Networks. In: *Computer Engineering and Applications (ICCEA), 2010 Second International Conference on* Bd. 1, 2010, S. 486–490

[17] Zimmermann, Werner ; Schmidgall, Ralf: *Bussysteme in der Fahrzeugtechnik.* 2. Vieweg, 2011. – ISBN 978–3–658–02419–2

[18] Sinha, Purnendu: Architectural design and reliability analysis of a fail-operational brake-by-wire system from ISO 26262 perspectives. In: *Elsevier* (2011)

[19] Sinha, P. ; Agrawal, V.: Evaluation of electric-vehicle architecture alternatives. In: *Vehicle Power and Propulsion Conference (VPPC), 2011 IEEE*, 2011. – ISSN Pending, S. 1–6

[20] Naidu, M. ; Gopalakrishnan, S. ; Nehl, T.W.: Fault-Tolerant Permanent Magnet Motor Drive Topologies for Automotive X-By-Wire Systems. In: *Industry Applications, IEEE Transactions on* 46 (2010), March, Nr. 2, S. 841–848. `http://dx.doi.org/10.1109/TIA.2009.2039982`. – DOI 10.1109/TIA.2009.2039982. – ISSN 0093–9994

[21] Barcaro, M. ; Bianchi, N. ; Magnussen, F.: Six-phase supply feasibility using a PM fractional-slot dual winding machine. In: *Energy Conversion Congress and Exposition (ECCE), 2010 IEEE*, 2010, S. 1058–1065

[22] Barcaro, M. ; Bianchi, N. ; Magnussen, F.: Analysis and tests of a dual three-phase 12-slot 10-pole permanent magnet motor. In: *Energy Conversion Congress and Exposition, 2009. ECCE 2009. IEEE*, 2009, S. 3587–3594

[23] Debouk, Rami ; Fuhrman, Thomas ; Wysocki, Joseph: Architecture of By-Wire Systems Design Elements and Comparative Methodology. In: *SAE Technical Paper*, SAE International, 03 2003

[24] Matthe, Roland ; Turner, Lance ; Mettlach, Horst: VOLTEC Battery System for Electric Vehicle with Extended Range. In: *SAE International Journal of Engines* 4 (2011), Nr. 1, 1944-1962. `http://dx.doi.org/10.4271/2011-01-1373`. – DOI 10.4271/2011–01–1373

[25] Reif, Konrad: *Sensoren im Kraftfahrzeug.* 2. Springer Vieweg, 2012. – ISBN 978–3–8348–1778–5

[26] Süss, Christopher: *Maßnahmen der funktionalen Sicherheit für einen elektrischen Fahrzeugantrieb*, Hochschule für Technik und Wirtschaft Berlin, Diss., 2015

[27] Teigelkötter, Johannes: *Energieeffiziente elektrische Antriebe.* 1. Springer Vieweg, 2012. – ISBN 978–3–8348–1938–3

[28] Eilenberger, A. ; Schrödl, M. ; Demmelmayr, F.: Elektrofahrzeuge mit Permanentmagnet- Synchronmaschinen. In: *e & i Elektrotechnik und Informationstechnik* 128 (2011), Nr. 1-2, 40-46. `http://dx.doi.org/10.1007/s00502-011-0804-z`. – DOI 10.1007/s00502–011–0804–z. – ISSN 0932–383X

[29] Wagner, Bernhard ; Haala, Oliver ; März, Martin ; Hofmann, Max: The externally excited synchronous machine as a traction drive, 2012

[30] Bianchi, N. ; Bolognani, S. ; Zigliotto, M.: Analysis of PM synchronous motor drive failures during flux weakening operation. In: *Power Electronics Specialists Conference, 1996. PESC '96 Record., 27th Annual IEEE* Bd. 2, 1996. – ISSN 0275–9306, S. 1542–1548 vol.2