
Safety Concepts for future Electromechanical Brake Systems

Von der Fakultät für Ingenieurwissenschaften, Abteilung Maschinenbau und Verfahrenstechnik
der
Universität Duisburg-Essen

zur Erlangung des akademischen Grades

eines

Doktors der Ingenieurwissenschaften

Dr.-Ing.

genehmigte Dissertation

von

Simon Daniel Schrade
aus
Weingarten

Gutachter: Univ.-Prof. Dr.-Ing. Dr. h.c. Dieter Schramm
Univ.-Prof. Dr.-Ing. Lars Mikelsons

Tag der mündlichen Prüfung: 24.07.2024

DuEPublico

Duisburg-Essen Publications online

UNIVERSITÄT
DUISBURG
ESSEN

Offen im Denken

ub | universitäts
bibliothek

Diese Dissertation wird via DuEPublico, dem Dokumenten- und Publikationsserver der Universität Duisburg-Essen, zur Verfügung gestellt und liegt auch als Print-Version vor.

DOI: 10.17185/duepublico/82265

URN: urn:nbn:de:hbz:465-20240809-155016-7

Alle Rechte vorbehalten.

Kurzfassung

Elektromechanische Bremssysteme (EMB-Systeme) erlangen derzeit große Aufmerksamkeit in der Automobilindustrie. Ein erster Einsatz in der Großserie steht unmittelbar bevor. Hierbei werden die EMB-Aktuatoren jedoch lediglich auf der Hinterachse in Kombination mit einem hydraulischen Bremssystem auf der Vorderachse eingesetzt, wodurch die Sicherheitsanforderungen an das EMB-System erheblich reduziert sind. Diese Promotion befasst sich mit den hierfür notwendigen Sicherheitskonzepten für reine EMB-Systeme auf Basis aktueller Gesetzgebung und Normen.

Das EMB-System stellt hierbei einen *Item* (gemäß ISO 26262) dar, für den durch eine Gefahren- und Risikoanalyse Sicherheitsziele mit entsprechendem ASIL ermittelt werden. Die Analyse zeigt, dass das EMB-System geringe Verzögerungen mit ASIL D gewährleisten muss, während hohe Verzögerungen grundsätzlich niedrigere ASIL zuzuordnen sind. Des Weiteren wird gezeigt, dass durch den Einsatz von dissimilaren Redundanzen, wie zum Beispiel eines verzögerungsfähigen Parkbremssystems oder rekuperationsfähigen Antriebs, die erforderliche Sicherheit des EMB-Systems gesenkt werden kann.

Der Nachweis der Sicherheit des *Items* EMB-System erfolgt durch eine unabhängige Analyse der einzelnen Sub-Systeme, die aus Pedal, Energieversorgung, zentrale Steuerung und EMB-Aktuator bestehen. Hierzu wird zunächst eine Komponenten-Bibliothek erstellt, die verschiedene Ausführungsoptionen (z.B. die Implementierung von internen Sicherheitsmechanismen und Redundanzen) berücksichtigt. Der Nachweis der Sicherheit erfolgt anschließend durch die Anwendung einer Methodik, die in einer Vorarbeit (Ebner, 2024) entstanden ist, auf Basis einer vollständigen Sub-System-Permutation. Abschließend wird anhand der, als *sicher* bewerteten, Sub-Systeme gezeigt wie *sichere* EMB-Systeme aussehen können.

Ein weiterer Fokus dieser Arbeit besteht in der Berücksichtigung von elektrischen Fahrzeugantrieben (Stichwort: X-Domain) zur Bereitstellung der Bremsfunktionalität. Hierbei werden zwei Ansätze verfolgt. Der erste Ansatz besteht in der Aktuierung einer Verzögerung durch die Rekuperation des elektrischen Antriebs. Der zweite Ansatz nutzt das zur Verfügung stehende Steuergerät des Antriebs als Backup für ausgefallene Steuergeräte des EMB-Systems durch die Anwendung sog. Graceful Degradation. Es wird gezeigt, dass in Abhängigkeit der Antriebstopologie (Ein- vs. Zwei-Achs-Antriebe) und der Leistungsfähigkeit des Antriebs verschiedene Ansätze zur Sicherstellung der Bremsfunktionalität vielversprechend sind.

Schlagwörter: Funktionale Sicherheit, ISO 26262, Gefahren- und Risikoanalyse, Elektromechanische Bremse, EMB-System, X-Domain

Abstract

Electromechanical brake systems (EMB-systems) are currently attracting big interest in the automotive industry. Their first use in large-scale production is imminent. However, the EMB-actuators are only used on the rear axle in combination with a hydraulic brake system on the front axle, which significantly reduces the safety requirements for the EMB-system. This work deals with the safety concepts required for pure EMB-systems on the basis of current legislation and standards.

The EMB-system represents an *item* (according to ISO 26262) for which safety goals with corresponding ASIL are determined by the means of a hazard analysis and risk assessment (HARA). The analysis shows that the EMB-system must guarantee low decelerations with ASIL D, while high decelerations are generally to be assigned to lower ASILs. Furthermore, it is shown that the required safety of the EMB-system can be lowered by using dissimilar redundancies, such as deceleration-capable parking brake systems or recuperation-capable powertrains.

The safety assessment of the *item* EMB-system is performed by an independent analysis of the individual sub-systems consisting of the pedal, power supply, central control and EMB-actuator. For this purpose, a component library is first created that takes into account different implementation options (e.g., internal safety mechanisms and redundancies). The proof of safety is then performed by applying a methodology, which has been developed in a preliminary work (Ebner, 2024), on the basis of a complete sub-system permutation. Finally, the sub-systems evaluated as *safe* are used to show how *safe* EMB systems can look like.

A further focus of this PhD consists of considering electrical powertrains regarding their capability to provide a braking functionality. Therefore, two approaches are followed. First, the recuperation is considered as a means to decelerate. Second, the control unit of the powertrain is used as a backup for a failed control unit dedicated to the braking system due to the application of graceful degradation. It is shown that different approaches to guarantee the braking functionality are promising, depending on the powertrain topology (single vs. dual axle powertrain) and the performance of the powertrain.

Keywords: Functional Safety, ISO 26262, Hazard Analysis and Risk Assessment, HARA, Electromechanical Brake, EMB-System, X-Domain

Table of Contents

Kurzfassung	III
Abstract	V
Table of Contents	VII
Table of Figures	XII
Table of Tables	XV
Abbreviations.....	XVII
Symbols	XXI
1 Motivation and Structure	1
1.1 Motivation	1
1.2 Scientific Questions	1
1.3 Structure.....	2
2 Introduction to Vehicle Safety	5
2.1 Safety in General	5
2.1.1 Public Safety	5
2.1.2 Traffic Safety	7
2.2 Motivation for Functional Safety	9
2.2.1 Boeing 737-Max Aircraft.....	9
2.2.2 Fukushima Daiichi Nuclear Powerplant	9
2.3 Safety related to Legislation	11
2.4 Safety related to Norms: ISO 26262 for E/E-Systems of Vehicles	14
2.4.1 Item Definition.....	14
2.4.2 Hazard Analysis and Risk Assessment	14
2.4.3 ASIL Decomposition	14
2.4.4 Impact of the ASIL related to the development	15
2.5 Methodologies in the Functional Safety Domain	17

2.5.1	Fault Tree Analysis (FTA).....	17
2.5.2	Markov Analysis	18
2.5.3	Failure Mode and Effect Analysis (FMEA).....	19
2.5.4	Common Cause Analysis	20
2.5.5	Applied Methodology	20
2.6	Fundamentals of Functional Safety	22
2.6.1	Failure Classification	22
2.6.2	Fault Reaction and Failure Effects.....	22
2.6.3	Safety Concepts	23
2.7	Determination of Hardware Part Failure Rates	25
2.7.1	Models for predicting the lifetime of components.....	25
2.7.2	E/E Components	26
2.7.3	Mechanical Components.....	27
3	Derivation of X-Domain Safety Goals	29
3.1	X-Domain Hazard Analysis and Risk Assessment.....	29
3.1.1	Definition by ISO 26262-3	29
3.1.2	State of the Art	31
3.1.3	Determination of the Exposure	34
3.1.4	Determination of the Severity	36
3.1.5	Derivation of X-Domain Safety Goals	38
3.2	Safety Assessment of Braking System Malfunctions.....	40
3.2.1	Determination of the Safety Goals.....	40
3.2.2	Decomposition of Availability between Service- and Parking Braking System	42
3.3	Availability Decomposition between Braking and Powertrain System	45
3.3.1	Safety-Impact of a reliable Powertrain onto the Braking System.....	45
3.3.2	Deceleration-Potential of a Powertrain	45
3.3.3	Decomposition Options	47
4	Safety Concepts of Electromechanical Brake Systems	51
4.1	Definition of the ‚Item‘	51

4.2 Related Work.....	53
4.2.1 Brake-by-Wire Pedal Boxes	53
4.2.2 Electromechanical Brake Actuators.....	54
4.2.3 Energy Supply.....	57
4.2.4 Central-Control-System	58
4.3 Brake-by-Wire Pedal Box	60
4.3.1 System Definition and Safety Goals	60
4.3.2 Conventional Safety Concepts	62
4.3.3 X-Domain Safety Concepts	63
4.3.4 Safety Concepts with Virtual Sensors for Diagnosis.....	63
4.3.5 Intermediate Conclusion	65
4.4 Electromechanical Brake Actuator	67
4.4.1 Related Safety Goals.....	67
4.4.2 Actuation Unit Redundancy Concepts.....	68
4.4.3 Failure Effects due to Sensor Failures	69
4.4.4 Simple Actuator	70
4.4.5 Semi-Smart Actuator	71
4.4.6 Smart Actuator	74
4.4.7 Intermediate Conclusion	77
4.5 Central Control System of the Brake System.....	79
4.5.1 System Definition	79
4.5.2 Related Safety Goals.....	81
4.5.3 Failure Effects due to Sensor Failures	81
4.5.4 Brake Topologies with Simple Actuators	82
4.5.5 Brake Topologies with smart and semi-smart Actuators.....	84
4.5.6 Intermediate Conclusion	88
4.6 Excuse: Energy-Supply	89
4.6.1 System Definition and Safety Goals	89
4.6.2 Results.....	90
4.7 Composition of the EMB-System.....	91

4.7.1	Simple Actuators.....	91
4.7.2	Semi-Smart and Smart Actuators.....	92
4.7.3	Comparison of the Concepts	93
5	Safety Concepts for Joint Braking and Powertrain Systems	95
5.1	Definition of the ,Item‘	95
5.2	Related Work.....	97
5.2.1	Safety Goals related to the Item Powertrain	97
5.2.2	Powertrain System	98
5.3	Drive Pedal Box.....	100
5.3.1	Conventional Safety Concepts	100
5.3.2	X-Domain Safety Concepts	101
5.4	Safety Analysis of the reference Powertrain Systems	104
5.4.1	Design Space.....	104
5.4.2	Failure Effects due to Sensor Failures	105
5.4.3	Safety Analysis of a single Powertrain	106
5.4.4	Safety Analysis of Dual Powertrains	108
5.5	Graceful Degradation at X-Domain ECUs.....	110
5.5.1	Introduction to X-Domain Graceful Degradation.....	110
5.5.2	Safety Assessment of generic X-Domain ECUs.....	111
5.5.3	Safety Assessment of an increased Availability Approach	112
5.5.4	Application of the increased Availability Approach	113
5.6	Composition of a Joint Braking and Powertrain System.....	117
5.6.1	Initial Considerations	117
5.6.2	Single Powertrain System	118
5.6.3	Dual Powertrain System with increased Availability	120
5.6.4	Conclusion	123
6	Conclusion and Outlook.....	125
6.1	Conclusion.....	125
6.2	Outlook	126

Appendix	129
References	160
Publications of the Author.....	182
Patents of the Author	184
Supervised Theses	187

Table of Figures

Figure 2.1: Death Probabilities of different societies.....	6
Figure 2.2: Death Probability by Causes in US society	7
Figure 2.3: Dependence of Traffic Safety on Country	8
Figure 2.4: Exemplary FTA logic diagram	17
Figure 2.5: Markov state graph for a single unit, oriented at	18
Figure 2.6: Markov flow diagram	19
Figure 2.7: Types of Redundancy	24
Figure 2.8: Idealized bathtub curve.....	26
Figure 2.9: FE-Shares for the allocation of the FM 'blocking'.....	28
Figure 3.1: Derivation of the ASIL	30
Figure 3.2: Operation space at a specific friction coefficient	34
Figure 3.3: Hat-function to determine the merged probabilities	35
Figure 3.4: Exposure of the operation space at μ_{high}	35
Figure 3.5: Exposures of the operation space at reduced friction coefficients	36
Figure 3.6: Introduction of the <i>safe area</i>	36
Figure 3.7: Driving situation under analysis	37
Figure 3.8: Crash scenarios	37
Figure 3.9: Generic SGs for high friction coefficients ($\mu=1.1$)	38
Figure 3.10: Generic SGs for degraded braking at reduced friction coefficients	39
Figure 3.11: Data foundation of deriving the recuperation probability	46
Figure 3.12: Availability of the recuperation capability	47
Figure 3.13: Remaining deceleration on the braking system	48
Figure 4.1: Definition of the item.....	52
Figure 4.2: Generic hardware of an ECU.....	56
Figure 4.3: Generic Actuation Unit.....	56

Figure 4.4: Exemplary pedal box topology	60
Figure 4.5: Definition of the brake pedal system	62
Figure 4.6: Failure rates of conventional pedal box architectures	63
Figure 4.7: Safety comparison of Drive pedal and VS as means for diagnosing faults.....	63
Figure 4.8: SaRA of a circuit equipped with a VS	64
Figure 4.9: Fail behavior of two circuits equipped with VS, no COM	65
Figure 4.10: Fail behavior of number of sensors vs. VS, no COM.....	65
Figure 4.11: Failure Mode Distribution of Simple Actuator architectures	70
Figure 4.12: Safety assessment <i>semi-smart</i> actuator.....	71
Figure 4.13: Safety assessment of a <i>semi-smart</i> actuator with PB backup	72
Figure 4.14: Safety assessment of a <i>semi-smart</i> actuator with PB system backup.....	73
Figure 4.15: Safety assessment of a <i>semi-smart</i> actuator with PB as SM	73
Figure 4.16: Safety assessment of a <i>semi-smart</i> actuator with a default backup.....	74
Figure 4.17: Safety assessment of a <i>smart</i> actuator	75
Figure 4.18: Safety assessment of a <i>smart</i> actuator with a backup PB	75
Figure 4.19: Safety assessment of a <i>smart</i> actuator with a backup PB system.....	76
Figure 4.20: Safety assessment of a <i>smart</i> actuator with a PB as SM	76
Figure 4.21: Safety assessment of a <i>smart</i> actuator with a default backup.....	77
Figure 4.22: Comparison of the safety concepts	78
Figure 4.23: Impact of the design options onto the safety of centralized design.....	80
Figure 4.24: Safety assessment of a X-Circuit equipped with simple actuators	82
Figure 4.25: Safety assessment of an H-Circuit equipped with <i>simple</i> actuators	83
Figure 4.26: Safety assessment of a centralized topology equipped with <i>simple</i> actuators.....	83
Figure 4.27: Safety assessment of <i>smart</i> and <i>semi-smart</i> X-Circuit topologies	85
Figure 4.28: Safety assessment of <i>smart</i> and <i>semi-smart</i> H-Circuit topologies.....	86
Figure 4.29: Safety assessment of <i>smart</i> and <i>semi-smart</i> centralized topologies	86
Figure 4.30: Safety assessment of <i>smart</i> and <i>semi-smart</i> ring-topologies.....	87
Figure 4.31: Overview of the PMHF related to the energy-supply.....	90
Figure 4.32: Composition of <i>simple</i> actuator systems achieving functional safety.....	91
Figure 4.33: Composition of <i>simple</i> actuator systems avoiding product liability.....	92

Figure 4.34: Composition of <i>semi-smart</i> or <i>smart</i> actuator systems achieving functional safety	92
Figure 4.35: Composition of <i>semi-smart</i> and <i>smart</i> actuator systems avoiding product liability	93
Figure 5.1: Definition of the item powertrain	96
Figure 5.2: Generic architecture of a PT	99
Figure 5.3: E-Gas concept.....	100
Figure 5.4: Safety assessment of drive pedals.....	101
Figure 5.5: Minimum X-Domain pedal box.....	102
Figure 5.6: Safety analysis of the X-Domain pedal box	103
Figure 5.7: Design space of the PT system	104
Figure 5.8: PT related to FE due to sensor failures	105
Figure 5.9: Main effects of the components related to failures and costs	106
Figure 5.10: Safety assessment of a single PT	107
Figure 5.11: Safety assessment of dual PT with single MCU.....	108
Figure 5.12: Safety assessment of a dual PT with two MCUs.....	109
Figure 5.13: Markov-diagram of a tri-lane ECU with one spare lane.....	111
Figure 5.14: X-Domain graceful degradation for a reference ECU.....	112
Figure 5.15: X-Domain graceful degradation with functionalities as comfort features.....	113
Figure 5.16: Application of the increased availability approach as PMHF [1/h]	116
Figure 5.17: Powertrain as active redundancy to achieve ASIL D SaRA.....	117
Figure 5.18: Powertrain as passive redundancy to achieve increased availability.....	118
Figure 5.19: X-Domain architectures with <i>simple</i> actuators.....	119
Figure 5.20: X-Domain systems with <i>semi-/smart</i> actuators	120
Figure 5.21: X-Domain highly available <i>simple</i> actuator systems.....	121
Figure 5.22: X-Domain highly available centralized <i>semi-/smart</i> actuator systems.....	122
Figure 5.23: X-Domain highly available H-Circuit <i>semi-/smart</i> actuator systems.....	122

Table of Tables

Table 2.1: Legislation related to the design of intact service braking systems.....	11
Table 2.2: Legislation related to the performance of intact service braking systems.	12
Table 2.3: Legislation related to the design concerning failures of service braking systems.	12
Table 2.4: Legislation related to the performance of degraded service braking systems	12
Table 2.5: Hardware metrics	16
Table 2.6: Reference Diagnostic Coverages of Safety Mechanisms	27
Table 3.1: Determination of the exposure	30
Table 3.2: Determination of the severity.....	31
Table 3.3: Determination of the controllability.....	31
Table 3.4: Disclosed ASILs for malfunctions considering deceleration.....	32
Table 3.5: Failure patterns.....	40
Table 3.6: Overview of analyzed configurations	41
Table 3.7: Summary of the Safety Goals	42
Table 3.8: Suitability of the PB as backup	43
Table 3.9: Options for lowering the ASIL of a brake-system.....	45
Table 3.10: PT as standby redundancy for an ASIL C brake-system	48
Table 3.11: PT as a standby-redundancy for an ASIL B brake-system.....	49
Table 4.1: Degrees of Complexity of an EMB actuator.....	54
Table 4.2: Redundancy concepts EMB-actuator.....	57
Table 4.3: Power supply topologies	57
Table 4.4: CCS topologies	59
Table 4.5: Similar redundancy concepts	68
Table 4.6: PB concepts.....	69
Table 4.7: Design space options for the topology.....	79

Table 4.8: ‘Best’ design options for CCS connected to <i>simple</i> actuators	84
Table 4.9: ‘Best’ design options for CCS connected to <i>semi-smart</i> and <i>smart</i> actuators	87
Table 4.10: Energy-supply topologies	89
Table 5.1: Installed MCUs within PT systems.....	114
Table 5.2: Installed VCUs within the EMB-CCS	114
Table 5.3: VCU designs suitable to increase the availability.....	115

Abbreviations

Abbrev.	Terminology
ABS	Anti-Blocking System
ADC	Analog-Digital-Converter
AEB	Automatic Emergency Brake
AIS	Abbreviated Injury Scale
ASIC	application-specific integrated circuit
ASIL	Automotive Safety Integrity Level
ASM	Asynchronous Motor
AU	Actuation Unit
BBW	Brake-by-Wire
C	Controllability
CAN	Controller Area Network (Communication Bus)
CCS	Central Control System
CoG	Centre of Gravity
COM	Communication
Config	Configuration
CPU	Central Processing Unit
DC	Diagnostic Coverage
DPF	Dual-point faults
E	Exposure
E/E	Electric and Electronic
ECC	Error detection Correction Code
ECE	Economic Commission for Europe

ECU	Electronic Control Unit
EGAS	Electronic Gas
eM	Electric Motor
EMB	Electromechanical Brake
ESM	Externally excited Synchronous Motor
ESP	Electronic Stability Program
F	Front
fd	fail-degraded
FE	Failure Effect
FHA	Functional Hazard Analysis
FM	Failure Mode
FMEA	Failure Mode and Effect Analysis
FMVSS	Federal Motor Vehicle Safety Standards
fo	fail-operational
fooc	fail-out-of-control
fp	fail-passive
FSC	False Situation Classification
FTA	Fault-Tree Analysis
GD	Graceful Degradation
HARA	Hazard Analysis and Risk Assessment
HASS	Highly Accelerated Stress Screening
HV	High Voltage
I	Current-Sensor
IIHS	Insurance Institute for Highway Safety
ISS	Injury Severity Scale
LFM	Latent Fault Metric
LiDAR	Light imaging, Detection And Ranging

LV	Low Voltage
MAIS	Maximum Abbreviated Injury Scale
MCU	Motor Control Unit
NHTSA	National Highway Traffic Safety Administration
NOP	Normal Operation
PB	Parking Brake
PDU	Power Distribution Unit
PE	Power Electronics
PMHF	Probabilistic Metric for Hardware Faults
PMSM	Permanent Magnet Synchronous Motor
PT	Powertrain
QM	Quality-Managed
R	Rear
RAM	Random Access Memory
ROM	Read-Only Memory
RPS	Rotor Position Sensor
S	Severity
S _{ACC}	Accelerator/Drive Pedal
SaRA	Safety-related Availability
S _{BRK}	Brake Sensor
SG	Safety Goal
SM	Safety Mechanism
SoC	State of Charge
SOTIF	Safety Of The Intended Functionality
SPFM	Single Point Fault Metric
T	Temperature-Sensor
T _x	Torque

VCU	Vehicle Control Unit
VS	Virtual Sensor
WSS	Wheel Speed Sensor
RPS	Motor-Position-Sensor

Symbols

Latin Signs:

Sign	Unit	Description
a	m/s ²	Deceleration
b	-	Braking
c _a	-	Cornering Stiffness
DC	-	Diagnostic Coverage
F	N	Force
g	m/s ²	Gravitational Constant
l	m	Length
m	kg	Mass
P	-	Probability
P	kW	Power
P*	kW/kg	specific Power
R	-	Reliability
s	-	Share
t	h or s	Time
T	°C	Temperature
v	km/h	Vehicle Speed
wf	-	Weighting factor
x	m	Distance in x-Direction to CoG
y	m	Lateral Expansion of the vehicle
z	m	Height from CoG

Greek Signs:

Sign	Unit	Description
α	rad	Tire Slip Angle
β	rad	Vehicle Slip Angle
δ	rad	Steering Angle
λ	1/h	Failure Rate
μ	-	Friction Coefficient
π	-	Constant
σ	%	slope
ψ'	rad/s	Vehicular Angular Speed

1 Motivation and Structure

1.1 Motivation

Current braking systems, such as those used in passenger vehicles, rely on hydraulic fluid that actuates a piston in the base brake on the wheel to decelerate the vehicle. The pressure of the hydraulic fluid itself is created by an (e)booster (Verband der Automobilindustrie, 2016) which amplifies the pressure of the brake pedal. These proven hydraulic braking systems are currently being challenged by Electromechanical Brake (EMB) systems. Research into EMB-systems has been going on for decades (Semsch, et al., 2012). Nonetheless, the safety challenges and the costs associated with a reliable power supply have prevented its use for series production. However, with the market penetration of electric vehicles and the introduction of steer-by-wire, the boundary conditions will soon change. Finally, a market launch of a hybrid braking system with EMB-actuators on the rear and a hydraulic system on the front axle has been announced in late 2022 (Continental AG, 2022).

EMB-systems replace the hydraulic fluid with an x-by-wire system that controls electric motors located at the base brake that eventually apply a force. On the one hand, the automotive industry expects a reduction in maintenance and manufacturing costs due to the elimination of hydraulic fluids in the braking system. On the other hand, the technology change poses significant safety challenges. Current hydraulic systems ensure safety through a purely mechanical connection that provides a mechanical push-through in the event of an E/E (electric- and/or electronic) failure. This backup-concept is, however, abandoned, if the use of hydraulic fluid is discontinued. Therefore, new safety concepts need to be developed to ensure true electronic fail-operational capability of EMB-systems.

1.2 Scientific Questions

The introduction of EMB-systems poses significant safety challenges. Therefore, this thesis aims to answer the main question:

Q: *How can safety be ensured for future EMB-systems?*

First of all, however, it is necessary to be specified what *safety* is. Hence, a first sub-question has to be answered:

Q.1: *What requirements must be met to ensure that an EMB-system is safe?*

Based on the requirements, it may be possible to design *safe* EMB-systems. However, the means to ensure safety are not yet defined. On the one hand, redundancy (similar) within the braking system can be implemented to ensure safety. On the other hand, dissimilar redundancy, implemented by the parking brake (PB) or the powertrain (PT) system may also be used to ensure safety. A further sub-question must therefore be asked:

Q.2: *Which concepts guarantee the required safety?*

Finally, the concepts studied can be collected and analyzed to answer the last sub-question:

Q.3: *Which EMB-system designs are safe and suitable?*

1.3 Structure

This work starts with an **Introduction to Vehicle Safety** (chapter 2). It discusses what safety is (section 2.1) and illustrates the need for functional safety on behalf of two preventable catastrophes (section 2.2). It then presents legislation (section 2.3) and functional safety standards (section 2.4) related to the safety of braking. Important methodologies (section 2.5) and the fundamentals of functional safety (section 2.6) are also provided. Finally, the hardware failure rates that form the basis for the safety analyses are derived in section 2.7.

Chapter 3 derives the **X-Domain¹ Safety Goals** (SGs) that must be satisfied by the braking system, to answer the question *Q.1*. Therefore, a Hazard Analysis and Risk Assessment (HARA) is performed first (section 3.1). In addition, it is analyzed how the derived SGs can be assigned to dissimilar redundancies, such as the PB (section 3.2) or PT system (section 3.3). Finally, chapter 3 provides a basis for answering the question *Q.2*.

Chapter 4 applies the derived SGs and examines **Safety Concepts for EMB-Systems** based on the state-of-the-art (section 4.2). For this purpose, the item EMB-system (as defined in section 4.1) is divided into the following systems: pedal (section 4.3), EMB-actuator (4.4), central control system (section 4.5) and power-supply (section 4.6). Finally, these systems are assembled into an EMB-system (section 4.7) to satisfy safety from a functional safety and product liability point of view.

Finally, chapter 5 examines the **Safety Concepts for Joint Braking and Powertrain Systems**. Therefore, the item PT is defined (section 5.1) on the basis of the state-of-the-art (section 5.2). The item powertrain is then divided into the pedal (section 5.3) and the actuator at the axle (section 5.4). Section 5.5 examines the impact of X-Domain graceful degradation (GD) which can be applied by the braking and PT ECU (electronic control unit). Finally, the

¹ X-Domain describes a vehicle feature that is implemented by the application of different vehicle domains. These domains, generally, consist of: brake and powertrain (scope of this work), and steering and suspension (not scope of this work).

braking and the PT systems are merged in section 5.6 to analyze X-Domain synergies that can be exploited. This work ends with a short **Conclusion and Outlook** in chapter 6.

2 Introduction to Vehicle Safety

Safety is an important value, not only in engineering, but also in society. Section 2.1 discusses the current state of public and traffic safety. It also shows how traffic safety has been improved due to electronical and electrical (E/E) systems. It then describes, the consequences of poorly designed E/E-systems, which ultimately degrade safety, to motivate the need for functional safety. Sections 2.3 and 2.4 focus on safety from a requirements point of view, considering both legal and normative requirements. Finally, the methodologies used (section 2.5) and the state of the art (section 2.6) in functional safety are described, before concluding the chapter with the determination of hardware part failure rates (section 2.7).

2.1 Safety in General

Braking devices such as those presented in chapters 3 and 4 must be labelled as “safe” in order to be approved by societies and authorities. Therefore, it is necessary to first describe the operating environment of such “safe” systems. Finally, both public and traffic safety are briefly discussed.

2.1.1 Public Safety

Public safety is a broad topic influenced by various factors including region, age and gender of the population. The unit of measurement for *safety* may also vary depending on the context. For instance, the automotive industry measures *safety* by achieving specific failure rates. Therefore, this section focuses, similarly, on death rates as measurement unit.

The scope of this section is to compare the death probabilities of societies (taken from (Our World in Data, 2022)) with the required failure rates of automotive systems (refer to section 2.4). Figure 2.1 displays the selected death probabilities for comparison. It is clear that there is no universal probability of death. Figure 2.1, however, shows that the demanded PMHF (Probabilistic Metric for random Hardware Failures) for ASIL C (Automotive Safety Integrity Level) and ASIL D (refer to section 2.4) remain at the same probability level as the

age groups with the lowest mortality (5 to 29 years). This indicates that individuals in higher age groups are more likely to die than to experience a specific ASIL D or ASIL C malfunction in a car.

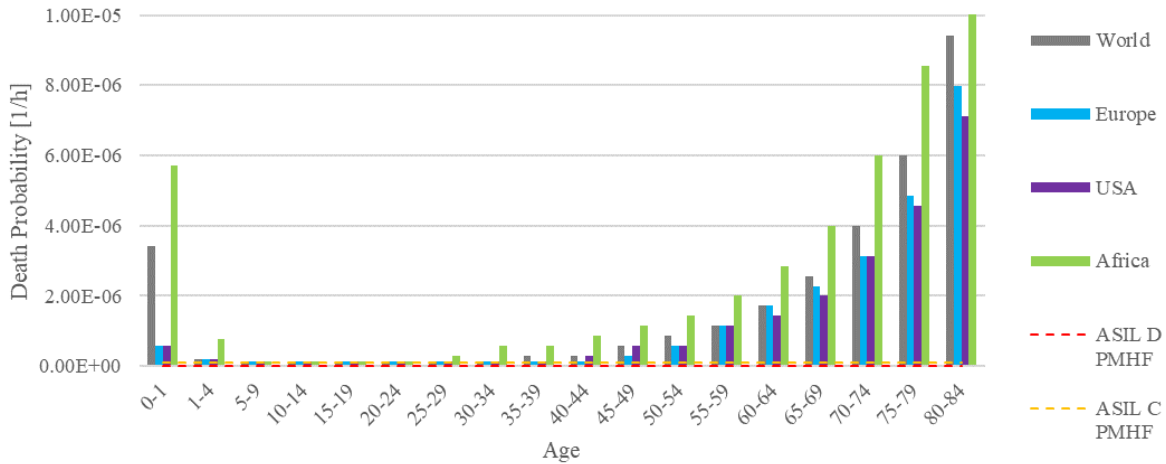


Figure 2.1: Death Probabilities of different societies, data from (Our World in Data, 2022) (year: 2019)

This analysis can be further deepened by considering the causes of death (retrieved from (Mosher & Gould, 2018)). As shown in Figure 2.2, the probability of a randomly selected person dying from heart disease or cancer is higher than experiencing an ASIL C malfunction in a car. When considering ASIL D malfunctions, even more causes of death become more likely. Additionally, being a victim of murder or gun assault is almost as likely as experiencing such a malfunction.

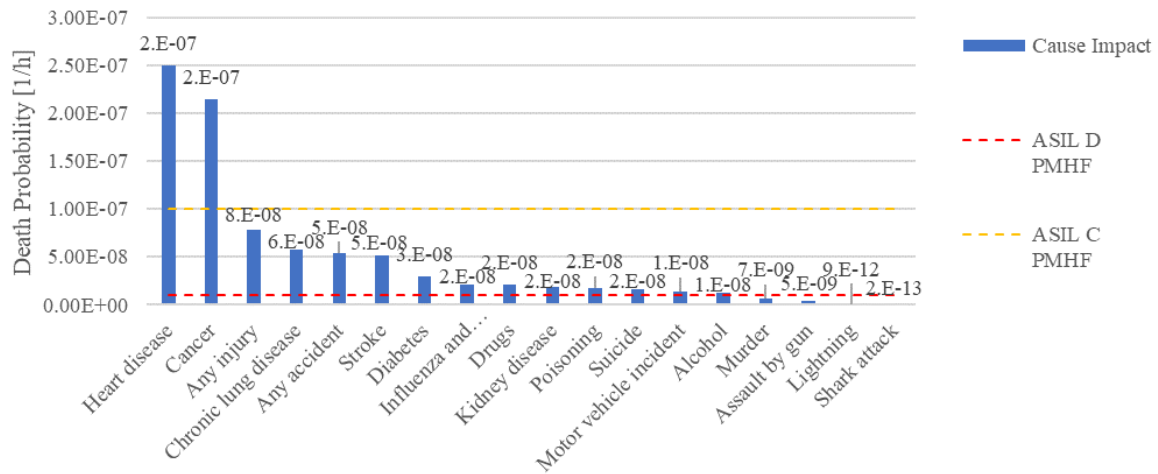


Figure 2.2: Death Probability by Causes in US society, data acquired by (Mosher & Gould, 2018)

2.1.2 Traffic Safety

Traffic safety varies by region, as does public safety (see Figure 2.1). Worldwide traffic safety improved by approximately 12% between 2000 and 2019, as shown in Figure 2.3. However, this trend does not apply to every country. For example, the Dominican Republic and Zimbabwe have experienced increasing traffic death rates, which are the highest in the world. In contrast, France and Germany have experienced a further decrease (approx. 60%) in traffic-related deaths, from an already low level in 2000 (Our World in Data, 2023). As a result, their death rates are below the PMHF of ASIL D systems since approx. 2010. It is important to note, however, that these death rates refer to the general population, including those who are not involved in traffic, while the PMHF typically only refers to vehicle operating time.

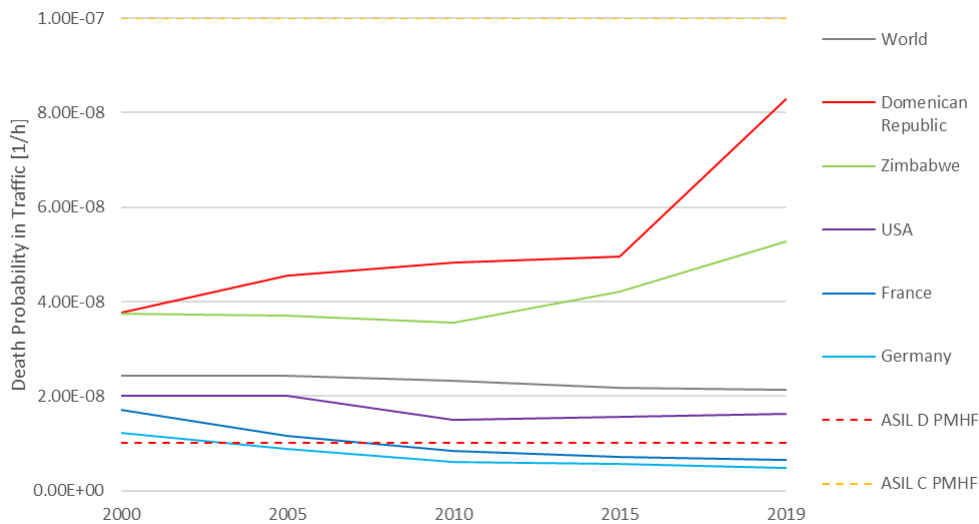


Figure 2.3: Dependence of Traffic Safety on Country, data acquired by (Our World in Data, 2023)

The decrease in traffic fatalities, both globally and in the European countries mentioned, can be partially attributed to the penetration of E/E safety-systems like ESP (electronic stability program). According to a study in 2006 by the Insurance Institute for Highway Safety (IIHS), ESP “*reduce[s] the risk of all kinds of fatal crashes by 43%*”. This success story, considering traffic safety due to a single system, led to a US market penetration of the ESP of 40% within 10 years after its introduction (Robert Bosch GmbH, 2020), (Insurance Institute for Highway Safety (IIHS), 2006). Additionally, since 2014, the European Union has mandated that all new cars be equipped with ESP (Robert Bosch GmbH, 2020). The European Union aims at going one step further in order to achieve zero traffic deaths by 2050 through the implementation of emerging safety-guaranteeing E/E-systems in vehicles (European Commission, 2023), as described in its “Vision 0” (European Commission, 2015) initiative.

2.2 Motivation for Functional Safety

Section 2.1.2 highlights the improvement in traffic safety resulting from the implementation of E/E-systems. However, it is important to note that this success story does not necessarily mean that E/E-systems always improve safety. It is crucial to consider the effort put into functional safety, which is typically linked to development. This section provides examples of situations where a lack of a proper functional safety concept resulted in a decline in traffic and/or public safety. The choice of the Boeing 737-Max and the Fukushima Daiichi nuclear power plant accident is based on the availability of detailed investigation reports.

2.2.1 Boeing 737-Max Aircraft

The Boeing 737-Max is the latest version of the 737 aircraft series which first flew in 1967. Over time, the series underwent several updates to increase fuel efficiency, resulting in larger engines (Hayward, 2020). The most recent update, called the ‘Max’, features engines that are too large to fit under the wing and are instead mounted slightly in front of it. However, this engine placement causes the aircraft to pitch up during high-thrust maneuvers, which is undesirable. Therefore, an additional system, called ‘MCAS’ was introduced to counter-act the pitch-up by a pitch-down momentum, implemented by actuating the trim-system. (Gates & Baker, 2019)

Two accidents in 2018 and 2019 resulted in the deaths of 346 people (Reuters, 2022), leading to the grounding of the 737-Max aircraft type (Hayward, 2020). Investigation into the accidents revealed that MCAS caused these accidents. The reason for these accidents was a poorly conducted Functional Hazard Assessment (FHA), which is comparable to the Hazard Analysis and Risk Assessment (HARA, see section 2.4.2) used in the automotive industry. The FHA incorrectly classified a malfunction of the MCAS as a small safety impact and a low probability of causing fatal crashes. As a result, the development of the MCAS was based on this false FHA. MCAS was designed to rely on a single sensor to control the pitch-down momentum. If this sensor delivered false information that was not validated (see ‘*fail-out-of-control*’ behavior in section 2.6.2), MCAS actuated false maneuvers based on this sensor’s data. These false maneuvers ultimately caused the accidents mentioned. For more information on the accidents and their causes, refer to (Gates & Baker, 2019).

2.2.2 Fukushima Daiichi Nuclear Powerplant

The Fukushima Daiichi nuclear power plant, located on the east coast of Japan, consisted of six operating units. It was designed to withstand earthquakes and tsunamis (Bundesamt für die Sicherheit der nuklearen Entsorgung, 2022). The core of the safety concept was to ensure the cooling of the nuclear cores to prevent a meltdown that was assessed as a catastrophe. To achieve this, a fault-tolerant power-supply was implemented, consisting of six external power

sources, backup diesel generators, and batteries. This redundant and dissimilar (refer to section 2.6.3) energy supply fed the eleven pumps of the cooling systems that prohibited the core meltdowns. (World Nuclear Association, 2023)

In 2011, an earthquake struck the east coast of Japan, causing several nuclear power plants with a total power of 9.4 Gigawatt to shut down as prescribed by emergency procedures in place. Fukushima Daiichi operating units 1-3 also shut down immediately, as designed. The earthquake caused an instantaneous failure of all six external power supplies. However, the backup generators and batteries were able to maintain the energy supply for the cooling system. Subsequently, two tsunamis caused by the earthquake itself, hit the power plant. These tsunamis flooded the backup diesel generators and batteries which were all located in the basement of the power plant, resulting in a complete power shutdown of operating units 1-4. This shutdown finally led to a core meltdown, known as the Fukushima Daiichi disaster. (World Nuclear Association, 2023)

The disaster serves as an example on behalf of the importance of common cause analyses (refer to section 2.5.4). Despite the implementation of dissimilar redundancy, a single event (the earthquake) can lead to a catastrophic failure of the entire system. Further information on the disaster can be withdrawn from (World Nuclear Association, 2023).

2.3 Safety related to Legislation

Products must comply with current legislation when being brought to market. Therefore, legislation can be seen as a minimum set of requirements that products or systems must meet. The legislation is enforced during the type certification process of a car by national authorities. An example of such a national authority is the ‘Kraftfahrtbundesamt’ which is responsible for type certification in Germany (Kraftfahrtbundesamt, 2023). However, safety regulations vary by country. Therefore, an analysis must be conducted to consider the legislation of the ‘relevant’ countries. For this work, the legislation of the four largest car markets, which account for 71% of all car sales worldwide (statista, 2023), will be considered as ‘relevant’: USA (FMVSS 135 (U.S. Department of Transportation - National Highway Traffic Safety Administration, 2005)), EU (ECE 13-H (United Nations ECE, 2015)), China (GB 12676 (General Administration of Quality Supervision, Inspection and Quarantine of People’s Republic of China., 2014)) and India (IS 11852 (Bureau of Indian Standards, 2001), (Bureau of Indian Standards, 2003)).

The legislative requirements for deceleration can be divided into design requirements, which specify a certain architecture, and performance requirements, that specify a specific, design-agnostic performance. Further granularity can be achieved by considering intact and degraded braking systems. Tables 2.1 to 2.4 present the results of an analysis conducted to identify the most demanding requirement when legislation differs. This section is an excerpt from (Schrade, et al., 2022).

Table 2.1: Legislation related to the design of intact service braking systems

ID	Requirement	EU+UK	USA	China	India
D.01	Two independent energy reserves	5.2.2 5.2.4	-	4.2.2	4.2.1
D.02	Two independent energy transmissions	5.2.2 5.2.4	-	4.2.2	4.2.1
D.03	Each energy reserve must be connected to two or more wheels	5.2.2	-	4.2.2	4.2.1
D.04	Each energy transmission must be connected to two or more wheels	5.2.2	-	4.2.2	4.2.1
D.05	All 4 wheels shall be actuated by brakes	5.2.6	14.24	4.2.7	4.2.1
D.06	ESP shall apply braking torque to the wheels individually	UN ECE R140	FMVSS 126	-	-
D.07	Brake shall return to OFF position when released	5.2.2	-	-	-

Table 2.2: Legislation related to the performance of intact service braking systems.

ID	Requirement	EU+UK	USA	China	India
P.01	Provide more than 6.43 m/s ² deceleration with the engine disconnected	A3.2	14.7	5.2.1	4.1.1
P.02	Provide more than 5.67 m/s ² deceleration with the engine connected	A3.2	14.8	5.2.1	4.1.1
P.03	Energy reserve must be dimensioned to halt vehicle 10 times in series from 100 km/h	5.2.4 5.2.20	14.18	-	4.2.1
P.04	Energy supply must be dimensioned to halt vehicle according to P.11	5.2.4	-	4.2.5 4.2.14	4.2.1
P.05	Transmission delay must be less than 0.6 seconds	A3.3	-	5.4.1	4.3.1

Table 2.3: Legislation related to the design concerning failures of service braking systems.

ID	Failure	Requirement	EU+UK	USA	China	India
D.11	any	No unintended application	5.2.9	-	-	-
D.12	E-Supply	E-reserves must tolerate it	5.2.15	-	-	-
D.13	Transmission	No unintended application of PB	5.2.19	-	-	-
D.14	Any 1st	Application still possible	5.2.20	-	-	-

Table 2.4: Legislation related to the performance of degraded service braking systems

ID	Failure	Requirement	EU+UK	USA	China	India
P.11	1 st Circuit	Provide more than 2.6 m/s ² deceleration	A3.2	14.14	5.2.1	4.1.2
P.12	ABS	Provide more than 5.15 m/s ² deceleration	A6.4	14.12	-	9.5.4
P.13	Brake Distribution	Provide more than 3.86 m/s ² deceleration with the engine disconnected	A5.4	14.13 14.17	A6	-
P.14	Power Brake Unit	Performance of P.11	-	14.18	-	-
P.15	Booster	Performance of P.11	-	14.21	5.2.3	-

P.11 and D.14 are the two most important requirements for braking system failure tolerance. These requirements prescribe that a vehicle needs to have the potential of decelerating with 2.6 m/s^2 with only one brake circuit and to tolerate any first failure within its system, at least in a degraded state. However, if Canadian legislation (Transport Canada, Motor Vehicle Safety, 2015) is also considered (not scope of this work), a remaining deceleration of P.01 is required after any first E/E-failure that also reflects current strict liability demands (refer to Annex A).

2.4 Safety related to Norms: ISO 26262 for E/E-Systems of Vehicles

ISO 26262 is the standard for reducing product liability (refer to Annex A) from a functional safety perspective. While other standards as IEC 61508, ARP 4761, and DO178 also address functional safety, these do not specifically focus on the safety of road vehicles. Therefore, this work focuses solely on ISO 26262.

2.4.1 Item Definition

In the scope of ISO 26262, safety concepts (and the safety analysis) are established for an ‘item’ which is defined by (International Organization for Standardization, 2018) as a “*system [...] or combination of systems [...] that implements a function or part of a function at the vehicle level*”. Such an item can be a power supply (Kilian, et al., 2022) or steering system (Kilian, et al., 2021), for instance. The item description shall be specified, according to:

- *“legal requirements, national and international standards;*
- *the functional behavior at the vehicle level, including the operating modes or states;*
- *the required quality, performance, and availability of the functionality, if applicable; and [...]*
- *potential consequences of behavioral shortfalls including known failure modes and hazards [...]*” (International Organization for Standardization, 2018)

2.4.2 Hazard Analysis and Risk Assessment

The item must be ‘safe’ or respectively free of “*unreasonable risk*”, as defined by (International Organization for Standardization, 2018), which can be specified from a product liability perspective (refer to Annex A) or from a functional safety perspective due to the application of a Hazard Analysis and Risk Assessment (HARA) and a development according to section 2.4.4. The purpose of the HARA is “*to identify and classify the hazardous events caused by [a] malfunction of the item and to formulate the safety goals [SG] with their corresponding ASILs related to the prevention [...] of the hazardous events [...]*” (International Organization for Standardization, 2018). Finally, these SGs are annotated with an ASIL A to D depending on the safety impact of the malfunction. The process for determining an ASIL from a HARA is explained in detail in section 3.1.

2.4.3 ASIL Decomposition

The HARA specifies SGs with annotated ASILs that must be met by an item and its (sub-) systems. It is possible, however, that a SG may be ‘redundantly’ fulfilled (International Organization for Standardization, 2018) by different, “*sufficiently independent*” (International Organization for Standardization, 2018) systems. A common cause analysis (see section 2.5.4) and cascading failure analysis can be used to demonstrate this independence. ASIL

decomposition is allowed if freedom from interference of the redundant systems is ensured. This ASIL decomposition ensures initial safety by reducing the ASIL of each independent and redundant system.

2.4.4 Impact of the ASIL related to the development

E/E-system development is divided into hardware (as described in (International Organization for Standardization, 2018)) and software (as described in (International Organization for Standardization, 2018)) components. Software safety is achieved by avoiding systematic faults or errors, as described in (International Organization for Standardization, 2018), section 7.4.1. To achieve this, certain development processes are applied, as described in (International Organization for Standardization, 2018).

In addition to systematic faults, hardware development also focuses on random hardware faults besides (International Organization for Standardization, 2018). While (International Organization for Standardization, 2018) provides certain development process recommendations, it also recommends meeting three hardware failure metrics, which are presented in the following paragraphs.

The **Single-point Fault Metric (SPFM)** is defined as the proportion that a “*hardware fault in an element leads directly to the violation of a safety goal and no fault [...] is covered by any safety mechanism*” (SM) (International Organization for Standardization, 2018). Herein, the SM is a device that can implement measures to prevent the specified failure such as a diagnosing device that prevents undiagnosed faults. The SPFM can be determined by the ratio of the sum of the single-point failure² rates of n elements (λ_{SPF}) and the failure rate of the complete system (λ_{total}), as shown in equation (2.1) (International Organization for Standardization, 2018).

$$SPFM = \sum_{i=1}^n \frac{\lambda_{i,SPF}}{\lambda_{total}} \quad (2.1)$$

The **Latent Fault Metric (LFM)** describes the share of “*multiple point fault[s] whose presence is not detected by a safety mechanism [...] within the [...] detection time interval*” (International Organization for Standardization, 2018). Similarly to the SPFM, the LFM is determined by adding the latent failure rates of n elements (λ_{LF}) and their division by the failure rate of the complete system (λ_{total}), as shown in (2.2) (International Organization for Standardization, 2018).

$$LFM = \sum_{i=1}^n \frac{\lambda_{i,LF}}{\lambda_{total}} \quad (2.2)$$

² single-point failure: a single failure of a single (sub-)component that causes a complete failure of the entire system (regarding the specified failure effect (refer to section 2.6.2))

The **Probabilistic Metric for random Hardware Failures (PMHF)** is defined as the probability of a system failing due to a random hardware fault during one hour of operation, according to (International Organization for Standardization, 2018) (section 9.4.2). ISO 26262-5 emphasizes that the PMHF “*does not have an absolute significance but [is] useful for comparing*” different designs, which is the focus of this work. The PMHF considers single-point failures (λ_{SPF}), faults that remain undetected by the SM (residual faults λ_{RF}), detected and latent dual-point faults (DPF) and the operation time³ ($T_{Lifetime}$) of the vehicle, as defined by equation (2.3) (International Organization for Standardization, 2018).

$$PMHF = \lambda_{SPF} + \lambda_{RF} + \lambda_{DPF,detected} \times \lambda_{DPF,latent} \times T_{Lifetime} \quad (2.3)$$

Section 2.7 presents methods for determining the failure rate (λ) of a component, as well as techniques for analyzing the failure rates of elements and systems. Reference values for the presented hardware metrics for the respective ASILs can be found in Table 2.5.

Table 2.5: Hardware metrics, data acquired from (International Organization for Standardization, 2018)

	Abbreviation	ASIL A	ASIL B	ASIL C	ASIL D
Single-point fault metric	SPFM	-	90%	97%	99%
Latent-fault metric	LFM	-	60%	80%	90%
Probabilistic Metric for random Hardware Failures	PMHF	-	$10^{-7} 1/h$	$10^{-7} 1/h$	$10^{-8} 1/h$

³ (International Organization for Standardization, 2018), (International Organization for Standardization, 2018) provide $T_{Lifetime} \approx 10,000 h$ as an example

2.5 Methodologies in the Functional Safety Domain

This section presents several commonly used methodologies for analyzing the system safety. These methodologies generally link basic (hardware) faults on a hardware part level to the SGs on the vehicle level. However, applying multiple methodologies can take advantage of each methodology while avoiding potential disadvantages, as proposed in (International Organization for Standardization, 2018).

2.5.1 Fault Tree Analysis (FTA)

The Fault Tree Analysis (FTA) is a top-down approach, similar to Markov Analysis (see section 2.5.2). Top-down analyses start from a top-event being the topic under investigation. In the case of FTA, the top event could be a system shutdown, normal operation (NOP), or any malfunction. FTA, then identifies all potential faults related to the top-event to determine all contributing factors. Contributing factors whether single or multiple faults may be responsible for evoking the top-event. The FTA outcome can determine the causes of a top-event (qualitative assessment) or the probability or failure rate of the top-event (quantitative assessment). (U.S. Department of Defense, 1998)

Figure 2.4 displays an FTA of a system under analysis consisting of the redundant components A and B, as well as the required components C and D. The redundant components contribute to the top-event with an ‘AND’ logic, while the required components contribute with an ‘OR’ logic. The top-event in this case is a system failure (i.e. shutdown of the system). The probability of the top-event can be determined by replacing letters A-D with their respective probabilities. (U.S. Department of Defense, 1998)

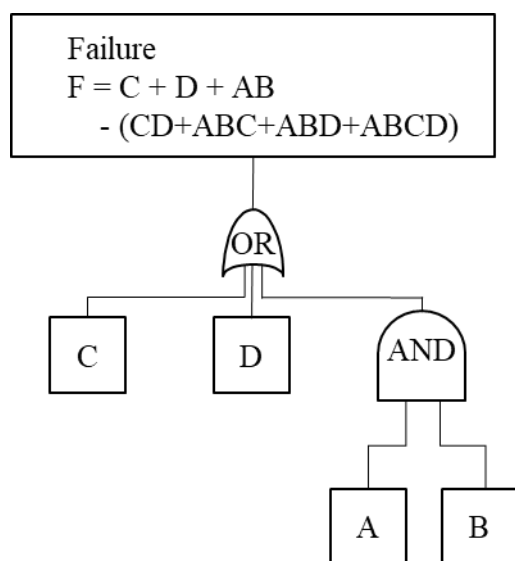


Figure 2.4: Exemplary FTA logic diagram, oriented at (U.S. Department of Defense, 1998)

The FTA is a commonly used methodology in the automotive industry due to its ability to account for various faults. It can also help to identify safety-critical failures resulting from a

combination of faults, none of which are safety-critical on their own. FTAs offer clear and formal descriptions of the causes of a top-event. They can be conducted during early design phases, such as with functional blocks, or in more detail at later design states. This chapter summarizes (U.S. Department of Defense, 1998), which should be consulted for additional information.

2.5.2 Markov Analysis

The Markov Analysis is a state-driven methodology (von Alven, 1964) that relies on a system always being in a single state and state transition probabilities that are time-independent, at least during the defined time interval under investigation. The *system states* (S_0, S_1) can be NOP, ‘fail’ or others. The transition from one state to another is triggered by an event, such as a fault, which has a certain (*fault*) probability λ . It is assumed that this probability remains constant over time and that the system can only be in one single state at a time. It should be noted that events are not limited to ‘fault’ events but can also include ‘repair’ events with a certain (*repair*) probability μ (U.S. Department of Defense, 1998). However, this work does not cover repair events. Figure 2.5 shows a Markov state graph for a single unit.

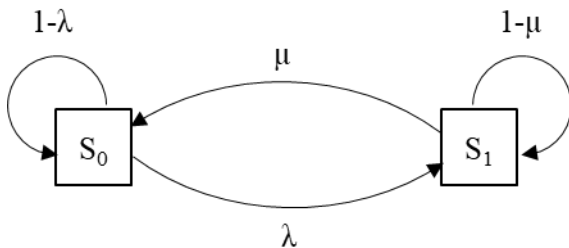


Figure 2.5: Markov state graph for a single unit, oriented at (U.S. Department of Defense, 1998)

Markov Analyses can be used to determine dedicated occurrence probabilities P_i for a given *state* i . An exemplary state diagram, based on (U.S. Department of Defense, 1998), is shown in Figure 2.6. *State 1* represents NOP. *States 2* and *3* may be *failed states* with different failure modes. The transition probability for a fault leading to *states* $i \in \{2,3\}$ during a defined timespan Δt can be approximated by $\lambda_i \times \Delta t$. By applying this principle, equation (2.4) can determine the probability of transitioning to a *failed state* i (U.S. Department of Defense, 1998). Additionally, remaining in *state 1* can be described as not transitioning to another state, as defined in (2.5) (U.S. Department of Defense, 1998). Finally, a multi-step failure process can be modelled by a cascade of (2.4), where *state 1* is replaced by an *intermediate state* of the failure process (i.e. a state after a first fault).

$$P_i(t + \Delta t) = P_1(t) \cdot \lambda_i \cdot \Delta t \quad (2.4)$$

$$P_1(t + \Delta t) = P_1(t) \cdot [1 - \sum_{i=1}^n \lambda_i \cdot \Delta t] \quad (2.5)$$

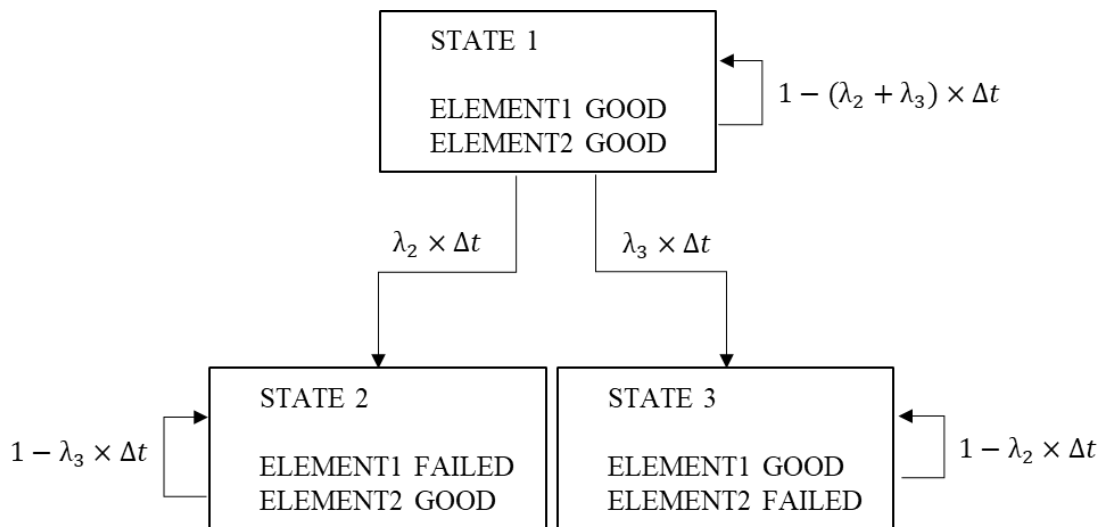


Figure 2.6: Markov flow diagram, adapted from (U.S. Department of Defense, 1998)

Compared to FTA, the advantage of the Markov Analysis is that it allows for modeling different operating/failure modes within a single chart, as shown in Figure 2.6. Markov Analysis is an efficient means of analyzing various state transitions or failures. However, the complexity of Markov Analysis increases significantly with increasing system complexity, resulting in challenges (U.S. Department of Defense, 1998), (Calabro, 1962). For further information, please refer to (U.S. Department of Defense, 1998), (von Alven, 1964), (Calabro, 1962).

Chapter 4 applies Markov analyses to determine the (redundant) system behaviour of the analysed systems, which have limited architectural complexity but inherit a variety of different operating modes.

2.5.3 Failure Mode and Effect Analysis (FMEA)

The FMEA is, unlike the aforementioned methodologies, an inductive bottom-up approach that only considers single faults at the lowest level of the system hierarchy such as hardware parts. These basic faults can be allocated to different *failure modes* FM_i that describe how a component may fail, such as increased resistance due to corrosion. These FM can be allocated to different *failure effects* FE_i on the next higher system level such as undetected wrong measurements. This allocation is done quantitatively. FMEAs are generally conducted using tables.

FMEA is best suited to be used in conjunction with FTA as these are “*the two most common techniques for analyzing faults and failures*” (International Organization for Standardization, 2018). Therefore, the FMEA is used to determine the distribution of FM for the components in this work. For more information, refer to MIL-HDBK-338B, Section 7.8, if necessary.

2.5.4 Common Cause Analysis

The common cause analysis is a recommended qualitative safety analysis in the scope of ISO 26262-9. Its purpose is to examine redundancies and errors in hardware and software. It analyzes root causes that may lead to multiple failures, potentially in different components (Biolini, 2014). The Fukushima accident (refer to section 2.2.2) is an example of a single root cause (the earthquake) successfully demolishing all redundancies (several dissimilar energy supplies) at once. It demonstrated that perceived safety, due to the implementation of redundancies, did not represent actual safety.

ISO 26262-9 (International Organization for Standardization, 2018) uses the term '*unintended coupling*' to identify such common cause failures and differentiates between the following '*coupling factor classes*':

- Shared resources
- Shared information input
- Insufficient environmental immunity
- Systematic coupling
- Components of identical type
- Communication
- Interface

The common cause analysis is a qualitative assessment that does not provide probabilities for any failure. Unlike the other methodologies, it is not quantitative. In the aviation industry, it is crucial to prevent any single root cause from provoking a catastrophic failure (comparable to ASIL D in an ISO 26262-context) (European Aviation Safety Agency, 2011). This necessitates (dissimilar) redundancies in airplanes. Although this requirement is not mandatory in the automotive industry, SPFM should still be met. Common cause analyses can be helpful in this regard.

2.5.5 Applied Methodology

This work applies the methodology outlined in (Ebner, 2024), which describes a holistic model-based system optimization while also considering safety. This chapter provides a brief excerpt of (Ebner, 2024), which can be consulted for further information.

The first step of the methodology involves creating a user-defined function block diagram and signal flow. These functional blocks have both a functional behavior, consisting of mathematical operations, and assigned components (refer to Figure 4.2 for an example of a generic ECU (electronic control unit)). The components in the system have associated failure rates and FMs. These FMs are then injected into the function block diagram to assess the system's behavior under specific fault conditions. For this work, a maximum of two consecutive faults are selected to be analyzed. After injecting all possible faults, the components are rearranged to repeat the fault injection process. This repetition continues until all component combina-

tions have been simulated. The function block diagram can be rearranged according to predefined rules, as described in section 4.5.

However, for the scope of section 4.5, a major adaption has been implemented. The methodology described, only takes into account a single output (i.e. the sum of the torques applied at the wheels). This is not suitable for this work, as the correct sum of torques may be applied, but with an incorrect allocation onto the wheels. An example could be a car that meets a requirement specifying a *deceleration* $a_x = 4 \text{ m/s}^2$, but with two rear wheels blocked (as one FM) and no brake actuation at the front wheels (as another FM). In this case, a one-dimensional safety analysis, which only considers a sum of torques, is insufficient and a multi-dimensional analysis is required. The implemented safety analysis considers a malfunction with the same FM of:

- Each (4) wheel individually
- Circuits (X-, H-) (refer to section 4.2.4)
- All Wheels

2.6 Fundamentals of Functional Safety

Section 2.6 gives an overview of the key terminology related to the scope of this work. It distinguishes between faults and failures and discusses fault reaction and failure effects FE. Additionally, it covers the basics of safety concepts and their implementation through safety mechanisms (SM) and redundancies.

2.6.1 Failure Classification

A *failure*, also referred to as a *malfunction* (International Organization for Standardization, 2018), is the termination of a system's required functionality due to the manifestation of a *fault* (International Organization for Standardization, 2018), (U.S. Department of Defense, 1998), (Birolini, 2014). Consensus exists that a *fault* is the (root) cause of a *failure* (International Organization for Standardization, 2018), (U.S. Department of Defense, 1998), (Birolini, 2014). An example to illustrate the relation between *faults* and *failures* could be a resistor that burns out (*fault*) but it becomes a *failure* only when it is used.

The term *fault* can be further specified. The obvious manner of part *faults* is the *permanent fault*. *Permanent faults* occur at a specific point in time and persist until any kind of a repair event happens, while *transient faults* appear briefly and disappear without intervention (Koren & Krishna, 2007). An example of a *transient fault* is a single event upset in a memory caused by a charged particle. Once the memory is rewritten, the *malfunction* (wrong data) is resolved. Finally, also *intermittent faults* should be outlined. These faults occur irregularly (Koren & Krishna, 2007). For example, a loose connector could cause such a fault. This thesis focuses only on *permanent faults* and establishes the related failure rates in section 2.7.

Another term that is frequently used in the context of *failures* is *error*. But, various definitions exist. While there is a widespread definition of an *error* “as a result of a fault” (similar to a *failure*) (International Organization for Standardization, 2018), other sources (U.S. Department of Defense, 1998), (Birolini, 2014) particularly in the software domain, define an *error* as a design “*flaw*” that is part of a functionality once delivered. This thesis adopts the latter definition which is closely linked to systematic/deterministic failures. A current example is a software *error* in the Airbus 320 that caused a strong asymmetric thrust during landing abortions under strong crosswind conditions, as described in (Boyer, et al., 2023).

2.6.2 Fault Reaction and Failure Effects

Functional safety recognizes two commonly used *fault reaction* patterns: *fail-safe* and *fail-operational (fo)* (Isermann, 2006). *Fo* describes a system's ability to tolerate a first failure while remaining operational. *Fail-safe*, on the other hand, specifies that the system transitions into a safe state after a failure. This safe state is usually achieved by deactivating the failed component and activating a mechanical backup (Isermann, 2006).

This thesis uses a further specification of the term *fo*, also referred to as fail-active. Whereas *fo* is used to describe a system's performance that does not deteriorate after an initial failure, *fail-degraded* (*fd*) specifies a system's behavior that does deteriorate after an initial failure, but not cease its operation, as specified in (U.S. Department of Defense, 1998).

The *fail-safe* terminology defined by (Isermann, 2006) cannot be used in the context of this work because the absence of a mechanical backup is a key element of EMBs. Additionally, the safety effect⁴ 'safe' is highly dependent on (external) SMs that may not be part of the component or functionality itself and may not be defined. Therefore, the safety effect of a malfunction cannot be determined. That is why, the safety-neutral *fail-passive*⁵ (*fp*) terminology, also known as *fail-silent* (refer to (Isermann, 2006), (Isermann, 2011), (Kopetz, 2011)) is used to describe a suppressed system's response to an input after a failure. Additionally, the FE *fail-out-of-control* (*foc*) is introduced for failures that remain undiagnosed and provoke an unspecified system behavior. This *foc* is linked to the FE that are generally referred to as "unintended" braking/ acceleration/ steering/ etc., if no (external) SMs are in place.

2.6.3 Safety Concepts

The scope of this work is to ensure the safety of a system, which is divided into two dimensions: integrity and availability. Integrity refers to a system's behavior that guarantees the absence of false system output, related to a potential *foc*-behavior. It is often ensured by an internal or external SM (refer to section 2.7.2) that diagnoses faults, as defined by (International Organization for Standardization, 2018). In this work, availability (also known as safety-related availability (SaRA)) refers to the "*capability of a product to provide a stated function if demanded, under given conditions over its defined lifetime*" (International Organization for Standardization, 2018). This availability is frequently achieved by implementing redundancy.

Redundancy stems from the Latin term '*redundantem*', which can also be translated as 'overabundance' (Harper, 2021). It refers to "*the existence of more than one means for accomplishing a given function*" (U.S. Department of Defense, 1998). Figure 2.7 displays various options for implementing redundancy. One major differentiation is based on whether the redundant entity/entities are considered. Systems that consider all entities (e.g., via a voting mechanism, or parallel units) are known as *active* redundancy. *Graceful degradation* (GD) is a failure-tolerant approach that establishes new function allocations after an initial fault to guarantee the availability of the most important/safety-relevant functions while discontinuing less important functions. In contrast to *active* redundancy, an approach could be chosen where

⁴ The safety effect specifies the severity or impact of a failure condition regarding the safety a system (European Aviation Safety Agency, 2011)

⁵ *fail-passive* (*fp*) is used instead of *fail-silent*, as the abbreviation for *fail-silent* (*fs*) could be mistaken as the abbreviation for fail-safe (*fs*); furthermore, it is an expression known within the aviation industry (SKYbrary, 2023), (European Aviation Safety Agency, 2017)

only one entity is in command, while other entities remain in *standby*. For more information, refer to (U.S. Department of Defense, 1998).

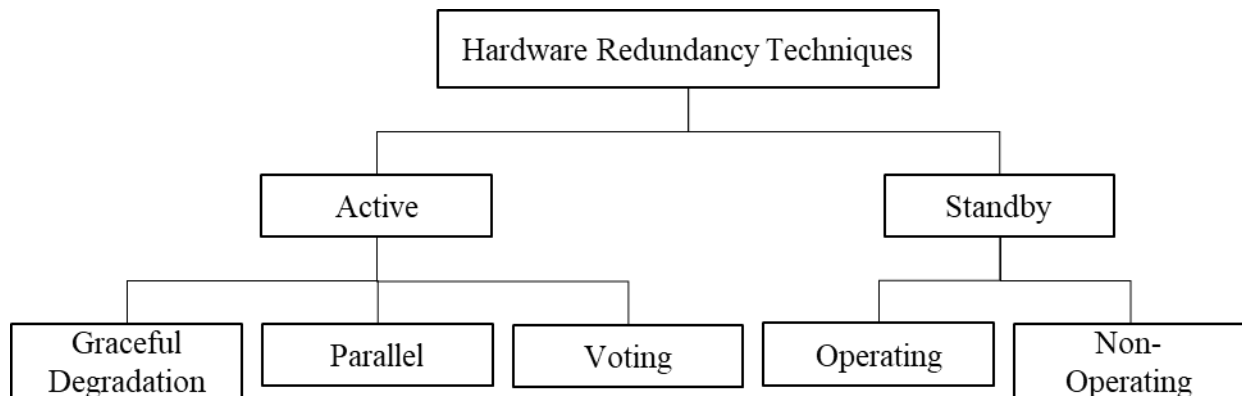


Figure 2.7: Types of Redundancy, excerpt from (U.S. Department of Defense, 1998)

Apart from differentiating between *active* and *standby* redundancy, it is also possible to distinguish between *similar* and *dissimilar* redundancy. *Similar* redundancy refers to a system, where redundancy is achieved through identical entities or replication. In contrast, *dissimilar* redundancy, also known as *divers*, involves redundant entities with different design implementations. An example of this is the Airbus flight control system, which consists of a primary and secondary flight control system implemented using dissimilar hardware and software solutions. (Sommerville, 2004)

2.7 Determination of Hardware Part Failure Rates

The purpose of determining failure rates or predicting reliability is to assess whether a system meets the acceptable reliability level, as defined by ISO 26262 (refer to chapter 2.4). These failure rates can be obtained by analyzing incoming parts, conducting tests during manufacturing, or evaluating returns or products in the field (Kapur & Pecht, 2014). This section includes an evaluation of the components lifetime prediction.

2.7.1 Models for predicting the lifetime of components

There are several methods available to predict component lifetime (refer to (Kapur & Pecht, 2014)). However, since the applicable methodology (refer to section 2.5.5) and the failure rate handbooks (refer to (Siemens AG, 2004), (U.S. Department of Defense, 1991), (Cadwallader, 2018), (Naval Surface Warfare Center, Carderock Division, 2006)), combined only support the commonly used exponential distribution with a constant failure rate, this approach is used to estimate hardware part failure rates. More information on this approach is provided in the following paragraphs.

The exponential distribution describes the *reliability* $R(t)$, which is defined as the “*probability that an item can perform its intended function*” (U.S. Department of Defense, 1998). It depends on the *failure rate* λ_0 and the *operation time* t , as shown in (2.6) for components without repair (Kapur & Pecht, 2014). The *reliability* $R(t)$ decreases as *operation time* increases. On the other hand, the likelihood of a *failure* $F(t)$ can be determined as the complement of the *reliability* $R(t)$, as explained in (2.7) (Kapur & Pecht, 2014). The probability of failure increases with longer *operation time*. If the *failure probability* $F(t) \ll 1$, which is typically the case for the failure rates of interest, (2.7) can be simplified to (2.8) (International Organization for Standardization, 2018). Appendix B.1 also includes a visual representation of the impact of this approximation. (International Organization for Standardization, 2018)

$$R(t) = \int_t^{\infty} \lambda_0 \cdot e^{-\lambda_0 \tau} d\tau = e^{-\lambda_0 t} \quad (2.6)$$

$$F(t) = 1 - R(t) = 1 - e^{-\lambda_0 t} \quad (2.7)$$

$$F(t) = 1 - e^{-\lambda_0 t} \approx \lambda_0 \cdot t \quad (2.8)$$

The determination of unreliability described above is based on constant failure rates, which assumes the idealized bathtub curve model as its foundation. Figure 2.8 illustrates the relationship between the *failure rate* $\lambda(t)$ and time increments. The bathtub curve model distinguishes between three phases of a component’s lifetime:

1. *Infant mortality period*: Components experience an increased failure rate at the beginning of their lifetime due to inadequate manufacturing, for instance. This period is referred to as ‘burn-in’ phase. According to (Siemens AG, 2004), this phase is assumed

to cease at $t_1 = 3,000$ hours of operation for electronic components. To prevent an increased failure rate in the field, manufacturers may implemented so-called highly accelerated stress screenings (HASS) (Hobbs, 2000) before delivering the product.

2. *Useful life period*: The component experiences its lowest *failure rate* λ_0 , assumed of being constant. This failure rate is used for the lifetime predictions (also in the scope of this work).
3. *Wear-out period*: When approaching the end of life, the component's failure rate starts to increase again. Maintenance events are necessary to decrease the *failure rate* λ_0 . (Kapur & Pecht, 2014)

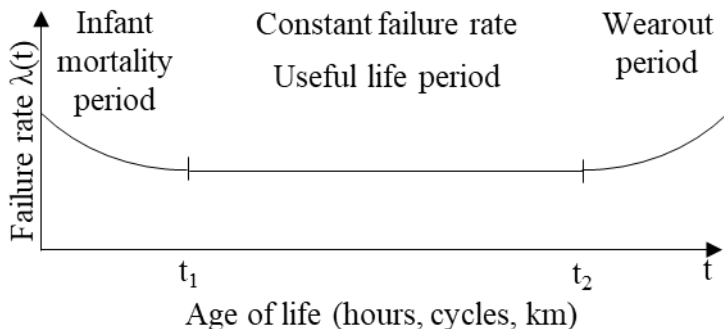


Figure 2.8: Idealized bathtub curve, oriented at (Kapur & Pecht, 2014)

2.7.2 E/E Components

This section outlines the approach for determining the failure rates of E/E components. The rates themselves are provided in Annex B.2. ISO 26262-5 recommends using “*handbook data, which are recognised as being conservative*” for determining hardware part failure rates. SN29500 (refer to (Siemens AG, 2004), (Siemens AG, 2004)) is such a conservative handbook and is therefore being also used in this work. It separates the derivation of failure rates into two parts:

- the *reference failure rate* λ_{ref} of the component related to the complexity, and
- the environmental or operational conditions π_i that influence the component's reliability.

This work assumes certain complexities of the involved E/E components without further discussion. However, the complexity classes can be retrieved from Annex B.2. The operational conditions are partially considered. Equation (2.9) (Siemens AG, 2004) provides the formula to determine the *failure rate* λ of an electronic component, in general. λ_{ref} is hereby multiplied by the operational factors ($\pi_i \geq 1$), reflecting:

- π_U : the voltage dependency (chosen to be 1)
- π_T : the dependency on the environmental temperature
- π_D : the drift dependency (application-specific considered)

$$\lambda = \lambda_{ref} \cdot \pi_U \cdot \pi_T \cdot \pi_D \quad (2.9)$$

According to equation (2.9), the *failure rate* λ is directly affected by the environmental temperature. To determine the temperature profiles for vehicles, ISO/PAS 5101 (International Organization on Standardization, 2021) is consulted. The temperature *shares* s_i are taken into account, resulting in the updated equation (2.10).

$$\lambda = \lambda_{\text{ref}} \cdot \pi_U \cdot \pi_D \cdot \sum_{i=1}^n s_i \cdot \pi_{T,i} \quad (2.10)$$

Furthermore, the *failure rate* λ can be determined by the related *FM*. Section 2.6.2 introduced two *FM fp* and *fooc*. An *fp*-behavior is triggered by a diagnosed failure (see (2.11) (International Organization for Standardization, 2018)), while undiagnosed failures are categorized as *fooc* (see (2.12) (International Organization for Standardization, 2018)). These diagnostic routines may be implemented by external or internal SMs that are linked to certain *Diagnostic Coverages* (DC). Table 2.6 provides reference DCs for some SMs.

$$\lambda_{fp} = DC \cdot \lambda \quad (2.11)$$

$$\lambda_{fooc} = (1 - DC) \cdot \lambda \quad (2.12)$$

Table 2.6: Reference Diagnostic Coverages of Safety Mechanisms, data from (International Organization for Standardization, 2018), (International Organization for Standardization, 2018)

DC	Central Processing Unit (CPU)	Random Access Memory (RAM)	Flash-Memory	Communication Bus
60%	Software self-test	Parity bit	Parity bit	1-bit hardware redundancy
90%	Watchdog	Pattern test		Frame counter
99%	Lockstep-core	March test	Block replication	Test pattern

2.7.3 Mechanical Components

Mechanical components are not within in the scope of ISO 26262. Therefore, their failure rates are generally not considered for safety assessment, as specified in section 2.4.4. However, a mechanical component may cause the same FE as an E/E component. For example, a broken shaft may comprise a braking maneuver just as a CPU (Central Processing Unit) in a *fp-state* would. Therefore, the failure rates of mechanical components are considered as equally important to those of the E/E-components.

The sources of choice for the specification of the failure rates in this work are (U.S. Department of Defense, 1998) and (Naval Surface Warfare Center, Carderock Division,

2006). The obtained failure rates can be distributed to different FE, similar to E/E-components. In (U.S. Department of Defense, 1998) the proportions of the FM are given, which are assigned to the FE in a second step. However, this allocation has to be done carefully because, for example, a blocking gear (as a FM) can provoke different FE, depending on the situation. The blocking gear can provoke:

- No braking capability: if appearing during ‘*no load*’
- Partial remaining braking: if appearing during ‘*partial braking*’
- Full remaining braking (even potential for blocking wheels): if appearing during ‘*full braking*’

ISO/PAS 5101 (International Organization on Standardization, 2021) is consulted to determine the proportions of the situations described above. It is assumed that the specified braking maneuvers start and end with no braking force, so that the proportion of ‘*no load*’ is finally determined to be 50%. Furthermore, braking maneuvers with an $a_x < 0.1 \text{ m/s}^2$ are also declared as ‘*no load*’ due to their insignificant forces. Finally, the distribution shown in Figure 2.9 is applied. From this, it can be estimated, that only 0.6% of the FM “blocking gear” causes the FE of a full remaining braking. Similarly, it can be estimated that 22.8% of the FM cause the FE of partial remaining braking and that 76.7% of the FM cause the FE fp , because no braking can be initiated at the respective wheel. The failure rates of the mechanical components and their distribution among the different FE are shown in Appendix B.3.

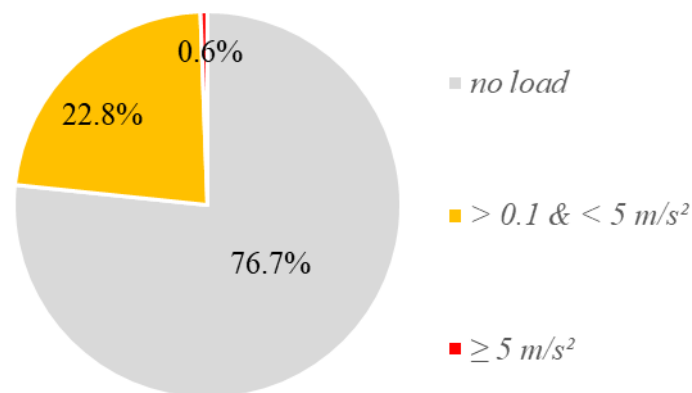


Figure 2.9: FE-Shares for the allocation of the FM 'blocking'

3 Derivation of X-Domain Safety Goals

Safety-critical automotive systems, such as those developed in this work, must provide functionality with a certain level of reliability to prevent damage and loss of life. This chapter elaborates the top-level safety requirements that form the basis for the designs presented in the chapters 4 and 5. Therefore, a Hazard Analysis and Risk Assessment (HARA) is carried out, specifying exposure (E), severity (S) and controllability (C), as defined in ISO 26262-3. In addition, the safety impact of braking system malfunctions on reference vehicles is analyzed to derive ASILs and establish safety goals (SG).

3.1 X-Domain Hazard Analysis and Risk Assessment

Top-level safety requirements are generally established to avoid “*unreasonable risk*” (International Organization for Standardization, 2018). ISO 26262-3 suggests performing a HARA to determine what level of risk is considered “*unreasonable*”. The HARA determines the E, S and C⁶ to derive the ASIL of the SGs associated with the two malfunctions *degraded* and *uncommanded braking*. Section 3.1 is an excerpt from a contribution presented at an SAE conference (Schrade, et al., 2023).

3.1.1 Definition by ISO 26262-3

ISO 26262-3 defines the ASIL of an SG by the superposition of E, S and C. The specific superposition scheme is shown in Figure 3.1. It highlights that a combination of the maximum values E4, S3 and C3 results in an ASIL D, while a combination of E2, S2 and C2 results in a QM (quality-managed) classification. The following paragraphs specify the determination of E, S and C.

⁶ The controllability is not assessed in the scope of this work, but is conservatively set to 3 being the maximum value

		Exposure	Controllability Class		
			C1	C2	C3
Severity Class	S1	E1	QM	QM	QM
		E2	QM	QM	QM
		E3	QM	QM	A
		E4	QM	A	B
	S2	E1	QM	QM	QM
		E2	QM	QM	A
		E3	QM	A	B
		E4	A	B	C
	S3	E1	QM	QM	A
		E2	QM	A	B
		E3	A	B	C
		E4	B	C	D

Figure 3.1: Derivation of the ASIL, data from (International Organization for Standardization, 2018)

The **exposure E** is determined by the likelihood of the applicable driving situations “*that can be hazardous if coincident with the failure mode under analysis*” (International Organization for Standardization, 2018). Therefore, a comprehensive situation analysis must be performed. The E can be derived from the probability of the specific situation by applying Table 3.1

Table 3.1: Determination of the exposure, data from (International Organization for Standardization, 2018), (Verband der Automobilindustrie e.V., 2015)

	E1	E2	E3	E4
Average operation time	...	<1%	1% - 10%	> 10%
Duration [hours per year]	< 0.4	0.4 ≤ x < 4	4 ≤ x ≤ 40	> 40
Frequency [1 per year]	< 1	1 ≤ x < 10	10 ≤ x ≤ 100	> 100
Exemplary Situation	People on the roof	Service activity	>2 passengers	Driving in the darkness

The **severity S** describes the “*extent of harm [...] that can occur in a potentially hazardous event*” (International Organization for Standardization, 2018), where the “*hazardous event*” is represented by a failure. The “*extent of harm*” is determined by classifying potential injuries into the (Maximum) Abbreviated Injury Scale ((M)AIS). Table 3.2 shows the criteria for the derivation of the S.

Table 3.2: Determination of the severity, data from (International Organization for Standardization, 2018)

	S0	S1	S2	S3
Injury	No	Light and moderate	Severe and life-threatening	Life-threatening
AIS	0-6	1-6	3-6	5-6
Probability ⁷	< 10%	> 10%	>10%	>10%
exemplary Situation	Bumps with roadside	Rear/front collision with very low speed	Rear/front collision with low speed	Rear/front collision with medium speed

The **controllability C** is defined as the “*ability [of any person involved] to avoid a specified harm*” (International Organization for Standardization, 2018), such as an injury to a car occupant or pedestrian. The C itself, depends on the estimated proportion of people involved who are able to cope with the specific situation. Table 3.3 provides a rationale for deriving the C.

Table 3.3: Determination of the controllability, data from (International Organization for Standardization, 2018)

	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control
Percentile of average drivers that are able to control situation	In general	> 99%	90% - 99%	< 90%

3.1.2 State of the Art

An important source for HARAs is the National Highway Traffic Safety Administration (NHTSA) in the USA. It has published HARAs for a generic hydraulic braking system (Becker, et al., 2018), a steer-by-wire system (Becker, et al., 2018), and a gasoline propulsion system (Hommes & Becker, 2018). However, as (Kemmann & Trapp, 2011) point out, current approaches are based on creativity techniques that reduce the objectivity, as confirmed by (Khastgir, et al., 2017). Furthermore, these approaches result in extensive tables, as shown by the provided NHTSA-HARAs.

One project that has focused on improving the objectivity of HARAs is SAHARA. It implements a scenario consisting of functions, the vehicle and the environment, which together result in an ASIL of a SG. Here, the E is determined based on expert judgments that assess the probability of driving situations represented by the environment. The C is assessed by a com-

⁷ And not higher severity

bination of reaction time, time-to-collision and decision paths combined with Monte-Carlo simulations. Finally, the MAIS and the Injury Severity Scale (ISS) are determined at last to establish the ASIL, as specified in Figure 3.1. (Kemmann & Trapp, 2011)

In addition to the methodology, final ASIL assessments are also disclosed in the literature, although they are rare. Since the chapters 4 and 5 focus on the safety of a deceleration functionality, the respective ASILs are shown in Table 3.4 also considering a possible alerting of the driver. Finally, it is clear that the ASIL assessments of different sources are very different, especially for very low decelerations ($a_x \leq 2.44 \text{ m/s}^2$) highlighting the need for a detailed analysis.

Table 3.4: Disclosed ASILs for malfunctions considering deceleration

Alarm to driver	Mal-function	Range [m/s ²]		ASIL			
		from	to	D	C	B	A
✓	Degradation	10	6.5				(Auguste (Hitachi ASTEMO), 2021), (Schröder, et al., 2023)
		6.5	2.44		(Parker, et al., 2018)	(Auguste (Hitachi ASTEMO), 2021), (Schröder, et al., 2023)	
		2.44	0	(Auguste (Hitachi ASTEMO), 2021), (Parker, et al., 2018) (Cheon, et al., 2011), (Sinha, 2011), (Schröder, et al., 2023)	(Cheon, et al., 2011), (Schröder, et al., 2023)	(Cheon, et al., 2011)	
x		10	6.5			(Auguste (Hitachi	

Alarm to driver	Mal-function	Range [m/s ²]		ASIL			
		from	to	D	C	B	A
						ASTEMO), 2021), (Schröder, et al., 2023)	
		6.5	2.44		(Auguste (Hitachi ASTEMO), 2021), (Parker, et al., 2018), (Schröder, et al., 2023)		
		2.44	0	(Auguste (Hitachi ASTEMO), 2021), (Parker, et al., 2018) (Cheon, et al., 2011), (Sinha, 2011), (Schröder, et al., 2023)	(Cheon, et al., 2011)	(Cheon, et al., 2011)	
✓	Uncommanded	0	2.44	(Putz, et al., 2016)			
		2.44	6.5	(Putz, et al., 2016)		(Auguste (Hitachi ASTEMO), 2021)	
		6.5	10	(Putz, et al., 2016)	(Auguste (Hitachi ASTEMO), 2021)		
-	Incorrect	-	-	(Parker, et al., 2018)			

3.1.3 Determination of the Exposure

ISO 26262-3 requires the consideration of operational situations that may be hazardous in case of a faulty operation. Therefore, a 4-dimensional generic operating space is chosen, as published in (Schrade, et al., 2023). It considers the initial speed, the longitudinal deceleration and the lateral acceleration, as shown in Figure 3.2 and as a fourth dimension the friction coefficient μ (Figure 3.2 only shows the operating space for a defined $\mu=const$).

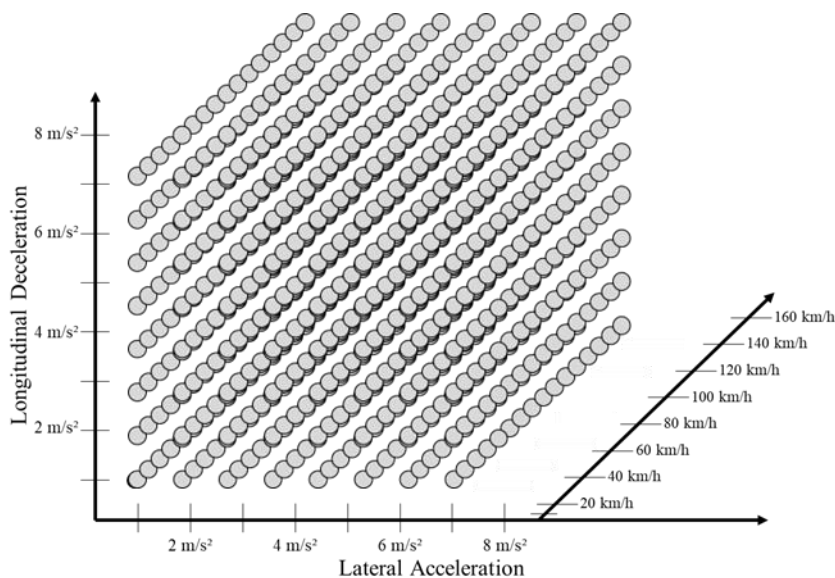


Figure 3.2: Operation space at a specific friction coefficient

This operating space provides the basis for the derivation of E. It is derived from fleet data collected by Robert-Bosch GmbH with a resolution of $\Delta v = 10 \text{ km/h}$ (speed), $\Delta a_{x/y} = 1 \text{ m/s}^2$ (longitudinal/lateral acceleration). However, the fleet data may not be suitable to be applied to the operating space without further consideration, as ISO 26262-3 requires that “it shall be ensured that the chosen level of detail of the list of operational situations does not lead to an inappropriate lowering of the ASIL”. Therefore, the resolution is adapted to VDA702 to avoid an “inappropriate lowering of the ASIL”. It provides E for generic driving situations considering $\Delta a_x = 2 \text{ m/s}^2$ at different speed resolutions of $\Delta v \in [12, 50] \text{ km/h}$.

Therefore, a hat-function is chosen to account for the merging of multiple fleet data points into a single driving situation, as shown in Figure 3.3. It derives the *probability* $p_{i,result}$ of a *driving state* i , as given by (3.1) Therefore, the hat-function also considers the data of the *driving state* i , itself and adjacent *driving states* $i\pm 1$ and $i\pm 2$ in relation to a certain *weighting factor* wf , as well. The wf is introduced to take into account a higher influence of data points closer to the *state* i and lower influence of points further away from i . The sum of wf ensures a resolution of $\Delta v = 40 \text{ km/h}$ and $\Delta a_x = 2 \text{ m/s}^2$, similar to the resolutions given by VDA702. Figure 3.4 shows the E of the operating space after applying the hat-function.

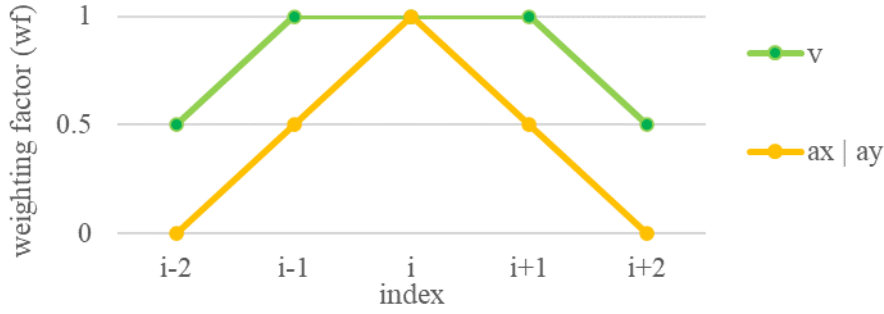
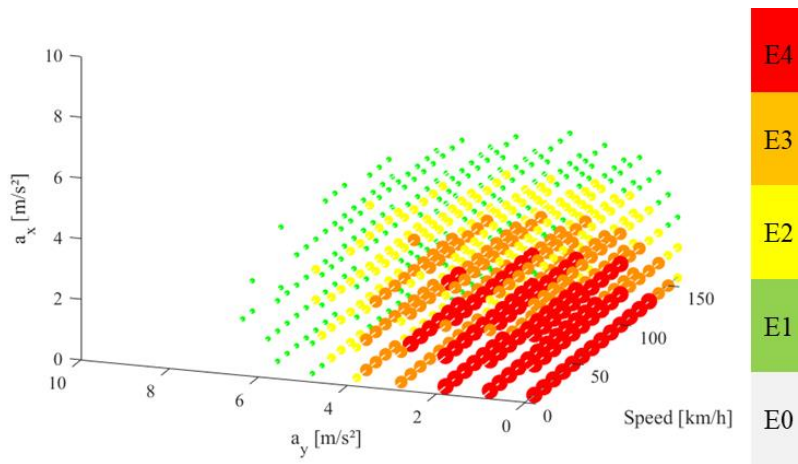


Figure 3.3: Hat-function to determine the merged probabilities

$$\begin{aligned}
 p_{i,result} = & p_{i,init} + 0.5 \cdot (p_{a_x,i-1,a_y,i,v_i} + p_{a_x,i+1,a_y,i,v_i}) + 0.5 \\
 & \cdot (p_{a_x,i,a_y,i-1,v_i} + p_{a_x,i,a_y,i+1,v_i}) \\
 & + 1 \cdot (p_{a_x,i,a_y,i,v_{i-1}} + p_{a_x,i,a_y,i,v_{i+1}}) + 0.5 \cdot (p_{a_x,i,a_y,i,v_{i-2}} + p_{a_x,i,a_y,i,v_{i+2}})
 \end{aligned} \tag{3.1}$$

Finally, the *friction coefficient* μ is also considered. However, since the fleet data do not provide any information on the friction coefficients of the braking maneuvers, a *combined probability* $p_{combined}$ must be derived considering both, the *probability* $p_{i,result}$ of the *driving state* i and the *probability of a certain friction coefficient* p_μ . Therefore, the *final probability* $p_{combined,i}$ of a *driving state* i is evaluated using the probabilities of the friction coefficients provided by VDA702 and the application⁸ of (3.2) given by VDA702.

$$p_{combined,i} = p_{i,result} \cdot p_\mu \tag{3.2}$$


 Figure 3.4: Exposure of the operation space at μ_{high}

The final E of the operating space is shown in Figure 3.4 and Figure 3.5. Figure 3.4 shows the E of the driving situations at μ_{high} and the initial operating space (without considering μ), respectively. Obviously, the E peaks at the origin of the operating space. Furthermore, there is a

⁸ (3.2) can be only correctly applied if the probabilities being combined are *independent*. This, however, may be arguable regarding drivers that may take the friction coefficient into account while driving. An example could be that drivers tend to drive slower under snowy (μ_{low}) conditions.

decrease in E with respect to higher lateral accelerations, longitudinal decelerations and speeds. The decrease of the E coincides with the data provided by VDA702 regarding the speed and the longitudinal decelerations. Finally, Figure 3.5 shows the decrease in E for lower coefficients of friction by one order of magnitude.

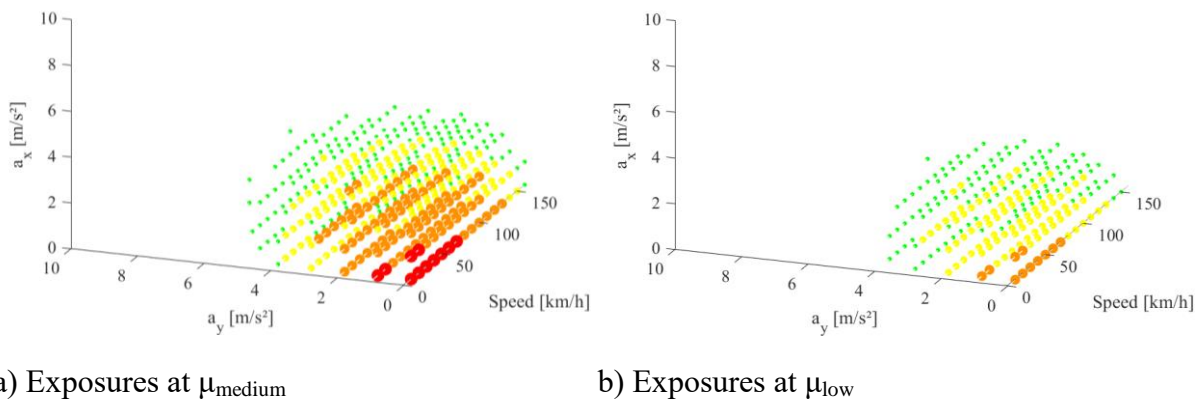


Figure 3.5: Exposures of the operation space at reduced friction coefficients

3.1.4 Determination of the Severity

The S is determined on the basis of a so-called *safe area*. It is assumed that driving situations generally remain safe ($S = 0$) as long as a vehicle remains within its *safe area*. This *safe area* extends longitudinally with a distance equivalent to $t_{\text{distance}} = 2 \text{ s}$ and laterally over the whole lane (see Annex C.2.2), as shown in Figure 3.6. However, a malfunction (e.g., of the braking system) may cause the vehicle to deviate from its desired position resulting in an excursion from the *safe area* and a $S \neq 0$, as shown in Figure 3.6b.

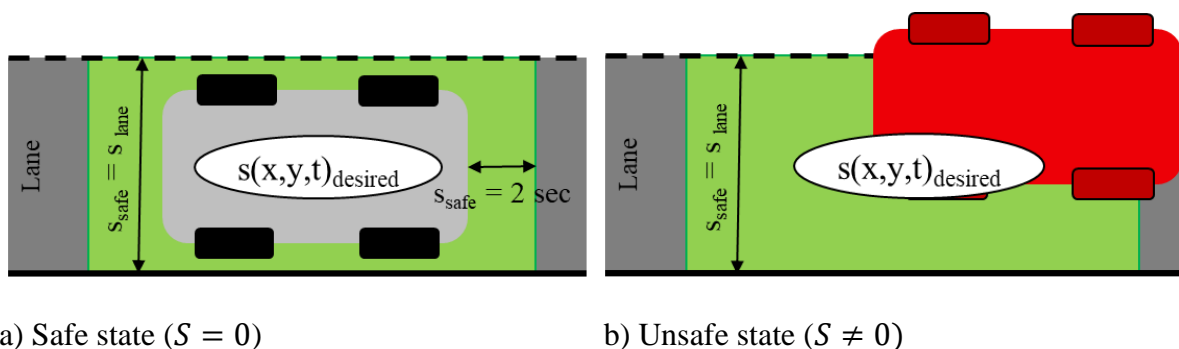


Figure 3.6: Introduction of the *safe area*

Furthermore, a follow-up driving situation is introduced as shown in Figure 3.7. Here, the (ego-) car with a braking system malfunction is colored red. Two malfunctions are analyzed. The first malfunction is a degraded braking functionality. Here, the driver of the (ego-) car reacts after $t_{\text{react}} = 1.2 \text{ s}$ to the braking of the car in front, as evaluated by (Triggs & Harris, 1982). The second malfunction to be analyzed is uncommanded braking. In this case, the (ego-) car starts to decelerate, possibly without activating the brake lights, and additionally surprising the driver of a following car. This can lead to an increased reaction time of

$t_{react} = 1.4 \text{ s}$ (Triggs & Harris, 1982) of the following driver. Finally, the S depends on the exit speed from the safe area, as published in (Schrade, et al., 2023).



Figure 3.7: Driving situation under analysis

In addition, the environment of the driving situation is considered, since a malfunction of the braking system can lead to a car versus car crash, or a car versus pedestrian crash (especially for the degraded braking malfunction), which significantly influences the S of a crash (see (Najm, et al., 2007), as published in (Schrade, et al., 2023)). Therefore, two scenarios are introduced, distinguishing between urban (pedestrian crashes, $v_{start} \leq 50 \text{ km/h}$) and rural (car crashes, $v_{start} > 50 \text{ km/h}$). These two scenarios consider the longitudinal nature of a potential crash (referred to as ‘Crash 1), as shown in Figure 3.8a.

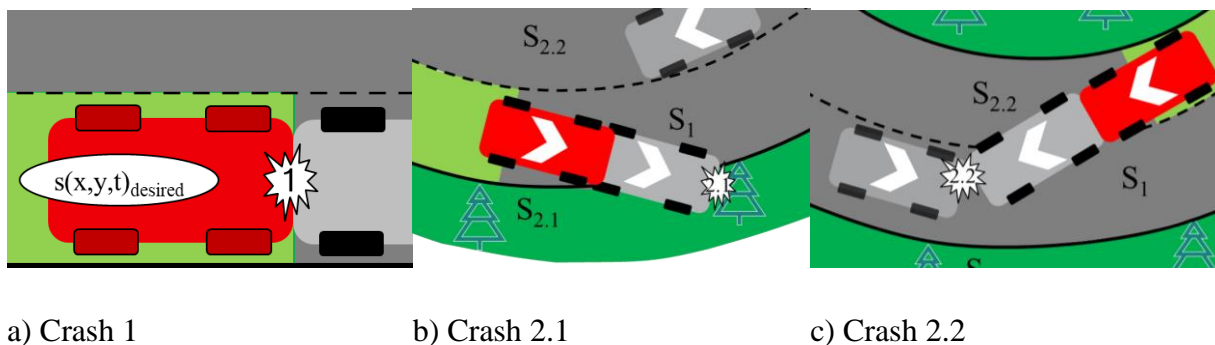


Figure 3.8: Crash scenarios

However, the initial crash (Crash 1⁹) can cause the vehicles to lose control, which, if combined with lateral acceleration (e.g., a turn), can cause a second crash (Crash 2). Therefore, there are, two additional scenarios for Crash 2:

- 1) Crash 2.1: Outbound excursion (Figure 3.8b)
 - a. Collision with trees, ditch or any form of infrastructure: S is determined by the impact speed; associated to an assumed probability of 50% within the situation.
 - b. No further collision because of excursion into the meadow: $S = 0$; associated to an assumed probability of 50% within the situation.
- 2) Crash 2.2: Inbound excursion (Figure 3.8c)
 - a. Collision with opposing traffic or pedestrians, resulting in death: $S = 3$, if pedestrians or opposing traffic is apparent (associated with an assumed $E = 3$ within the situation)

⁹ For the purpose of this study, Crash 1 is assumed to be an inelastic collision.

Additional crashes with further vehicles are not analyzed as it is unlikely that a further crash (related to a decrease of the overall kinetic energy) increases the S of the involved cars.

3.1.5 Derivation of X-Domain Safety Goals

The ASIL for the defined operating space is finally derived by superposition of E, S and C¹⁰. However, as discussed in section 3.1.4 a single driving state may inherit different S (see Crash 1, 2.1 and 2.2) associated with different E. To provide a worst case scenario, only the combination that results in the highest ASIL, is considered further. Figure 3.9 shows the color-coded ASILs for both *degraded* (a) and *uncommanded braking* (b) at high friction coefficients. It is clear that ASIL D maneuvers are only given for small decelerations combined with small lateral accelerations in the case of a *degraded braking* malfunction. On the other hand, only very strong *uncommanded braking* malfunctions lead to ASIL D malfunctions. This is in agreement with the results of (Auguste (Hitachi ASTEMO), 2021). Figure 3.10 also shows the SGs for *degraded braking* malfunctions considering reduced friction coefficients. *Uncommanded braking* malfunctions at reduced friction coefficients are not shown because high decelerations would be required to generate ASIL relevant SGs that cannot be actuated at reduced friction coefficients.

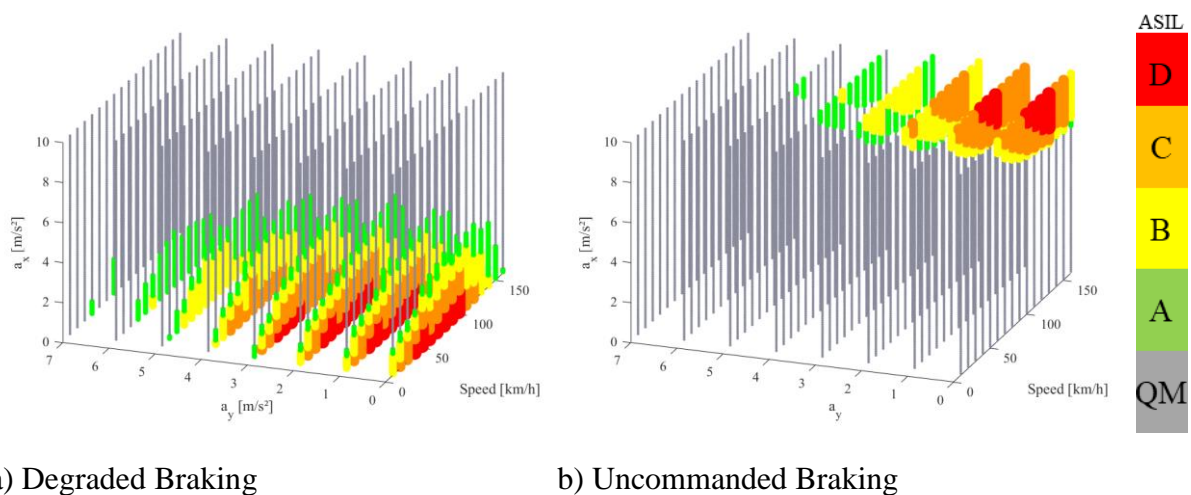
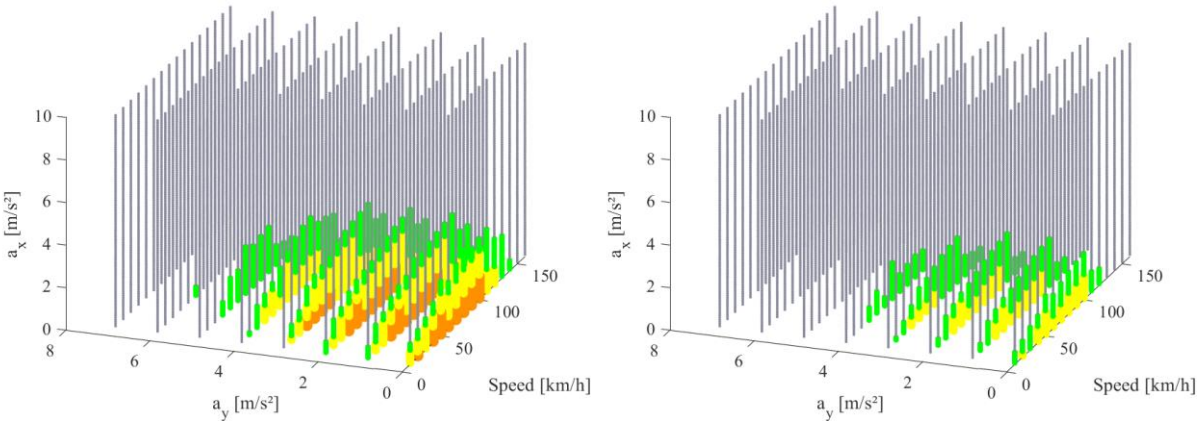


Figure 3.9: Generic SGs for high friction coefficients ($\mu=1.1$)

¹⁰ C is conservatively assumed to be 3



a) SG at μ_{medium}

b) SG at μ_{low}

Figure 3.10: Generic SGs for degraded braking at reduced friction coefficients

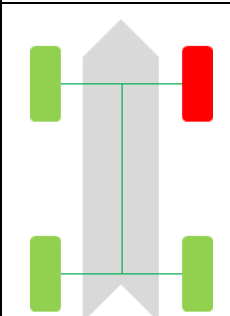
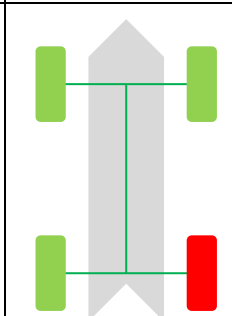
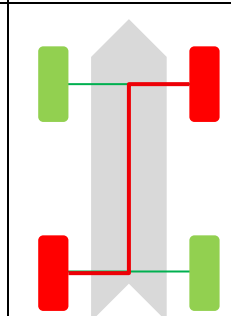
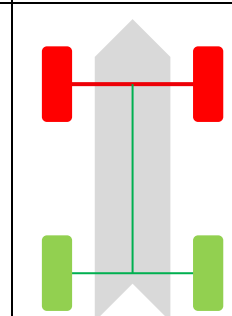
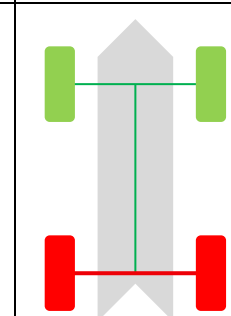
3.2 Safety Assessment of Braking System Malfunctions

This safety assessment applies the developed SGs to braking system malfunctions of four electric reference vehicle types: VW ID.3, Tesla Model S, Mercedes EQS and VW ID.4. These vehicles are chosen as representative because their dynamic brake force distribution (see Annex C.2) and their inertia (see Annex C.1) are distributed over a wide range. The vehicle data are given in Annex C.1.

3.2.1 Determination of the Safety Goals

The SGs are determined by applying expected *failure patterns*. These consist of individual actuator and circuit failures. Table 3.5 shows these patterns with failed wheels in red and wheels in normal operation (NOP) in green.

Table 3.5: Failure patterns

Front Actuator	Rear Actuator	X-Circuit	H-Front-Circuit	H-Rear-Circuit
				

In addition, several so-called vehicle configurations (config) are introduced. These configs represent levels of automation¹¹ starting with a ‘dumb’ config 1 that simply increases braking forces equally on all wheels until the required deceleration is achieved. Configs 2 and 3 introduce a ‘smart’ brake force distribution that keeps the brake forces laterally balanced if possible. The difference between the two configs lies in the friction circle used. While the configs 1 and 2 use the entire friction circle, the configs 3 and 4 use only 80% and 90% of the friction circle on the front and rear axle respectively, to account for imperfect control implementations. Finally, config 4 also actively counter-steers to account for yawing. Table 3.6 provides an overview of the configs analyzed.

¹¹ not to be mistaken with SAE automatization levels, as defined by (SAE International, 2021)

Table 3.6: Overview of analyzed configurations

	Smart brake force distribution	Active (counter-) steering	Friction circle exploitation	
			Front	Rear
Config 1	X	X	100%	100%
Config 2	✓	X	100%	100%
Config 3	✓	X	80% ¹²	90% ¹²
Config 4	✓	✓	80% ¹²	90% ¹²

The failure patterns and the configs are applied to the reference vehicle types to perform driving dynamics simulations (see Annex C.2) for the whole operating space as defined in section 3.1.3. These derive the SGs with the associated ASIL. The simulations consider both lateral deviations during braking maneuvers and maximum achievable decelerations. The elaborated results in Table 3.7 show the *maximum deceleration* $a_{x,max}$ during straight line driving and the SGs considering all operating states and potential yawing. Two examples (using front actuator failures of a VW iD.3) are given to show the derivation of the final ASIL, as it is displayed.

First, the front actuator failure of config 1 is analyzed. It achieves a maximum deceleration $a_{x,max} = 6.6 \text{ m/s}^2$ while driving straight under μ_{high} conditions. This rather high residual deceleration suggests a classification as a QM malfunction. However, the vehicle tends to yaw due to the uneven brake torque distribution between the left and right wheels. This yawing causes a lane excursion of $\Delta y > 0.45 \text{ m}$ at $v = 50 \text{ km/h}$ when braking with $a_x = 2 \text{ m/s}^2$ (E4 situation), even if the driver counter-steers manually (as described in Annex C.2.2). Such a lane departure may cause injury to pedestrians (S3). The front actuator malfunction of config 1 is therefore finally assessed as ASIL D.

The second example is the failure of a front actuator of config 3. Again, rather high residual decelerations of $a_{x,max} = 6.2 \text{ m/s}^2$ can be achieved in straight line driving under μ_{high} conditions. Nevertheless, the malfunction is classified as ASIL A. Since config 3 ‘smartly’ distributes the braking torques to avoid yawing up to a deceleration of $a_{x,straight} = 3.9 \text{ m/s}^2$, no yawing is noticeable at $a_x = 2 \text{ m/s}^2$ (in contrast to config 1). However, required decelerations beyond $a_{x,straight}$ will cause yawing. In the specific example, a track excursion of $\Delta y > 0.46 \text{ m}$ at $v = 40 \text{ km/h}$ when braking with $a_x = 5 \text{ m/s}^2$ (E1 situation) provokes an ASIL A assessment.

Table 3.7 shows the summarized SGs with their associated ASILs from a vehicle dynamics perspective, which may not correspond to the decomposition rules as defined in ISO26262.

¹² considering a non-optimal control of a controller

Obviously, all braking circuits can be designed with an ASIL A, despite config 1 cars being equipped with X-Circuits. This is due to the different deceleration levels achieved by the different configs. Furthermore, it can be seen that single actuator failures result in ASIL D malfunctions for config 1, while they are classified as approx. ASIL A for the other configs. However, as explained, this differentiation is not due to the different achievable deceleration levels, but to the large lateral deviations caused by potential yaw.

Table 3.7: Summary of the Safety Goals

Car	Con-fig	Front Actuator		Rear Actuator		X-Circuit		H-Front-Circuit		H-Rear-Circuit	
		$a_{x,max}$	ASIL	$a_{x,max}$	ASIL	$a_{x,max}$	ASIL	$a_{x,max}$	ASIL	$a_{x,max}$	ASIL
VW iD.3	1	6.6	D	8.1	D	3.1	B	4.2	A	7.2	A
	2	7.1	A	9.2	A	5.3	A	4.2	A	7.2	A
	3	6.2	A	7.3	QM	4.5	A	3.9	A	5.4	A
	4	6.0	QM	8.1	A	4.3	A	3.9	A	5.2	A
Tesla Model S	1	6.9	D	8.1	D	3.3	B	4.5	A	6.6	A
	2	7.3	A	8.9	A	5.3	A	4.5	A	6.6	A
	3	6.4	A	7.2	A	4.5	A	4.1	A	5.0	A
	4	6.0	QM	6.8	QM	4.4	A	4.1	A	4.9	A
Mercedes EQS	1	6.8	D	8.1	C	3.2	B	4.4	A	6.8	A
	2	7.3	A	9.0	A	5.3	A	4.4	A	6.8	A
	3	6.3	A	7.2	A	4.5	A	4.0	A	5.2	A
	4	6.3	QM	7.2	QM	4.3	A	4.0	A	5.0	A
VW iD.4	1	6.4	D	8.1	D	3.1	B	4.1	A	7.5	A
	2	7.0	A	9.3	A	5.3	A	4.1	A	7.5	A
	3	6.1	A	7.4	A	4.5	A	3.8	A	5.5	A
	4	6.1	A	7.0	QM	4.3	A	3.8	A	5.4	A

3.2.2 Decomposition of Availability between Service- and Parking Braking System

The driving simulations show that some *failure patterns* undermine the required backup deceleration performance of $a_{x,res} = 6.4 \text{ m/s}^2$, which is necessary to avoid product liability (see Annex A). However, since a braking system consists of a service and a parking brake (PB), the PB can take over the residual braking performance, if it has a deceleration capability (see section 4.4.2).

The main load case of a PB is to stop the vehicle on a slope σ with a *weight* F_G dependent on the *vehicle mass* m and the *gravitational constant* g . Legislation (United Nations ECE, 2015) requires this capability on a slope of $\sigma \leq 20\%$. However, this requirement can be transformed

into a *deceleration capability of the PB* $a_{x,pb}$ or a *force* F_{PB} by using equation (3.3) with the slope translated into an angle.

$$F_G = F_{PB}$$

$$\langle \Rightarrow \rangle \quad m \cdot g \cdot \sin(\sigma) = m \cdot a_{x,pb} \quad (3.3)$$

$$\langle \Rightarrow \rangle \quad a_{x,pb} = g \cdot \sin(\sigma)$$

Finally, the PB could decelerate a vehicle by $a_{x,pb} = 1.92 \text{ m/s}^2$. With the same consideration, the case of an improved PB capable of stopping the vehicle on a slope of $\sigma \leq 30\%$ results in a deceleration potential of $a_{x,pb} = 2.82 \text{ m/s}^2$. Table 3.8 shows the required backup performance $a_{x,res}$ of a PB depending on the failure pattern, the vehicle and the level of automation to achieve a deceleration of $a_x = 6.43 \text{ m/s}^2$ (as specified in Annex A).

Table 3.8: Suitability of the PB as backup

Car	Con-fig	Front Actuator		Rear Actuator		X-Circuit		H-Front-Circuit		H-Rear-Circuit	
		$a_{x,max}$	$a_{x,res}$	$a_{x,max}$	$a_{x,res}$	$a_{x,max}$	$a_{x,res}$	$a_{x,max}$	$a_{x,res}$	$a_{x,max}$	$a_{x,res}$
VW iD.3	1	6.6	-	8.1	-	3.1	3.3	4.2	2.2	7.2	-
	2	7.1	-	9.2	-	5.3	1.1	4.2	2.2	7.2	-
	3	6.2	0.2	7.3	-	4.5	1.9	3.9	2.5	5.4	1.0
	4	6.0	0.4	8.1	-	4.3	2.1	3.9	2.5	5.2	1.2
Tesla Model S	1	6.9	-	8.1	-	3.3	3.1	4.5	1.9	6.6	-
	2	7.3	-	8.9	-	5.3	1.1	4.5	1.9	6.6	-
	3	6.4	-	7.2	-	4.5	1.9	4.1	2.3	5.0	1.4
	4	6.0	0.4	6.8	-	4.4	2.0	4.1	2.3	4.9	1.5
Mercedes EQS	1	6.8	-	8.1	-	3.2	3.2	4.4	2.0	6.8	-
	2	7.3	-	9.0	-	5.3	1.1	4.4	2.0	6.8	-
	3	6.3	0.1	7.2	-	4.5	1.9	4.0	2.4	5.2	1.2
	4	6.3	0.1	7.2	-	4.3	2.1	4.0	2.4	5.0	1.4
VW iD.4	1	6.4	-	8.1	-	3.1	3.3	4.1	2.3	7.5	-
	2	7.0	-	9.3	-	5.3	1.1	4.1	2.3	7.5	-
	3	6.1	0.3	7.4	-	4.5	1.9	3.8	2.6	5.5	0.9
	4	6.1	0.3	7.0	-	4.3	2.1	3.8	2.6	5.4	1.0

no Backup required: - $\sigma \leq 20\%$ suited $\sigma \leq 30\%$ suited better PB required

The analysis shows that a regular PB (blue) is able to provide the required backup deceleration for both front actuator and H-Circuit rear failures. All H-Circuit front failures can be compensated by an enhanced PB (purple). However, no general conclusion can be drawn for X-Circuit failures, which may require even better PB than the improved ones analyzed (red).

Regardless of the PB type, an important point to consider is the installation location of the PB. Obviously, the PB is only able to provide backup deceleration if it is located at the specific

failed wheel(s) and is still operational, for example due to a redundant power-supply. However, the PB is usually only mounted on a single axle, which must also be considered.

3.3 Availability Decomposition between Braking and Powertrain System

Electric powertrains (PT) are capable of decelerating the vehicle through recuperation. However, this recuperation can only be provided if the PT (especially the battery) has the potential to absorb electrical energy. The potential impact of reliable PT onto the braking system is first analyzed (section 3.3.1). Then, a probabilistic analysis (section 3.3.2) is performed to investigate the potential for recuperation. Finally, decomposition options are provided considering both active and backup redundancies (as defined in section 3.3.3).

3.3.1 Safety-Impact of a reliable Powertrain onto the Braking System

ISO 26262-3 defines that the ASIL of an item is directly related to its E. Therefore, the ASIL of an item can be reduced by reducing its E. Finally, the ASIL of the braking system can be reduced if, from its point of view, it is used sufficiently infrequently because the PT provides the required deceleration. An example could be a reduction of the E from E4 to E3, if the PT recovers strongly enough in 90% of the ASIL D braking maneuvers, thereby reducing the ASIL of a braking system from ASIL D to ASIL C. Table 3.9 summarizes two ways to reduce the ASIL of a braking system to ASIL C or even ASIL B by formulating requirements for the availability of the PT.

Table 3.9: Options for lowering the ASIL of a brake-system

Option	Initial ASIL Brake-System	Req. Availability of Powertrain ¹³	Lowering of the ASIL/Exposure	Resulting ASIL Brake-System
1	ASIL D	> 90%	-1	ASIL C
2	ASIL D	> 99%	-2	ASIL B
	ASIL C	> 90%	-1	ASIL B

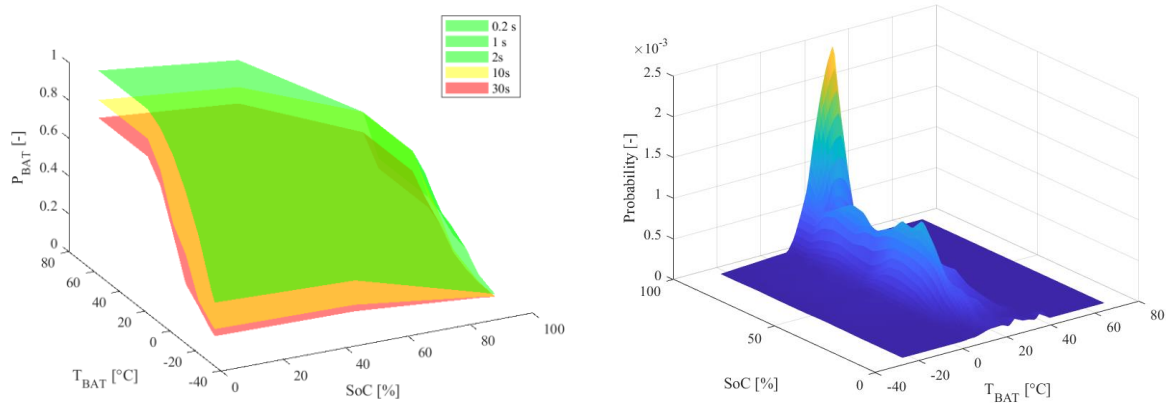
3.3.2 Deceleration-Potential of a Powertrain

The deceleration potential of a PT depends on the eDrive ‘actuator’ for recuperation, the power supply to conduct the electrical energy, the thermal management system to cool the components and the battery to absorb the recuperated energy. For this investigation, it is assumed that the availability of the battery is the key to the recuperation capability. In addition, it is assumed (see Annex D) that the specific power (power per mass), rather than the absolute power itself is the key determinant of the deceleration potential of an electric vehicle.

Therefore, the charging behavior of the batteries is analyzed. Figure 3.11a shows the relative charging power P_{BAT} of a reference battery compared to its maximum charging power P_{max} . It

¹³ For respective ASIL x brake maneuver

shows that the ability of a battery to absorb energy is strongly dependent on the battery temperature T_{BAT} , its state of charge (SoC) and the charging time (color-coded). However, it can also be concluded that there is almost no degradation between charging/braking durations of less than two seconds (marked in green) which represent 57 % (International Organization on Standardization, 2021) of all braking maneuvers.



a) Charging behavior of batteries

b) Probability of a combined SoC and Temperature

Figure 3.11: Data foundation of deriving the recuperation probability

The fleet data used to derive the E (see section 3.1.3) is used to derive the probability of the specified decelerations. However, the data source does not provide information on braking maneuvers. Therefore, assumptions must be made. It is assumed that long braking maneuvers (of more than two seconds) tend to require lower decelerations and though do not demand high recuperations/charging power. Therefore, this work concentrates on braking maneuvers with high deceleration (high recuperation demand), which tend to be short ($t < 2 s$, representing the majority of braking maneuvers (57 % (International Organization on Standardization, 2021))), since the vehicle motion stops quickly.

In addition to the charging capability dependence, shown in Figure 3.11a, the actual probability of a combination of SoC and battery temperature needs to be determined. This probability is derived from fleet data, as shown in Figure 3.11b.

Finally, the data from Figure 3.11 are merged to derive the probability of the PT recovering a given power. Figure 3.12 shows the result, with the lowering of one, and two ASILs marked in red and yellow, respectively. Finally, this probabilistic assessment concludes that:

- approx. 29% of the recuperation power is > 90 % of the time available; and
- approx. 12% of the recuperation power is > 99 % of the time available.

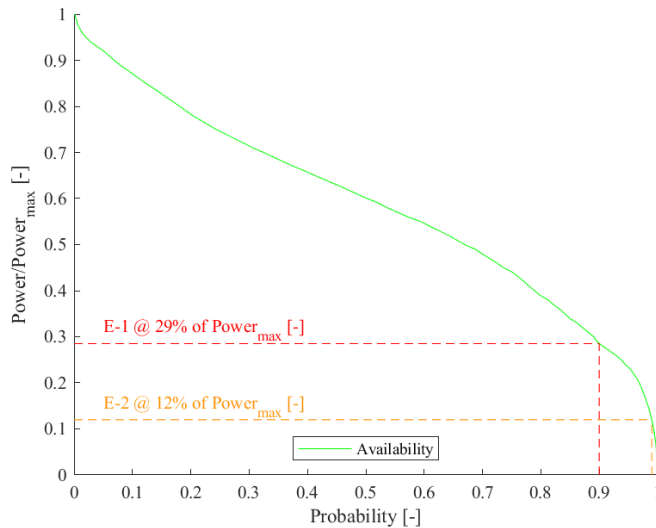
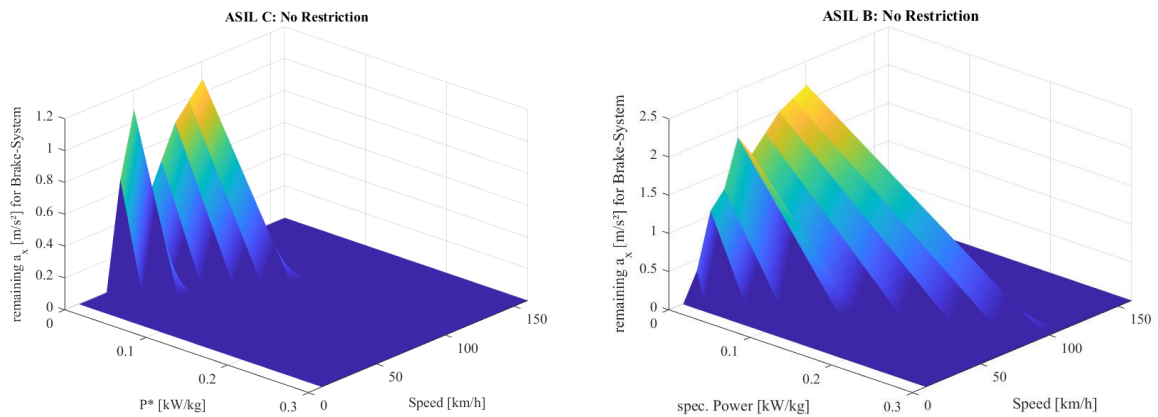


Figure 3.12: Availability of the recuperation capability

3.3.3 Decomposition Options

The deceleration requirements can be decomposed between the PT and braking system using either active or passive redundancy. Active redundancy refers to a concept that requires the powertrain to be sufficiently available in all situations to ensure safety. Ultimately, a PT malfunction will cause the vehicle to degrade to an *unsafe* condition and finally to stop operation. In contrast, a standby PT redundancy is only required to overcome a failure in the braking system. In such a case, the PT could implement the lost redundancy of the braking system, possibly combined with a reduction of the operating space. For example, the reduction in the operating space could consist of limiting the maximum speed.

Active Redundancy. The PT can be used as active redundancy to reduce the ASIL of the braking system to either ASIL C or ASIL B with respect to its SaRA. Figure 3.13 shows the remaining required deceleration of the braking system as a function of vehicle speed and PT specific power. In the case of an ASIL C braking system, the PT must implement at least a specific power of $P^* = 0.099 \text{ kW/kg}$ to eliminate all ASIL D deceleration requirements associated with the braking system. Finally, a vehicle that could implement such an ASIL C braking system is, for example, the Audi Q8 e-tron (see Annex D.2). However, a further reduction of the SaRA of the braking system to ASIL B is not possible (at the moment), as no vehicle has been found that exceeds a required minimum specific power of $P^* = 0.292 \text{ kW/kg}$.



a) ASIL C braking system

b) ASIL B braking system

Figure 3.13: Remaining deceleration on the braking system

Standby Redundancy. Using the PT as a standby or backup redundancy can exploit an additional degree of freedom: the reduction of the operating space. This reduction can be applied after an initial failure within the braking system and may eventually allow vehicles with lower specific powers to enable ASIL C or even ASIL B braking systems (after an initial failure). Appendix D.3 provides an overview of all possible specific powers, while this section highlights the implications for four reference vehicles.

Table 3.10: PT as standby redundancy for an ASIL C brake-system (after initial failure)

V	SoC	Buddy Cab	Renault eTwingo	Ford Mach-E	BYD Han
limit	limit	$P^* = 0.02 \text{ kW/kg}$	$P^* = 0.05 \text{ kW/kg}$	$P^* = 0.1 \text{ kW/kg}$	$P^* = 0.15 \text{ kW/kg}$
$\leq 50 \text{ km/h}$	60%	-	NOP	NOP	NOP
	80%	-	NOP	NOP	NOP
	no	-	NOP	NOP	NOP
$\leq 80 \text{ km/h}$	60%	-	NOP	NOP	NOP
	80%	-	NOP	NOP	NOP
	no	-	-	NOP	NOP
No	60%	-	NOP	NOP	NOP
	80%	-	+15 °C	NOP	NOP
	no	-	-	NOP	NOP

Table 3.10 shows options for limiting the operating space to achieve a safe ASIL C braking system. First, it should be noted that vehicles that inherit a higher specific energy than the Audi Q8 e-tron (Ford Mach-E and BYD Han in the table) do not require any restrictions and

can be operated in normal operation (NOP). However, the Renault eTwingo can also be operated without further restrictions if its maximum speed is limited to $v \leq 50 \text{ km/h}$. Furthermore, a speed restriction of $v \leq 80 \text{ km/h}$ combined with a charging restriction of $SoC \leq 80\%$ can also provide the required safety. A third option for limiting the operating space may be a combination of $SoC \leq 80\%$ and preventing operation below a temperature of $T \leq 15 \text{ }^\circ\text{C}$.

Table 3.11 shows the consequences of further exploiting the standby-redundancy to implement an ASIL B braking system (after an initial failure) with respect to SaRA. It is obvious that the Renault eTwingo's capabilities are very limited for such a case, limiting the speed to $v \leq 50 \text{ km/h}$, the SoC and the temperature to achieve a safe vehicle. Furthermore, even more powerful vehicles can only achieve safety by limiting the operating space.

Table 3.11: PT as a standby-redundancy for an ASIL B brake-system (after initial failure)

V limit	SoC limit	Buddy Cab $P^* = 0.02 \text{ kW/kg}$	Renault eTwingo $P^* = 0.05 \text{ kW/kg}$	Ford Mach-E $P^* = 0.1 \text{ kW/kg}$	BYD Han $P^* = 0.15 \text{ kW/kg}$
$\leq 50 \text{ km/h}$	60%	-	-16 °C	NOP	NOP
	80%	-	+15 °C	NOP	NOP
	no	-	-	-	NOP
$\leq 80 \text{ km/h}$	60%	-	-	NOP	NOP
	80%	-	-	-12 °C	NOP
	no	-	-	-	-
No	60%	-	-	-7 °C	NOP
	80%	-	-	-	-18°C
	no	-	-	-	-

Intermediate Conclusion. The study shows that high segment cars (e.g., Audi Q8 e-tron) are able to provide enough recuperation power frequently enough to allow the implementation of an ASIL C braking system with respect to SaRA. Other vehicles with less specific power (e.g., Renault eTwingo) can only use the PT as a redundancy option as a backup while limiting the operating space. The implementation of an ASIL B braking system (SaRA) cannot be classified as safe for any of the vehicles analyzed with respect to the data base provided (fleet and battery data). However, especially for high segment vehicles, the PT can be used as an ASIL B backup with a certain limitation of the operating space (see Table 3.11). Apart from the feasibility of the decomposition from a SaRA point of view (as analyzed), it should be noted that an ASIL qualification of the PT may not be useful from an economic point of view.



4 Safety Concepts of Electromechanical Brake Systems

Chapter 4 analyzes the safety for the item braking system (as defined in section 4.1), which is divided into four systems: pedal box (section 4.3, as published in (Schrade, et al., 2023)), actuator (section 4.4, as described in (Schrade, et al., unpublished yet)), central control system (section 4.5, as described in (Schrade, et al., unpublished yet)) and energy supply (section 4.6), as shown in Figure 4.1. The aim is to investigate the safety concepts of the systems independently. Finally, the systems are reintegrated in section 4.7 to evaluate holistic concepts considering both functional safety and product liability.

4.1 Definition of the ‚Item‘

There is no state-of-the-art on how to define an *item* in the context of ISO 26262 in the scope of an Electromechanical Braking System (EMB-System). Therefore, reference must be made to ISO 26262-1, which requires that an *item* implements “*a function or part of a function at the vehicle level*” (International Organization for Standardization, 2018). However, this statement can be interpreted in different ways. If the complete braking system is specified as a ‘*function*’, the EMB-system could be an *item*. However, since an *item* can also be specified as ‘*a part of a function*’, any part of the EMB-system (e.g., the brake pedal) could also be specified as an *item*. Furthermore, *items* can consist of up to ten systems, with each system satisfying the initial hardware metrics on its own (International Organization for Standardization, 2018). This raises the question of how to define a system when a brake pedal was already the item. Annex E.1 provides an overview of some options to specify the *item*.

Finally, an analogy is drawn from the current hydraulic system, which is implemented by two *items* (ESP and eBooster), suggesting the definition of the EMB-system (not its sections) as one *item*. The functionality of the *item* is defined as “*providing the correct (with a certain accuracy) deceleration*”. This functionality is related to the safety goals (SG), elaborated within section 3.2.

Figure 4.1 shows a generic architecture of the *item* without redundancies. Following this approach, the sections can be specified as systems, shown in the figure as layers of different

colors. The *item* EMB-system is therefore divided into the systems: brake pedal, central control system (CCS) (with communication bus), energy-supply and EMB-actuators.

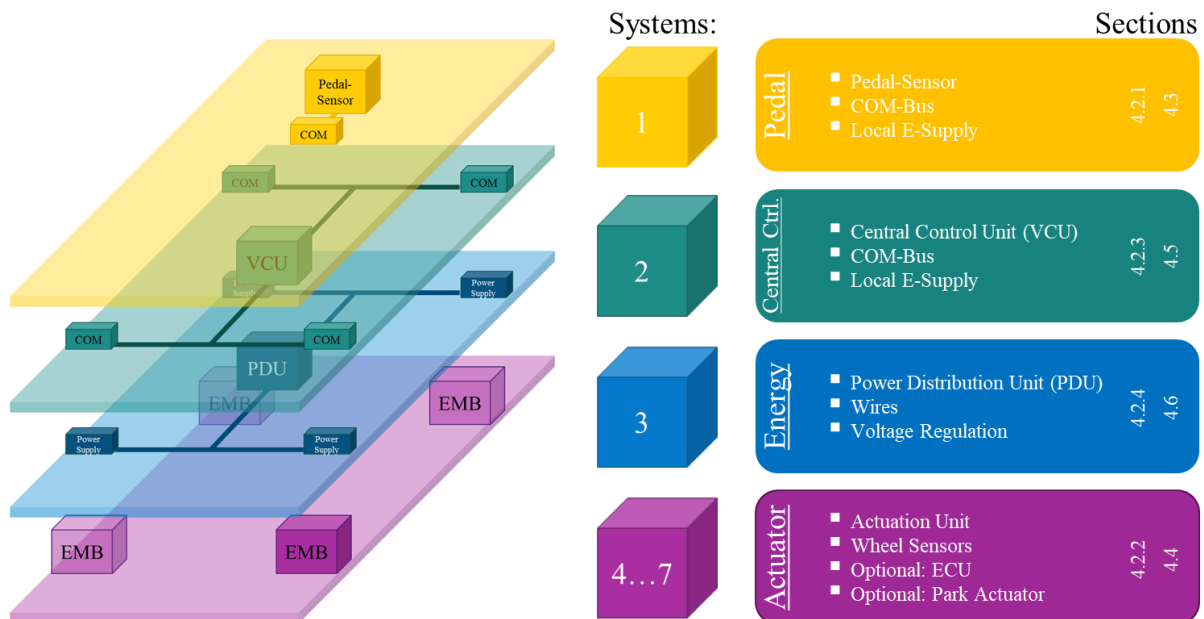


Figure 4.1: Definition of the item

4.2 Related Work

It is generally accepted that the braking system has an ASIL D SaRA (safety-related availability) (see Table 3.4). As ASIL D SaRA is very demanding, many authors have addressed functional safety of EMB-systems. This section provides an overview of the current state-of-the-art considering brake-by-wire (BBW) pedal boxes (section 4.2.1, as published in (Schrade, et al., 2023)), EMB-central-control-systems (section 4.2.4, as published in (Schrade, et al., 2022)), energy-supply (section 4.2.3, as published in (Schrade, et al., 2022)) and EMB-actuators (section 4.2.2, as published in (Schrade, et al., 2022) and (Schrade, et al., unpublished yet)).

4.2.1 Brake-by-Wire Pedal Boxes

The topic of BBW pedals gained interest in 2022, when Hella GmbH announced that it would be the first supplier to start mass production (HELLA GmbH & Co. KGaA, 2022). A major challenge for the introduction of BBW pedal boxes is the safety concept. Since a BBW pedal eliminates a mechanical connection between the pedal and the brakes, current state-of-the-art safety concepts of hydraulic systems, which revert to mechanical push-through in the event of a failure (Robert Bosch GmbH, 2013), become infeasible. This challenge is well known and accepted. For this reason, various authors addressed this issue.

As one system of the item EMB, the pedal box must satisfy ASIL D SaRA if no decomposition is applied. However, a decomposition can be applied, as (Cheon, 2010) argues by considering the parking brake (PB) knob as a backup-system that can be preserved as a user interface in case of a *fail passive (fp)* behavior of the pedal. Despite this proposal, authors (see the following paragraphs) generally agree on the requirement of a *fail-operational (fo)* capability by the BBW-pedal itself, avoiding any decomposition.

A minimum architecture for *fo*-capability is a duplex design consisting of two brake pedal sensors. However, if there is an undiagnosed discrepancy between the sensors, the current driver intent cannot be resolved after an initial fault. Therefore, (Jeon, et al., 2012) demand a diagnostic coverage $DC=100\%$, when proposing such a duplex design.

The disadvantage of reliable diagnosability can be addressed by triplex redundancy. Such a design is considered a safe concept by many authors (Cheon, et al., 2011), (Isermann, et al., 2002), (Hwan, 2009), (Hwan, 2009). (Cheon, 2010) also prefers the *fo*-capable triplex brake pedal to the proposed PB backup.

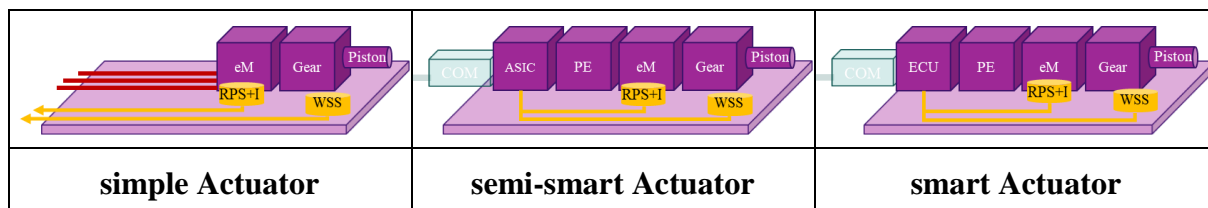
The implementation of an additional sensor creates a quadruplex system. Such a system may be advantageous in a two-braking circuit design, since each circuit can have access to one duplex unit, thus creating a local *fp*-entity. Therefore, the implementation of the two *fp*-entities realizes a global *fo*-capability of the BBW pedal. (Isermann, et al., 2002)

4.2.2 Electromechanical Brake Actuators

There is currently a growing interest in EMB-actuators within the automotive industry. This interest became apparent in 2022, when a supplier announced a €1.5 billion EMB series program to start production in 2025 (Continental AG, 2022). The supplier argues that “*safety redundancy*” is provided by the use of smart actuators that assign ECUs (electronic control unit) to the wheels. However, there are concurrent design options that do not use an ECU at the wheels (see (Cheon, et al., 2011), (Kügeler, et al., 2021), (Schumann, et al., 2002)) also referred to as EMB-actuators.

There is a common understanding in the literature that an EMB-actuator converts a command and electrical energy into a force that presses the brake pads onto the disc or shoes onto the drum respectively. However, the nature of the aforementioned command can vary depending on the complexity of the EMB-actuator, itself. In this work, a distinction is made between *simple*, *semi-smart* and *smart* actuators (see Table 4.1). The differences are explained in the following paragraphs.

Table 4.1: Degrees of Complexity of an EMB actuator



Different design options exist for the E/E architecture of an EMB-actuator. First, an actuator consisting only of an electric motor (eM) and a gear unit consisting of a reduction and a rotary/translation gear attached to a piston, as described in (Cheon, et al., 2011), (Kügeler, et al., 2021), (Schumann, et al., 2002), shall be introduced. Such an actuator will be referred to as a *simple* actuator in this work.

In addition, an ECU and power electronics (PE) can be attached to the *simple* actuator to form a *smart* actuator. A *smart* actuator is capable of processing local sensor information such as rotor position (RPS), current (I), and wheel speed (WSS). Therefore, the ECU can host complex functionalities such as ABS (Anti-Blocking System).

Finally, it is possible to replace the ECU with an ASIC with reduced capabilities (i.e., ASIC application-specific integrated circuit) to create a *semi-smart* actuator. However, the ASIC is not able to host any complex functions. Therefore, it must receive the current braking command (including the modulated higher functions such as ABS) in real-time. In this way, the ASIC can act as a gateway to collect the local sensor signals and provide them to a central control unit via the communication (COM) bus.

Finally, it should be noted that the different actuators inherit different functionalities that need to be aligned with the CCS. Therefore, reduced costs of the actuator (i.e. *simple* actuator) may be associated with increased costs within the CCS.

The EMB-actuator can be divided into two subsystems. One of these subsystems is the Actuation Unit (AU) consisting of the (electro-) mechanical components. It converts electric current and commands into mechanical force, which covers the components between PE and piston (inclusive). The other subsystem is the ECU itself, which can be implemented in a central control unit (see *simple* actuators) or at the wheel (see *semi-/smart* actuators).

The focus of this section is on the safety concept of an EMB-actuator, of which the most important sub-functionalities (logic and AU) are described in terms of safety.

Electronic Control Unit. ISO26262-5 (International Organization for Standardization, 2018) provides a generic hardware of a system that is adapted for the purposes of this work and is displayed as ECU in Figure 4.2. The ECU consists of:

- Central Processing Unit (CPU),
- Clock,
- ROM (Read-Only Memory), and
- RAM (Random Access Memory).

The ECU can drive the PE (of the AU) if all of the aforementioned components work in normal operation (NOP). Additionally, the ECU acquires sensor data from:

- RPS
- I to control the AU (Schwarz, et al., 1999) and
- WSS.

Furthermore, it is assumed that RPS and I can be so-called dumb sensors that only provide a current as a sensor signal, which is converted into digital signals by an ADC (Analog-Digital Converter). In contrast, the WSS (as specified in (Robert Bosch GmbH, 2023), (Bosch Engineering GmbH, 2023), (Bosch Rexroth AG, 2016)) is assumed to be a so-called smart sensor that provides data directly via a bus interface. (Lee, et al., 2014) present a qualitative safety concept for ECUs in an EMB context, which is based on a similar architecture and refers to safety mechanisms (SM), as listed in Table 2.6. However, the topic of hardware redundancies (as presented in Annex E.2) operating in an *fp* or *fo* operating mode is not addressed at all.

In addition, there are two interfaces that are considered part of the respective systems. These interfaces are for COM- and energy-supply purposes.

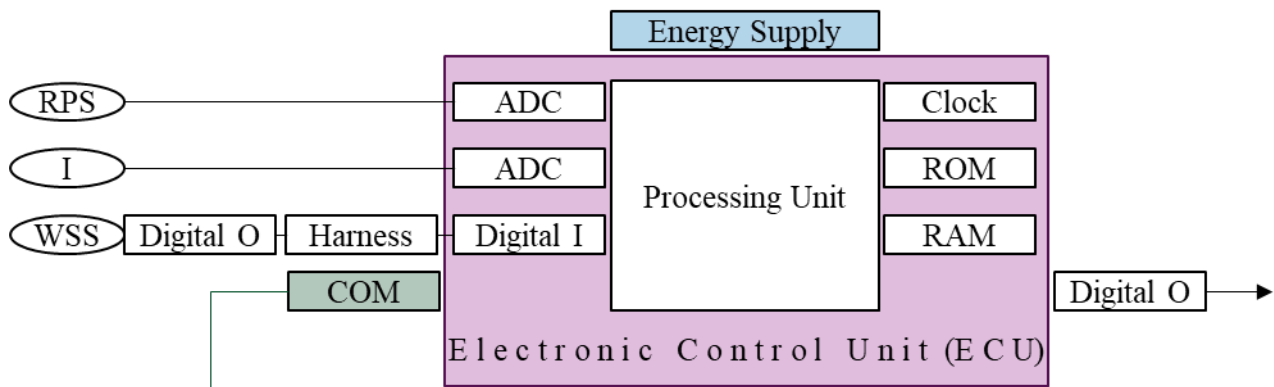


Figure 4.2: Generic hardware of an ECU, adapted from (International Organization for Standardization, 2018)

Actuation Unit. The AU converts the command given by the ECU, and the power supplied by the energy-supply, into a force. First, the PE inverts the direct current into an alternating current that drives the eM. The eM then generates the *torque* T_1 . Since eM tend to operate at high angular velocities and low torques, T_1 is increased to T_2 ($T_2 > T_1$) by a reduction gear, which forms a gear unit, combined with a rotation/translation gear. Finally, the rotation/translation gear produces a *force* F that pushes a piston on the brake pad/shoe that is part of the caliper.

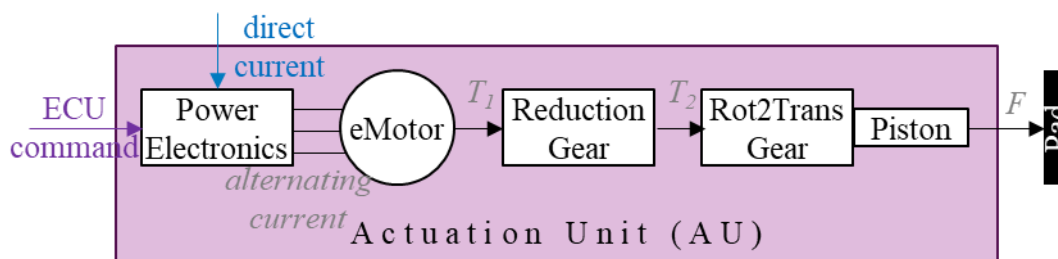


Figure 4.3: Generic Actuation Unit, oriented at (Schrade, et al., 2022)

Various AU designs can be found in the literature that consider redundancy concepts. Table 4.2 provides an overview showing 2x3 phase eM (Weiberle, 2021), full redundancy (duplex) (Bei, et al., 2017), (Takahashi & Takahashi, 2010)), two eM with addition gear (Takahashi & Takahashi, 2010), (Nuesse, 2020), (Gohbrandt & Stroschein, 2021) (Martin, 2004), (Schumann, 1997), (Kim, 2009), (Hartmann & Schautt, 2004), (Sim & Jian, 2021), (Fu, et al., 2020)¹⁴ and finally a PB as a potential SM (Hartmann & Schautt, 2004), (Saitner & Keller, 2009), (Schade & Linhoff, 2012), (Keski-Luopa, 2007), (Yang, et al., 2020), (Laxhuber, et al., 2004), (Friesen, 2005), (Schaffer, 1999) as implementation options.

¹⁴ Implemented as a series connection of two AUs

Simplex AU	2x3 Phase electric Motor	Duplex AU	Addition Gear	PB as SM
Legend:	PE and eM	Gear	Shaft / Piston	PB Actuator

Table 4.2: Redundancy concepts EMB-actuator, oriented at (Schrade, et al., 2022)

4.2.3 Energy Supply

An obvious safety concept of an EMB-system regarding the energy-supply is to mimic the current hydraulic X- or H-circuits, as presented in (Isermann, 2007), (Bergmiller, 2013), (Nilsson & Linidqvist, 2021), (Niedermeier, 2001), (Stoelzl, et al., 2000), (Yan, et al., 2021), (Weiberle, 2011), (Doericht & Schmid, 2000), (Weiberle, et al., 2011). Here, a first fault in the power distribution unit (PDU) or any other central component of the energy-supply causes an instantaneous shutdown of the wheels. Therefore, such designs violate product liability requirements (refer to Annex A).

However, product liability violations can be avoided by implementing a certain level of redundancy. One possibility is full redundancy by connecting each EMB-actuator to two energy-supplies, as described in (Weiberle, 2011), (Winkler, 2010), (Kelling & Heck, 2002). Furthermore, there are approaches that implement both a circuit design (by the low voltage circuits) and an additional energy-supply to all EMB-actuators (by the high voltage energy-supply) (Holzwarth & Krausen, 2008) (Liu, et al., 2021). Finally, local energy storage at the EMB-actuators is also considered (see (Kilian, et al., 2021) (Kim, 2009)). This approach is slightly modified if the storage is replaced by a harvester using the kinetic energy of the wheel (Gehring, et al., 2005). Table 4.3 shows the described topologies.

Table 4.3: Power supply topologies, oriented at (Schrade, et al., 2022)

X-Circuit	H-Circuit	Full Redundancy	X-Circuit + HV	Local Energy as Backup

4.2.4 Central-Control-System

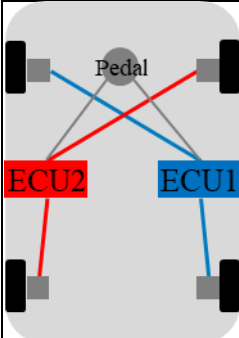
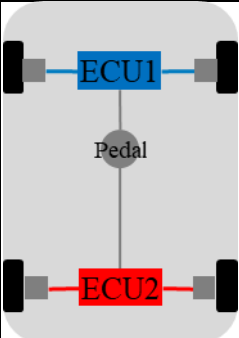
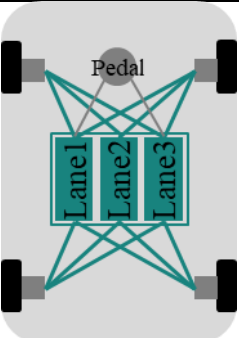
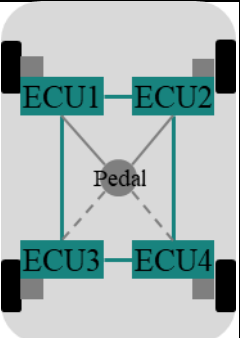
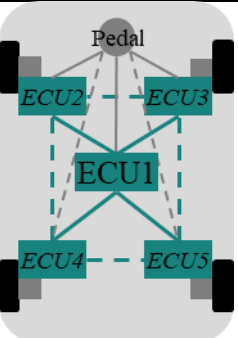
The CCS processes the driver's intent as determined by the BBW-pedal. Additional higher functions as ESP (Electronic Stability Program) (and ABS, depending on the complexity of the EMB-actuator) are modulated on the basis of the intent. Finally, the wheel-specific braking command is sent via COM-busses (*semi-/smart* actuator) or as three-phase current (*simple* actuator) to the actuators. Therefore, a shutdown of the CCS will ultimately cause a shutdown of the EMB-system.

Many EMB-CCS designs mimic the dual circuit designs of the current hydraulic systems (Weiberle, 2021), (Weiberle, 2011), (Doericht & Schmid, 2000), (Huang, et al., 2016), (Weiberle, et al., 2011) with the same potential for product liability violations as described in the previous section. However, centralized designs are also being promoted that inherit multiple computing units (hereafter referred to as 'lanes') in parallel. These lanes can provide both a backup in case of failure (i.e., *fp*) and a monitoring instance in case of a *fooc* (*fail-out-of-control*) behavior of a lane. A triplex configuration consisting of three parallel lanes that jointly command all actuators is presented in (Stoelzl, et al., 2000), (Holzwarth & Krausen, 2008), (Holzwarth, 2010).

Furthermore, quadruplex systems (four lanes, see (Choi & Hyun, 2021) and (Fijalkowski, 2010)) are also proposed, which generally increase the SaRA and the integrity of the CCS compared to triplex configurations. However, such quadruplex systems can also dispense with a central control unit and instead implement the lanes of the central control unit distributed on the four EMB-actuators (see (Putz, et al., 2016), (Kelling & Heck, 2002)). These actuators, in turn, could independently apply the higher functionalities as ESP. Although adding an additional lane, a distributed approach can be very cost effective compared to triplex configurations, as explained in (Kelling & Heck, 2002).

Finally, the centralized and distributed approaches can be combined by implementing both a central control unit (duplex or simplex) and distributed lanes on the EMB-actuators. For this purpose, there are approaches (Niedermeier, 2001), (Isermann, et al., 2002), (Molfetta, et al., 2008) that implement the higher functionalities (such as ESP or ABS) on the central control module, while ensuring a backup capability through a direct connection between the BBW pedal and the EMB-actuators.

Table 4.4: CCS topologies, oriented at (Schrade, et al., 2022)

				
X-Circuit	H-Circuit	Triplex-Topology	Quadruplex-Topology	Hybrid Topology

4.3 Brake-by-Wire Pedal Box

The pedal box is the only interface that evaluates the driver's request to brake. Therefore, it must ensure that it can reliably assess the true pedal position or force. The associated safety goals (SG) and the design space are identified in section 4.3.1. Based on this, the current state-of-the-art safety concepts are confirmed (section 4.3.2). However, these safety concepts can be improved by diagnosing sensor faults by consulting the drive pedal (section 4.3.3) or by consulting a virtual sensor (VS) (section 4.3.4). Finally, a short conclusion is given in section 4.3.5. This section is strongly oriented on the results, published in (Schrade, et al., 2023).

4.3.1 System Definition and Safety Goals

The 'pedal box' system must be defined as an element in the context of the braking system as the item (see section 4.1). The scope of the pedal box is extended from an exclusive measurement of the current position or force of the pedal to an identification of the driver's intent. The difference between these two concepts lies in the quality of the output. While an exclusive measurement provides unvalidated sensor data (potentially consisting of *fooc*-data), the intent identification validates the data by using monitoring and voting functionalities to provide one consolidated measurement. However, this intent identification must take place within the ECU of the CCS (see section 4.5), as the COM bus between the pedal box and the ECU may corrupt the consolidated data. The ECU, on the other hand, is not considered part of the brake pedal as it is already assigned to the CCS.

Therefore, the pedal box (as shown in Figure 4.4) is defined as consisting of the following components, with their abbreviation:

- Brake Pedal Sensor (neglecting the measuring principle), S_{BRK}
- Sensor Communication Bus Controller, SENT
- Wires (for communication and electric supply), -
- Inter-ECU Communication Bus Controller, CAN (controller area network)

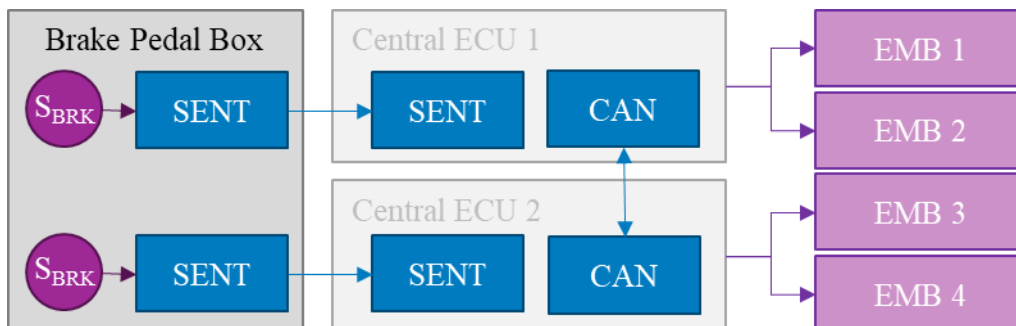


Figure 4.4: Exemplary pedal box topology

State-of-the-art safety concepts for BBW pedals ensure safety either by adding additional sensors or by improving the DC. The means to diagnose sensor faults are often limited to signal analysis (out-of-range, physical model, etc.). The objective of this work is to analyze the impact of consulting data from other sensor sources in addition. Therefore, both the drive pedal data (S_{DRV}) and VS are considered. Finally, these sensor data can be analyzed when a sensor discrepancy occurs that cannot be resolved. Such a stalemate situation could occur if two sensors are implemented and one of them fails *fooc*, to give just one example.

There is a growing trend towards the automation of vehicles. For example, EU legislation (European Parliament, 2019) requires new cars to be equipped with Automatic Emergency Braking (AEB) capability. In addition, many modern cars are equipped with traffic sign recognition systems to inform the driver about current speed limits to name just a few. Finally, this trend is taken into account by synthesizing all available sensor data related to the environment (traffic sign recognition, LiDAR, radar etc.) to implement a VS that guesses the driver's intention (as described in (Schrade, et al., 2022)). This guess can be more or less reliable depending on the reliability of the hardware and on the strictness of the application of SOTIF (Safety Of The Intended Functionality) as defined in ISO 21448 (International Organization for Standardization, 2022). As such a VS can be a very complex component, it is ambitious to assign a specific failure rate. Therefore, a False-Situation-Classification-rate (FSC) as a variable is introduced, which covers a wide range from $FSC=10^{-2} 1/h$ to $FSC=10^{-8} 1/h$. Finally, if a stalemate situation occurs during an FSC-state of the VS, the sensor in Normal Operation (NOP) is assessed as failed and the wrong driver intent is determined.

A second means of diagnosing brake sensor faults during stalemate situations is to evaluate the current driver intent derived from the drive pedal sensors (S_{DRV}). If the drive pedal is depressed during a BBW pedal stalemate, the S_{BRK} providing the lower deceleration value (ideally 0) is selected as valid while the other S_{BRK} is classified as *fooc* to passivate it.

This principle is reversed when the drive pedal is not depressed. This procedure may end up passivating the wrong sensor in a floating condition when neither brake nor drive pedal is pressed by the driver. On the one hand, floating conditions are rare in electrified vehicles because the recuperation directly applies a deceleration. On the other hand, a procedure as presented in (Schrade, et al., 2022) could be implemented. This procedure limits the deceleration in a stalemate situation of the BBW pedal for a certain duration and waits for the driver to react by pressing the drive pedal. If the driver reacts, the S_{BRK} with the higher demand is marked as *fooc*; if the reaction keeps missing the full desired deceleration is applied and the S_{BRK} sensing the lower demand is marked as *fooc*. The determination of the driver's intention with respect to the drive pedal is generally designed as a duplex sensor unit, following the EGAS-concept (as defined in (Audi AG, BMW AG, Porsche AG, Volkswagen AG, 2013)).

Figure 4.5 shows the system to be analyzed. The implementation of the dashed components is optional while the DCs and FSCs of all components are permutated.

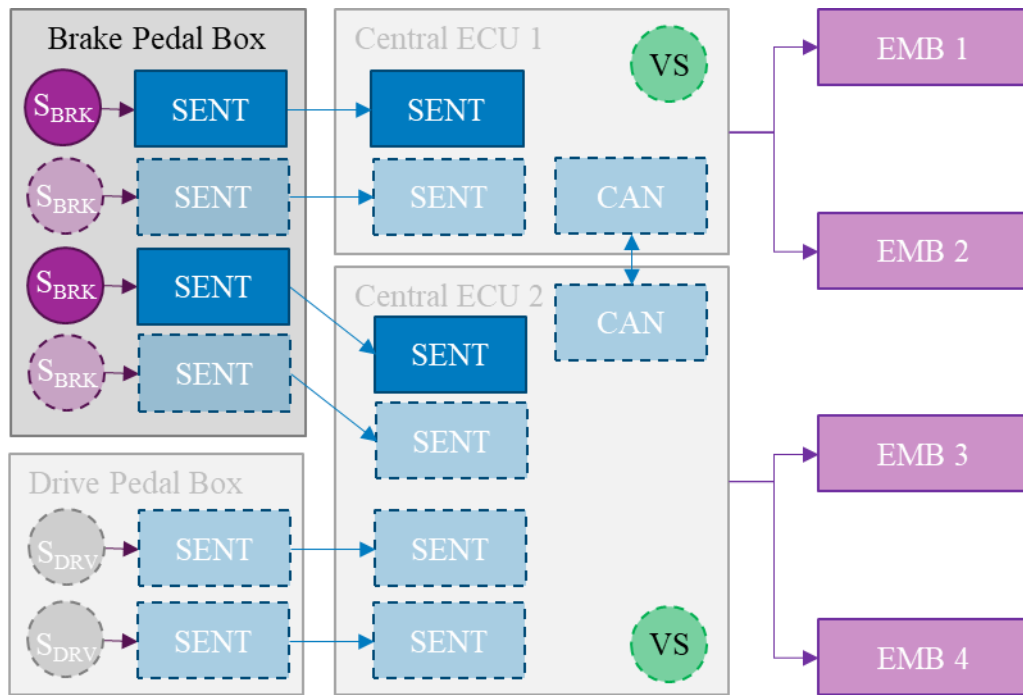


Figure 4.5: Definition of the brake pedal system

The designs that can result from the design space as shown in Figure 4.5 are analyzed considering the failure effects (FE) fp and $fooc$. Furthermore, an additional FE $fail$ is introduced for the investigation, which specifies a state in which none of the circuits evaluates a true brake request.

A sensor data fusion that results in a fp -behavior of the circuit can be evaluated as ASIL B, since the second circuit can generally apply enough deceleration to achieve a certain level of safety. A $fooc$ -behavior can result in either no braking, if desired (which is equivalent to fp) or in a braking command if not desired, which is evaluated as ASIL C¹⁵. Finally, if both circuits cannot process valid data, this corresponds to a complete braking system shutdown, which is rated as ASIL D. A complete braking system shutdown could also be ‘achieved’ by a shutdown of the (redundant) energy supply.

4.3.2 Conventional Safety Concepts

The results of the safety assessments for conventional safety concepts that do not use VS and S_{DRV} , but implement only redundancy are shown in Figure 4.6. Obviously, the installation of two sensors achieves only QM (shown in grey), regardless of the implemented DC within the COM. However, any triplex (inter-ECU communication required) and quadruplex designs meet ASIL D if both circuits are considered. Finally, the results of the related work are confirmed.

¹⁵ This undesired braking remains still coordinated as the (central) ECU is in NOP

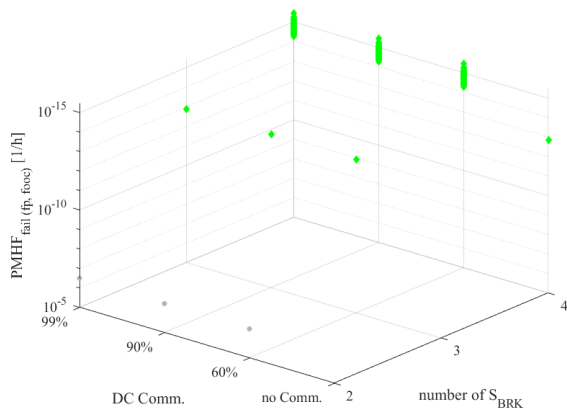


Figure 4.6: Failure rates of conventional pedal box architectures

4.3.3 X-Domain Safety Concepts

The drive pedal is connected to the central ECU 2, as described in section 4.3.1. Therefore, its use as a diagnostic tool is limited to the second brake circuit. Figure 4.7 shows that the SaRA (Figure 4.7a) remains almost unchanged when considering only VS (purple) or a combination of VS and drive pedal (blue). However, the integrity (Figure 4.7b) of the second brake circuit is significantly improved when the drive pedal is considered in addition to the VS to diagnose S_{BRK} faults. The integrity remains almost constant for the combined means of diagnosis regardless of the FSC-rate of the VS. However, when only the VS is used to diagnose S_{BRK} faults, the integrity is highly dependent on the FSC-rate.

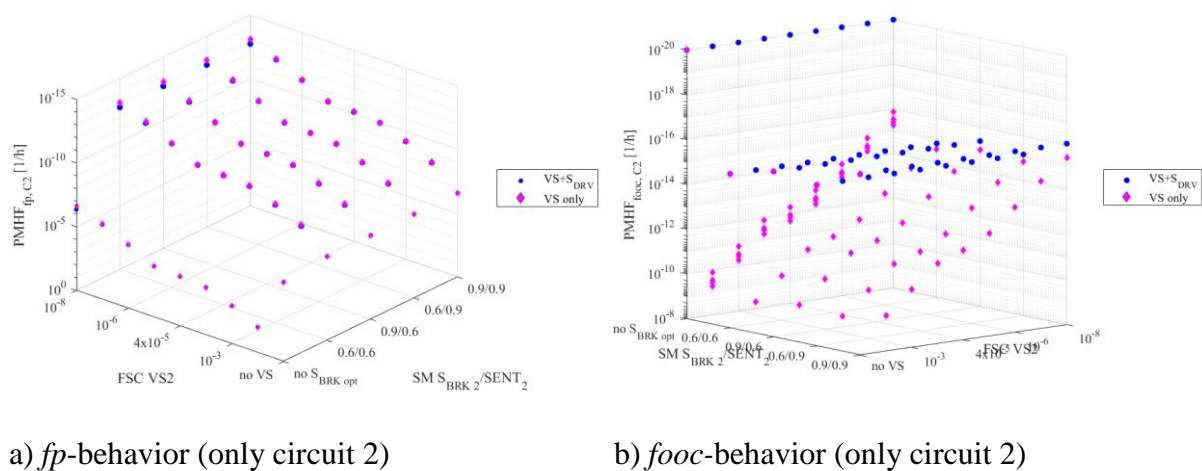


Figure 4.7: Safety comparison of Drive pedal and VS as means for diagnosing faults

4.3.4 Safety Concepts with Virtual Sensors for Diagnosis

The use of VS significantly affects the reliability of the driver intent detection. Figure 4.8a shows that the SaRA of a circuit is strongly dependent on the FSC-rate of the VS. In addition,

it can be seen that a circuit equipped with a single S_{BRK} or no VS does not achieve ASIL D¹⁶ but only QM (grey). However, a circuit equipped with both the VS and a second S_{BRK} always achieves ASIL D. Furthermore, it can be seen that an inter-ECU COM-bus (see Figure 4.8b) also increases the SaRA enabling ASIL D SaRA for simplex sensor designs and designs without VS. This increase in SaRA is achieved by allowing the ECU to access the sensor(s) of the other circuit via the COM-bus.

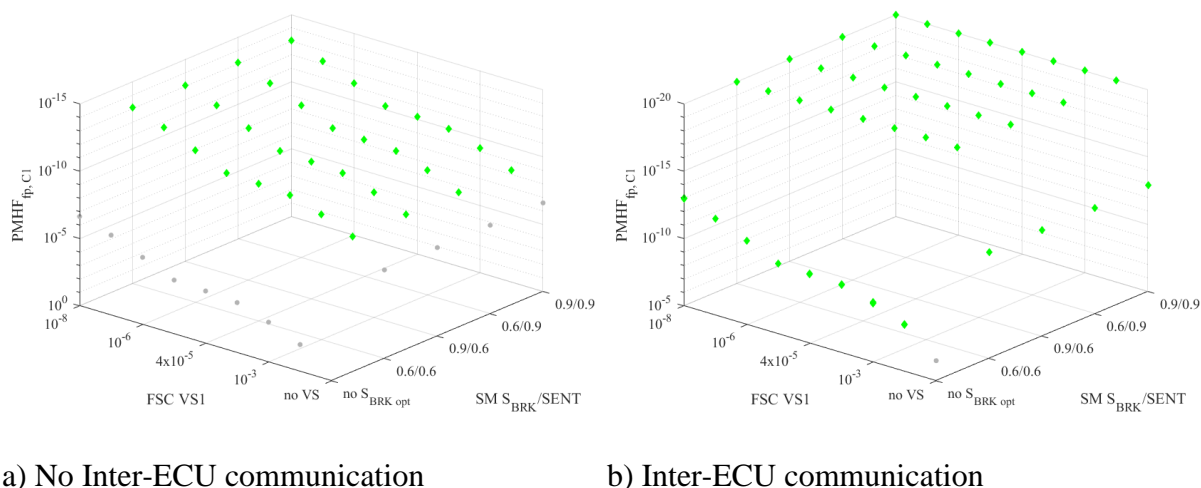


Figure 4.8: SaRA of a circuit equipped with a VS

The previous section showed the importance of the FSC-rate on the SaRA of a single circuit. This analysis is continued in Figure 4.9, which shows the safety (combined SaRA and integrity) of the two brake circuits, each equipped with one S_{BRK} , as a function of the FSC-rate of the two VS. As it can be seen, the safety of the braking system is strongly dependent on the FSC-rate of the two VS, which must be aligned to meet the ASIL D (green), ASIL C/B (orange) or QM (grey) SGs. Furthermore, it can be highlighted that architectures that do not meet ASIL D for a single circuit (no optional S_{BRK} in Figure 4.8a) do meet ASIL D ($FSC \leq 10^{-8} 1/h$) when both circuits are considered. However, when the circuits are combined with a COM-bus (not shown), ASIL D safety is always achieved when two VS are used.

¹⁶ The circuit itself does not satisfy ASIL D, however the combination of the two circuits achieves ASIL D

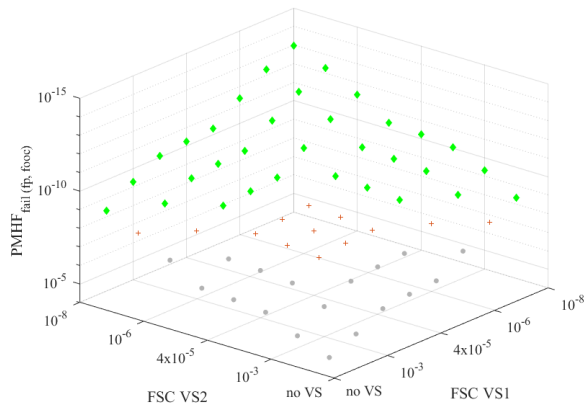


Figure 4.9: Fail behavior of two circuits equipped with VS, no COM

Figure 4.10 extends the analysis by additionally considering the number of S_{BRK} installed without the use of an inter-ECU COM-link. Again, low FSC-rates are required to achieve ASIL D or ASIL C safety in a duplex sensor configuration. Furthermore, combining the results of the conventional safety concepts (section 4.3.2) and the previous paragraphs, it can be assessed that a triplex redundancy achieves ASIL D (green) if a VS is implemented. Otherwise, only QM (gray) is achieved. On the other hand, quadruplex systems always meet ASIL D.

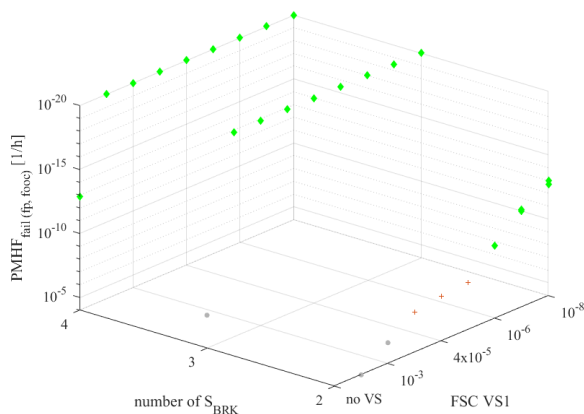


Figure 4.10: Fail behavior of number of sensors vs. VS, no COM

4.3.5 Intermediate Conclusion

The safety of BBW-pedals can be improved by implementing at least a triplex-redundancy, as discussed in related work. However, additional means of diagnosing S_{BRK} faults can be added. This can be a VS that accesses environmental data to infer the driver intent in sensor-stalemate situations. Nevertheless, such a VS requires a certain level of reliability if some S_{BRK} -redundancy is sacrificed. In addition, the drive pedal can be accessed to diagnose S_{BRK} faults. This design feature significantly improves the integrity. Another option to ensure safe-

ty is to merge the braking functionality onto the drive pedal in the event of a brake-pedal failure. Such architectures are discussed in section 5.3.2.

4.4 Electromechanical Brake Actuator

This section analyzes how safety can be implemented in the system ‘EMB-actuator’, as defined in section 4.1. Therefore, the SGs to be accomplished are summarized. In addition, section 4.4.2 presents options for improving safety by implementing redundancy. Section 4.4.3 briefly discusses the consequences of sensor failures, before the safety assessments of the actuators (*simple*, *semi-smart* and *smart*) are presented and discussed in the following sections. This section is strongly oriented on the results, described in (Schrade, et al., unpublished yet).

4.4.1 Related Safety Goals

In chapter 3, the SGs of the braking system malfunctions are derived. The analysis evaluates an actuator failure (*fp*) as ASIL D due to the induced yaw of the vehicle during braking maneuvers. This yawing is caused by the uneven brake torque distribution (left and right). However, it is also described that a shutdown of the specific axle, linked to the actuator, is only related to an ASIL A. Therefore, this work assumes that there is a feature that either actively distributes the brake torques between left and right or that passivates the entire axle in case of an actuator failure to mitigate yawing. However, this feature must be developed with an ASIL C (difference between the initial ASIL D and the final ASIL A) to realize ASIL A actuators.

Since the four actuators need to implement the ASIL D braking functionality, considering SaRA as a federation, the initial PMHF of $\lambda_{fp,total} = 10^{-8} 1/h$, can be eventually reduced to $\lambda_{fp,act} < 10^{-2} 1/h$ by using a simple budgeting approach. However, the procurement structure of OEMs and feasibility may suggest that each actuator is implemented at least in pairs. Therefore, it is questionable whether the actuators are *sufficiently independent* (see (International Organization for Standardization, 2018)) as required, to apply the budgeting described above. A dependency analysis would be required to prove independence. Furthermore, the ability of one actuator to satisfy both, the required deceleration and yaw-stability is questionable. Therefore, a budgeting approach resulting in $\lambda_{fp,act} < 10^{-4} 1/h$ is used as benchmark for the following sections.

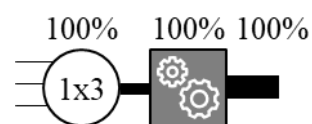
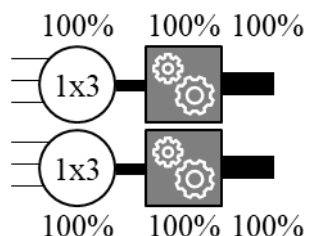
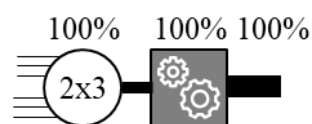
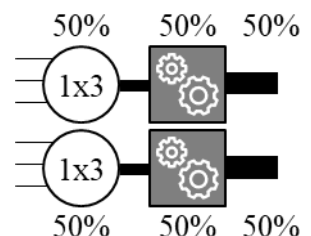
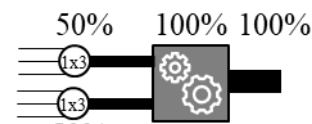
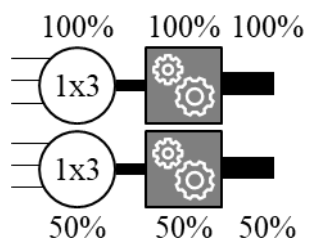
In addition to the SaRA, integrity must also be ensured. Annex C.2.3 g) and h) investigate that both the front and rear actuators are capable of inducing ASIL D relevant yawing if they develop *fooc*-behavior without any mitigation. Again, a function can be implemented to mitigate the yawing, in this case, by actively applying the remaining brakes to balance the braking torques of the left and right sides. However, the *fooc*-behavior may not be a constant, but a dynamic behavior that destroys the vehicle stability, since a *fooc* behavior is, by definition, non-deterministic. Therefore, a countermeasure is conservatively assessed as not feasible.

A special case of the *foc*-FE of the actuator is a residual torque after a braking maneuver, e.g, provoked by a blocking gear. Such a behavior is probably easier for the driver to control because it is constant and can be counteracted by counter-steering or increasing the braking torque, again. Therefore, only the *foc*-behavior of the ECU and a remaining brake torque at a deceleration of $a_{x, \text{vehicle}} > 5 \text{ m/s}^2$ is assessed as ASIL D relevant. Integrity budgeting is not possible because each actuator can violate the SG on its own, resulting in a target Probabilistic Metric for Hardware Faults (PMHF) of $\lambda_{foc} < 10^{-8} \text{ 1/h}$.

4.4.2 Actuation Unit Redundancy Concepts

Similar Redundancy. The similar redundancy concepts implement (partially) parallel force actuation paths within the service brake actuator. These concepts are oriented based on the results presented in section 4.2.2 and extend the design space from no redundancy at all up to full redundancy. Table 4.5 shows that partial redundancy consisting of a 2x3 phase eM, two eMs connected to an addition gear and also duplex actuators with different power levels (50% and 100%) are also considered. Finally, it is assumed that the implementation of a reduced eM is associated with a cost reduction of 1/3 and the implementation of a 2x3 phase eM with a cost increase of 1/3.

Table 4.5: Similar redundancy concepts

No/Partial Redundancy Concepts			Redundant Concepts		
ID	Redund.	Concept	ID	Redund.	Concept
AU1x3	Simplex		AU2	Duplex	
AU2x3	2x3 Phase		AU2x50	2x 50%	
AU2e	2 eMotors		AU150	Hybrid	

Dissimilar Redundancy. Dissimilar redundancy can be implemented by the parking brake (PB). The first option is to use a state-of-the-art PB equipped with its own eM and a self-locking gear to provide a (degraded) deceleration in case of failure of the above-described AU. This option can also be implemented with its own ASIC to provide redundancy in case of ECU failure. However, using the PB as a backup may significantly reduce the dynamic capabilities and, in the event of a second failure during a braking maneuver, may result in residual braking brake force at the specific wheel.

Another option to provide *fail-degraded (fd)* capability is a Default-actuator, as described in (Schrade, et al., 2022). This actuator is capable of applying a non-controllable force to a brake pad to produce a specified deceleration. This deceleration can be customized to prevent a wheel lock on the one hand and to provide a (combined) ASIL D or product liability deceleration with the other actuators on the other hand. It is therefore equipped with two springs (blue and yellow in Table 4.6) that provide a parking and a backup function. The specific springs are released by a solenoid actuator (green) in the event of a failure or a parking event.

Unlike the previous concepts, the PB can also be used as an external SM to prevent the service brake from failing *fooc*. This can be realized by a solenoid actuator (green) and a sensor (i.e., current sensor, as described in (Schrade, et al., 2023)) inside the service brake dedicated to monitor the (uncommanded) actions of the service brake. All PB concepts and their assembly with the service brake (exemplarily within a *semi-smart* actuator) are shown in Table 4.6.

Table 4.6: PB concepts

PB Actuator				
Assembly				
Act.	Backup	Backup System	Default	PB as SM

4.4.3 Failure Effects due to Sensor Failures

This work assumes that an actuator is equipped with an I-sensor and an RPS. These two sensors allow both the control of the eM and the estimation of the braking force, as shown by (Schwarz, et al., 1999). A WSS is also used to control the ABS. An overview of the sensors is given in Table 4.6.

Obviously, the I-sensor and RPS have a high correlation. In addition, WSS and braking force estimation (by I and RPS) also have a high correlation. Furthermore, this data is available at all four wheels, and the four wheels are also highly correlated. Therefore, it is assumed that a *foc*-behavior of any of these sensors can be diagnosed 100%, which provokes exclusively *fp*-sensor faults.

It is also assumed that any first *fp* sensor failure causes a degradation of the actuator capabilities. This degradation may be due to an I-sensor or RPS failure, which may affect the control of the eM. On the other hand, the failure of the WSS causes a degradation of the ABS on the specific wheel, since its blocking can no longer be detected. Therefore, a certain safety margin of the braking force is introduced to avoid blocking. Finally, if any two (out of three) sensors fail (*fp*), the operation of the specific actuator is considered to cease (*fp*).

4.4.4 Simple Actuator

Simple actuators consist of only an AU (without PE) as described in section 4.2.2. Therefore, failures within the ECU or the PE are not considered in this section. Figure 4.11 shows the distribution of the discussed FE for the respective architectures.

Obviously, the *foc*-SG is satisfied by all architectures analyzed. For example, simplex actuators (blue) inherit about half the failure rate to develop such a FE compared to redundant actuators because the main contributor to such a FE is the gear, which can be installed once (simplex) or twice (redundant).

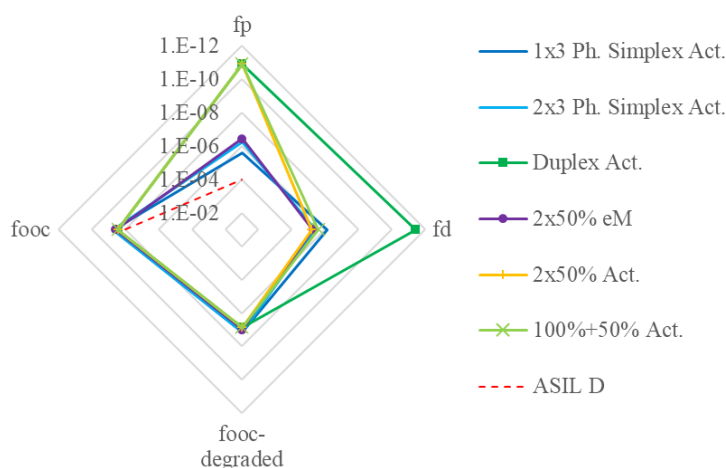


Figure 4.11: Failure Mode Distribution of Simple Actuator architectures

However, redundancy increases the SaRA. For example, the actuators that implement two completely independent transmission paths (green and yellow) even meet ASIL D SaRA SGs by a single actuator. In comparison, the implementation of a redundant eM in combination with an addition gear has only a minor impact on the SaRA. Finally, it should be noted that all actuators analyzed meet ASIL D SaRA when at least two independent actuators are installed.

4.4.5 Semi-Smart Actuator

The *semi-smart* actuators receive real-time braking commands that already inherit the wheel-specific braking force modulation, injected by higher-level functions such as ESP. Therefore, in addition to the AU, a simple (wheel) ECU (WECU) is implemented (i.e., ASIC). In the following figures, the redundancy within the AUs¹⁷ is represented by the shape of the icons, while the redundancy within the WECU is represented by the color.

Service Brake. In contrast to *simple* not all *semi-smart* actuators satisfy the associated SGs. The decisive factor for the analyzed actuator architectures is their probability of developing *fooc*-behavior, as can be seen in the lower part of Figure 4.12. The simplex WECUs (purple) show that there are three designs with almost the same cost differing only in their integrity. This differentiation is due to the implemented DC. The simplex-WECU architectures that satisfy the integrity SG all inherit a $DC \geq 90\%$. Duplex WECUs always satisfy the integrity SGs, due to their redundancy and monitoring capability. Furthermore, it can be seen that redundant AUs reduce the integrity by a factor of 2.

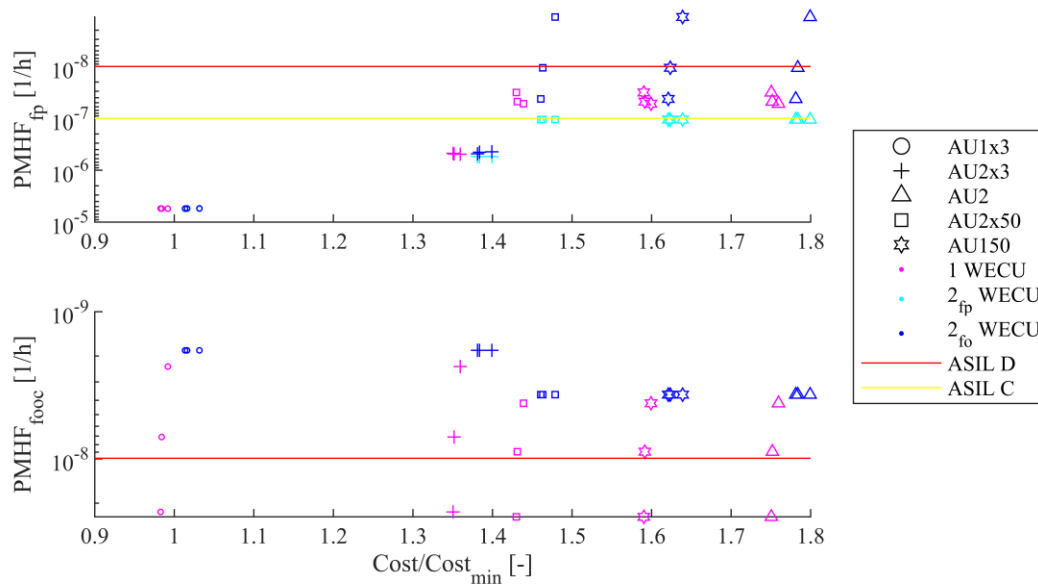


Figure 4.12: Safety assessment *semi-smart* actuator

Despite of the introduction of additional components (WECU and PE) compared to the *simple* actuator, all analyzed *semi-smart* actuators satisfy ASIL D SaRA, at least when implemented twice and independently. This is shown in the upper part of Figure 4.12. However, it can also be seen that the means of redundancy increases the SaRA. The different operating modes of the two duplex WECUs are also highlighted. While all the duplex WECUs operated fail-passively (cyan) remain at the same SaRA, the duplex WECUs operated in fail-operational

¹⁷ The AU-variant with two eMs and an addition gear (AU2e) is not investigated further as it is similar safe (refer to Figure 4.11) as a 2x3 phase eM (AU2x3) at increased costs. The AU2x3 can be, however, consulted to estimate the failure probability of AU2e.

mode (blue) are able to increase the SaRA by increasing the DC of the two lanes. This increase can even reach ASIL D for a single actuator if a $DC \geq 90\%$ and an AU with independent transmission paths are implemented.

Backup Parking Brake. Figure 4.13 shows the results when a PB actuator (see section 4.4.2) is connected to the previously analyzed service brake. It is obvious that such a backup PB mirrors the results of the service brake with a redundant (degraded) AU. However, the integrity remains unchanged compared to the service brake actuator.

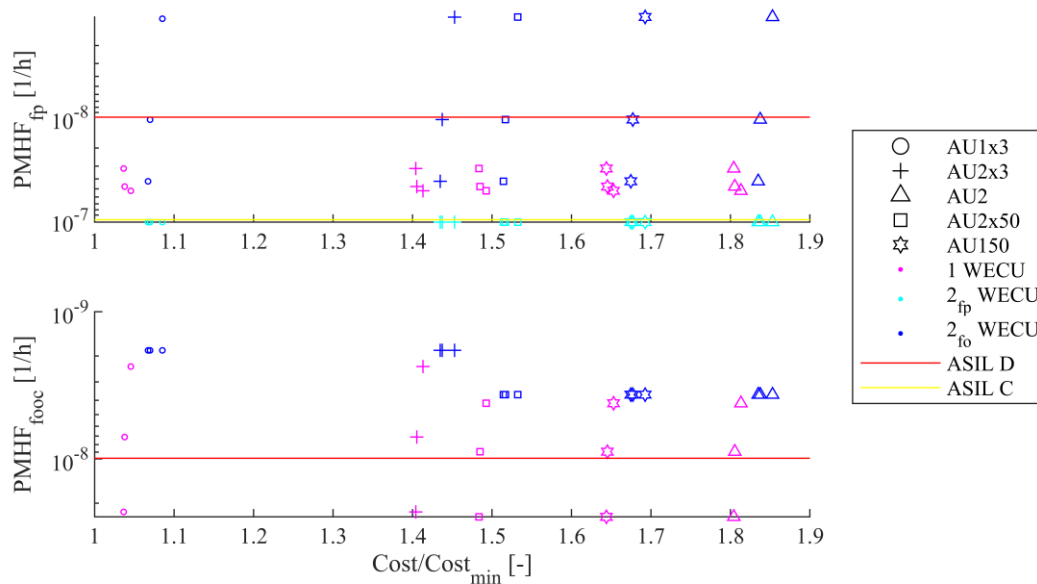


Figure 4.13: Safety assessment of a *semi-smart* actuator with PB backup

Backup Parking Brake System. Similar to the backup PB, the backup PB-system reflects the results of a fully redundant service brake. All concepts achieve an ASIL D SaRA as shown in Figure 4.14. However, it should be noted that the additional ECU actuating the PB may reflect an additional source of *fooc*-behavior. Nonetheless, since the PB generally applies relatively small forces with low dynamics the FE is considered non-critical.

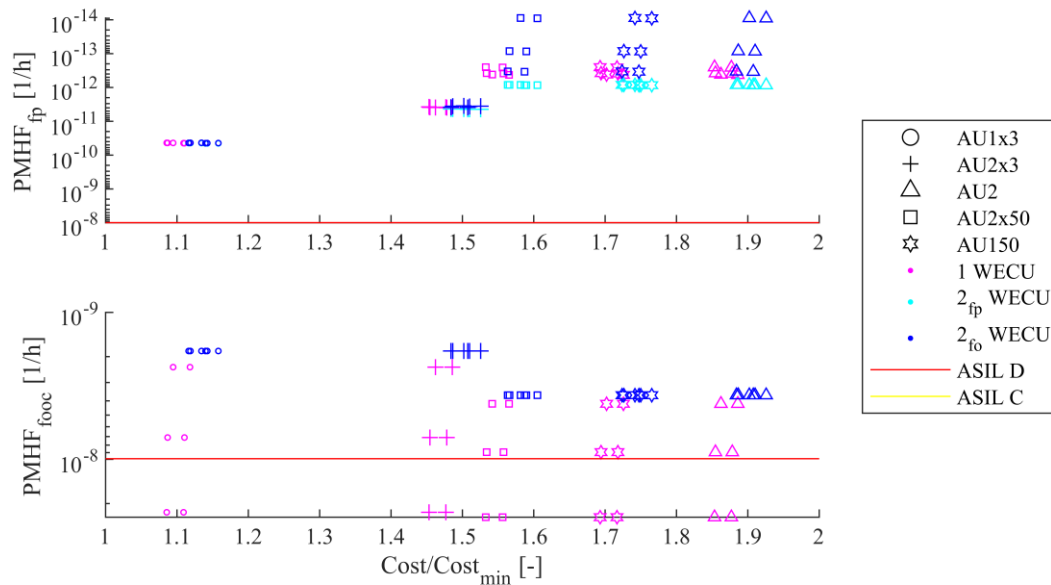


Figure 4.14: Safety assessment of a *semi-smart* actuator with PB system backup

Parking Brake as SM. Unlike the backup PB concepts, the PB as SM reduces the SaRA while improving integrity. The PB is implemented as an external SM. The impact is shown in Figure 4.15. Due to the additional external SM, all actuators achieve ASIL D integrity regardless of the SMs implemented within the ASIC.

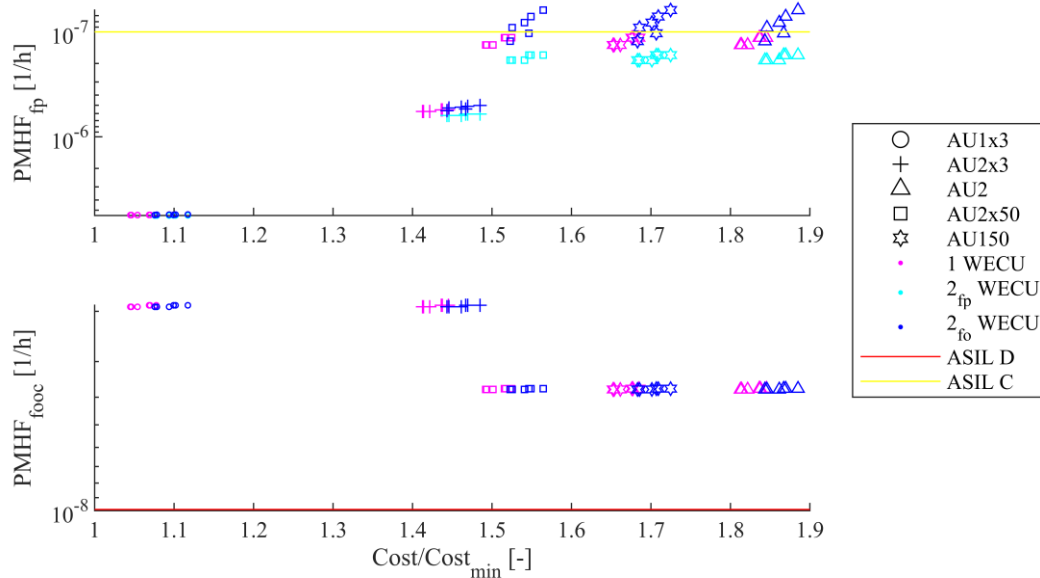


Figure 4.15: Safety assessment of a *semi-smart* actuator with PB as SM

Default Brake. The default brake safety concepts as shown in Figure 4.16 meet all a SaRA of ASIL D at a similar level as fully redundant service brakes. However, the cost is significantly reduced by the disadvantage of non-controllability after a failure. The integrity remains at the same level as the analyzed service brake.

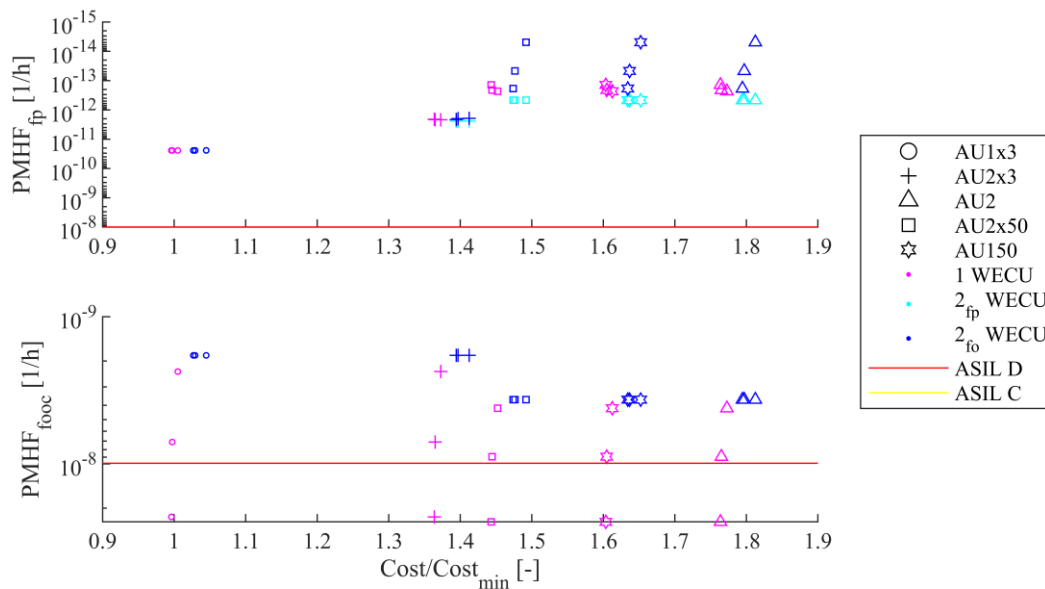


Figure 4.16: Safety assessment of a *semi-smart* actuator with a default backup

4.4.6 Smart Actuator

The safety concepts that can be implemented in a *smart* actuator are very similar to the safety concepts of the *semi-smart* actuators. However, since the *smart* actuator is more complex and consists of a microcontroller and its peripherals, SMs can be assigned on a component level. Nevertheless, the results of the *smart* actuator are similar to the results of the *semi-smart* actuator.

Service Brake. *Smart* actuators must meet the same SG as *semi-smart* and *simple* actuators. However, because *smart* actuators tend to be more complex than the other variants, more sophisticated safety concepts must be applied. This is illustrated in the integrity section of Figure 4.17. While *semi-smart* actuators require a $DC \geq 90\%$ to achieve ASIL D integrity, *smart* actuators require a $DC \geq 99\%$, which could be implemented as an additional lockstep-core in the CPU and an error-detection-correction code (ECC) in the RAM, for instance. Another option is to implement redundant WECUs.

Also, all analyzed *smart* actuators meet ASIL D with respect to SaRA due to the distribution over several wheels. Again, it can be seen that the SaRA can be increased by implementing redundancy, even up to ASIL D with respect to a single actuator. However, this ASIL D SaRA can only be achieved by a duplex WECU operated as *fail-operational* inheriting a $DC \geq 99\%$ or by triplex WECUs (green). It is clear that the increase in complexity and failure rate associated with the *smart* actuator makes ASIL D SaRA difficult to achieve for a single actuator.

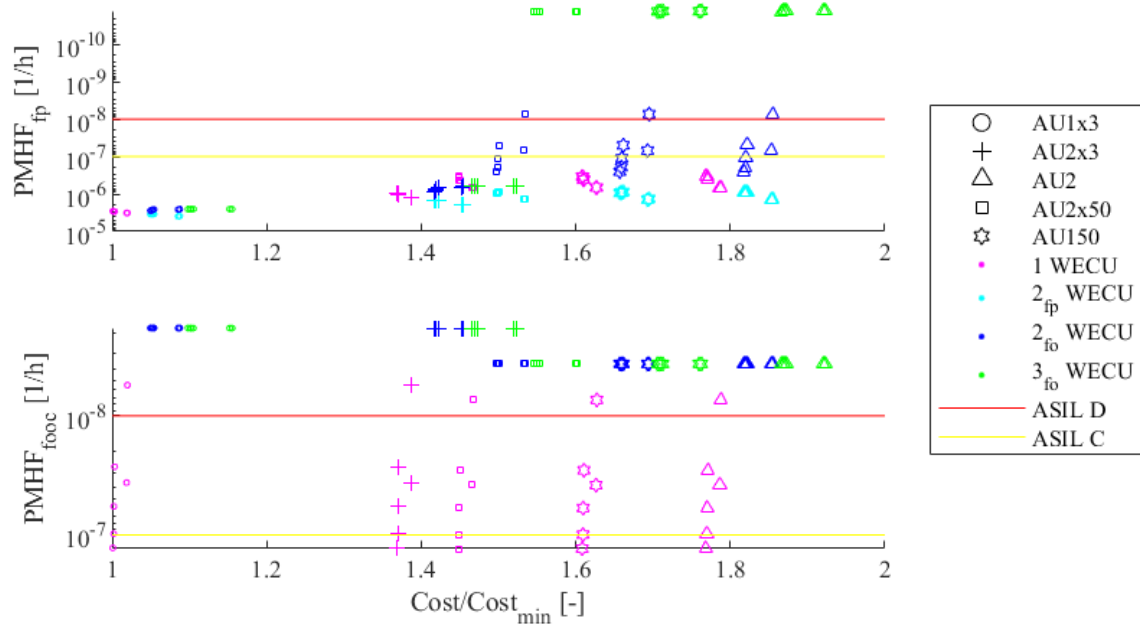


Figure 4.17: Safety assessment of a *smart* actuator

Backup Parking Brake. The backup PB must implement the same SMs or redundancy in the WECU to achieve the required integrity as the service brake itself. This is shown in the lower part of Figure 4.18. In addition, the SaRA of all service brakes is increased due to the additional AU implemented as a PB.

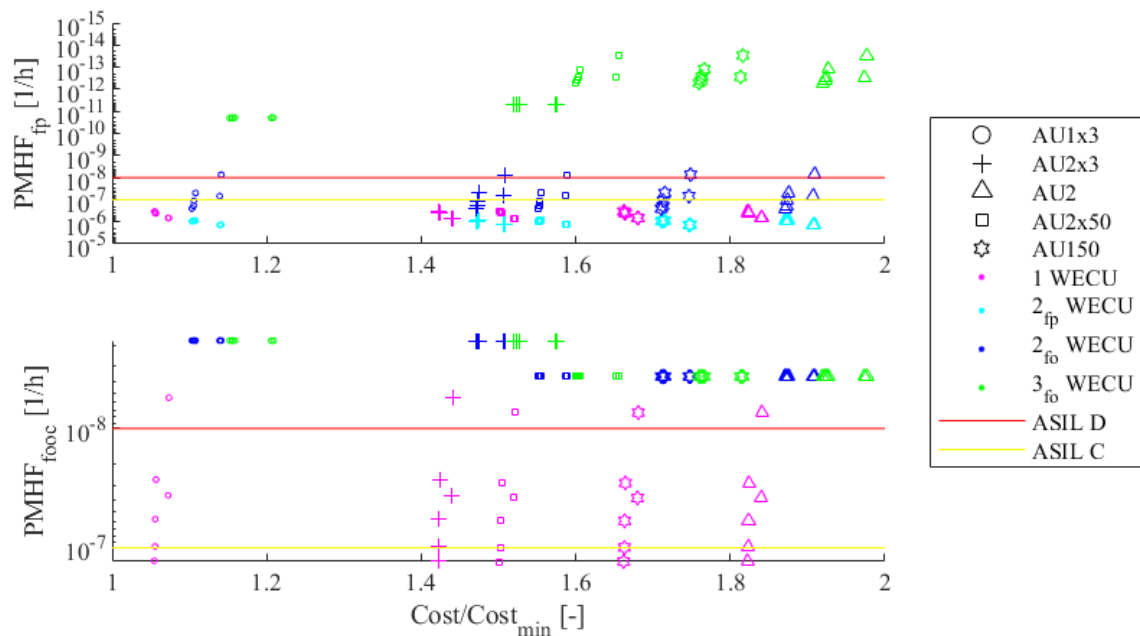


Figure 4.18: Safety assessment of a *smart* actuator with a backup PB

Backup Parking Brake System. The backup PB systems achieve similar integrity as the service brake and the backup PB. However, the SaRA is further increased because there is full redundancy implemented by the PB ASIC and the AU. All safety concepts meet ASIL D SaRA, as shown in Figure 4.19.

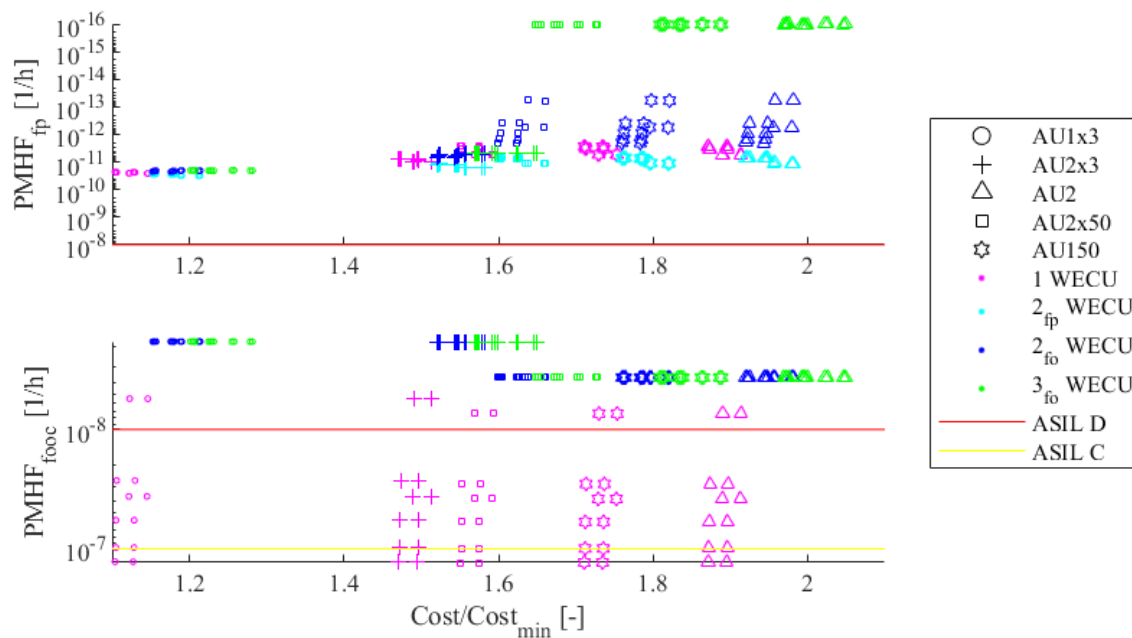


Figure 4.19: Safety assessment of a *smart* actuator with a backup PB system

Parking Brake as SM. The PB is a very valuable SM because no SM within the ECU is necessary to achieve the required integrity (see Figure 4.20). However, the SaRA is reduced to a level below ASIL C if redundancy is not implemented in both the ECU and the AU.

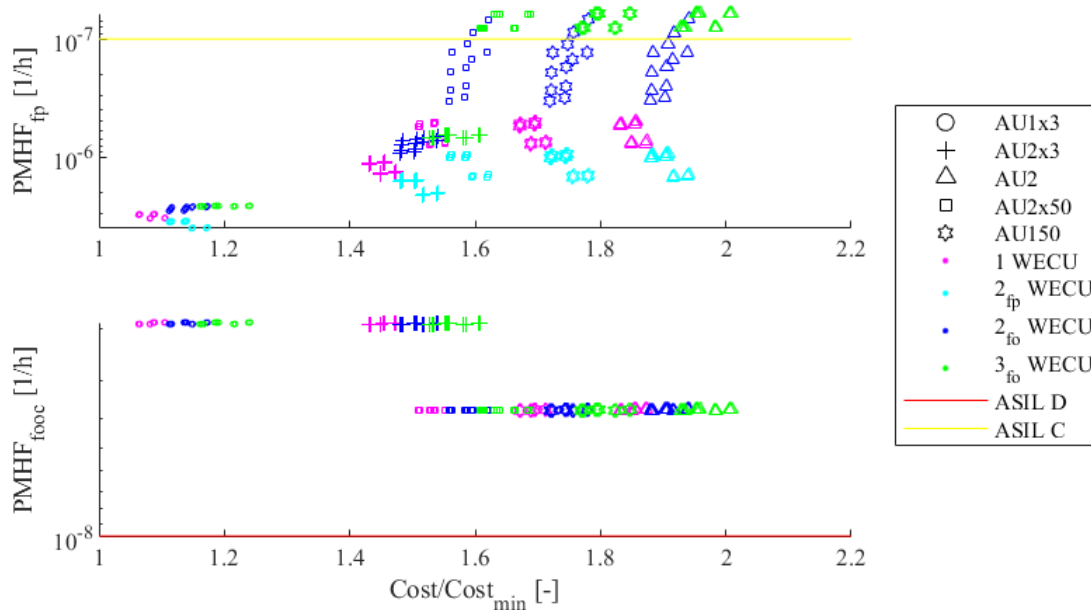


Figure 4.20: Safety assessment of a *smart* actuator with a PB as SM

Default Brake. The default brake needs the same SMs in the ECU as the service brake does. Nevertheless, the SaRA is increased at almost no additional cost. Figure 4.21 shows the safety in terms of integrity and SaRA.

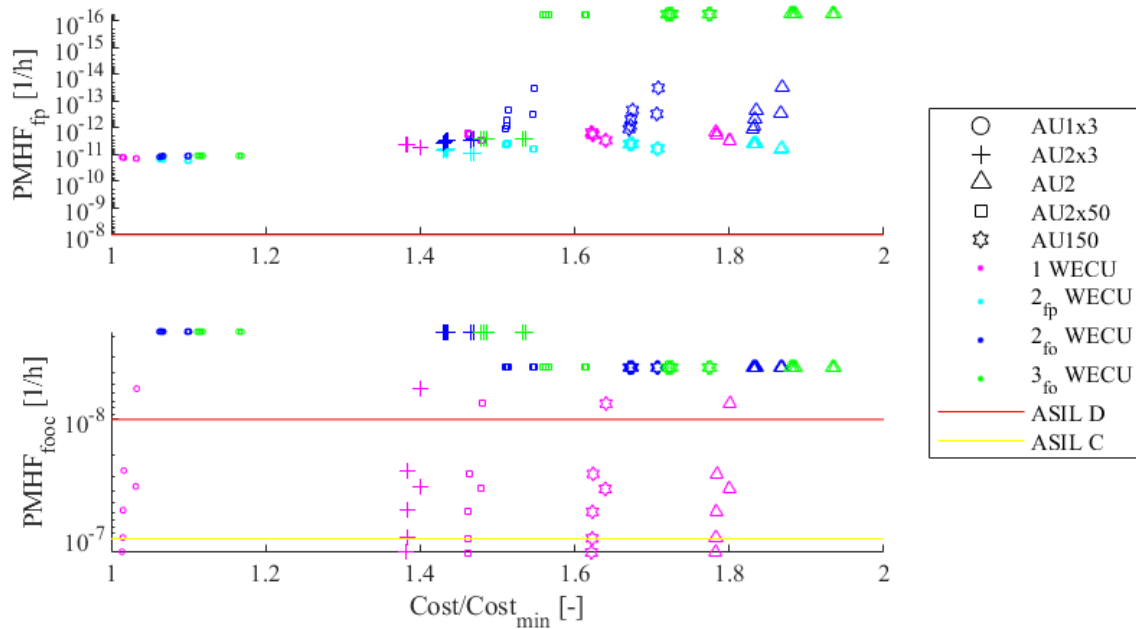


Figure 4.21: Safety assessment of a *smart* actuator with a default backup

4.4.7 Intermediate Conclusion

The previous sections show that EMB-actuators can meet ASIL D integrity SGs either by implementing the right SMs or by implementing redundancy. This is true for all complexity classes analyzed, although more enhanced SMs may be required for more complex ECUs. In addition, all analyzed actuators meet the required ASIL D SaRA SG, at least when considering two actuators mounted on the vehicle. The safety concepts can even be improved by considering the PB, either in terms of integrity or SaRA. Furthermore, it can be concluded that a complete redundancy (logic and AU) is necessary to significantly increase the SaRA on the single actuator level.

A comparison of the analyzed safety concepts in terms of cost is shown in Figure 4.22. It shows the cheapest architecture of each concept that meets the required SGs. Obviously, the more complex the actuator, the higher the cost. However, it should be noted that the lack of complexity in the actuator must be implemented in the CCS which increases the cost of that system. The comparison also shows that it is advantageous to implement a PB as an SM in a *smart* actuator instead of a *semi-smart* actuator. Since this PB eliminates the SMs within the logic; the more complex the logic, the more savings can be achieved. Therefore, the cost reduction potential is highest within the *smart* actuator.

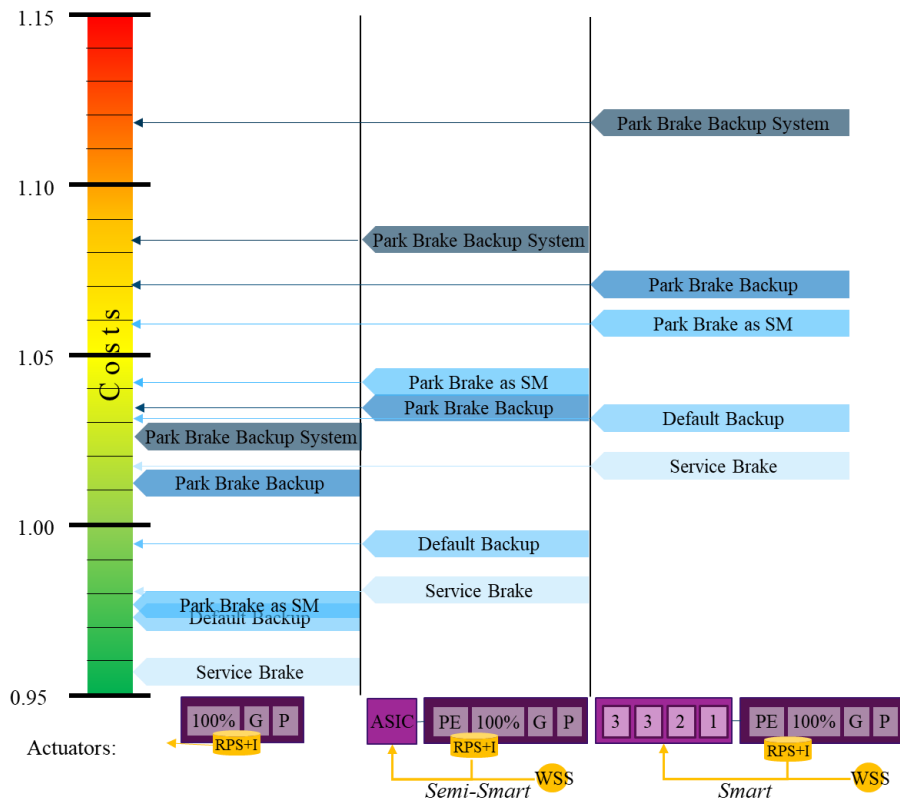


Figure 4.22: Comparison of the safety concepts¹⁸

¹⁸ Numbers in ECU represent SMs to achieve integrity of simplex WECU: CPU, RAM, ROM, number of clocks

4.5 Central Control System of the Brake System

The CCS distributes the braking command received from the pedal to the EMB actuators. It also implements higher control functions as ESP, depending on the function assignment also ABS on the brake command. However, the CCS must be aligned with the attached actuators described in section 4.4. Therefore, a distinction must be made between CCS connected to *simple* and *semi-smart/smart* actuators. This section is strongly oriented on the results, described in (Schrade, et al., unpublished yet).

4.5.1 System Definition

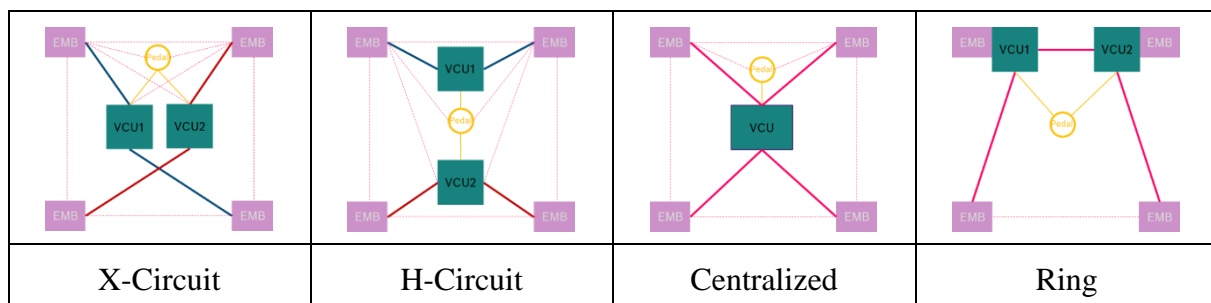
Design Space. The design space of the CCS consists of the variations within the VCU (Vehicle Control Unit) (number of lanes and VCUs, and SMs) and the COM-bus (number of buses and SMs). A detailed overview of the options is given in Annex B.2. The connections, as part of the analysis, between the VCU and the EMB-actuators at the wheel are based on the results presented in section 4.2.4, as shown in Table 4.7.

In addition, there is an option to connect EMB-actuators directly to the BBW pedal box or to exchange data between them via an explicit COM-bus. However, this option is only applicable if the actuators are implemented as *smart* or *semi-smart* actuators, as these actuators can receive digital signals, compare them, and then actively decide on a response. Though, different decision paradigms or operating modes can be applied within the WECUs of the *semi-smart* actuators if different signals are received from different sources:

1. Actuation of the command received from the brake pedal (if connected);
2. *Fail-passive* as obviously at least one *fooc*-failure developed; or
3. Actuation of the command received from the VCU

Since all buses are optional, despite the four connections between the VCU and the EMB-actuators, they are shown with dotted lines. However, the mandatory buses are shown in bold in Table 4.7.

Table 4.7: Design space options for the topology



Reduction of the Evaluation. Table 4.7 provides a variety of topologies. In addition, internal redundancies and SMs in the components, as well as the operating modes of the EMB-actuators, can be permuted. Finally, there are 1,400 different COM-bus routing options con-

sidering only an X-Circuit topology. Additionally, each X-Circuit-topology (of the 1,400) allows for 13,000 different combinations of SMs and internal redundancies. Finally, there is a design space of approx. 50 million different architectures considering only X-Circuit-topologies.

In order to assess the factors that most influence vehicle safety, a pre-evaluation is performed to reduce the design space. Therefore, the main effects of the different components are evaluated (as an example for a centralized topology), as shown in Figure 4.23. It provides the FEs as rows, starting with a complete *fp*- and continuing with axle-specific *fp*- behavior. It also shows the likelihood of a wheel developing *fooc*-behavior and the cost associated with implementing a particular component.

The impact of the different components is analyzed in the columns of Figure 4.23. These consider the implementation of optional backup COM-buses between pedal and front EMBs (F1-2), the axles (F3-4), SMs on the mandatory COM¹⁹ (F5-8), COM from front to rear actuators (F9-10), the architecture of the VCU²⁰ (F11-17), the operating mode of the brakes (F18-21), and the number of optional buses (F22). The background color of the subplots of Figure 4.23 is related to their influence. If the correlation is positive, the subplots are colorized in green, if the correlation is negative, the subplots are red. The intensity of the background color is related to the degree of correlation.

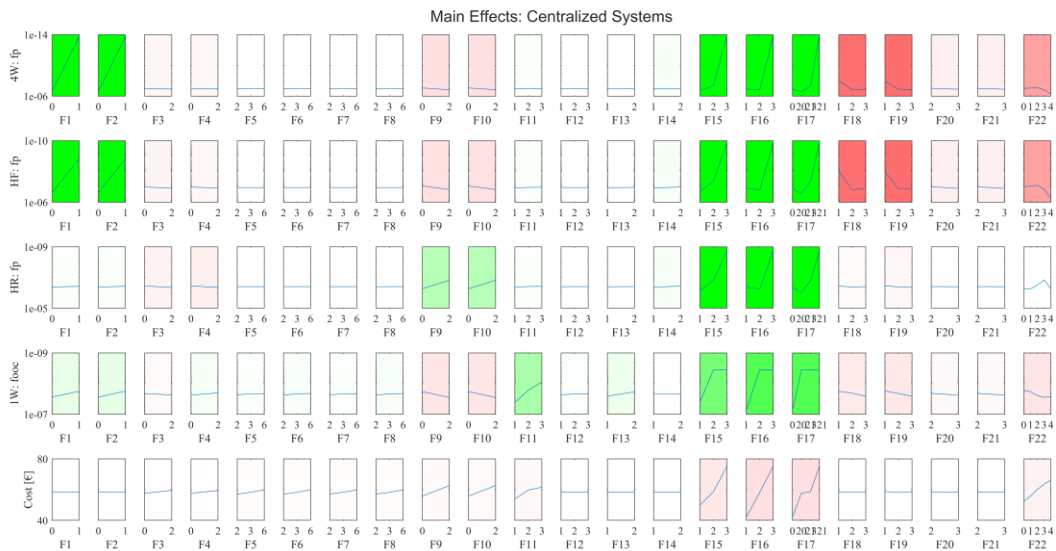


Figure 4.23: Impact of the design options onto the safety of centralized design

¹⁹ The design options considering the compulsory COM-buses consist of implementing SMs with a DC of 60% ($x=1$ in Figure 4.23), 90% ($x=2$) and 99% ($x=3$) and their redundant implementation ($x=4;5;6$)

²⁰ The design options of the VCU can be further specified into: SMs of CPU (F11), RAM (F12), Flash (F13), number of clocks (F14, 1 or 2), number of DC/DC-converters (F15, related to number of lanes), number of lanes (F16, 1-3), operating mode of the VCU (F17, simplex, duplex(fp), duplex(fo), triplex(fo))

The backup COM-busses between pedal and front EMBs (F1-2) have a positive impact on vehicle safety (both SaRA and integrity) at minimal cost, obviously. Furthermore, the implementation of internal redundancy within the VCU (F15-17) also improves safety. Finally, the implementation of SMs within the VCU (F11-13) increases the integrity of the CCS. Therefore, the following sections will focus on the impact of these components on the safety of the CCS.

The other factors have little or no effect on safety. Therefore, they are not analyzed further, but are set to default values. For example, the operating mode of the EMBs is set to passivate itself if it receives inconsistent data. The mandatory COM-busses are equipped with ASIL D integrity capable $DC=99\%$.

4.5.2 Related Safety Goals

The CCS must satisfy safety regarding the two dimensions: SaRA and integrity. In section 3.2, the impact of various braking system malfunctions is evaluated and it is concluded that a shutdown (*fp*) of a first axle or circuit can be classified as ASIL A. However, a complete passivation of the braking system is associated with ASIL D, as shown in section 3.1.5. In addition, the effect of *fooc*-behavior is evaluated. If the CCS commands an EMB-actuator (in NOP) with signals that have failed *fooc*, the intact actuator will actuate these *fooc* signals and eventually implement the *fooc*-behavior. Therefore, similar to the actuators, commanding a single wheel with *fooc* state signals must be avoided at ASIL D.

4.5.3 Failure Effects due to Sensor Failures

The FE due to sensor failures at the actuator level is already discussed in section 4.4.3. However, an analysis is required that also examines the impact of sensor failures on the functionality of the CCS. Therefore, the required and optional sensors of a vehicle related to the braking functionality are collected and the FEs are analyzed.

Necessary sensor information that is directly available (*simple* actuators) or available through a gateway (*semi-smart* and *smart* actuators) are the current-sensor, the RPS and the WSS, as these sensors are required to operate the EMB actuator. Since four EMB actuators are installed, the associated data is available four times. In addition, steering angle sensors and an inertial measurement unit (translational and angular accelerations (Robert Bosch GmbH, 2023)) are required to operate the ESP (Robert Bosch GmbH, 2023).

As described in the previous paragraph and in section 4.4.3, there is a large number of sensors that are highly correlated. Therefore, *fooc* sensor data should be easily diagnosable, which ultimately leads to the conclusion that a *fooc* behavior of the CCS due to a sensor failure is improbable. Furthermore, due to the high number of sensors and their strong correlation, *fp*

sensor failures (at least up to a degree of two) should be tolerable by the CCS. This failure tolerance could be implemented by a physical model. Finally, CCS failures due to sensor failures are not investigated further.

4.5.4 Brake Topologies with Simple Actuators

X-Circuit. The f_0 -capability of X-Circuit designs is strongly supported by the two VCUs installed (see Table 4.7). Therefore, the ASIL D SaRA does not pose a significant challenge, as indicated in the upper part of Figure 4.24. It shows that all the designs analyzed meet the ASIL D hardware metrics.

In contrast, the hardware metrics related to ASIL D integrity pose a challenge. As shown in the lower part of Figure 4.24, X-Circuit designs with only simplex VCUs do not meet ASIL D integrity, even if the best SMs with the highest DCs are installed. Therefore, at least one duplex VCU (cyan and blue data points) is required, while the simplex VCU must implement a high DC.

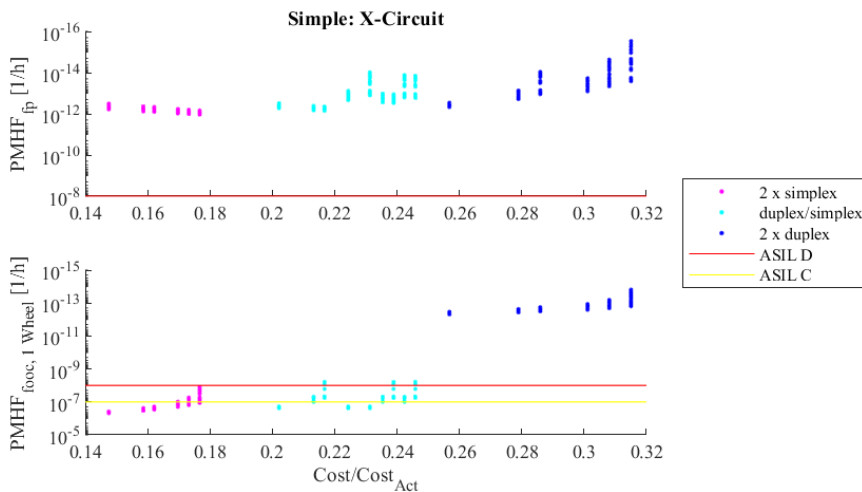


Figure 4.24: Safety assessment of a X-Circuit equipped with simple actuators

Finally, it should be noted that there are several different architectures for each design option (see Figure 4.24). These architectures differ in terms of their implemented SMs, which improve safety but are also associated with certain costs.

H-Circuit. H-Circuits implement two circuits, as do X-Circuits. Therefore, the hardware metrics for ASIL D SaRA are easily achieved. Similar to X-Circuits, at least one redundant VCU must be implemented to achieve ASIL D integrity. However, unlike X-Circuits, the allocation of the redundant VCU within H-Circuits can make a difference. It can be suggested that the redundant VCU (which may provide a higher SaRA) be assigned to the front axle, since the front axle contributes more to the deceleration capability than the rear axle (see Table 3.7).

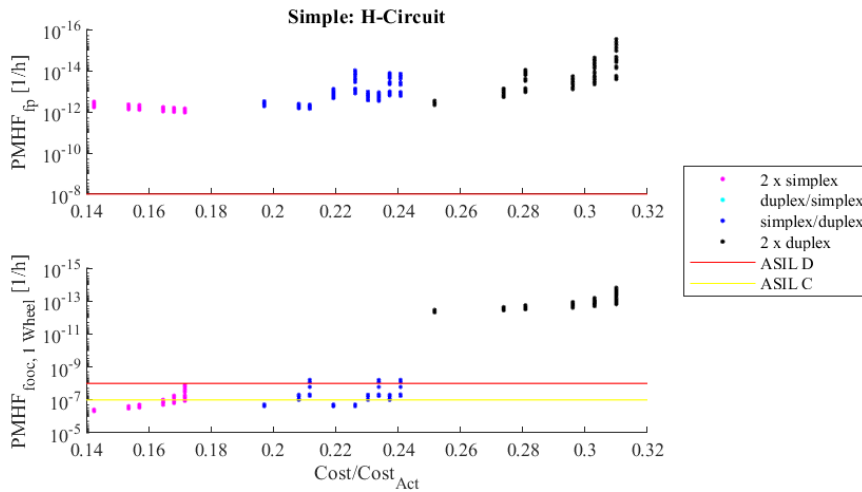


Figure 4.25: Safety assessment of an H-Circuit equipped with *simple* actuators

Centralized. While SaRA does not pose a significant challenge to circuit-designs, as described in the previous paragraphs, centralized designs do not always meet the hardware metrics related to ASIL D. This is shown in the upper section of Figure 4.26. It also shows that at least three lanes are required to achieve ASIL D SaRA.

However, the ASIL D integrity hardware metrics can be met by a single lane (with high DCs) or by any of the redundancy concepts examined. The lower part of Figure 4.26 also shows the consequences of the implemented operating mode of the VCU. While the duplex VCUs operating as *fo* (marked in blue) realize an improved availability, almost reaching ASIL D, the *fp* VCUs clearly miss the ASIL D SaRA, but increase the integrity. The cost difference between the *fp* and *fo* duplex VCUs can be explained by a redundant energy input module that is integrated in *fo* VCUs to be truly *fo*.

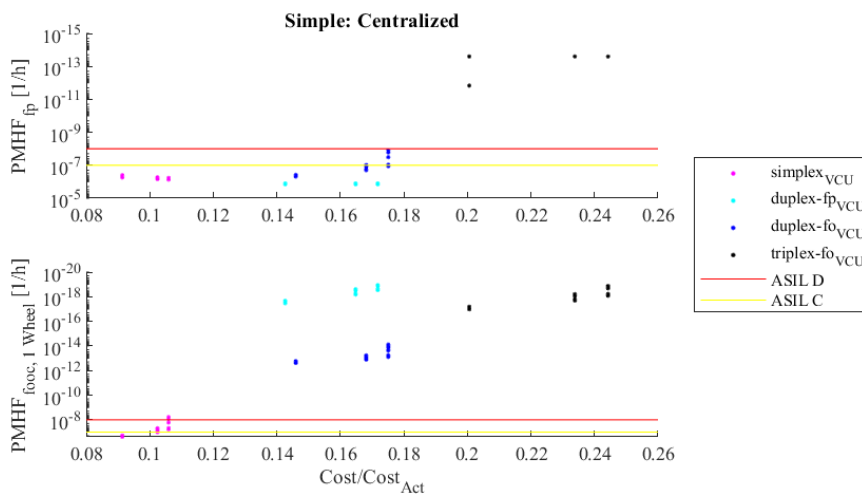
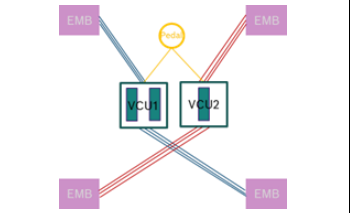
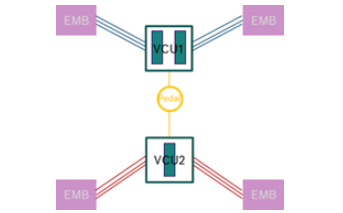
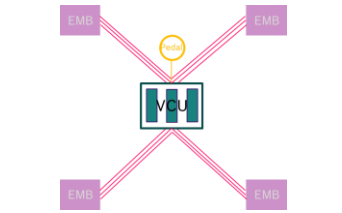


Figure 4.26: Safety assessment of a centralized topology equipped with *simple* actuators²¹

²¹ The PMHF is limited to 10^{-20} 1/h, as a maximum value, in the analysis

Intermediate Conclusion. The CCS requires three lanes to provide the required safety in terms of both ASIL D SaRA and integrity. However, the lanes may be allocated to a single VCU (see centralized design) or to two VCUs (see H- and X-Circuit). While integrity is inherently ensured by the lanes within the centralized design, dedicated SMs must be implemented within the simplex VCU within the circuit designs to ensure integrity. Table 4.8 shows the designs that meet the required ASIL D hardware metrics at minimal cost. Here, the green rectangles represent the lanes, while the lines represent the wires.

Table 4.8: ‘Best’ design options for CCS connected to *simple* actuators

Name	X-Circuit	H-Circuit	Centralized
Costs	0.217	0.212	0.201
Architecture			

4.5.5 Brake Topologies with smart and semi-smart Actuators

X-Circuit. The two-circuit design of the X-Circuit enables ASIL D SaRA due to the topology, itself, as already described for *simple* actuators. However, at least one duplex VCU and one simplex VCU with high DCs are required to meet the hardware metrics related to ASIL D integrity, similar to the *simple* actuators, as well.

Furthermore, the advantage of implementing a backup bus between the front EMB actuators and the brake pedal (S_{BRK}) could be exploited. Such designs further improve SaRA, as shown in Figure 4.27. However, since SaRA is generally not important for two-circuit designs, such implementations are not preferred especially in terms of cost. A safe design at a minimum of cost is presented in Table 4.9.

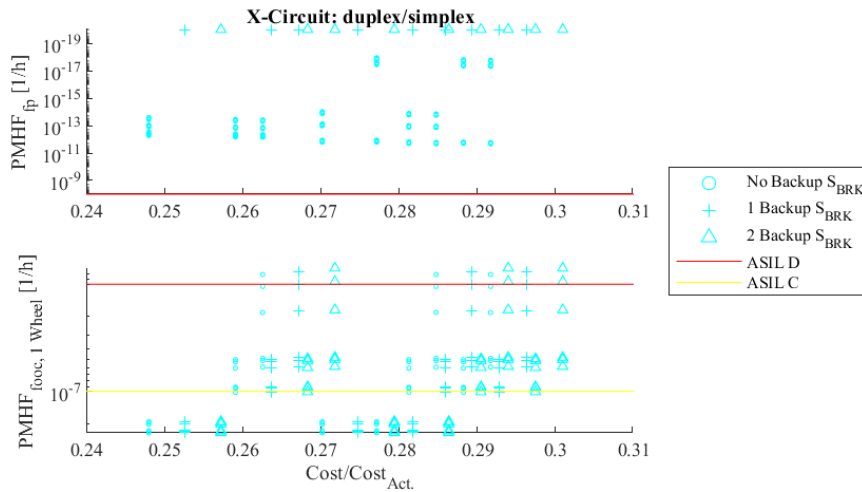


Figure 4.27: Safety assessment of *smart* and *semi-smart* X-Circuit topologies²²

A special X-Circuit design, outside the scope of the analysis described in section 4.5.1, consists of implementing at least one backup bus between the front EMB-actuator and the brake pedal with an additional COM-bus between the two rear EMB-actuators. Such a design allows for two simplex VCUs, because any *foc*-failure of a COM-bus or a VCU could be detected by providing a second source (rear axle bus or backup bus to the brake pedal) being provided to the *semi-/smart* actuator. The SaRA is put in place by the two circuits.

H-Circuit. The H-Circuit is able to take advantage of a backup connection between the front EMB-actuators and the brake pedal. Since the *semi-/smart* actuators are able to compare messages from the different sources (e.g., VCU and brake pedal), *foc*-failures of one of the components can be reliably detected. Therefore, since any *foc*-failure of the front VCU can be detected, no SMs need to be implemented. If such a VCU is combined with a simplex VCU with high DCs on the rear axle, ASIL D integrity can be provided. On the other hand, SaRA is implemented by the two-circuit design as already described in the previous sections.

²² Analyses are conducted investigating simplex/simplex, simplex/duplex and duplex/duplex VCU-configurations. However, as the space of the article is limited, only the results of the configurations with the minimum amount of lanes in the VCUs is displayed within this chapter.

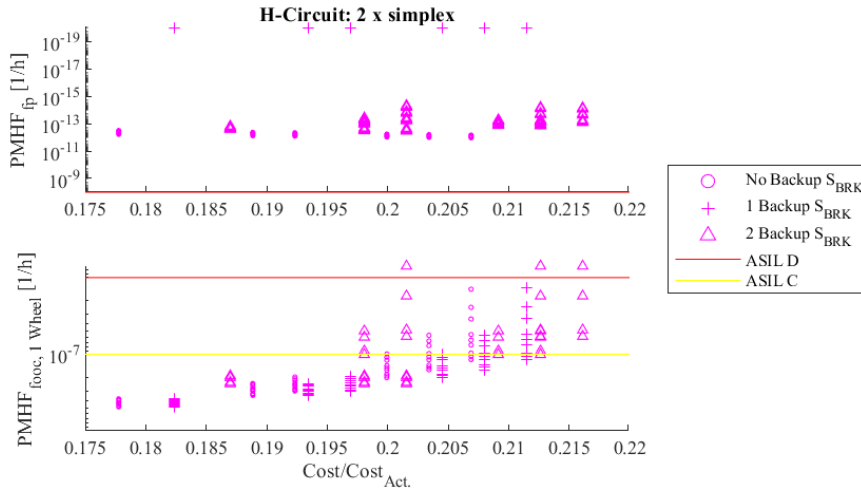


Figure 4.28: Safety assessment of smart and *semi-smart* H-Circuit topologies

Centralized. The centralized designs generally suffer from a low SaRA (see *simple* CCS designs). However, this challenge can be overcome by the implementation of a backup bus between the front EMB-actuators and the brake pedal (see Figure 4.29). Finally, a simplex VCU with high DCs combined with a single backup bus can meet the hardware metrics for both ASIL D SaRA and integrity.

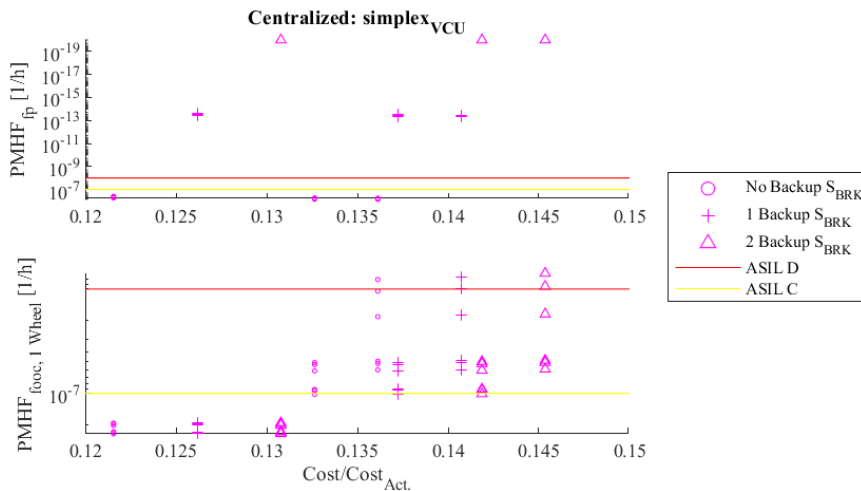


Figure 4.29: Safety assessment of *smart* and *semi-smart* centralized topologies

Ring. Unlike the topologies presented in the previous sections, all EMB-actuators, installed in a ring-topology, receive data from both VCUs and the brake pedal backup connections, if implemented. Since all actuators are able to compare the VCU messages, an inherently safe system in terms of integrity is established (see the lower part of Figure 4.30).

However, if no backup bus to the brake pedal is installed, every single *fooc*-failure of a VCU creates a stalemate situation within the *semi-/smart* EMB-actuator resulting in a low SaRA. Therefore, at least one duplex VCU is required to reduce the potential for VCU *fooc*-failures, while the second VCU must implement a high DC, or at least one backup bus to the pedal is

required to provide a third source of information for the actuators to provide the potential to vote for the correct command. Finally, ring-topology-designs that meet the hardware metrics for ASIL D SaRA are possible.

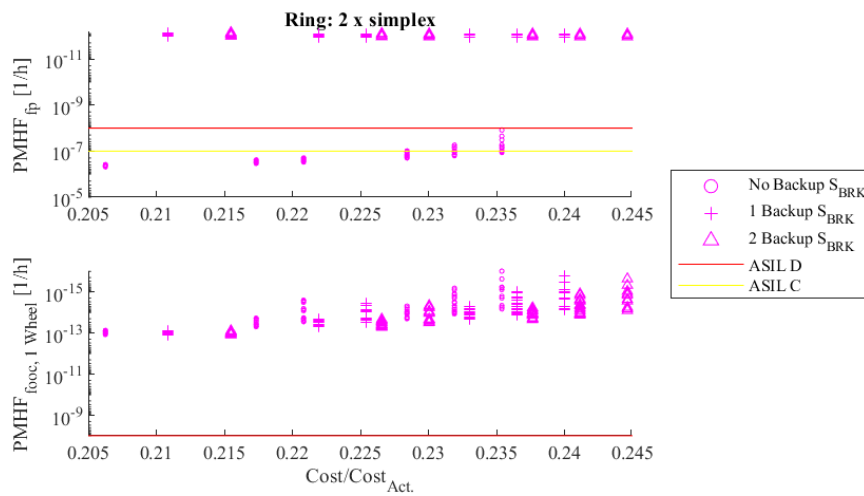


Figure 4.30: Safety assessment of *smart* and *semi-smart* ring-topologies

Conclusion. The analyses performed show that at least three lanes must be implemented to achieve ASIL D SaRA- and integrity-capable CCS, comparable to the designs presented for *simple* CCS. However, the implementation as *semi-/smart* EMB-actuators allows the installation of a backup bus connecting the brake pedal and the front EMB-actuators. Such a backup bus has been shown to be an effective means of increasing the safety of future CCS, as discussed in section 4.5.1. However, the purpose of the backup bus depends on the topology. While ring- and centralized-topologies benefit from an increase in SaRA, the H-Circuits increase integrity with respect to the front EMB-actuators. Ultimately, X-Circuit designs cannot be significantly improved by implementing such a backup bus. Designs that meet the required hardware metrics at a minimal cost are presented in Table 4.9.

Table 4.9: ‘Best’ design options for CCS connected to *semi-smart* and *smart* actuators

Name	X-Circuit	H-Circuit	Centralized	Ring
Costs	0.263	0.202	0.141	0.211
Architecture				

4.5.6 Intermediate Conclusion

Different topologies of CCS consisting of centralized-, ring-, X- and H-Circuit- designs are investigated. These can be connected to either *simple* or *semi-/smart* EMB-actuators. In general, safety (in terms of ASIL D SaRA and integrity) can be ensured by implementing three lanes in the VCU(s). These lanes can be split between two VCUs, resulting in one VCU inheriting two lanes and a second VCU inheriting only one lane. In such a case, a high DC within the simplex VCU is required to ensure that *foc*-failures are sufficiently infrequent.

In addition, the investigation shows that backup COM-busses between the front EMB-actuators and the brake pedal can also improve the safety of CCS. However, this option only exists for CCS connected to *semi-/smart* EMB-actuators as these are capable of comparing multiple signals to detect failures. Finally, it is shown that the number of lanes can be reduced to one lane for centralized and two lanes for H-Circuit- and ring-topologies. By implementing such backup buses, the generally more expensive *semi-/smart* topologies can be achieved at lower cost than *simple* CCS-designs.

4.6 Excuse: Energy-Supply

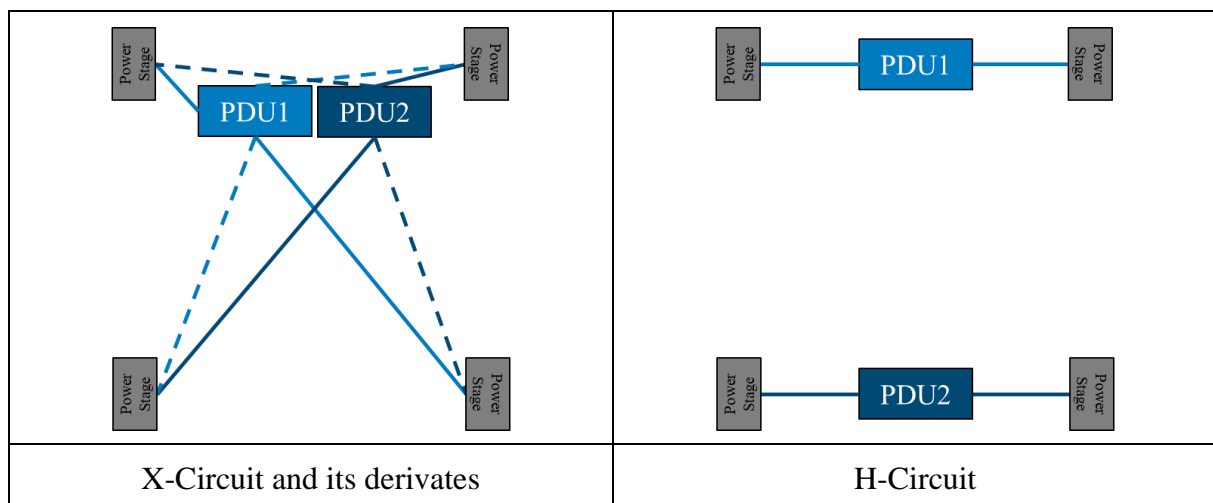
The fourth system required to implement the braking functionality, as defined in section 4.1, is the energy-supply. However, the energy-supply is a system that is shared by several items, as it is also required to implement, for example, electrical power to steering, powertrain (PT) and display functionalities. In addition, its implementation is highly dependent on the function assignment, as defined in Table 4.1. *Simple* actuators, for example, do not require a local energy supply, as the energy is supplied by the already commutated three-phase current provided by the CCS. Therefore, this section only provides a very brief overview of possible design options related to *semi-smart* and *smart* actuators, derived from section 4.2.3. Additionally, the energy-supply of the pedal box is not specifically considered, as it is supplied locally by the VCU (as described in section 4.3.1).

4.6.1 System Definition and Safety Goals

The energy supply system must comply with ASIL D SaRA, as must the entire EMB-system item. Therefore, redundancy is generally implemented in the form of a two-circuit design, as described in section 4.2.3. However, blended designs with some redundancy at the wheel are also possible.

Table 4.10 provides an overview of the design space under analysis, showing the two energy supplies (in the form of a PDU) in different shades of blue. The power stages of the EMB-actuators are shown in grey. These can be simple DCDC-converters for the local ECU or ASIC, or an ideal diode²³ if the specific wheel is redundantly supplied by two circuits. This redundancy is also displayed in the X-Circuit topology as a dotted line.

Table 4.10: Energy-supply topologies



²³ The ideal diode is capable of switching the energy supply from a failed one to one in normal operation while guaranteeing the independence of the two energy grids

4.6.2 Results

The SaRA of the energy supply system needs to meet ASIL D. Its complete failure (due to a single- or dual-point failure) is related to the failure rate $\lambda_{fp,global} = 6.3 \times 10^{-13} 1/h$. This probability remains constant over all analyzed topologies because it can only be caused by the failure of both PDUs. Therefore, ASIL D SaRA is easily met by the energy supply system when implemented as a two-circuit design.

In addition to the complete failure, a partial power failure is also analyzed. Both local (at a specific wheel) and circuit-specific²⁴ failures are considered. Figure 4.31 shows the impact of redundancy options on these failure modes.

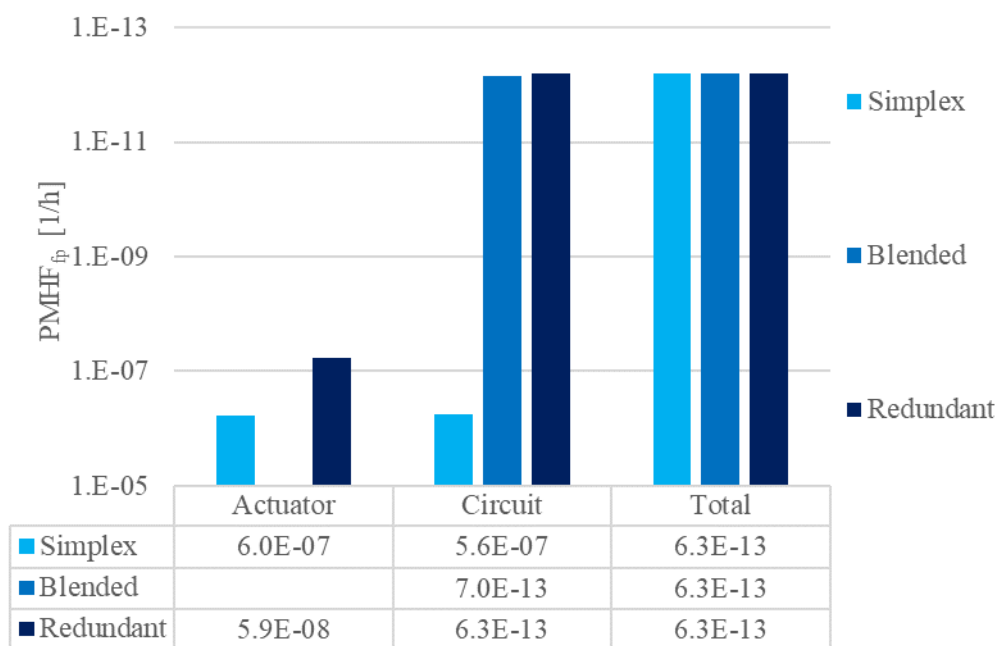


Figure 4.31: Overview of the PMHF related to the energy-supply

Figure 4.31 indicates that a redundant energy supply improves the availability of a single actuator by one order of magnitude. The availability achieved by the redundant supply is directly related to the assumed failure rate of the ideal diode ($\lambda_{fp} = 5.9 \times 10^{-8} 1/h$). The ideal diode limits availability because it is the only single-point failure. Redundancy, even partial redundancy (blended), greatly increases the availability of circuits by far. However, it should be noted, that a redundant energy-supply is not required from a functional safety point of view, as a simple failure rate budgeting approach suggests target failure rates of $\lambda_{fp,wheel} = 10^{-2} 1/h$ for a single wheel and $\lambda_{fp,circuit} = 10^{-4} 1/h$ for a circuit.

²⁴ The PMHF is independent of a circuit being implemented as H- or X-Circuit

4.7 Composition of the EMB-System

The previous chapters present safety concepts related to the individual systems of the item EMB-system. However, these systems have to be synchronized in order to meet the elaborated requirements in an ensemble, consisting of:

- Legislation (section 2.3)
- Functional Safety (section 3.2)
- Product Liability (Annex A).

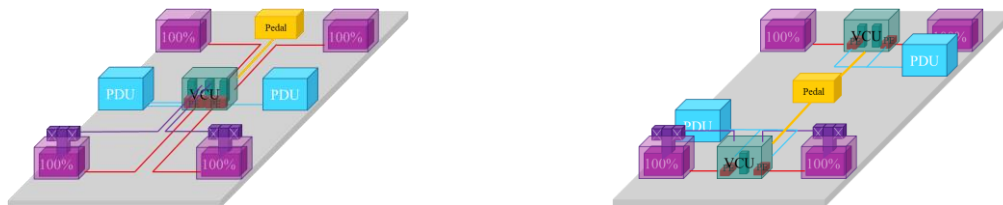
The most promising, harmonized concepts are presented below. A distinction is made between concepts that meet only the functional safety requirements of legislation and systems that also comply with the product liability regime.

4.7.1 Simple Actuators

Functional Safety. The use of any redundancy at the actuator-level (similar or dissimilar in the form of a PB) can be dispensed with, as the required SaRA is met distributing four actuators to the wheels. Therefore, the cheapest option to implement a parking functionality (latch-mechanism) can be chosen.

However, there are different options for the CCS. Either a centralized approach (Figure 4.32a) or an H-Circuit approach (Figure 4.32b) can be used. The advantage of the centralized approach is that it is highly failure-tolerant, since it can tolerate any failure of the first lane in the VCU. However, there is a potential for common cause failures as all lanes are installed within a single VCU.

The H-Circuit solves this problem by assigning three lanes to two different VCUs. Nonetheless, the disadvantage is that any first failure of the lane in the rear VCU will cause the entire axle to shut down. Similarly, the H-Circuit could be implemented as an X-Circuit, which provides the same level of safety at a slightly higher cost due to increased cable lengths.



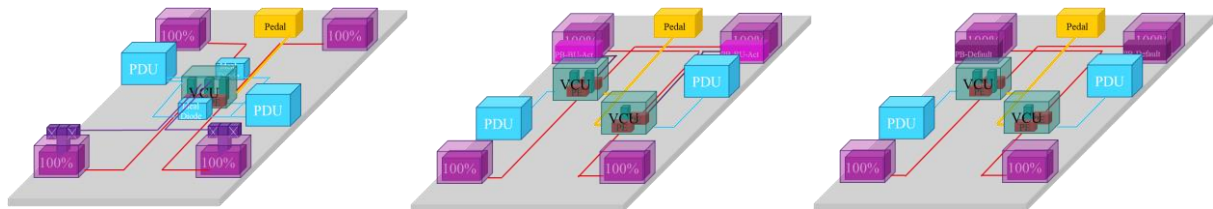
a) Centralized system with park latch mechanism
b) H-Circuit with park latch mechanism

Figure 4.32: Composition of *simple* actuator systems achieving functional safety

Product Liability. In contrast to the functional safety approach, the concepts presented here need to establish a failure tolerance, since any first failure can only cause one actuator to fail. This can be achieved either by implementing an ideal diode (see section 4.6.1) for the VCU of

the centralized approach (Figure 4.33a) or by implementing redundancy at the actuator level (Figure 4.33b and c). However, the centralized approach inherits the risk of common cause failures, especially for the ideal diodes, which can both shut down the entire energy-supply and/or the entire VCU.

The X-Circuit approaches (Figure 4.33b and c) resolve the common cause potential by separating the lanes into two VCUs with independent energy supplies. On the other hand, the H-Circuit approach (of the functional safety concept) evolves into an X-Circuit as this design addresses both axles by each circuit, reducing the deceleration requirement of the backup parking actuators (see section 3.2.2). This backup at the actuator level can be used as a backup actuator or as a default actuator to save costs. However, the backup PB actuator of the front axle must be controlled by the VCU that controls the service brake actuator of the other side in order to guarantee the required backup capabilities.



a) Centralized system with park-latch

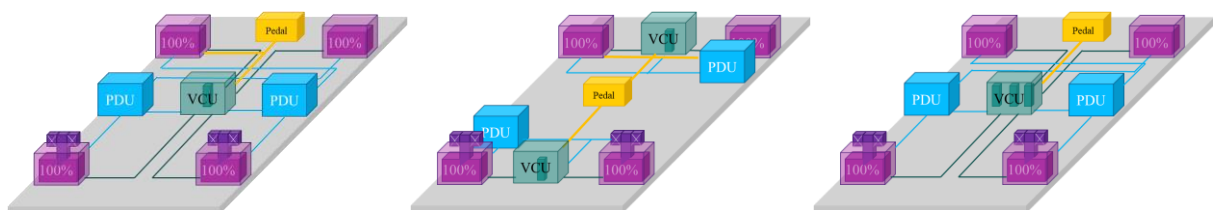
b) X-Circuit with backup PB actuator

c) X-Circuit with default actuator

Figure 4.33: Composition of *simple* actuator systems avoiding product liability

4.7.2 Semi-Smart and Smart Actuators

Functional Safety. The *semi-smart* and *smart* actuators like the *simple* actuators, use only latch mechanisms to implement the PB functionality to save costs. However, these smarter actuators can exploit their potential to receive information from the brake pedal in addition to the information from the VCU. This ultimately leads to a reduction in the number of lanes within the VCU, if implemented (see Figure 4.34a and b), while still meeting SaRA requirements. If this backup connection to the brake pedal is removed (refer to Figure 4.34c), a design similar to the one implemented within the *simple* actuator designs is obtained.



a) Centralized system with park-latch

b) H-Circuit with park-latch

c) Centralized system with park latch

Figure 4.34: Composition of *semi-smart* or *smart* actuator systems achieving functional safety

Product Liability. The challenge of providing a three-wheel backup in the event of any first E/E failure can be addressed by a variety of solutions in the case of *semi-smart* and *smart* actuator systems. However, the implementation of backup buses between pedal and front actuators (as shown in the functional safety section) is not a solution as it only provides an up to two-wheel backup. This limitation is due to the restricted design space analyzed. However, architectures with three backup buses between the actuators and the pedal could provide the required safety.

Figure 4.35a shows a centralized system that supplies each lane (out of three) of the VCU with one energy-supply. Furthermore, the EMB-actuators on the front axle are supplied redundantly (with an ideal diode) to overcome a first failure in the energy supply while the rear actuators receive only a single supply.

In addition to the centralized approaches, X-Circuits can also avoid product liability. Figure 4.35b shows a solution with a backup PB system, while Figure 4.35c shows the same system implementing redundancy by using default actuators on the front axle. However, the backup PB must be commanded by the VCU that controls the service brake of the ‘other’ side to provide three-wheel backup in the event of a first E/E failure.

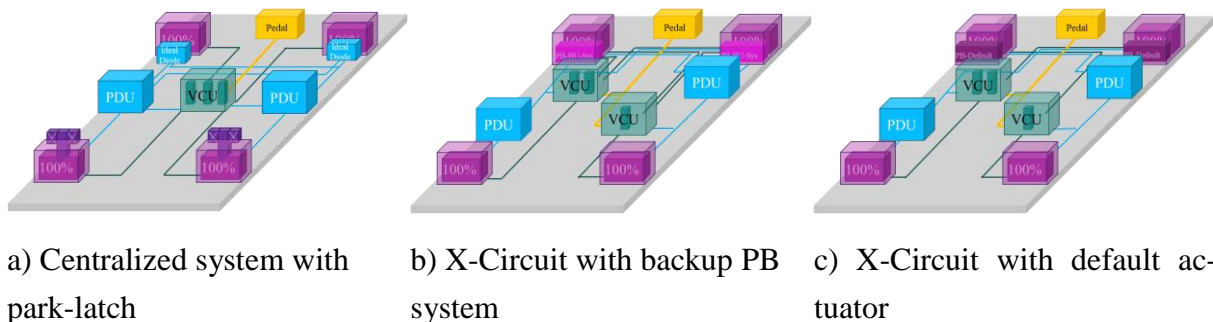


Figure 4.35: Composition of *semi-smart* and *smart* actuator systems avoiding product liability

4.7.3 Comparison of the Concepts

The concepts presented show that SaRA does not pose a significant challenge for future EMB-systems from a functional safety point of view if a certain degree of redundancy is implemented. However, the avoidance of product liability may require more sophisticated concepts, as a three-wheel backup may be required. This implies the use of redundant energy supplies, at least on the front axle, which can be implemented using ideal diodes or redundant EMB-actuators. These redundant actuators can be implemented by using similar redundancy or dissimilar concepts (e.g. a PB system). Integrity, as the second dimension of the analysis, is satisfied at the component level of the systems.

5 Safety Concepts for Joint Braking and Powertrain Systems

Electric vehicles are equipped with electric powertrains (PT) (as defined in sections 5.1 and 5.2) that are able to recuperate and eventually decelerate. Therefore, PT can support the braking system in its deceleration function and can have a positive impact on vehicle safety (as shown in section 3.3). Safety concepts are hence developed to exploit this effect. These concepts consider pedal boxes (section 5.3) and the PT, as a single-domain architecture (section 5.4) and an X-Domain architecture (section 5.5). The design space is limited here to consider only PTs that drive an entire axle with no internal redundancies, such as a 2x3 phase eDrive.

5.1 Definition of the ,Item‘

Conventional requirements for the item *powertrain* are to “*provide the demanded acceleration or propulsion torque*”. However, in the context of this chapter, since the *powertrain* may also provide a deceleration, the scope of the item is extended to “*provide any required torque (within its capabilities)*”, emphasizing that a torque may also be negative and cause a deceleration.

The safety goals (SG) related to the conventional item *powertrain* are mainly related to ensuring integrity (see section 5.2.1). However, as the scope of the item is increased, the elaborated SG to provide a certain deceleration, as defined in section 3.3 may also be considered, in addition.

Figure 5.1 shows the systems of the item *powertrain*, based on the definition of the EMB-system in section 4.1. It is important to note that the item *powertrain*, which provides the functionality also inherits the system powertrain (PT). However, to avoid misunderstandings, the system powertrain (PT) will be referred to by its abbreviation.

In addition to the PT, the (drive) pedal box, low-voltage- (LV) and high-voltage-energy-supply (HV) are also required to implement the functionality of the item *powertrain*. A thermal system is needed to cool the electrical components. However, the thermal system is as-

sumed to be out of scope because a temporary operation of the powertrain is possible even if the thermal system fails.

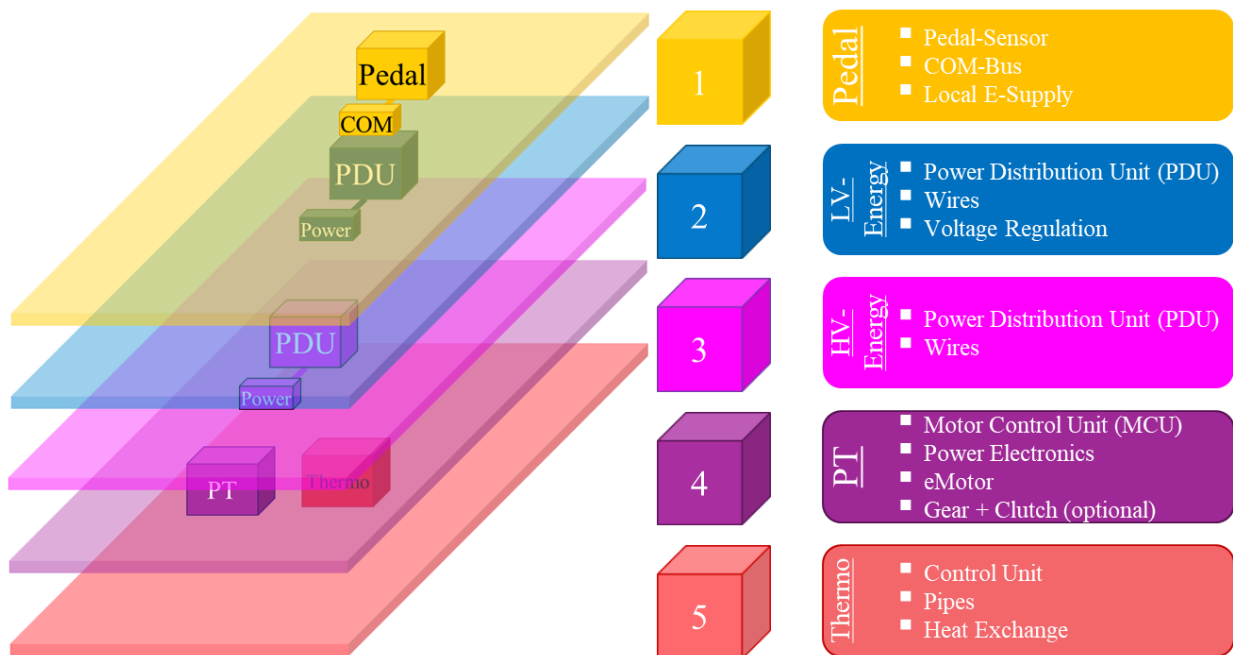


Figure 5.1: Definition of the item powertrain

5.2 Related Work

This section is the basis for the following sections. It presents the SGs related to the item *powertrain* (section 5.2.1). In addition, the definition of a state-of-the-art PT system is given (section 5.2.2).

5.2.1 Safety Goals related to the Item Powertrain

The SGs related to the item *powertrain* focus on integrity. In general, the absence of propulsion functionality is considered as safe operating condition, while the application of undesired torques is considered more critical. The E-Gas monitoring concept (Audi AG, BMW AG, Daimler AG, Porsche AG, VW AG, 2013)²⁵ and the publications (Ross, 2016)²⁵, (Christiaens, et al., 2012), (Messnarz, et al., 2019) establish the following SGs:

1. Avoid unintended acceleration with ASIL B (Audi AG, BMW AG, Daimler AG, Porsche AG, VW AG, 2013), (Ross, 2016), (Christiaens, et al., 2012), or ASIL D (Messnarz, et al., 2019)
2. Avoid missing acceleration with QM (Audi AG, BMW AG, Daimler AG, Porsche AG, VW AG, 2013)
3. Avoid missing deceleration with QM (Audi AG, BMW AG, Daimler AG, Porsche AG, VW AG, 2013)
4. Avoid unintended deceleration with QM (Audi AG, BMW AG, Daimler AG, Porsche AG, VW AG, 2013), ASIL A (Ross, 2016) or ASIL B (Christiaens, et al., 2012)
5. Avoid blocking of the axle (especially rear) with ASIL C (Ross, 2016), (Christiaens, et al., 2012) or ASIL D (Messnarz, et al., 2019)

The different ASIL assessments may result from the analysis of weaker (lower ASIL) or stronger (higher ASIL) *powertrain* implementations, which may cause different degrees of damage and may be more or less controllable. However, since the E-Gas concept (Audi AG, BMW AG, Daimler AG, Porsche AG, VW AG, 2013) is developed by OEMs (original equipment manufacturer) with much expertise, these ASIL assessments will be considered in the following, with the addition of axle lock prevention (SG5) with ASIL C.

In addition to the aforementioned SG, non-functional SGs may also be applicable to the item *powertrain*. These may consist of ensuring HV touch protection, or fire safety, for example (Ross, 2016), (Christiaens, et al., 2012). However, this work does not focus on these non-functional SGs.

²⁵ Source refers to internal combustion engines (ICE); however, safety goals are still applicable as these refer to the vehicle level

5.2.2 Powertrain System

The PT system consists of a motor control unit (MCU), an electric drive (eDrive) and gear units, as displayed in Figure 5.2.

MCU. The MCU combines the data from the drive pedal and the sensors of the eDrive to command the eDrive and the power electronics (PE), respectively. Its hardware is similar to the architecture presented as the generic hardware of an ECU (see section 4.2.2). However, the architecture must be adopted by adding (following the concepts presented in (Zhang, et al., 2016), (Gächter, et al., 2014)):

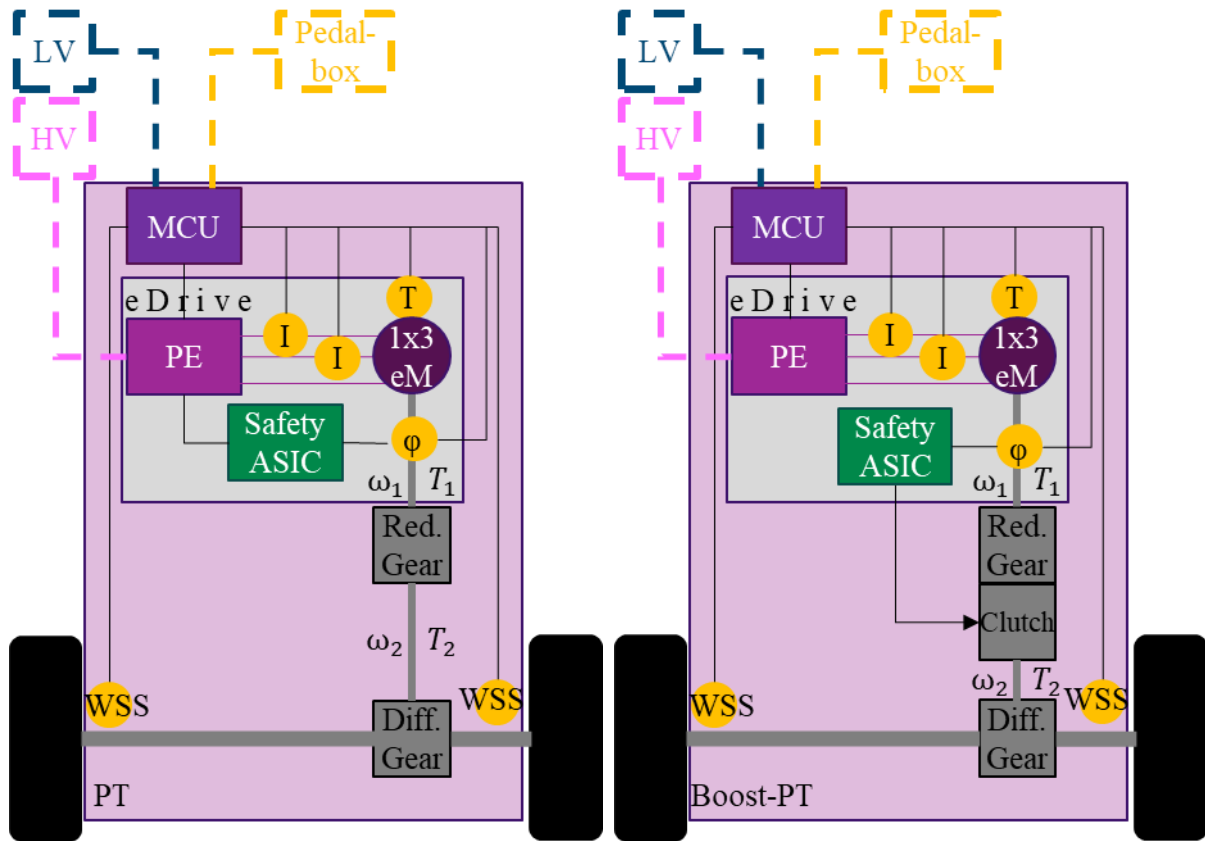
- One current sensor (I),
- One wheel speed sensor (WSS)
- One temperature sensor (T)

eDrive. The eDrive (as described in (Gächter, et al., 2014) and (Robert Bosch GmbH, 2023)) consists of the PE and an electric motor (eM). The eM converts the electrical (HV) into mechanical energy in the form of rotation. It can be implemented as a PMSM (permanent magnet synchronous motor), ESM (externally excited synchronous motor) or ASM (asynchronous motor). However, only PMSMs will be considered further in this work. Further information on eMs can be found in (Doppelbauer, 2020).

Gear Unit. A reduction gear reduces the rotation speed ($\omega_1 > \omega_2$) while increasing the torque ($T_1 < T_2$) of the eM, usually by a ratio of about 10 (Knödel, et al., 2011). This reduced rotation is finally applied to the axle by a differential gear.

The preceding paragraphs refer to the components necessary to implement the basic functionality of a PT. However, a failure within the PT may cause the PE to shut down, which could ultimately cause the specific axle to lock up (SG5, related to ASIL C as defined in section 5.2.1), as described in detail in (Chen, et al., 2023). Therefore, a safety mechanism (SM) (in the form of an ASIC) can be implemented that activates a so-called ‘active short circuit’. This active short circuit allows the eDrive to reduce its drag torque and to avoid lock up the entire axle in case of a failure. (Doppelbauer, 2020), (Chen, et al., 2023)

However, an active short circuit is only necessary if the eDrive cannot be disconnected from the axle. Current electric vehicles equipped with two PTs on two axles generally implement the second PT as a ‘booster’, as shown in Figure 5.2b. However, this PT is usually (see (Spånberg, 2022), (Yang, et al., 2023), (Jennings, et al., 2023)) equipped with a decoupling clutch to reduce induction and transmission losses when not in use. This clutch can be designed similarly to a parking actuator (section 4.4.2, ‘backup’), inheriting an almost self-locking gear that opens by default when not actuated. A design investigation of such a clutch mechanism (also considering solenoid actuators) can be found in (Yang, et al., 2023). Finally, the disconnect clutch can replace the active short circuit as a SM, since it is able to provide a countermeasure in case of axle-blocking due to an E/E-fault if it opens fast enough.



a) Nominal PT

b) Boost-PT

Figure 5.2: Generic architecture of a PT

5.3 Drive Pedal Box

This section presents safety analyses of current state-of-the-art drive pedal boxes (section 5.3.1). The basis of the failure rates is derived in section 2.7.2 and presented in Annex B.2. The analyses also consider the E-Gas concept (Audi AG, BMW AG, Daimler AG, Porsche AG, VW AG, 2013). Furthermore, the approaches presented in section 4.3, are further developed in section 5.3.2 to an X-Domain *fail-operational (fo)* approach.

5.3.1 Conventional Safety Concepts

The state of the art of current drive pedal box safety concepts is the E-Gas concept as defined in (Audi AG, BMW AG, Daimler AG, Porsche AG, VW AG, 2013). It is displayed in Figure 5.3. It shows the architecture consisting of two drive pedal sensors, a central vehicle control unit (VCU), which could also be an MCU, that determines the driver's intent and finally an eDrive that applies the drive torque.

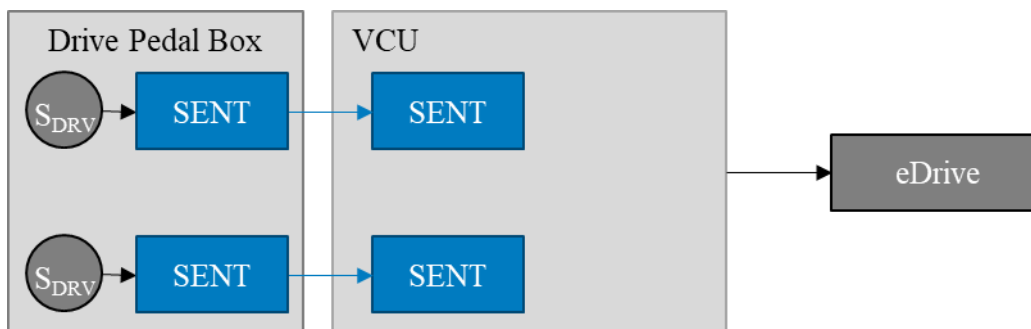


Figure 5.3: E-Gas concept, derived from (Audi AG, BMW AG, Daimler AG, Porsche AG, VW AG, 2013)

Figure 5.4 shows the results of the safety analyses described. Here, the E-Gas oriented architectures are referred to as Duplex_{fp}. However, alternatives such as simplex, duplex (*fo*) and even triplex architectures are also examined. The results displayed are similar to those for conventional brake-by-wire (BBW) pedal boxes (refer to section 4.3.2). However, the drive pedal box has to meet different SGs (QM regarding SaRA and ASIL B regarding integrity). Furthermore, it is only connected to a single VCU, which eliminates the risk of an inter-communication bus to manipulate data.

Finally, all architectures analyzed meet the SGs, even those equipped with simplex sensors. However, as described in the E-Gas concept, architectures equipped with duplex sensors are preferred because their implementation is associated with a huge improvement in integrity for the cost of a single sensor.

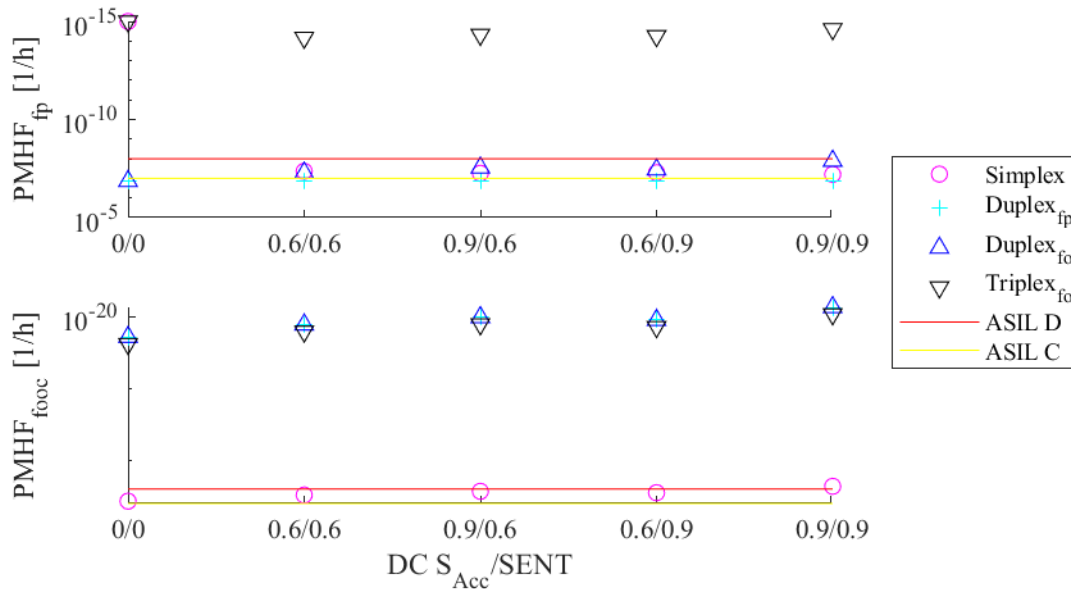


Figure 5.4: Safety assessment of drive pedals

5.3.2 X-Domain Safety Concepts

The safety analyses of BBW pedal boxes (section 4.3.3) show that both virtual sensors and drive pedal sensors can improve the integrity of brake pedal boxes. This improvement may even allow duplex architectures to meet the required ASIL D availability and integrity when used for diagnostic purposes.

This section extends the results to an X-Domain level and analyzes how X-Domain approaches can improve the safety of both brake- and drive-by-wire pedal boxes. Therefore, a minimal configuration for an X-Domain pedal box is analyzed, as displayed in Figure 5.5. The architecture shown is characterized by the two VCUs establishing the two braking circuits and thus a *fo* capability of the braking functionality. Therefore, each brake pedal sensor is allocated to one VCU. On the other hand, since no *fo* capability of the powertrain functionality is required, both drive pedal sensors are connected to one VCU that controls the eDrive.

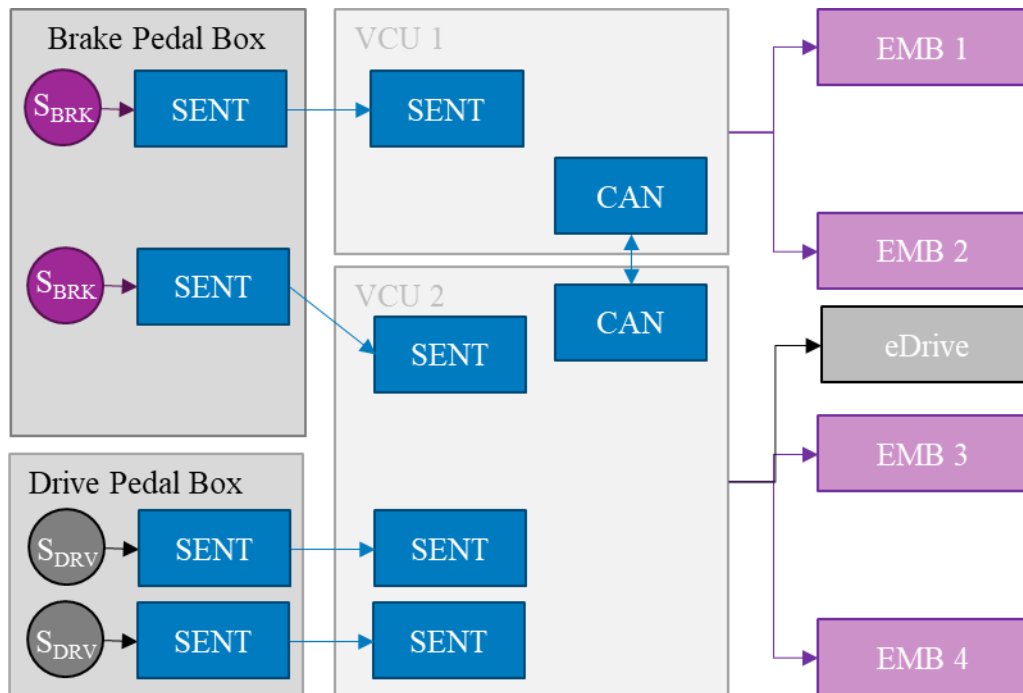


Figure 5.5: Minimum X-Domain pedal box

The X-Domain pedal box replaces the X-Domain diagnosis (section 4.3.3) with an X-Domain backup, as described in (Schrade, et al., 2022). The inventors disclose that each domain guarantees the integrity by its own, representing two *fail-passive* (*fp*) systems. However, in case of a *fp* failure of one domain, the lost functionality of one pedal is merged²⁶ to the other pedal, implementing a global *fo* behavior of both the powertrain and the braking functionality.

The implementation as *fp*-systems causes the functionalities to stop working after the first failure of a related component. This is particularly detrimental to the braking functionality and VCU1. A failure (*fp* or *fooc* (*fail-out-of-control*)) of any brake pedal sensor or the inter-communication bus causes a shutdown of the associated driver intent determination of VCU1. Ultimately, the only way to avoid a shutdown of VCU1 is if the driver intent is obtained from the inter-communication bus after the first failure. However, this is not evaluated as a safe operation strategy because the inter-communication bus itself (*fp* or *fooc* failure) could be the root cause of the shutdown. Therefore, the driver intent determination of VCU1 tends to fail *fp* frequently (refer to Figure 5.6), but rarely *fooc*.

An exception to the above strategy is a failure of VCU2 itself. This causes all sensors except of the brake pedal sensor of VCU1 to fail immediately. In this case, VCU1 must continue (emergency) operation relying on its single remaining sensor. Therefore, VCU1 requires reliable awareness of the state of VCU2.

In contrast to VCU1, VCU2 implements X-Domain driver intent determination because it has access to both drive pedal sensors and a brake pedal sensor. Therefore, any first failure can be

²⁶ This concept is also referred to as “OnePedalDrive”. Nilsson et al. (Nilsson, 2002) analyzed the controllability and driver comfort and concluded that one-pedal-driving is accepted by the drivers under analysis.

tolerated by VCU2 because the functionality of one pedal is merged into the other. This has a direct impact on availability (by a magnitude of approx. 12 compared to VCU1), as shown in Figure 5.6. It also depicts that the X-Domain approach achieves both the required safety-related availability (SaRA) and integrity to implement ASIL D systems and also provides ASIL D driver intent determination for the powertrain functionality.

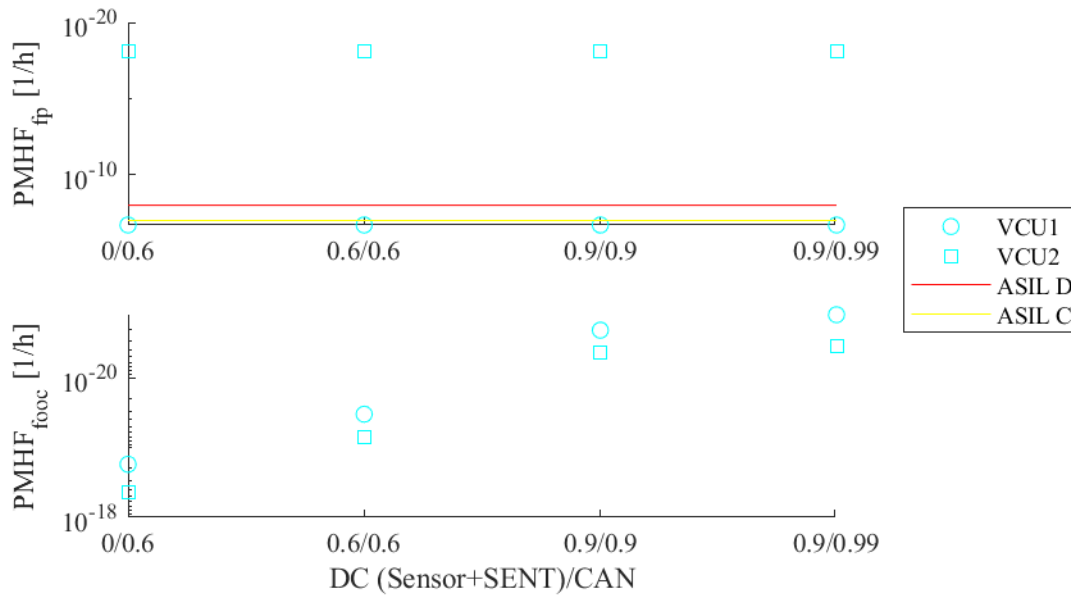


Figure 5.6: Safety analysis of the X-Domain pedal box

5.4 Safety Analysis of the reference Powertrain Systems

This section presents the design space (section 5.4.1) that is within the scope of this work with respect to PT systems. This design space is then analyzed regarding the defined SGs starting with a brief investigation related to sensors (section 5.4.2). The following sections focus on safety concepts of single PTs (section 5.4.3) and PTs installed on two axles (section 5.4.4).

5.4.1 Design Space

The design space inherits two main options. The first option is a single powertrain (Figure 5.7a), which is very similar to the definition displayed in Figure 5.2a. In addition to the single PT, dual axle PTs are also analyzed. These are additionally equipped with a boost PT (as displayed in Figure 5.2b). However, the boost PT can be controlled by the MCU of the nominal PT (Figure 5.7b) or by its own MCU (Figure 5.7c).

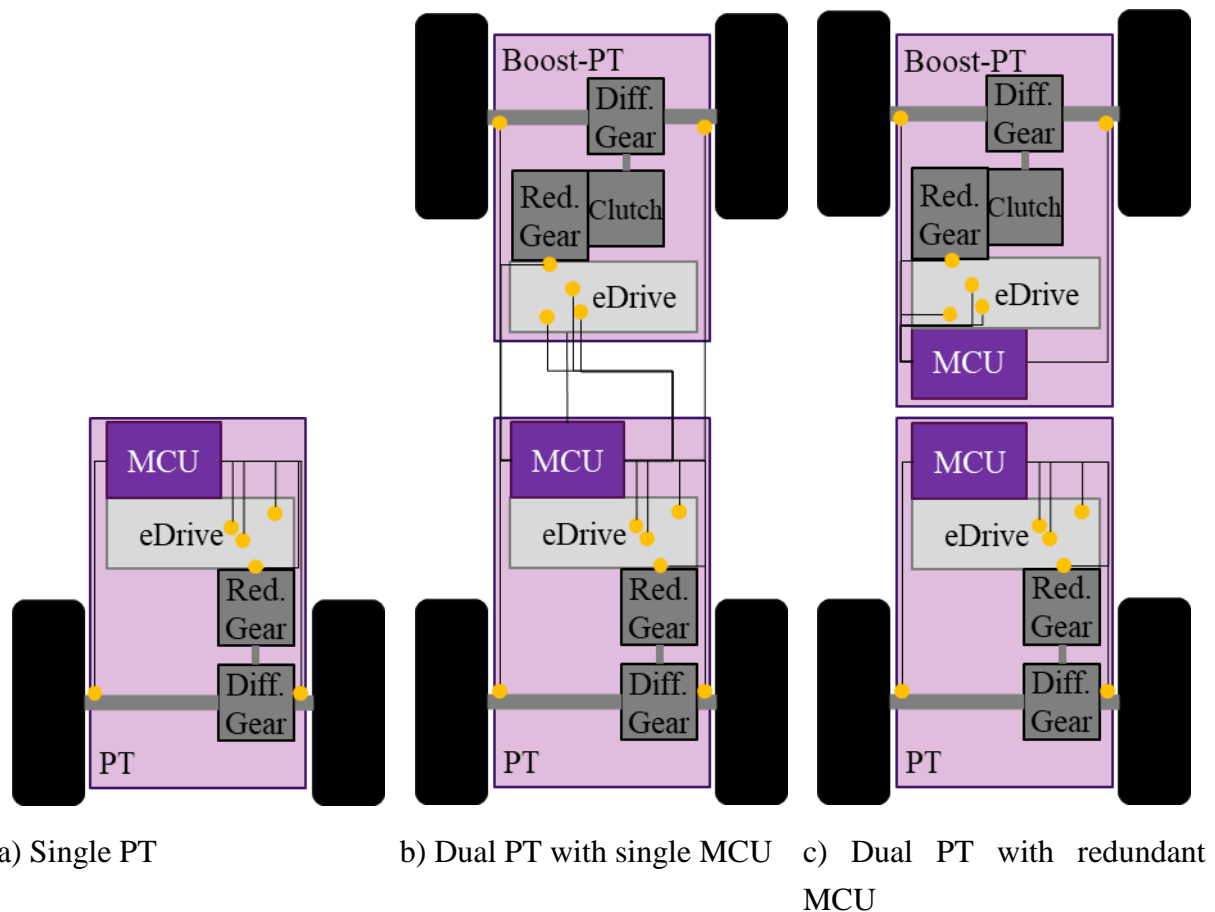


Figure 5.7: Design space of the PT system

In addition to implementing a boost PT, the installed components are also permuted, focusing on the E/E components. On the one hand, the SM within the ECU (CPU, RAM, ROM) are varied, as provided in Table 2.6. On the other hand, the failure-tolerance of the Safety-ASIC is also varied. This variation consists of either passivating the powertrain or tolerating the fault of the Safety-ASIC and continuing normal operation (with the failed SM). Failure-

tolerant operation can be triggered either by an active decision to continue operation or by a dormant fault of the Safety-ASIC, which describes a case where the ASIC has failed but this failure has not been detected by the system. The share of dormant faults is permuted (instead of the diagnostic coverage (DC)) from 0% (always detected or *fp*-approach) to 100% (never detected or *fo*-approach). Finally, the DC (from 60% to 99%) of the RPS is considered, which triggers the Safety-ASIC to activate the active-short-circuit operation.

5.4.2 Failure Effects due to Sensor Failures

The PT system is equipped with a variety of sensors. The purpose of this section is to analyze the failure effect (FE) that a sensor failure can cause. A PT reduced to its sensors and the associated FE is displayed in Figure 5.8.

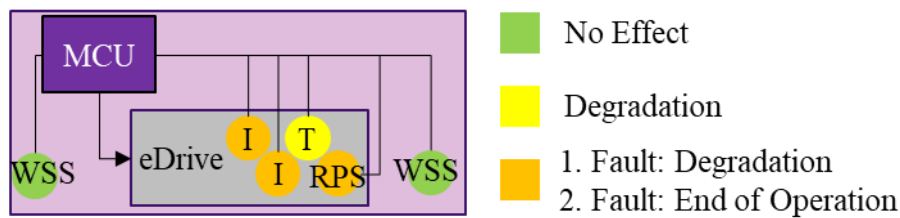


Figure 5.8: PT related to FE due to sensor failures

The rotation sensors (WSS and RPS) have a strong correlation because they are connected²⁷ to the differential gear. With three sensors in place, it is assumed that any first failure can be diagnosed and tolerated. For example, a missing WSS can be extrapolated by evaluating the remaining WSS and the RPS. In addition, the WSS are not required to operate the eM, but to provide functions such as traction control, which are not considered safety relevant. Therefore, the failure of the WSS is not considered to have any FE on the PT. In contrast to the WSS, the RPS is required to operate the eM. However, fault-tolerant control of the eM is possible without using the RPS, as presented by (Jeong, et al., 2005). Therefore, an RPS-failure is assumed to be related to a degradation of the PT. A special situation occurs when the RPS-sensor fails *fooc* in case of the nominal PT, as the RPS triggers the SM to activate the active short circuit of the eDrive. In this case, a single failure will eventually passivate the PT.

(Jeong, et al., 2005) also show that fault-tolerant control of the eM is possible in case of current (I)-sensor failures. Therefore, a degraded operation is also assumed. However, a combined I-sensor and RPS failure is deemed to result in a shutdown of the PT. Finally, a T-sensor failure is assumed to cause a PT degradation because this data can be replaced by a (inaccurate) physical model.

²⁷ This connection can only be ceased by a release of the disconnect clutch in case of boost-PT

5.4.3 Safety Analysis of a single Powertrain

Impacts. This section analyzes the effects of varying the design of a single PT as specified in the previous section. Figure 5.9 shows the main effects of the discussed components on the analyzed FE and cost. The background color of the subplots indicates a positive (green) or negative (red) correlation, while the opacity highlights its intensity. It is obvious that none of the design options has a significant impact on the probability of fp or fd . However, these FE are not associated with any ASIL-related SG.

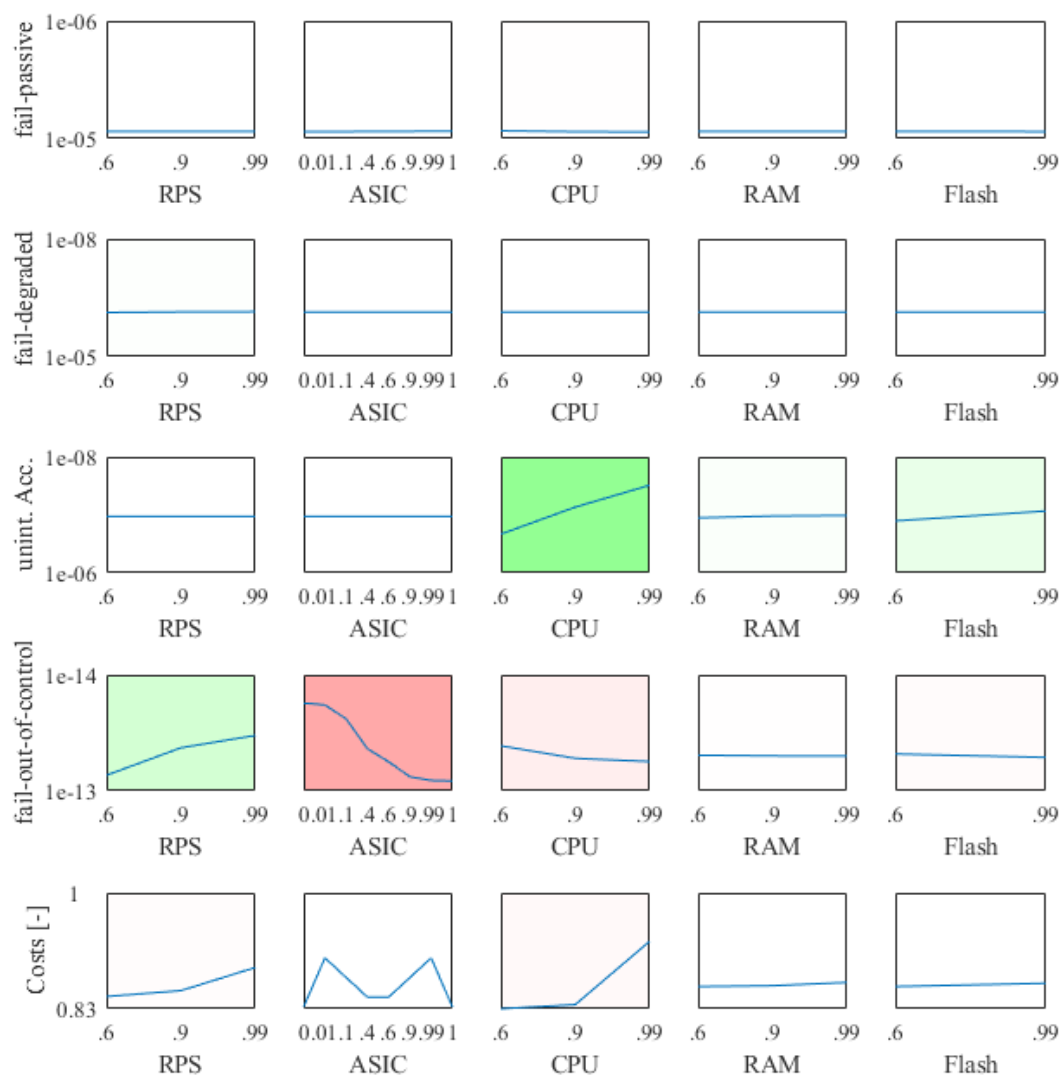


Figure 5.9: Main effects of the components related to failures and costs²⁸

On the other hand, the SGs “avoid unintended acceleration” (SG1) and “avoid a blocking of the axle” (SG5) must be provided with ASIL B and ASIL C respectively. Figure 5.9 indicates that the internal SMs of the ECU (especially within the CPU) have a major impact on the

²⁸ The y-axis describes the PMHF [1/h] of the FE

probability of unintended acceleration events. In addition, the Safety-ASIC and its associated RPS influence the probability of axle lockup events.

Safety Analysis. The SMs within the CPU have a major impact on the probability of violating SG1 (“*unintended acceleration*”, ASIL B). Therefore, they are highlighted in Figure 5.10. The middle part of Figure 5.10 shows that the SM within the CPU is the key to meet SG1 ($DC \geq 90\%$) or not ($DC < 90\%$).

The lower part of Figure 5.10 shows that all analyzed designs meet ASIL D with respect to SG5 (“*axle blocking*”, ASIL C), regardless of the specific operating mode of the Safety-ASIC. In addition, it can be observed that none of the architectures satisfies ASIL B or D with respect to SaRA (SG2 and 3). However, this is also not the target of the item *powertrain*. The MCU design that satisfies all SGs at minimum cost is presented in section 5.5.4.

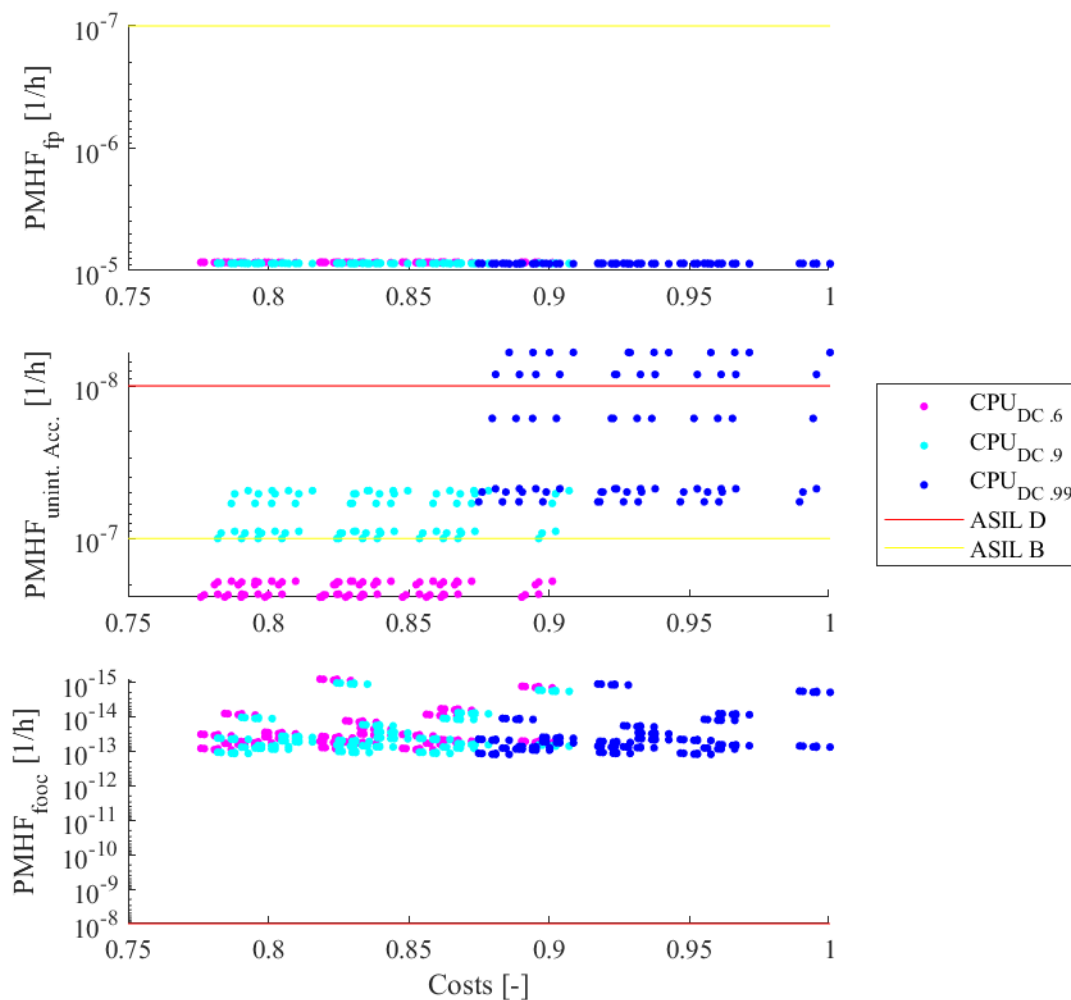


Figure 5.10: Safety assessment of a single PT

5.4.4 Safety Analysis of Dual Powertrains

Single MCU. Installing a boost PT controlled by the same MCU as the nominal PT has a very limited effect on safety. On the one hand, there is a small reduction in safety (factor 2) in terms of integrity, since two PTs are capable of provoking an axle lockup. On the other hand, the availability (not related to safety) is increased (by a factor 20, compared to a single PT). Availability is limited by the reliability of the MCU itself. For example, the SM within the CPU directly results in the *fp*-behavior displayed in Figure 5.11. Finally, the probability of “*unintended acceleration*” events remains constant (compared to a single PT) because the only root cause is the MCU, which remains unchanged compared to a single PT system.

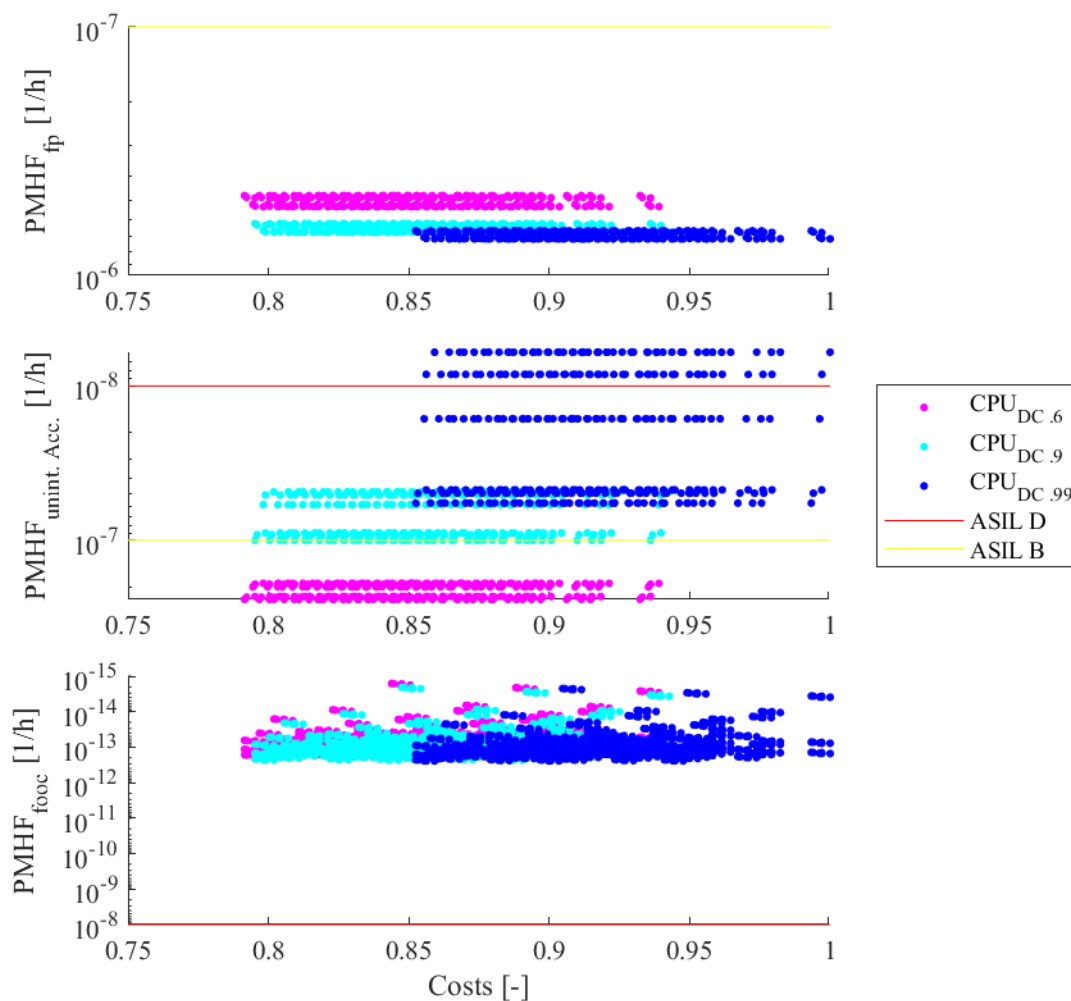


Figure 5.11: Safety assessment of dual PT with single MCU

Redundant MCU. The redundant PT equipped with a redundant MCU (see Figure 5.7c) results in a significant increase of the availability of the propulsion functionality, as displayed in the upper part of Figure 5.12. The availability (not safety-related) could even be increased to a level beyond ASIL D. On the other hand, the second MCU doubles the probability introduc-

ing an “*unintended acceleration*” FE (middle part in Figure 5.12). Therefore, enhanced SMs are required compared to single MCUs. This is illustrated by the need for a $DC \geq 99\%$ of the CPU within the two MCUs, instead of a $DC \geq 90\%$ within the single MCUs. Finally, the probability for axle lockup remains almost constant (at a very safe level) compared to the architectures equipped with a dual PT and a single MCU. The MCU design that satisfies all SGs at minimum cost is provided in section 5.5.4.

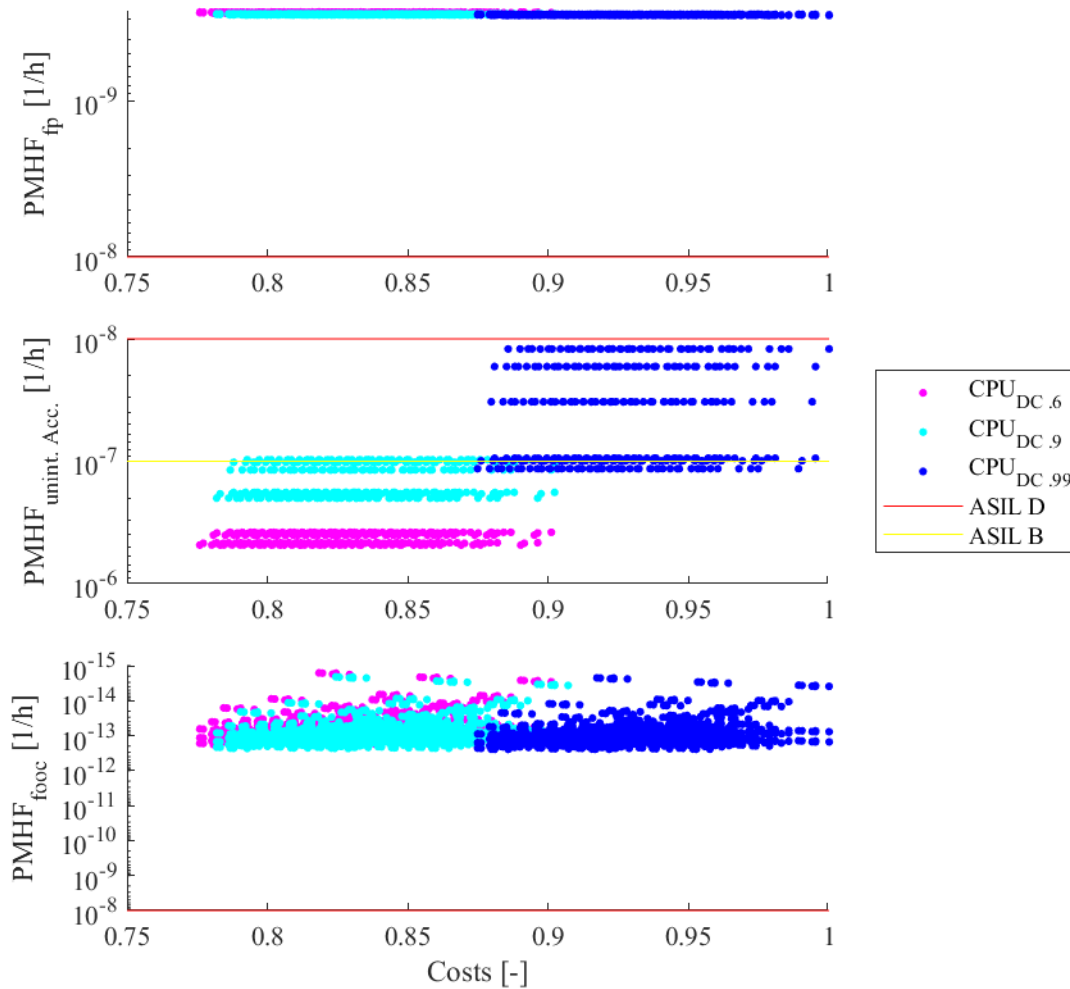


Figure 5.12: Safety assessment of a dual PT with two MCUs²⁹

²⁹ Displayed architectures apply same SMs in both MCUs

5.5 Graceful Degradation at X-Domain ECUs

This section examines the possibilities of operating the braking and PT systems together within one ECU on separate lanes. It focuses on the opportunities that exist if the functionalities can be flexibly allocated in case of a failure of a lane. Section 5.5.1 provides a brief introduction to this flexible allocation, called graceful degradation (GD). It should be noted that the analysis presented assumes that the (software) functions of a braking and a PT system can be run interchangeably on the same hardware, only by the constraint of different implemented SMs. Furthermore, a short transient time of the lanes to switch from one functionality (i.e., powertrain) to another functionality (i.e., braking) must be ensured to guarantee safety. Section 5.5.2 examines the safety implications of using GD. Finally, it is analyzed, how safety can be ensured with increased availability due to the use of GD (refer to section 5.5.3 and 5.5.4).

5.5.1 Introduction to X-Domain Graceful Degradation

The PT and the braking system must satisfy different SGs for SaRA and integrity (see sections 3.1.5 and 5.2.1). While the braking system has to achieve both ASIL D SaRA and integrity, the PT system does not have to meet any SaRA and only ASIL C integrity. Therefore, the braking functionality is considered more safety-critical than the powertrain functionality. Hence, GD can be applied to continue the operation of the braking, while the powertrain functionality is shut down due to a reassignment of functions to other lanes within the ECU after an initial fault.

Figure 5.13 presents a two-fault Markov-diagram of a triplex-lane ECU applying GD. It consists of:

- A VCU of the braking system (B),
- An MCU of the PT system (P) and
- Additionally provides one spare lane (S) that may take over after a first fault.

The main objective of the operation procedure of the specified ECU is to guarantee the braking functionality to be executed, since it is the most safety-critical functionality. This is achieved by assigning the braking functionality to the spare-unit after a first *fp*-failure of the dedicated brake-lane (see state c). Furthermore, an additional failure (*fp*) of the spare lane, which then executes the braking functionality, assigns the braking functionality to the lane dedicated to the powertrain functionality. The powertrain functionality is finally stopped. GD is not applied (in the context of this thesis) if a *fooc*-state is reached because the respective lane continues to operate (falsely), so that no backup can take over the specified functionality.

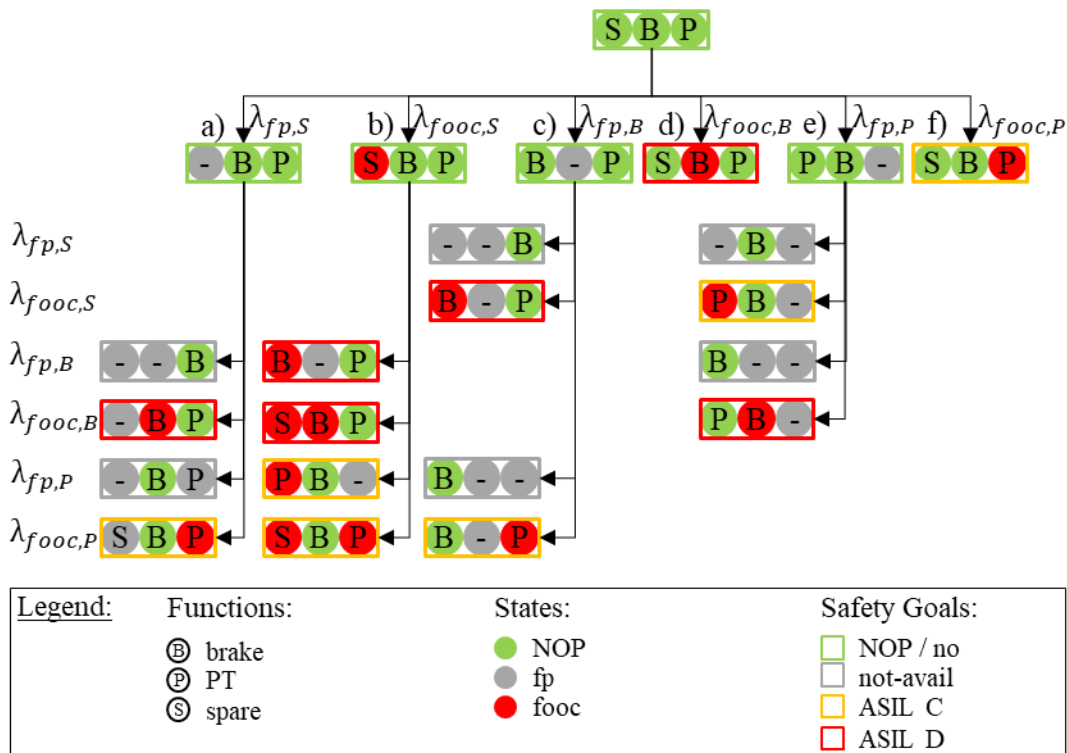


Figure 5.13: Markov-diagram of a tri-lane ECU with one spare lane

5.5.2 Safety Assessment of generic X-Domain ECUs

The impact of the application of GD on the safety of a generic ECU is displayed in Figure 5.14, considering three faults, since the operation of a vehicle in a faulty state may be increased compared to the previous chapters. Figure 5.14 demonstrates the dependencies between the FEs and the number of lanes dedicated to the braking (n_{BRK}) and PT system (n_{PT}). It is assumed that all lanes are similar (even with the same SMs) and inherit a reference failure rate $\lambda_{fp}=10^{-7} 1/h$ with a $DC=90\%$. The magenta curves show architectures that do not use spare lanes, while the blue curves show architectures that actively use a single spare lane after an initial failure.

Figure 5.14 shows that the SaRA of the braking functionality increases with the number of ECUs (regardless of their dedication). It can also be seen that the implementation of a spare- and a PT lane increase the SaRA of the braking functionality interchangeably. A similar effect can be seen for the availability of the powertrain functionality. However, if two PT lanes are required to operate the (two) PT systems, the probability of a degraded PT operation increases with the number of lanes dedicated to the braking functionality. Furthermore, the (not safety-related) availability of the PT system decreases as the number of brake-lanes increases, since the probability of the application of GD increases, which in-turn passivates the PT lanes.

The installation of a spare-lane negatively affects the integrity of the duplex braking systems if it is not actively monitored. This is because the spare-lane can develop a dormant *fooc*-

behavior. If one of the dedicated brake-lanes then develops another *fooc*-behavior, the spare-lane is consulted to disable the (wrong) lane in normal operation (NOP), causing an overall *fooc*-behavior of the braking functionality.

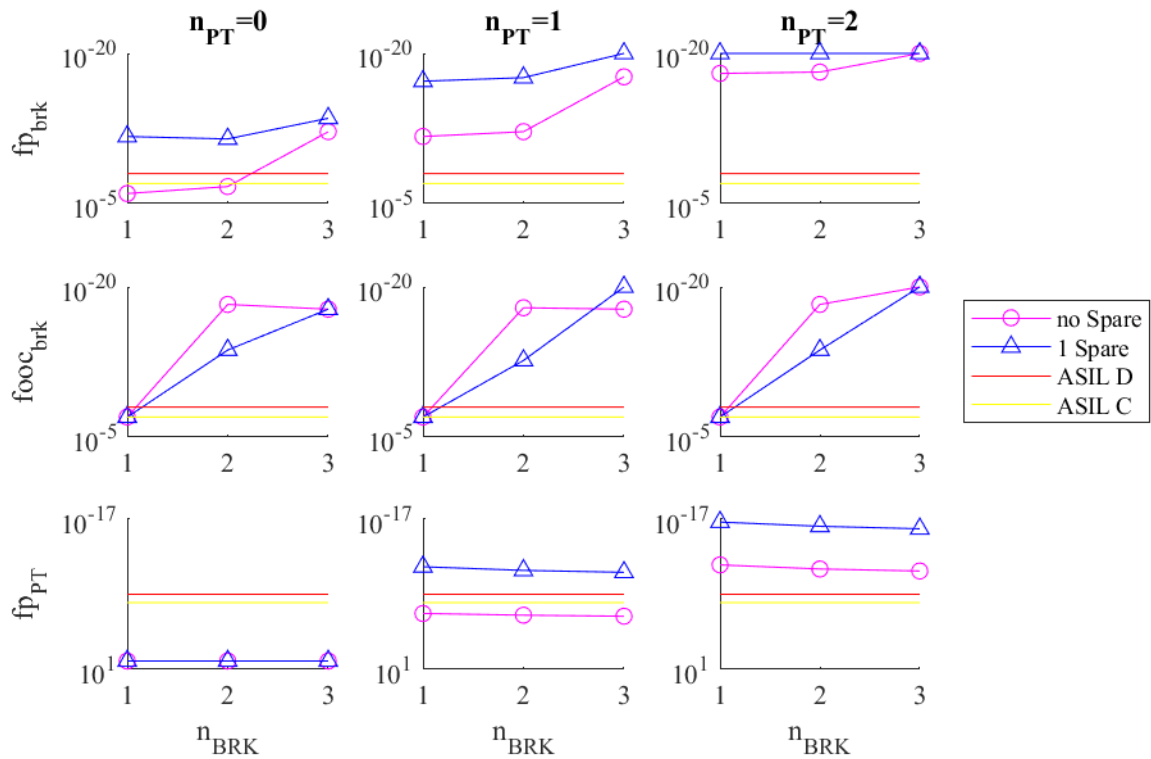


Figure 5.14: X-Domain graceful degradation for a reference ECU²⁸

5.5.3 Safety Assessment of an increased Availability Approach

One possible implementation of GD is to design a safe architecture while neglecting the potential for GD. In such a case, both the braking and the powertrain functionality are safe in an initial state. However, if a spare lane is added, a first failure of a lane may occur that does not violate any required hardware metric because the spare-lane can take over the respective functionality/redundancy. Finally, after a first failure, the vehicle could continue to operate without any safety restrictions. Therefore, a first failure can be classified as loss of a “*comfort feature*” and continuation of operation for another $t=200 h$ (as described in ISO 26262-5 (International Organization for Standardization, 2018)). However, such an approach can only be chosen if the potential for common cause failures is not considered. Figure 5.15 shows the effect of such fault-tolerant operation on the probabilities of the FEs.

Continued operation reduces the gain in (safety-related) availability of both braking and powertrain functionality that can be achieved by adding lanes. This becomes clear when considering the SaRA without a PT lane of a triplex brake-ECU. The (magenta) option that cannot apply GD and therefore limits the continuation of the operation to $t=1 h$. It achieves a higher SaRA than an ECU that applies GD (blue) by using the spare-lane and allowing the

continuation. However, the availability (not safety-related) is increased by implementing the spare lane.

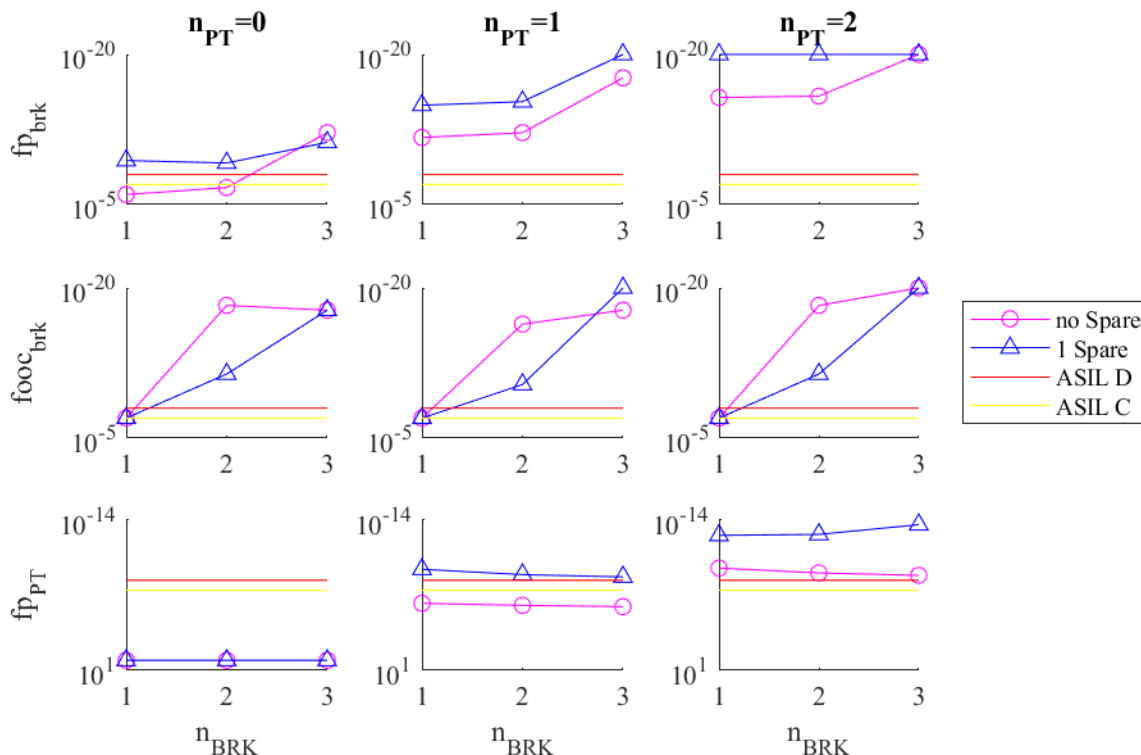


Figure 5.15: X-Domain graceful degradation with functionalities as comfort features²⁸

5.5.4 Application of the increased Availability Approach

The previous section analyzes that GD can increase the availability of the system if a spare unit is additionally applied. It focuses on similar lanes that can take over functionalities interchangeably. However, since the SGs related to the braking and the PT system are different, dissimilar lanes with different SMs can be implemented related to the braking and the PT system. Table 5.1 and Table 5.2 provide an overview of the ‘safe’ ECU designs, at the lowest cost presented in the previous chapters, considering both brake ECUs (VCU) and PT ECUs (MCU). In this section, the advantageous designs are also analyzed considering the safety dissimilarities.

Table 5.1: Installed MCUs within PT systems

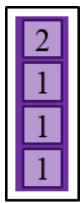
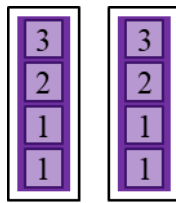
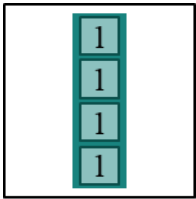
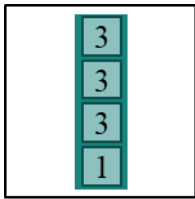
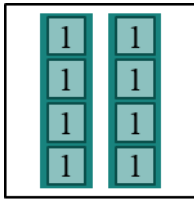
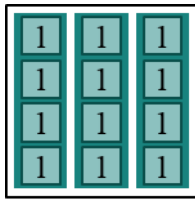
Design ³⁰		
Topology	Single PT Dual PT with single MCU	Dual PT with redundant MCU

Table 5.2: Installed VCUs within the EMB-CCS

Design ³⁰									
ID _{VCU.BRK}	1111		3331		2x(1111)		3x(1111)		
Backup Bus to Pedal	Yes	No	Yes	No	Yes	No	Yes	No	
Topology	X-Circ.			VCU2	VCU2	VCU1	VCU1		
	H-Circ.	VCU1		VCU2	VCU2		VCU1		
	Centr.			VCU				VCU	
	Ring	VCU1/2			VCU2		VCU1		

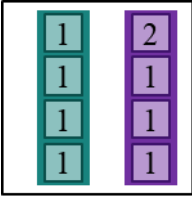
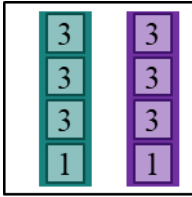
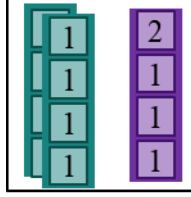
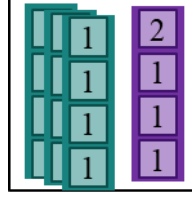
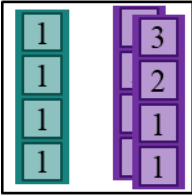
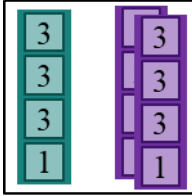
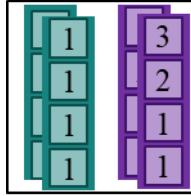
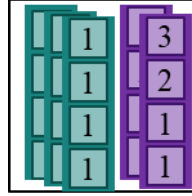
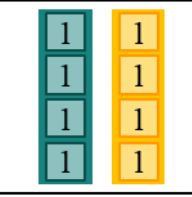
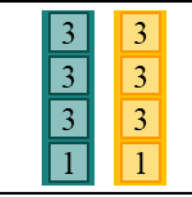
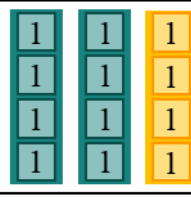
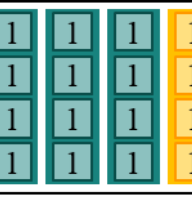
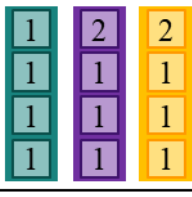
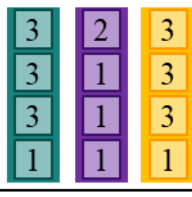
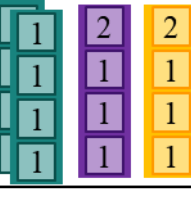
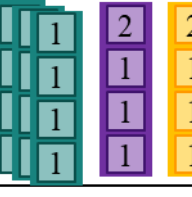
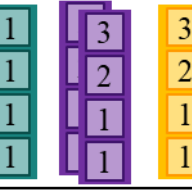
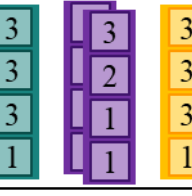
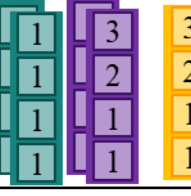
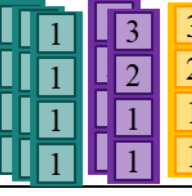
Since the braking functionality inherits the highest safety-criticality, an advantageous implementation of GD is to give the lane that takes over the braking functionality after an initial failure the same SM as the brake-lane itself. This is the spare lane, if implemented, or the PT lane. However, if the spare lane is implemented, the spare-lane must also take over the powertrain functionality. Therefore, it must provide at least the same level of safety as the PT lane, additionally. Table 5.3 provides an overview of the preferred ECU designs for applying GD.

Applying GD to specific ECU designs confirms the results of the previous section, as shown in Figure 5.16. The SaRA of the braking functionality generally increases while the availability of the powertrain functionality decreases as the number of lanes increases. However, the only exception is a triplex-lane brake configuration (ID: 3x(1111)) combined with a spare-lane, which reduces the SaRA. This is due to the potential of the spare lane to develop a dormant *fooc*-behavior that passivates the braking functionality if one of the three brake-lanes

³⁰ Numbers in ECU represent SMs to achieve integrity of ECU: CPU, RAM, ROM, number of clocks

develops a second *foc*-behavior, creating a stalemate situation, assuming all four lanes are used to diagnose the failure.

Table 5.3: VCU designs suitable to increase the availability

ID _{VCU.BRK}		1111	3331	2x(1111)	3x(1111)
No Spare	Single MCU				
	Red. MCU				
Spare	No MCU				
	Single MCU				
	Red. MCU				

A similar issue can be monitored with respect to the braking integrity of the duplex-lane (ID: 2x(1111)). A dormant *foc*-failure of the spare lane combined with a *foc*-failure of one brake-lane causes a *foc*-behavior of the VCU, while passivating the lane in NOP. In contrast, the integrity of the VCU is reduced (by a magnitude of 6) when GD is applied. However, the integrity level remains well above the required ASIL D. Therefore, such designs can still be applied. It can be concluded that the application of GD increases the SaRA of the discussed ECU-architectures while still enabling the required integrity. Therefore, GD can improve the safety of braking systems.

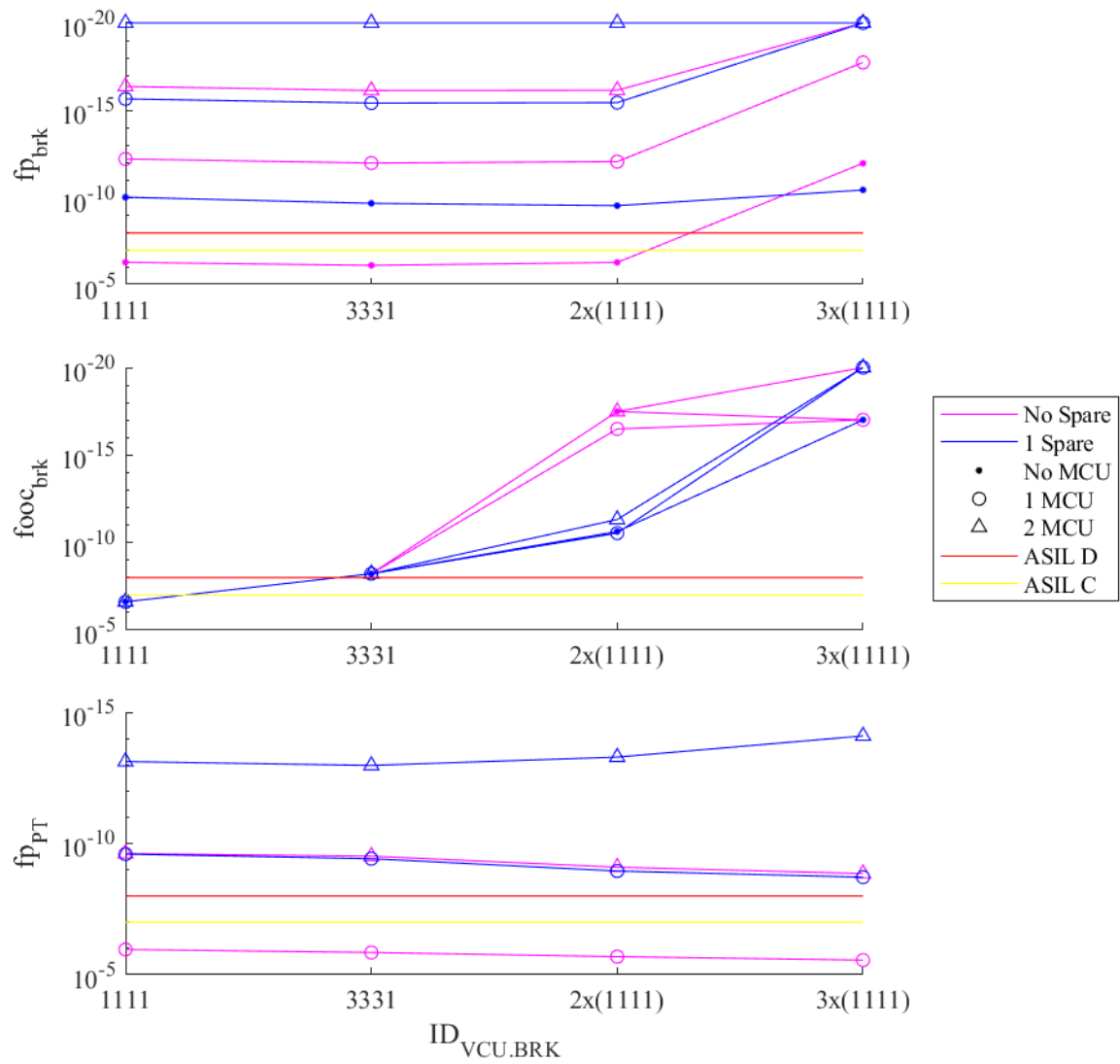


Figure 5.16: Application of the increased availability approach as PMHF [1/h]

5.6 Composition of a Joint Braking and Powertrain System

The previous sections introduced the item powertrain, its safety analysis and GD. In this section, these findings (section 5.6.1) are merged with the EMB-systems of chapter 4 taking into account the requirements for joint braking and powertrain systems evaluated in section 3.3. Finally, sections 5.6.2 and 5.6.3 present the architectures that take advantage of potential benefits of applying X-Domain features.

5.6.1 Initial Considerations

The safety of joint braking and powertrain systems can be analyzed in two dimensions: functional safety and product liability, as already discussed in section 4.7 for EMB-systems. The product liability perspective (as defined in Annex A) is more demanding as a residual deceleration of $a_x \geq 6.4 \text{ m/s}^2$ is required after an initial failure. This backup deceleration can only be achieved by a three-wheel backup, as presented in section 3.2.2. Using the powertrain to apply the backup deceleration could be a promising approach. However, the powertrain does not provide reliable deceleration, as presented in section 3.3. Therefore, from a product liability perspective, it is not considered further. Finally, a two braking circuit design implemented by the EMB-system itself is still required according to ECE R13H.

In contrast to product liability, the powertrain could be considered from a functional safety perspective through the application of ASIL decomposition as defined in section 2.4.3. In this case, the powertrain may be considered using active or backup redundancy, which may reduce the ASIL of the braking circuits. Such an ASIL reduction may facilitate the control law, software and hardware development of future EMB-systems, as pointed out in section 2.4.4.

Figure 5.17 shows decomposition options regarding the required SaRA of a powertrain with respect to the two braking circuits. Decomposition options that require a higher SaRA of the powertrain than ASIL B are not considered further (as analyzed in section 3.3.3), but are marked with a red X.

req. ASIL powertrain		Brake Circuit 1				
		QM(D)	ASIL A(D)	ASIL B(D)	ASIL C(D)	ASIL D(D)
Brake Circuit 2	QM(D)	X	X	B(D)	A(D)	QM(D)
	ASIL A(D)	X	B(D)	A(D)	QM(D)	-
	ASIL B(D)	B(D)	A(D)	QM(D)	-	-
	ASIL C(D)	A(D)	QM(D)	-	-	-
	ASIL D(D)	QM(D)	-	-	-	-

Figure 5.17: Powertrain as active redundancy to achieve ASIL D SaRA

Figure 5.17 highlights that it is possible to implement the braking circuits with ASIL B(D) and ASIL A(D)³¹ when combined with an ASIL A(D) powertrain in terms of SaRA. This being mentioned, the eventual braking system itself only meets ASIL C(D) regarding SaRA. This reduction of ASIL ultimately enables smart simplex ring-topologies without backup buses (Figure 4.30) and *simple* centralized duplex architectures operating as *fo* (Figure 4.26).

In addition, the powertrain could be used not only to achieve ASIL D SaRA, but also to provide backup redundancy to increase vehicle availability in the event of a braking circuit failure. Such systems must meet a combined ASIL D SaRA after an initial failure. Figure 5.18 shows possible solutions, assuming that the powertrain is implemented with the same ASIL as braking circuit 2. Options that do not satisfy ASIL D SaRA are marked with a red X, as these are not valid implementation options.

appl. ASIL powertrain		Circuit 1				
		QM(D)	ASIL A(D)	ASIL B(D)	ASIL C(D)	ASIL D(D)
Circuit 2	QM(D)	X	X	X	X	QM(D)
	ASIL A(D)	X	X	X	A(D)	-
	ASIL B(D)	X	X	B(D)	-	B(D)

Figure 5.18: Powertrain as passive redundancy to achieve increased availability

In general, the powertrain is capable of compensating for the lack of safety in the event of a failure of braking circuit 2. However, a special implementation is the option consisting of two ASIL B(D) braking circuits. This design allows ASIL D SaRA through the ASIL B(D) powertrain, regardless of which circuit failed first. However, as shown in section 3.3, an ASIL B(D) powertrain can only be achieved by vehicles with very high specific powers in combination with a reduction of the operating space after the first failure.

In addition to ASIL decomposition, GD can be applied to increase the SaRA of the braking system while neglecting the powertrain functionality. Such an approach may be particularly suitable for high-segment cars equipped with two powertrains with independent MCUs to provide a degraded powertrain functionality after an initial failure.

Additionally, the energy-supply must be considered. While improved availability can be implemented by the PT system (as discussed in Figure 5.18), the energy-supply must also be fault-tolerant to ensure ASIL D SaRA after an initial fault. Therefore, a third energy-supply with ASIL B(D) may be required.

5.6.2 Single Powertrain System

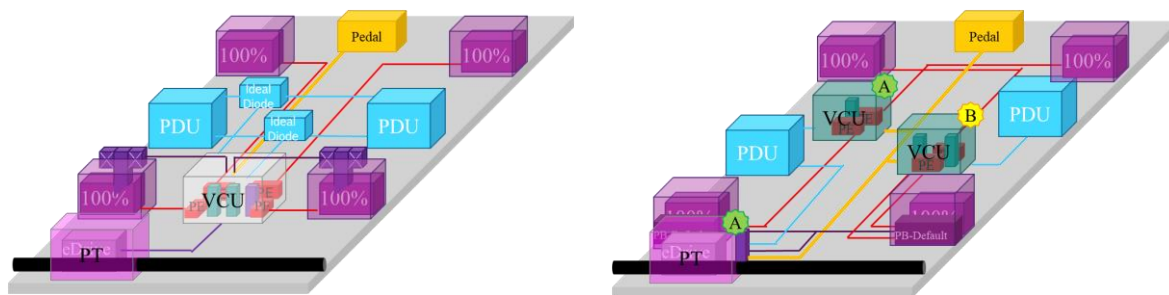
This section presents vehicle architectures that exploit the discussed X-Domain potentials while satisfying the requirements from a product liability perspective. Therefore, the first con-

³¹ The *A(D)* notation shows that the initial ASIL is ASIL D, but that the initial requirement is decomposed to an ASIL A

siderations are taken into account and both *simple* and *semi-/smart* EMB-actuator architectures are analyzed.

Architectures that only combine a PT system and the discussed EMB-systems without providing synergies are not considered further. The duplex-VCUs of the two-circuit EMB-designs (section 4.5.4 and 4.5.5) are examples of this. If the duplex-VCUs were needed to improve SaRA, GD could be applied and synergies could be exploited. However, the duplex-VCUs discussed are required to ensure integrity, which is not improved by GD. Therefore, such architectures are generally not analyzed in this section.

Simple EMB-Actuator. Figure 5.19a presents a centralized architecture that implements a single VCU combining two brake and one PT lane. These lanes together satisfy ASIL D SaRA either by an ASIL C(D) and ASIL A(D) decomposition approach³² or applying GD after an initial brake-lane failure. However, the corresponding transition time of the PT to divert to a brake-lane, if the GD-approach is used, must be short enough (i.e., $t=100\text{ ms}$). In addition, the VCU is supplied by two energy-supplies that are merged by two ideal diodes.



a) Centralized triplex architecture

b) X-Circuit with externally actuated PB

Figure 5.19: X-Domain architectures with *simple* actuators

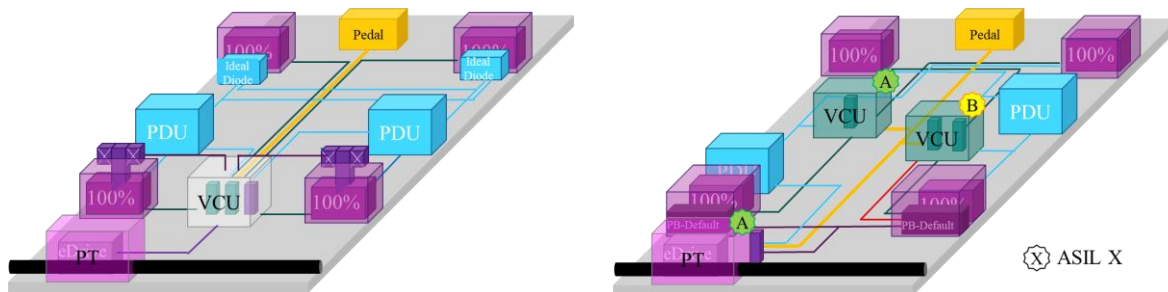
In addition, a conventional X-Circuit design is shown in Figure 5.19b. Here, ASIL decomposition is applied, resulting in an ASIL B(D) and ASIL A(D) brake circuit and an ASIL A(D)³² powertrain. The ASIL A(D) braking circuit and the ASIL A(D) powertrain are connected to one energy-supply (ASIL B(D)), while the other braking circuit is connected to the other energy-supply (ASIL B(D)), allowing the correct allocation of two ASIL B(D) energy-supplies.

The synergies of the powertrain and the EMB-system are discussed below. If one of the two VCUs fails, the corresponding two EMB-actuators are passivated. Nevertheless, the PT system can provide enough recuperation to achieve the required deceleration in many cases. However, this recuperation is not reliable (see section 3.3). Therefore, the PT lane is enabled to activate both default PBs (default PBs are described in section 4.4.2) on the rear axle if the required deceleration cannot be achieved. These default PBs must be designed as fail-active applications to compensate for the loss of power. In addition, the ASIL B(D) VCU must be connected to at least one default PB to provide a *fo*-capability of the PB-system in case of a

³² If the specific power of the vehicle satisfies the requirements in section 3.3

PT system shutdown, as required by ECE R13H. The advantage of the presented architecture is that the default PB is only activated during rare high deceleration maneuvers (above the powertrain deceleration potential) instead of always after an initial failure (unlike the default PB-actuators in section 4.4.2).

Semi-/Smart EMB-Actuator. Figure 5.20 shows the consequences of replacing *simple* with *semi-/smart* actuators. Obviously, the centralized architecture (Figure 5.20a) has moved the ideal diodes from the VCU to the front actuators. Since a power shutdown causes passivation of the two associated actuators, the ideal diodes provide a *fo* capability for the respective actuator that is closely linked to the PE. Therefore, when the PEs are moved from the VCU (see *simple* actuators) to the actuators (see *semi-/smart* actuators), the ideal diodes are also moved. However, this transition causes at least one lane within the VCU to passivate if one energy-supply fails.



a) Centralized triplex architecture with GD b) X-Circuit with externally actuated PB

Figure 5.20: X-Domain systems with *semi-/smart* actuators

The provided X-Circuit architecture (Figure 5.20b), on the other hand, avoids the use of ideal diodes, similar to the architecture shown in Figure 4.35c. The difference, however, is that the externally activated default PB is already implemented in the *simple* actuator system.

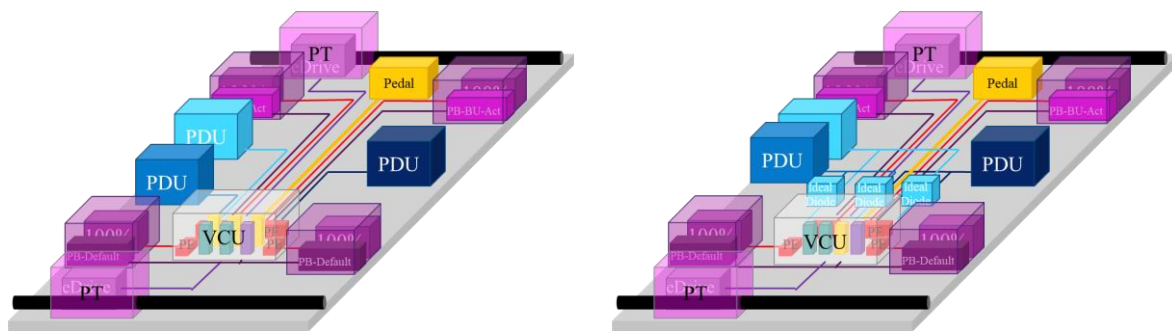
5.6.3 Dual Powertrain System with increased Availability

Dual powertrain systems can be used to improve vehicle performance (i.e., all-wheel drive) and vehicle availability (not safety-related). The previously discussed architectures can be adapted to a dual powertrain system by simply adding a PT system on the front axle, possibly controlled by the same MCU already present to improve vehicle performance. However, the goal of this section is to improve availability.

Therefore, architectures are presented that use the second powertrain to provide system architectures that establish a safe vehicle state (from a functional safety and product liability perspective) after an initial failure to improve vehicle availability. Therefore, there is a need to establish a third LV-system to provide duplex energy-supply (as presented in section 4.6) after the first failure. Furthermore, the exclusive use of ideal diodes is not sufficient to provide the required three-wheel backup after a second failure, since two ideal diodes may fail, even-

tually passivating two actuators. Obviously, some degree of redundancy is also needed in the thermal- and HV-system to significantly increase availability. However, this is beyond the scope of this work.

Simple EMB-Actuator. Centralized architectures are particularly advantageous for using GD. Therefore, two examples are presented in Figure 5.21. Both designs implement a parking-/service brake combination on each wheel. While the front axle is equipped with a PB-backup actuator (see section 4.4.2), the rear axle implements an externally actuated PB (see section 5.6.2). These options can also be installed vice versa. The difference between the two approaches shown in Figure 5.21 is the use of ideal diodes for the energy supply.



a) Centralized architecture with separate energy-supply

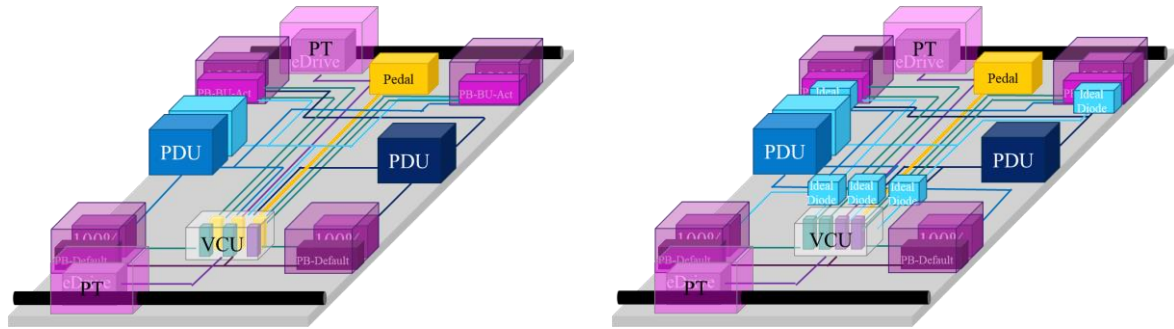
b) Centralized architecture with merged energy-supply

Figure 5.21: X-Domain highly available *simple* actuator systems

Figure 5.21a presents a design that avoids the use of ideal diodes by implementing six lanes (two brake, one PT, three spare lanes) that are equally distributed among the three energy-supplies. In addition, each energy-supply serves two brakes (service- or parking brakes) out of a total of six brakes. Therefore, only a second energy-supply shutdown will cause more than two wheels to be unbraked. It should be noted, however, that depending on which supplies have failed only one backup-PB remains on the front axle and one service brake remains on the rear axle. These two remaining brakes can be supported by powertrain recuperation, if available and by the externally actuated default brake on the rear axle. The analysis of the VCU shows that no dual-point failure of the lanes is able to passivate either the powertrain or the braking functionality. A design variant not shown is the initial allocation of the spare-lanes to the braking and powertrain functionality to improve redundancy, although this is not necessary.

The system presented in Figure 5.21b eliminates two of the six lanes mentioned above due to the cost and risk of implementing ideal diodes. The three ideal diodes are needed to compensate for the loss of two energy-supplies. The four lanes within the VCU can tolerate a first failure without losing any functionality. The number of lanes could even be reduced by the risk of a single lane failure to passivate the powertrain. The remainder of the system is very similar to the system shown in Figure 5.21a.

Semi-/Smart EMB-Actuator. The centralized architectures presented for *simple* EMB-actuators can be adapted for *semi-/smart* actuators, as displayed in Figure 5.22. In addition to the two architectures shown, there is a third hybrid variant. In the hybrid variant, the VCU is powered by ideal diodes reducing the number of lanes to four, while saving the ideal diodes on the front axle. This configuration ultimately allows only one backup PB after a second power failure, similar to the architecture shown in Figure 5.22a.



a) Centralized architecture with separate energy-supply

b) Centralized architecture with merged energy-supply

Figure 5.22: X-Domain highly available centralized *semi-/smart* actuator systems

In addition to the variants discussed, *semi-/smart* actuator systems offer the possibility of direct communication between the pedal box and the EMB-actuators at the wheel. Figure 5.23 shows an H-Circuit design equipped with a backup system. The backup system on the front axle provides a direct connection between the pedal box and the EMB-actuators. Therefore, a failure of the front VCU can be compensated. The failure of the VCU, itself can be caused by two lane failures when GD is applied between the brake- and PT lanes, or by the shutdown of the single energy supply. The same energy supply is used to power the backup PB on the front axle. In contrast, the front axle EMB-actuators are supplied by the other two energy supplies using ideal diodes. Therefore, these actuators can receive brake pedal data even if one of the associated energy supplies and the VCU shut down.

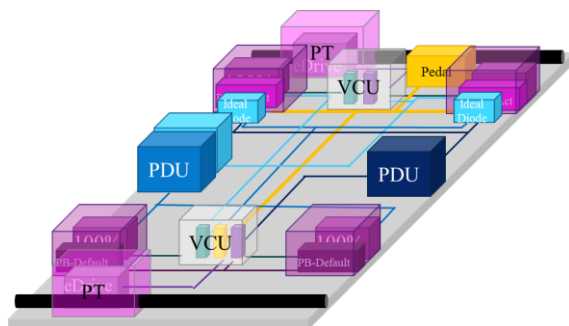


Figure 5.23: X-Domain highly available H-Circuit *semi-/smart* actuator systems

The rear axle is implemented using a triplex VCU (one brake-, PT and spare-lane), with each lane assigned to one energy supply. The rear axle actuators are only connected to a single

supply, as externally actuated default PBs may be actuated when high decelerations are requested by the driver.

5.6.4 Conclusion

One driver for the introduction of joint braking and powertrain systems is the exploitation of X-Domain redundancies. However, the analysis in section 5.6.1 shows that a frequently emphasized example, the replacement of one braking circuit by the powertrain system, is not safely applicable. Nevertheless, some synergies can be exploited. First, it is possible to decompose the SaRA requirements between the powertrain and the braking system reducing the ASIL of the braking system to ASIL C(D). Such systems are shown in section 5.6.2. Second, the application of GD can be used to reduce the number of lanes required. As an example, the evolution from a pure X-Circuit brake (Figure 4.33b) to a joint system (Figure 5.20b) with the same number of lanes can be shown.

Finally, section 5.6.3 analyzes high-availability concepts that tolerate any first failure without compromising product safety. However, the analysis shows that implementing such an over-redundant system requires an enormous effort, requiring a third energy-supply and, at least as implemented, four PB actuators. Therefore, it is concluded that it is questionable whether such systems are feasible at a reasonable cost.

6 Conclusion and Outlook

6.1 Conclusion

This work provides answers to the questions raised (see section 1.2), which are within the scope of this work. In chapter 3, requirements are derived that must be fulfilled by a safe EMB-system (*question Q.1*). Furthermore, safety concepts (*according to question Q.2*) are elaborated at the system-level for the items EMB-system and powertrain. Additionally, safety concepts for a joint EMB-system are presented to answer *question Q.3*. Finally, the two items are merged to form an X-Domain-system, which extends the answer to *question Q.3*. The results of the systems are discussed below.

Safety Goals. The Hazard Analysis and Risk Assessment (HARA) indicates that low decelerations are required for ASIL D SaRA (section 3.1). These decelerations may be sufficiently low to allow the powertrain as a backup under certain circumstances (section 3.3) from a functional safety perspective. However, the parking brake may be used to satisfy product liability requirements (section 3.2.2).

Pedal. The investigation shows that there is a potential to improve the current triplex- and quadruplex-pedal boxes. On the one hand, virtual sensors can be used to fuse sensor data collected by automated driving and active safety functions, such as Automatic Emergency Brake (AEB), to diagnose sensor failures (section 4.3.4). On the other hand, X-Domain diagnosis between the brake- and drive-pedals (section 4.3.3) can also be applied. In addition, the functionality of a failed pedal can be blended to the other pedal to increase failure-tolerance and SaRA (section 5.3.2), exploiting the X-Domain potentials. Finally, the triplex- and quadruplex-pedal boxes can be replaced by duplex sensors only, while providing sufficient safety.

EMB-Actuator. Simplex actuators (section 4.4) can be installed to meet ASIL D integrity requirements. Furthermore, the SaRA (ASIL D) is solved by distributing them on the four wheels. Therefore, it can be concluded that redundant actuators are not required from a functional safety point of view.

Central-Control-System. All central-control-system topologies (Centralized, H-/X-Circuit, Ring, section 4.5) can satisfy both ASIL D SaRA and integrity. However, the safety implementation efforts may vary, especially when considering direct connections between the pedal box and EMB-actuators. In general, centralized systems tend to be more advantageous from a functional safety perspective than the other topologies.

EMB-System. EMB-systems can satisfy both ASIL D SaRA and integrity. Generally, the central control system must be equipped with three lanes in the central ECU(s) to satisfy product liability or if the use of backup buses between pedal and EMB-actuators is waived. However, from a functional safety perspective, backup buses between the pedal and the EMB-actuator can reduce the number of lanes in the central ECU(s) to as few as one. Furthermore, it is shown that parking actuators implemented as backup brake actuators are a subtle means to ensure product liability while providing independence of the different energy supplies.

Powertrain. Current powertrain safety concepts are examined (section 5.4). It is assessed that these meet state-of-the-art QM SaRA and ASIL C integrity.

X-Domain-System. There are two approaches that can be exploited by X-Domain-systems. First, the SaRA of the braking system can be reduced to ASIL C(D), enabling new safe central-control-systems. Second, the use of graceful degradation between the braking and powertrain system can reduce the number of lanes required to safely operate a vehicle. In addition, it is analyzed that high-availability vehicle systems can be implemented with significant effort.

6.2 Outlook

This work presents safety concepts of both EMB-systems and joint EMB-powertrain systems. There are several options to further investigate the topic of this work. These are discussed below.

Focus. This work presents concepts at a high system-level that satisfy safety based on assumptions. Therefore, these assumptions have to be verified if a development towards series production is aimed. A possible starting point for the verification can be the assumed passivation time of the lanes $t_{passivation}=100\text{ ms}$. Furthermore, the failure rates of the installed components and the diagnostic coverages of the safety mechanisms must be verified. Additionally, time-dependent system behavior, such as intermittent failures, must be considered. Finally, the need to provide dissimilar implementations of the EMB-system to reduce the potential for common cause failures must be analyzed.

Adaptation. Eventually, it is very likely that the results of this work cannot be directly applied to a development for series production. Adaptations may be necessary (see section *Focus*). However, an adaptation of the findings of this work to customize the results is easily possible, since the simulation models and the tool chain exist. Nevertheless, a change may not be necessary, since the target hardware metrics regarding ASIL are only orientation values. Furthermore, small changes in diagnostic coverage and failure rates, for example, may have little impact on the results.

Expansion. Another possible next step is to expand the scope of this work by adding additional domains that strengthen the X-Domain aspects. Such an extension could include steering and/or suspension. Concepts are possible that consider torque-vectoring as a backup for

the steering system, or plow positioning of the front wheels if the steering system is implemented as single wheel actuators, to name two.

A. Product Liability

Chapter 2.3 presents the requirements that are demanded due to legislation. Besides of the legislation, product safety, from a product liability point of view, must be guaranteed. Different models for product safety, however, exist. As this work focuses on engineering instead of legal aspects, only two major models are presented shortly, others can be found in (Pepper, 2022).

The first model to be presented is **Strict Liability**. The main concern of strict liability, in the scope of this work, is to determine if a product was put into service “*in an unreasonably dangerous condition*” (Pepper, 2022). The other model that can be applied is **Negligence**. Hereby, the focus is set onto the issue if the manufacturer protected the customer “*against a foreseeable harm*” (Ross & Dorenkamp, 2020). Both models find application in jurisdiction. Whereas the European Union follows the principle of strict liability (De Luca, 2023), the jurisdiction in the US depends on the specific state (Pepper, 2022). However, as the braking systems, discussed within this work, shall be used worldwide the more demanding strict liability shall be used as the benchmark.

The key to develop ‘safe’ systems, under strict liability jurisdiction, is to define the terminology “*unreasonable danger*”. One aspect that should be met to avoid unreasonable danger, is the regulation. However, compliance to the regulation may not suffice if “*reasonable measures would suggest additional precautions*” (Pepper, 2022). Besides of meeting the regulation, liability could be avoided by confirming to industry standards (Boyd & Ingberman, 1995), as ISO 26262 is for functional safety. Additionally, the current state of the art concerning safety needs to be considered under strict liability. Liability could eventually be avoided if “*no competing product is safer*” (Boyd & Ingberman, 1995).

The “*no product is safer*” argument shall be discussed within this paragraph. The nominal braking performance of braking systems is a deceleration of approx. $a_x \geq 10 \text{ m/s}^2$ without any apparent fault. After a first fault, regulation demands a remaining deceleration of $a_x \geq 2.44 \text{ m/s}^2$ (United Nations ECE, 2015). The current state of the art is, however, a deceleration of $a_x \geq 6.4 \text{ m/s}^2$ as Bauer et al. (Bauer, et al., 2017) outline, showing that only meeting the regulation does not suffice to avoid strict liability.

Finally, it can be concluded that in the scope of this work, product liability can be avoided due to:

- Meeting regulation;
- The application of norms (i.e., ISO 26262);
- A nominal deceleration of $a_x \geq 10 \text{ m/s}^2$ and
- A remaining deceleration of $a_x \geq 6.4 \text{ m/s}^2$ after a first fault.

B. Hardware Part Failure Rates

B.1 Approximation of the exponential distribution

Fig. B.1 relates the *failure rates* $\lambda \in \{10^{-5} \text{ 1/h}, 10^{-6} \text{ 1/h}, 10^{-7} \text{ 1/h}, 10^{-8} \text{ 1/h}\}$ of generic components to the *approximation error* due to equation (2.8). Herein, the scale of the *approximation error* is reduced by two magnitudes compared to the respective *failure rates*. It becomes obvious that the error of the approximation remains insignificant ($< 1\%$), at least for *failure rates* $\lambda \leq 10^{-6} \text{ 1/h}$ and *operation times*³³ $t \leq 10,000 \text{ h}$.

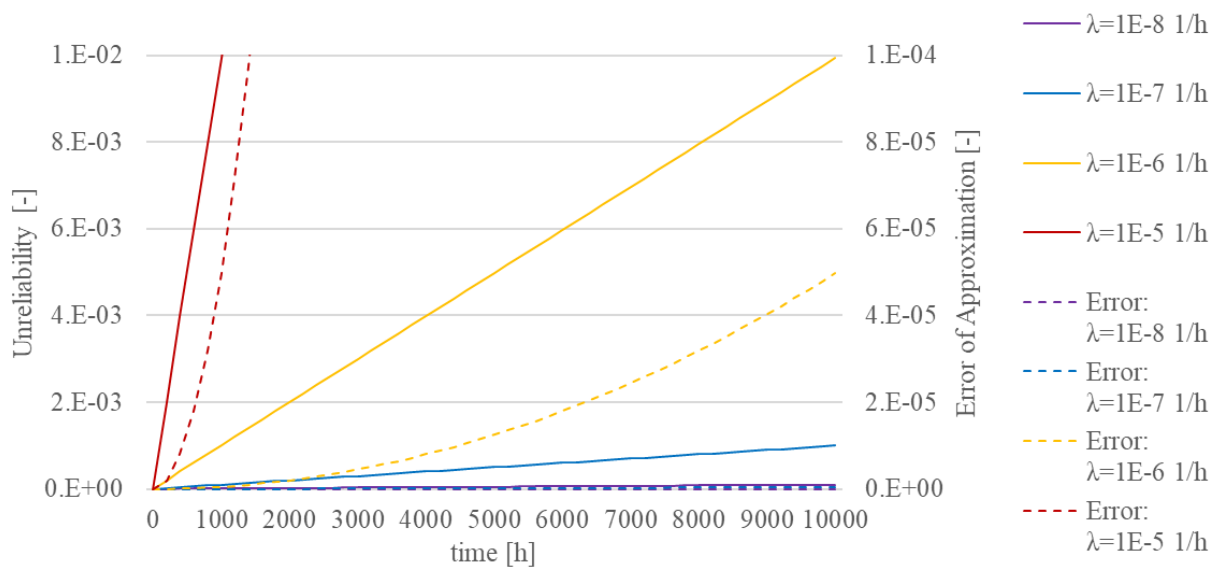


Fig. B.1: Impact of the approximation of the exponential distribution

³³ (International Organization for Standardization, 2018) provides $t_{operation} = 10,000 \text{ h}$ as a reference

B.2 E/E Components

Component	Function	Type	λ_{ref}	λ_{inst}	α_{fp}	α_{fooc}	α_{fd}	Cost
Unit			[10 ⁻⁹ 1/h]	[10 ⁻⁹ 1/h]	[%]	[%]	[%]	[%]
Harness	Power Wire	Front	5	5.00	64	0	36	1
		Rear	5	5.00	64	0	36	0
	COM-Wire	-	5	5.00	100	0	0	2
Processing Unit	VCU (ESP only, Dual-Core)	SW-Self-Test	50	472.53	60	40	0	36
		Lockstep	50	472.53	99	1	0	57
	VCU (ESP + ABS, Dual-Core)	SW-Self-Test	50	472.53	60	40	0	57
		Lockstep	50	472.53	99	1	0	89
	Smart WECU (Single Core)	SW-Self-Test	50	236.27	60	40	0	34
		Lockstep	50	236.27	99	1	0	52
	Semi-Smart WECU	SW-Self-Test	20	52.74	60	40	0	30
		Lockstep	20	52.74	99	1	0	54
Watchdog	(->DC=90%)	0	1.54	100	0	0	1	
Flash	VCU (ESP only)	Parity Bit	40	105.48	60	40	0	2
		Block Replica	40	105.48	99	1	0	3
	VCU (ESP + ABS)	Parity Bit	50	131.85	60	40	0	2
		Block Replica	50	131.85	99	1	0	4
	Smart WECU	Parity Bit	30	79.11	60	40	0	2
		Block Replica	30	79.11	99	1	0	3
RAM	VCU (ESP only)	Parity Bit	10	26.37	60	40	0	3
		Pattern Test	10	26.37	90	10	0	3
		Checksum	10	26.37	99	1	0	4
	VCU (ESP + ABS)	Parity Bit	10	26.37	60	40	0	4
		Pattern Test	10	26.37	90	10	0	4
		Checksum	10	26.37	99	1	0	5
	Smart WECU	Parity Bit	20	52.74	60	40	0	2
		Pattern Test	20	52.74	90	10	0	2
		Checksum	20	52.74	99	1	0	3
Oscillator	Oscillator	-	77.00	100	0	0	9	
Housing	Housing	-	0.00	0	0	0	2	
Analog Input	ADC	-	55.00	100	0	0	1	
Bus Interface	Ethernet Adapter	1-Bit HW-Red.	10	25.80	60	40	0	4
		Transmiss.Red.	10	25.80	90	10	0	5
		Test Pattern	10	25.80	99	1	0	6
	SPI Adapter	1-Bit HW-	5	13.19	60	40	0	0

Component	Function	Type	λ_{ref}	λ_{inst}	α_{fp}	α_{fooc}	α_{fd}	Cost
Unit			[10 ⁻⁹ 1/h]	[10 ⁻⁹ 1/h]	[%]	[%]	[%]	[%]
		Red.						
		Transmiss. Red.	5	13.19	90	10	0	0
		Test Pattern	5	13.19	99	1	0	1
Power Supply	Local Power Supply Unit	-	10	32.34	100	0	0	3
	Ideal Diode	-	20	59.00	100	0	0	12
	PDU	-	-	2000	28	0	72	-
Sensor	eMotor Angle	Valid Range	10	52.74	60	0	0	6
		Rationality Check	10	52.74	90	0	0	7
	Current	Valid Range	10	52.74	60	0	0	3
		Rationality Check	10	52.74	90	0	0	3
Powertrain	Power Electronics		-	12260	50	0	50	-
Actuation Unit	Power Electronics		-	6130	50	0	50	5

B.3 Mechanic Components

Component Unit	λ_{ref} [10 ⁻⁹ 1/h]	FM [-]	Share [-]	λ_{FM} [10 ⁻⁹ 1/h]	Cost [‰]		
Electric Motor ³⁴	2682	(U.S. Department of Defense, 1991)	1	75%	(U.S. Department of Defense, 1998),	2012	725
			2	22%	(U.S. Department of Energy National Laboratory, 2018)	590	
			3	1%		27	
			4	0.03%		1	
Gears	500	(U.S. Department of Energy National Laboratory, 2018)	1	59%	(U.S. Department of Defense, 1998),	295	2
			2	33%	(U.S. Department of Energy National Laboratory, 2018)	165	
			3	8%		40	
			4	0.2%		1	
Piston	7	(U.S. Department of Energy National Laboratory, 2018)	1	100%	(U.S. Department of Energy National Laboratory, 2018)	7	3
Solenoid Actuator for Parking	96	(U.S. Department of Defense,	1	57%	(U.S. Department of Defense,	96	3
			2	43% ³⁵		-	

³⁴ Determined with Temperature Distribution in (Standardization, 2021), Mobile Application, and Space-Factor of 1.5

³⁵ Is assumed to prohibit full retraction of latch and therefore causes fp (FM1)

		1991)			1991)		
Latch for Parking	7	(U.S. Department of Energy National Laboratory, 2018)	1	100%	(U.S. Department of Energy National Laboratory, 2018)	7	0
Spring for Default	1040	(U.S. Department of Energy National Laboratory, 2018)	1	100%	(U.S. Department of Energy National Laboratory, 2018)	1040	0

C. Additional Information on the Safety Assessment

C.1 Reference Vehicles

The vehicle type data provided in Fig. C.1 is used to determine the driving-dynamic principles of section C.2 and may differ from the actual properties of the real vehicles to a small extent. The inertia (of the z-axis (vertical to the plain earth)) of the electric vehicles is hereby determined by assuming a cuboid with the lengths of the wheelbase and the lateral expansion y .

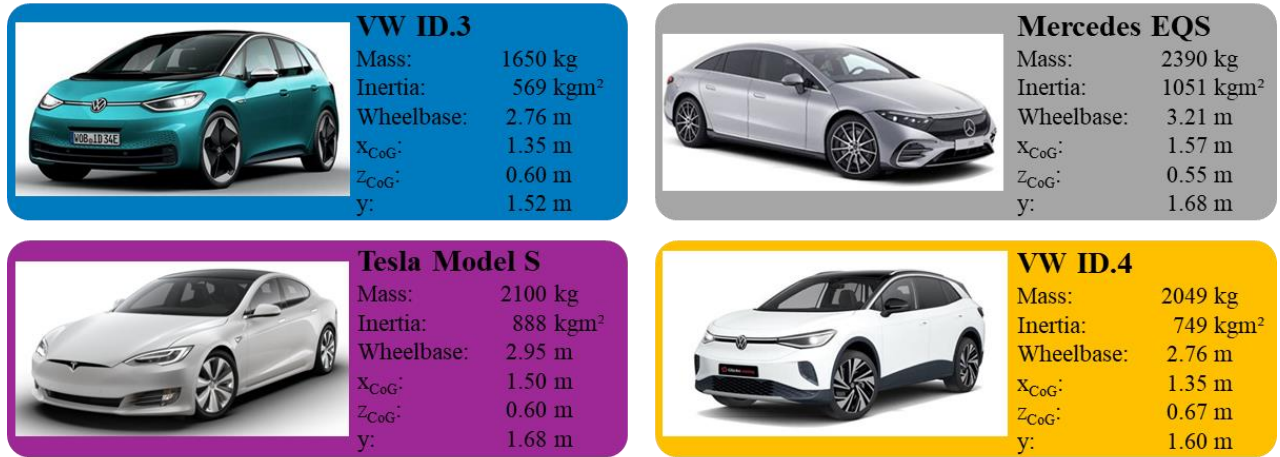


Fig. C.1: Reference vehicles, pictures by (carwow Ltd., 2023), (Mercedes-Benz AG, 2023), (greencarreports, 2023), (glücksleasing, 2023)

C.2 Driving-Dynamics Analysis

This work focuses on functional safety. Driving dynamics need, however, to be considered to determine the consequences of potential malfunctions and their safety impact. The results of the analyses are used to determine the ASIL of the SG and finally represent the development requirements of the chapters 4 and 5. The driving physics of section C.2.1 are retrieved from (Mitschke & Wallentowitz, 2014), if not stated otherwise.

C.2.1 Basic Driving Physics

a) Reference coordinate system

The coordinate system of DIN ISO 8855 is used.

b) Ideal Brake Force Distribution

At first, the *braking* b is introduced (Eq. C.1) that is defined by the *deceleration* a and the *gravitational constant* g . Then, the tire loads on the front F_{ZF} and the rear axle F_{ZR} depend on the *braking* b and on the distance of the Centre of Gravity (CoG) to the rear axle x and the

street z in reference to the *wheelbase* l and the *mass* m . The equations Eq. C.2 and Eq. C.3 can be referred to.

$$b = \frac{a}{g} \quad \text{Eq. C.1}$$

$$F_{zF} = m \cdot g \left(\frac{l - x_{CoG}}{l} + \frac{z_{CoG}}{l} b \right) \quad \text{Eq. C.2}$$

$$F_{zR} = m \cdot g \left(\frac{x_{CoG}}{l} - \frac{z_{CoG}}{l} b \right) \quad \text{Eq. C.3}$$

c) Friction Circle

A commonly used approach to determine the maximum transferable forces in x and y direction (F_x and F_y) between tire and road is the so-called *friction circle*, introduced by Prof. Dr.-Ing. E. H. W. Kamm. Herein, the maximum force depends directly on the *friction coefficient* μ and the *tire load* F_z , as described in Eq. C.4. The directions x and y are given in the tire coordinate system and may represent a brake force F_x and a steering force F_y , as described in Annex C.2.1 d). Whenever the vector sum of *tire forces* F_x and F_y remain below the threshold defined by the friction circle, the wheel remains spinning. However, if the actuated forces exceed the tire forces, the wheel starts to slip.

$$\sqrt{F_x^2 + F_y^2} \leq \mu F_z \quad \text{Eq. C.4}$$

d) Lateral Tire Forces

The *lateral tire force* F_y (Eq. C.5) depends on the *slip angle of the tire* α that can be approximated, according to Eq. C.6 and Eq. C.7, for small angles. Herein, the β represents the *vehicular slip angle*, δ is the *steering angle*, v is *vehicle speed* and $\dot{\psi}$ represents the *yaw rate* of the vehicle. Finally, the *cornering stiffness* c_α can be determined by using the Pacejka magic formula.

$$F_y = c_\alpha \cdot \alpha \quad \text{Eq. C.5}$$

$$\alpha_F = -\beta + \delta_F - x_{CoG} \frac{\dot{\psi}}{v} \quad \text{Eq. C.6}$$

$$\alpha_R = -\beta + (l - x_{CoG}) \frac{\dot{\psi}}{v} \quad \text{Eq. C.7}$$

e) Force and Momentum equilibrium

The equations Eq. C.8-Eq. C.10 provide the planar *force/momentum equilibria* for a vehicle (refer to Fig. C.2). As this work focuses on functional safety and not on driving dynamics, a

very simple, extended single-track model is used. The extension of the single-track model refers to the lateral distribution of the *tire forces* F . The simplification consists of neglecting all resistances (roll, aerodynamics, slope etc.) and assuming an equal steering angle on the right and the left side.

$$x: \quad F_x = (F_{x,RR} + F_{x,RL}) \cos(\beta) + (F_{x,FR} + F_{x,FL}) \cos(\beta - \delta) - 2 \cdot F_{y,R} \sin(\beta) - 2 \cdot F_{y,F} \sin(\beta - \delta) \quad \text{Eq. C.8}$$

$$y: \quad F_y = 2 \cdot F_{y,R} \cos(\beta) + 2 \cdot F_{y,F} \cos(\beta - \delta) + (F_{x,RR} + F_{x,RL}) \sin(\beta) + (F_{x,FR} + F_{x,FL}) \sin(\beta - \delta) \quad \text{Eq. C.9}$$

$$M_z: \quad M_z = 2 \cdot F_{y,R}(l - x_{CoG}) + (F_{x,RR} - F_{x,RL})y - 2 \cdot F_{y,F} \cos(\delta) x_{CoG} + (F_{x,FR} - F_{x,FL}) \cos(\delta) y + (F_{x,FR} - F_{x,FL}) \sin(\delta) x_{CoG} \quad \text{Eq. C.10}$$

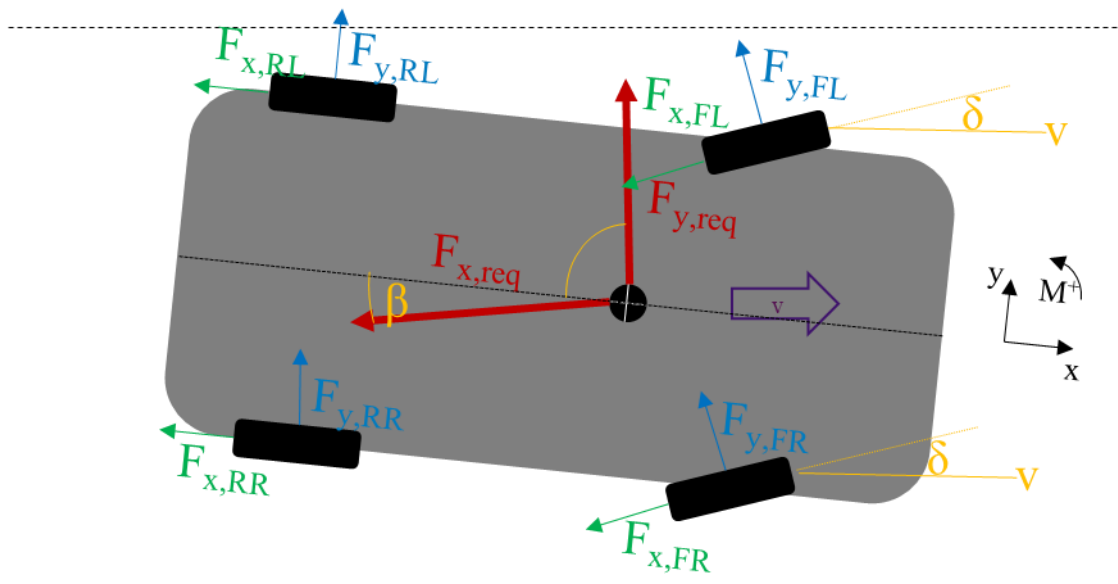


Fig. C.2: Forces at the vehicle

C.2.2 Simulation Approach

The approach being used for the simulations consists of manipulating the *tire forces* F_x at the defective wheel(s). This manipulation is either a constant braking in case of an *uncommanded braking* malfunction (refer to *fooc*) or no braking in case of a *fp*-behavior of the brake. A *degradation* of the brake remains out of scope to limit the work effort but could be simulated in the future. Four configurations accounting for the automatization degree are differentiated according to Table 3.6.

a) No Steering Assist (Config 1-3)

The Config 1-3 tend to yaw. Herein the Config 1 yaws always (from $a_x > 0 \text{ m/s}^2$), the Config 2 and 3 yaw only if the brake forces cannot be applied balanced (left and right) for the required decelerations. This yawing or applied momentum is modelled, assuming a similarity to lateral wind gusts, as described in (Maruyama & Yamazaki, 2003). Hereby, the driver is assumed to start a counter-steering at $t_{counter-steer} = 0.6 \text{ s}$ that eliminates the yaw after $t_{max.deviation} = 1.1 \text{ s}$.

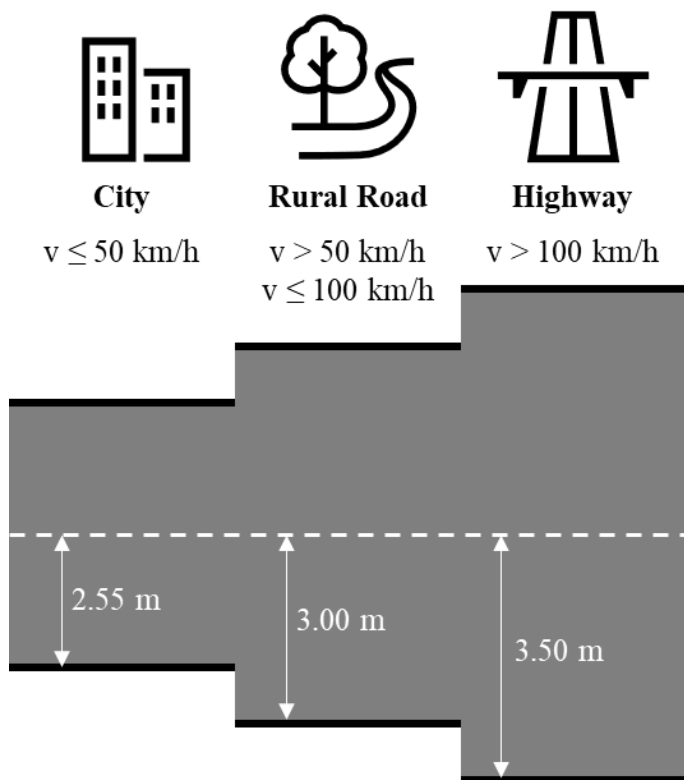


Fig. C.3: Infrastructure-based lateral constraints

Furthermore, lateral hazards are considered, depending on the infrastructure and the velocity, as shown in Fig. C.3. Additionally, the permissible lateral deviation is linked to an E, as defined in Tab. C.1.

Tab. C.1: Exposure linked to the permissible lateral deviation

Δy Lateral Displacement [m]	E2	E3	E4
City	≈ 0.12	≈ 0.25	≈ 0.37
Rural Road	≈ 0.20	≈ 0.40	≈ 0.60
Autobahn	≈ 0.28	≈ 0.56	≈ 0.85

b) Steering Assist (Configuration 4)

In contrast to the Configs 1-3, Config 4 does not allow for any lateral deviations. Therefore, Eq. C.10 is restricted to Eq. C.11.

$$M_z: \quad M_z = 0 \quad \text{Eq. C.11}$$

c) Operation Point Evaluation

The equations Eq. C.8 – Eq. C.11 are applied to evaluate all the operation points described in section 3.1. Hereby, the *required Forces* F_x and F_y to actuate a certain *lateral* and *longitudinal acceleration* a are determined as specified in the equations Eq. C.12 and Eq. C.13.

$$x: \quad F_x = m \cdot a_x \quad \text{Eq. C.12}$$

$$y: \quad F_y = m \cdot a_y \quad \text{Eq. C.13}$$

C.2.3 Results (excerpt)

This section presents the results of the simulation described in the preceding section C.2.2. These results can be divided into the driving capabilities during a *fp* malfunction (refer to sections a)-f)) and an *uncommanded braking* malfunction (refer to sections g)-k)) of the braking system. However, as presenting the capabilities of all four vehicle types, in detail, for the complete operation space (as defined in section 3.1) for all failure patterns would exceed the scope of this annex, only the results for an VW ID.3 under high friction coefficient conditions (μ_{high}) at the speed $v_{start} = 50 \text{ km/h}$ are shown in the following figures. Nonetheless, the other simulations are conducted and are considered for the results presented in section 3.2. Sub-section C.2.3 a) presents the figure-scheme in detail that is applied for the other sub-sections, as well.

a) Front Actuator *fp*-Failure

Fig. C.4 shows an operation space consisting of the *lateral acceleration* a_y and the *deceleration* a_x for the four different automatization degrees of a VW iD.3 at the *speed* $v_{start} = 50 \text{ km/h}$. The color of the bubbles (refer to the legend) represents the ASIL of the respective operational state. However, a discrimination needs to be made between the small bubbles and the big bubbles. The small bubbles refer to ASILs that originate from lateral hazards (as defined in section C.2.2 a)). It can be easily seen that only the Configs 1-3 inherit such ‘lateral’ hazards as these configurations may excure the lane, whereas configuration 4 only consists of small bubbles being grey. The big bubbles, at the top of the columns, represent the ASIL related to the maximum deceleration, not accounting for the lateral deviations and hazards.

Furthermore, the Configs 2 and 3 inherit a marker that describe the maximum deceleration that is applicable before lateral decelerations need to be tolerated, in this case $a|_{0;4} = 4.2 \text{ m/s}^2$ and $a|_{0;3} = 3.9 \text{ m/s}^2$ respectively, when driving straight.

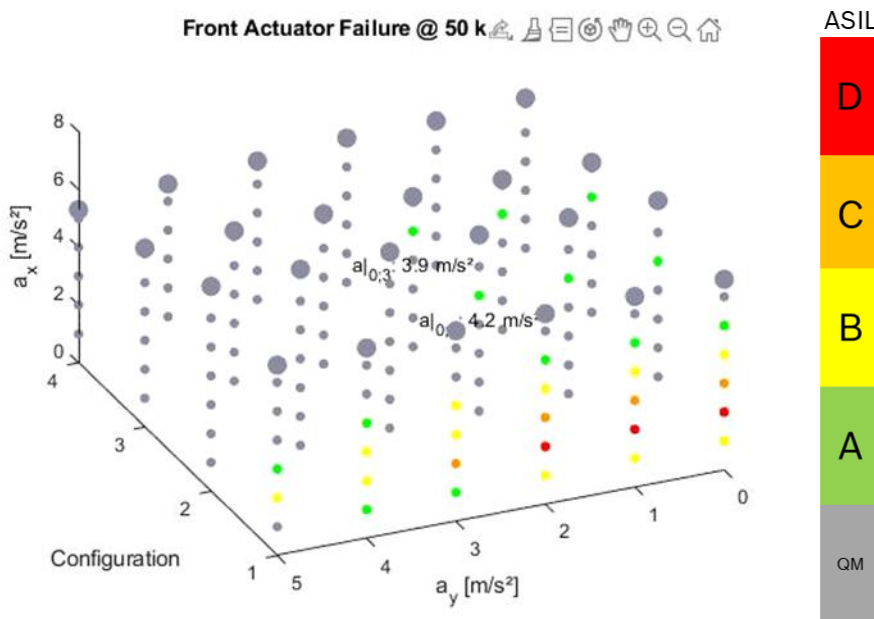


Fig. C.4: Driving-dynamic capabilities during front actuator *fp*-failure

Fig. C.4 indicates that Config 1 inherits an ASIL D for a front actuator *fp* failure, as medium decelerations of $a_x = 2 \text{ m/s}^2$ provoke a very strong yawing of the vehicle. In the contrary, the other configurations can avoid such a classification by applying at least a smart brake force distribution. However, applying only a smart brake force distribution classifies a front actuator *fp*-failure as ASIL A that can only be avoided by additionally applying a steering assist.

b) Rear Actuator *fp*-Failure

The yaw-tendency during a rear actuator *fp*-failure of Config 1 is lower than that of a front actuator *fp*-failure. This is caused by the dynamic brake force distribution that applies only $\sim 1/3$ of the brake force on the rear axle that causes a smaller brake force imbalance between the left and the right wheels. Nonetheless, a rear actuator *fp*-failure is classified as ASIL C for configuration 1. Configurations 2-4 seem to tolerate such a failure quite easily with a QM.

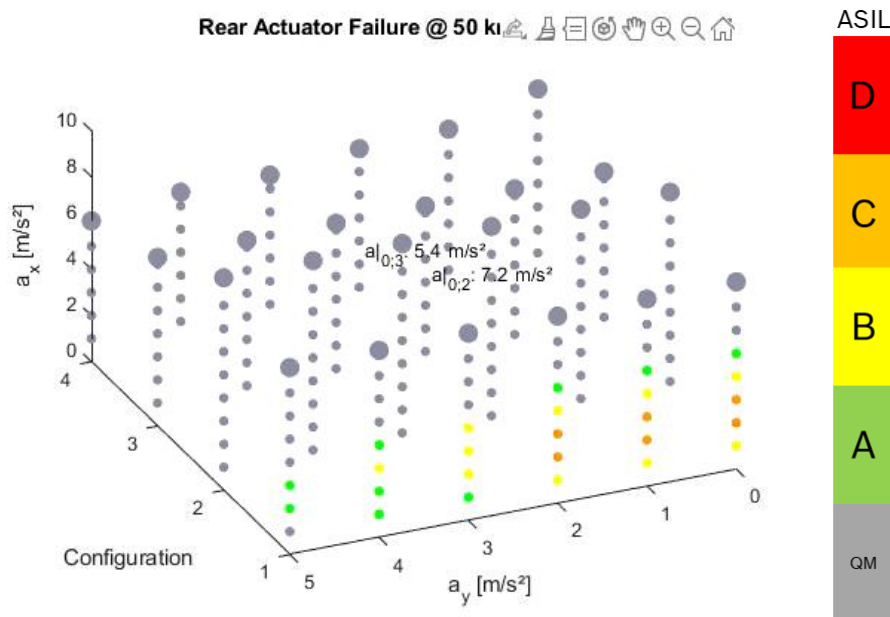


Fig. C.5: Driving-dynamic capabilities during rear actuator failure

c) X-Circuit *fp*-Failure

Config 1 is implemented in a way that the brake force is not further incremented, if one wheel exceeds the friction circle. This implementation restricts Config 1 to achieve only medium decelerations eventually causing ASIL A, as displayed. However, the deceleration is further deteriorated under μ_{medium} conditions, eventually classifying configuration 1 as ASIL B. The configurations 2 and 3 achieve ASIL A, because of provoking lateral displacement at high decelerations.

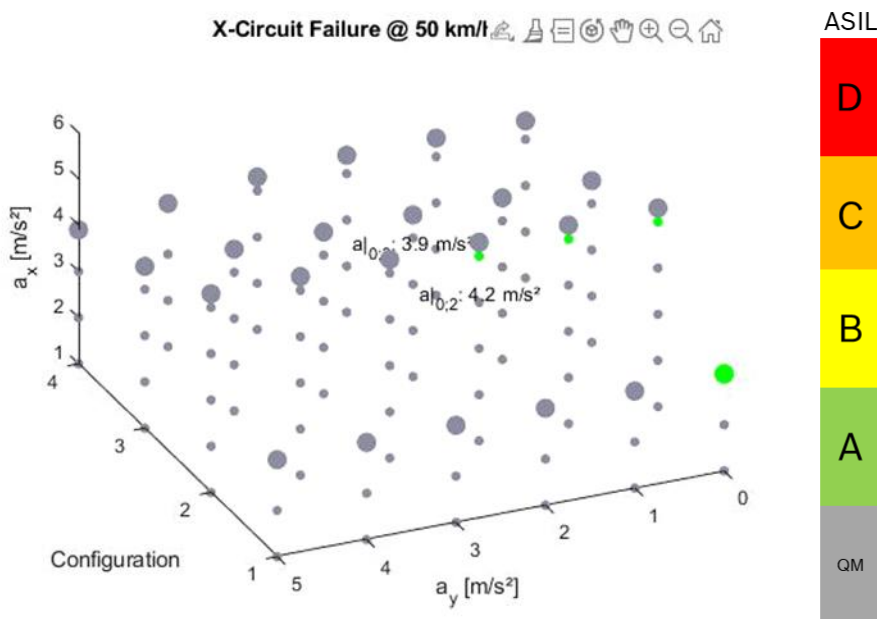


Fig. C.6: Driving-dynamic capabilities during X-Circuit failure

d) H-Circuit Rear *fp*-Failure

H-Circuit failures do not provoke any yawing causing all operation states being assessed as QM from a lateral perspective. Additionally, as the rear axle only contributes $\sim 1/3$ of the braking performance, the maximum (degraded) deceleration is assessed as QM, as well, at least for $v_{start} = 50 \text{ km/h}$. However, under μ_{low} conditions, the rear axle *fp* failure causes an ASIL A classification for all configurations.

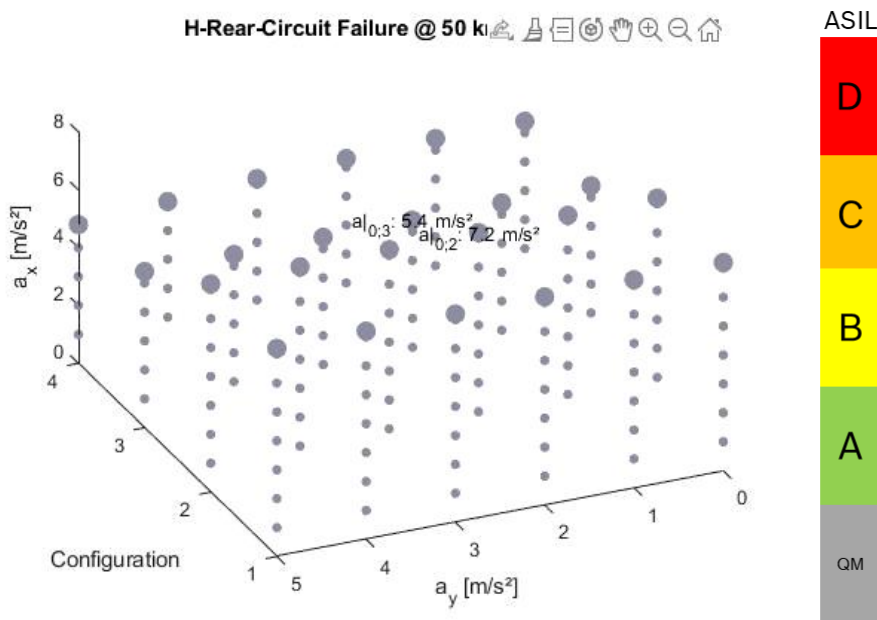


Fig. C.7: Driving-dynamic capabilities during H-Circuit rear failure

e) H-Circuit Front *fp*-Failure

The statements of the H-Circuit rear remain the same for the H-Circuit front *fp* failure that is classified as ASIL A for all configurations.

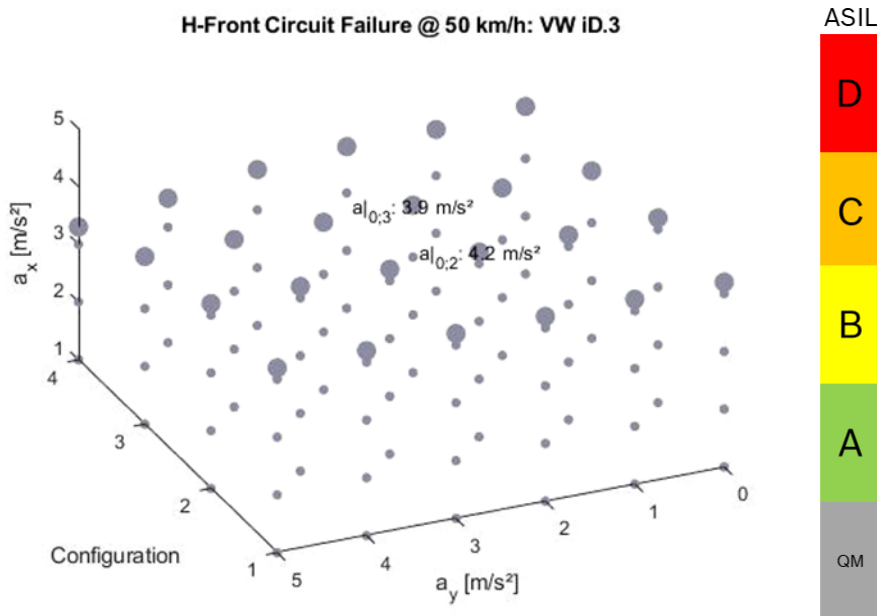


Fig. C.8: Driving-dynamic capabilities during H-Circuit front failure

f) Summary *fp*-Failure

It is clearly indicated that a smart brake force distribution may help to lower the ASIL of both complete brake-circuit and actuator *fp*-failures from ASIL D to ASIL A, eventually. This highlights the need of such a functionality for future braking systems. Furthermore, it is shown that all brake circuits may be developed by ASIL A from a driving-dynamics perspective³⁶. A steering assist may only lower the ASIL gradually.

g) Front Actuator uncommanded Braking

Fig. C.9 shows the ASIL assessments of the operation space due to the lateral displacement that is provoked by a single front actuator *uncommanded* braking event. Referring to the scale on the right, it becomes obvious that the ASIL of such a malfunction is rising fast, establishing an ASIL D for a deceleration of $a_{x,uncommanded} \geq 0.5 \text{ m/s}^2$. This amount of brake imbalance is assessed as intolerable by ECE R13-H (United Nations ECE, 2015), as well.

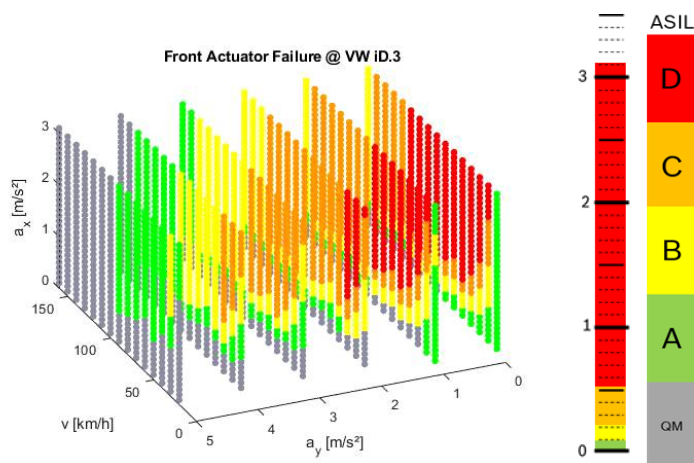


Fig. C.9: Driving-dynamic capabilities during front actuator uncommanded braking failure

h) Rear Actuator uncommanded Braking

Fig. C.10 shows that an *uncommanded* braking event causes the same ASIL assessment independent of the axis it appears.

³⁶ Important note: This statement ignores any decomposition rules of ISO26262 that need to be applied, as well!

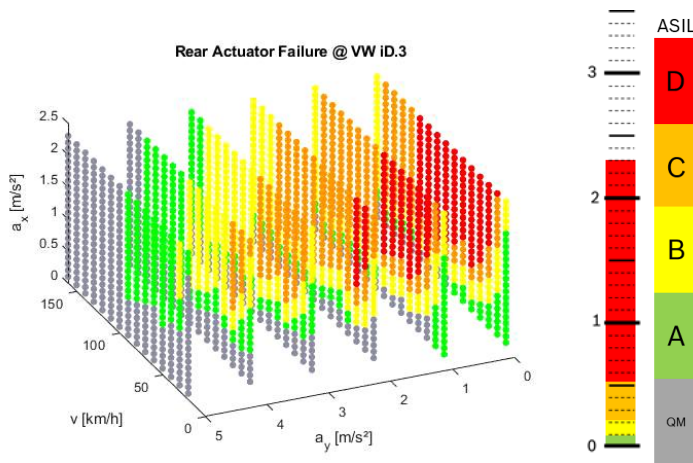


Fig. C.10: Driving-dynamic capabilities during rear actuator uncommanded braking failure

i) X-Circuit uncommanded Braking

In contrast to the previously described actuator failures, an *uncommanded* braking malfunction of a X-Circuit can be tolerated up to a deceleration of $a_{x,uncommanded} < 3 \text{ m/s}^2$ without provoking an ASIL D classification. This is caused by the *uncommanded* brake force appearing both on the right and on the left side, however distributed with an imbalance of 1/3 on the rear and 2/3 on the front axle. This imbalance causes high decelerations to eventually cause ASIL D malfunctions, as well.

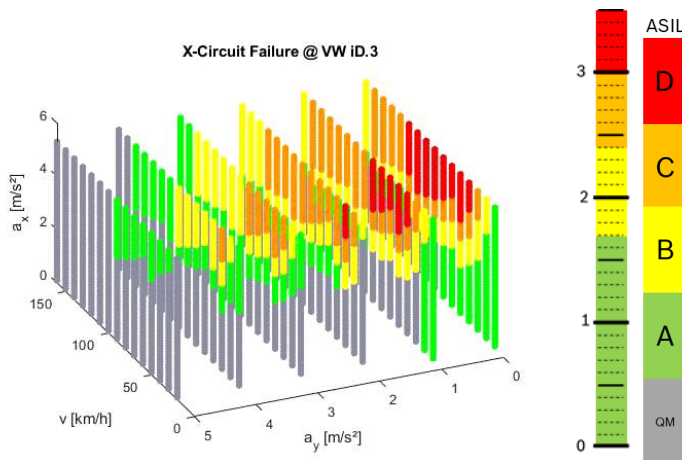


Fig. C.11: Driving-dynamic capabilities during X-Circuit uncommanded braking failure

j) H-Circuit uncommanded Braking

As the failure is symmetric, lateral deviations remain only residual. Additionally, as section 3.1.5 shows, only major *uncommanded* decelerations may provoke an ASIL-capable malfunction. These major decelerations cannot be applied due to a single circuit failure, despite of a H-Circuit front *uncommanded braking* failure of a VW ID.4 that is assessed as ASIL B with a maximum deceleration of $a_{x,uncommanded,max} = 7.5 \text{ m/s}^2$ under μ_{high} conditions.

k) Summary uncommanded Braking

Uncommanded braking events may provoke malfunctions classified of up to ASIL D, due to the strong induced yawing and the subsequent lateral deviation. This holds especially true for single actuator failures. However, these failures may be mitigated by applying an equal force onto the wheels of the other side to balance the brake forces.

D. Overview of the capabilities of vehicles to recuperate energy

D.1 Basic physics

Eq. D.1 shows that the *force* F depends directly on the *mass* m and the *deceleration* a of the vehicle. Furthermore, Eq. D.2 shows that the *power* P to recuperate is related to the actuated *force* F by the powertrain and the *vehicle speed* v .

$$F = m \cdot a \quad \text{Eq. D.1}$$

$$P = F \cdot v \quad \text{Eq. D.2}$$

Eq. D.3 inserts Eq. D.2 in Eq. D.1 to relate the *deceleration* a to the *specific power* P/m and the *vehicle speed*. It becomes obvious that the deceleration of a vehicle directly depends on its specific power.

$$a = \frac{P}{m} \cdot \frac{1}{v} \quad \text{Eq. D.3}$$

D.2 Exemplary powertrains of vehicles in the market

A quick internet research is conducted to evaluate current specific powers of electric vehicles in the market. The raw data is provided by Tab. D.1. Fig. D.1 provides an overview and shows that these vary between 0.016 kW/kg and 0.248 kW/kg

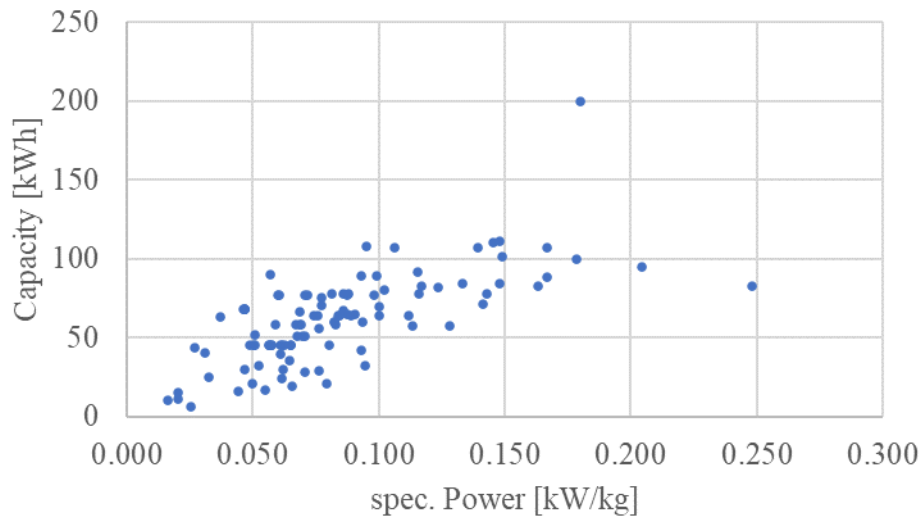


Fig. D.1: Exemplary specific Powers of electric vehicles

Tab. D.1: Overview of some electric vehicles on the market

Name	Mass [kg]	Power [kW]	Source	Name	Mass [kg]	Power [kW]	Source
Audi Q4 e-tron	2125	150	(EV Database, 2023)	Mazda MX-30	1720	107	(EV Database, 2023)
Audi Q8 e-tron	2520	250	(Audi AG, 2022)	Merc. EQA	2040	140	(evspecifications.com, 2023)
BMW i3	1345	125	(BMW AG, 2023)	Merc. EQB	2140	165	(Edmunds.com, Inc., 2023)
BMW i7	2684	400	(BMW AG, 2022)	Merc. EQC	2940	300	(EV Database, 2023)
BMW iX40	2440	240	(BMW AG, 2023)	Merc. EQE	2310	215	(evspecifications.com, 2023)
BMW iX50	2567	380	(Wikipedia, 2023)	Merc. EQS	2539	242	(Edmunds.com, Inc., 2023)
Boll. Bluecar	1070	50	(WatteV2Buy, 2023)	Merc. EQV	2635	150	(EV Database, 2023)
Buddy Cab	795	13	(Infogalactic, 2016)	Mini Cooper SE	1426	135	(Edmunds.com, Inc., 2023)
BYD ATTO 3	1825	150	(EV Database, 2023)	Mini Countryman	1775	135	(MINI UK, 2023)
BYD Han	2325	380	(EV Database, 2023)	Mits. I-MiEV	1100	49	(EV Compare, 2023)
BYD Tang	2564	380	(EV Database, 2023)	Nissan Ariya	1961	160	(Nissan USA, 2023)
Chev. Bolt EUV	1685	147	(Edmunds.com, Inc., 2023)	Nissan Leaf	1592	110	(Nissan USA, 2023)
Chev. Bolt EV	1628	147	(Edmunds.com, Inc., 2023)	Opel Astra e	1700	115	(EV Database, 2023)
Chev. Spark EV	1300	103	(Car and Driver, 2023)	Opel Combo e	1764	100	(EV Database, 2023)
Citr. eBerlingo	1739	100	(EV Database, 2023)	Opel Corsa e	1530	100	(EV Database, 2023)

Citr. E-C4	1636	100	(EV Database, 2023)	Opel Mokka e	1598	100	(EV Database, 2023)
Citr. E-C4 X	2040	100	(EV Database, 2023)	Opel Vivaro-e	2140	100	(EV Database, 2023)
Citr. E-Jumpy	2140	100	(EV Database, 2023)	Peug. E-Expert	2131	100	(EV Database, 2023)
Cupra Born	1811	150	(EV Database, 2023)	Peug. E-2008	1623	100	(EV Database, 2023)
Cupra Born	1946	170	(EV Database, 2023)	Peug. E-308	1650	115	(EV Database, 2023)
Dacia Spring	1012	33	(EV Database, 2023)	Peug. e-Rifter	1765	100	(EV Database, 2023)
DS 3 E-Tense	1625	115	(EV Database, 2023)	Peug. e-Traveller	1982	100	(EV Database, 2023)
Fiat 500e	1352	83	(Wolf, 2020)	Polestar 2	2198	170	(EV Database, 2023)
Fiat E-Ulysse	2167	100	(EV Database, 2023)	Polestar 3	2584	360	(EV Database, 2023)
Fiat E-Ulysse	1969	100	(EV Database, 2023)	Porsche Taycan	2125	300	(EV Database, 2023)
Fisker Ocean	2300	410	(EV Database, 2023)	Ren. Kangoo e	1870	51	(EV Database, 2023)
Ford eFocus	1633	107	(EV Charge +, 2023)	Ren. Megane e	1711	160	(EV Database, 2023)
Ford Mach-E	1948	196	(Hearst Autos, Inc., 2023)	Ren. eTwingo	1208	60	(EV Database, 2023)
Genesis G80	2325	272	(EV Database, 2023)	Ren. Twizy	474	12	(Ecomotors Inc., 2023)
Genesis GV60	2210	316	(Edmunds.com, Inc, 2023)	Ren. Zoe	1577	80	(EV Database, 2023)
GMC Hummer	4082	735	(Edmunds.com, Inc., 2023)	RR Spectre	2955	430	(EV Database, 2023)
Honda e	1595	113	(EV Database, 2023)	Skoda iV60	1965	132	(EV Database, 2023)

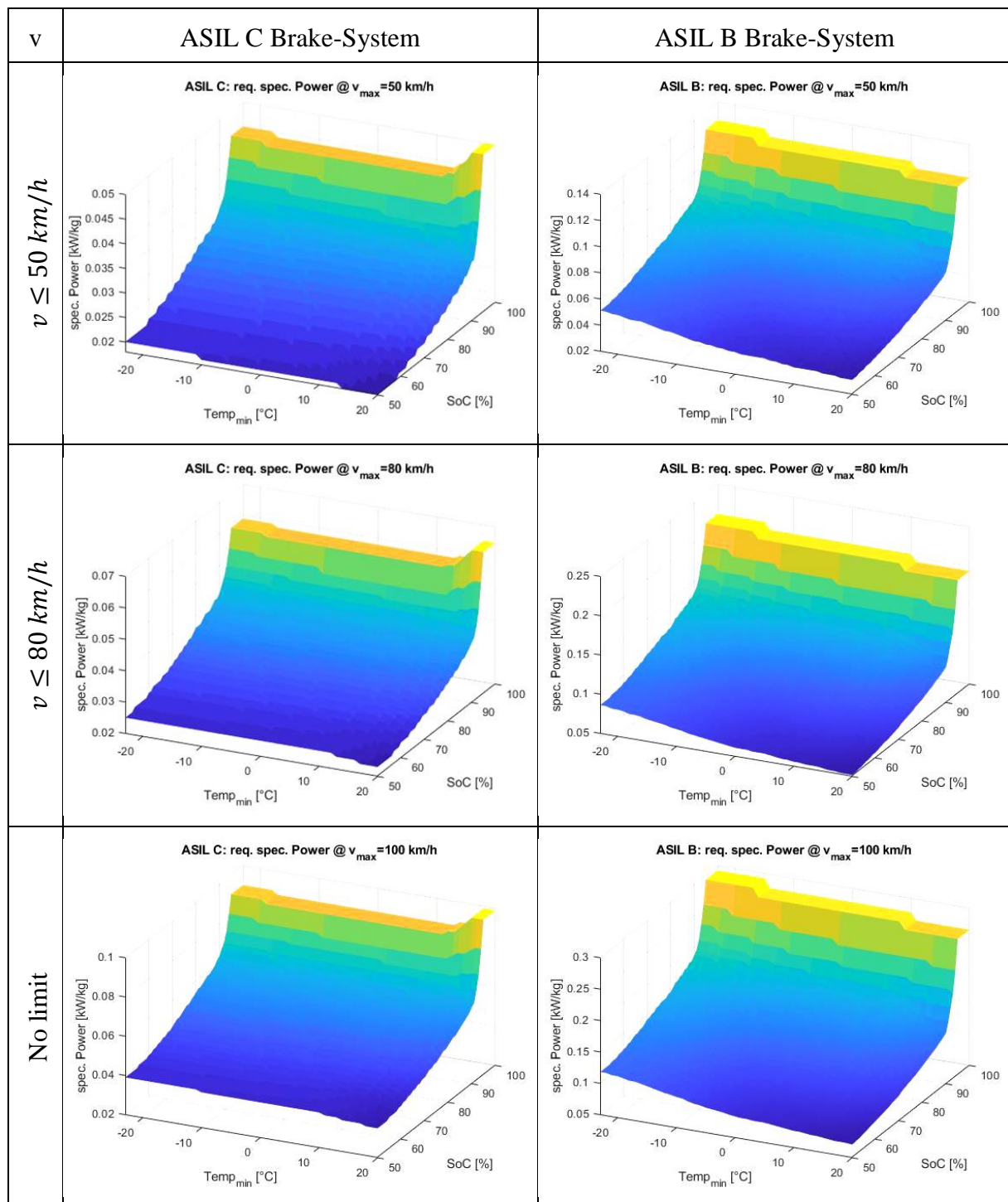
Hy. Ioniq 5 SE	1905	168	(Hyundai Motor America, 2023)	Skoda iV80	2090	150	(EV Database, 2023)
Hy. Ioniq 5 SEL	2062	168	(Hyundai Motor America, 2023)	Smart 1	2213	200	(EV Database, 2023)
Hy. Ioniq 5	1800	125	(Hyundai Motor America, 2023)	Smart Fortwo	1310	60	(EV Database, 2023)
Hy. Kona e	1685	150	(Hyundai Motor America, 2023)	SY Ko-rando	1840	140	(EV Database, 2023)
Jaguar iPace	2208	294	(EV Database, 2023)	Sub. Solterra	2110	160	(EV Database, 2023)
Kia EV6 GT	2059	239	(KIA Media, 2023)	Tesla M. 3	1835	208	(EV Database, 2023)
Kia EV6 Light	1822	125	(KIA Media, 2023)	Tesla M. X.	2444	500	(EV Database, 2023)
Kia EV6 Wind	1950	168	(KIA Media, 2023)	Tesla M. Y	1992	255	(EV Database, 2023)
Kia Niro EV	1748	148	(KIA Media, 2023)	Toyota bZ4X	2020	150	(EV Database, 2023)
Kia Soul EV	1757	148	(KIA UK, 2023)	Toyota Proace	1739	100	(EV Database, 2023)
Kia Soul EV	1610	99	(KIA UK, 2023)	VinFast VF 8	2100	260	(EV Database, 2023)
Lexus RZ	2296	230	(EV Database, 2023)	VinFast VF 9	2600	300	(EV Database, 2023)
Lexus UX300e	1860	150	(EV Database, 2023)	Volvo EX90	2818	300	(EV Database, 2023)
Lightyear 0	1575	130	(EV Database, 2023)	Volvo XC40	2030	175	(EV Database, 2023)
Lotus Eletre	2700	450	(EV Database, 2023)	VW eGolf	1569	101	(Edmunds.com, Inc., 2023)

Lucid Air	2150	358	(EV Charge +, 2023)	VW eUp	1160	61	(Volkswagen AG, 2019)
Mahindra P2	937	19	(Mahindra - Last Mile Mobility, 2023)	VW ID.3 Pro	1812	107	(EV Database, 2023)
Mahindra P4	932	19	(Mahindra - Last Mile Mobility, 2023)	VW ID.4 Pro	2123	128	(EV Database, 2023)
Maserati GT	2260	560	(EV Database, 2023)	VW ID.Buzz	2486	150	(EV Database, 2023)

D.3 Powertrain as Standby-Redundancy

Tab. D.2 gives an overview of the required specific powers of powertrains dependent on operation space restrictions considering speed, temperature and SoC. Every vehicle that disposes of at least the shown specific power (above the displayed curve) is capable of apply the described operation space restriction to implement a safe vehicle.


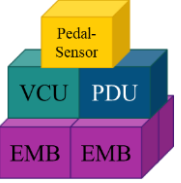
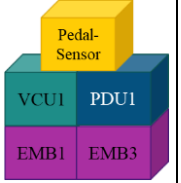
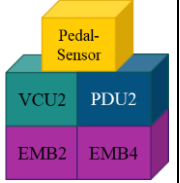


Tab. D.2: Valid operation space restrictions and necessary specific powers



E. Safety Concepts for Electromechanic Braking Systems

E.1 Item Definition

Tab. E.1: Overview on item definition options.

						
Approach	Hydraulic	Global	Circuit-specific	Horizontal	Hybrid	
Specification		Item is 1 system	Each circuit is 1 item that inherits different systems	The EMB-system is 1 item that inherits different systems	The EMB-system is 1 item that inherits different systems	
Advantages	Separate Development of items possible	Holistic safety concept for 1 system	Easy, independent development of the systems	Easy, independent development of the systems	Systems can be partly developed independently	
Disadvantages	Assumptions are made among other items	Energy-Supply would be part of many systems	Different topologies need to fulfill different safety-goals ³⁷		Actuators (from different suppliers) need to fulfill SGs combined	
Conclusion		Probably difficult to implement (see Disadv.)		Reflects sourcing structure of OEM	Compromise of global and horizontal definition	

³⁷ Centralized architectures may need to satisfy different SG than X-Circuits (refer to section 4.5)

E.2 Redundant ECUs

Different redundancy techniques are defined in (U.S. Department of Defense, 1998). This contribution focuses only on Active-Voting redundancy of up to three ECUs. The applied operating principles are shown in Fig. E.1 as Markov-trees for duplex fail-passive (a) and duplex fail-operational (b) systems. The colors mark the system states, as they are Normal Operation (green), *fp* (grey) and *fooc* (red). Hereby framed states represent stable states ($t > t_{passivation}$) and non-framed states represent volatile states ($t < t_{passivation}$). The passivation duration $t_{passivation}$ is assumed to be 100 ms in average.

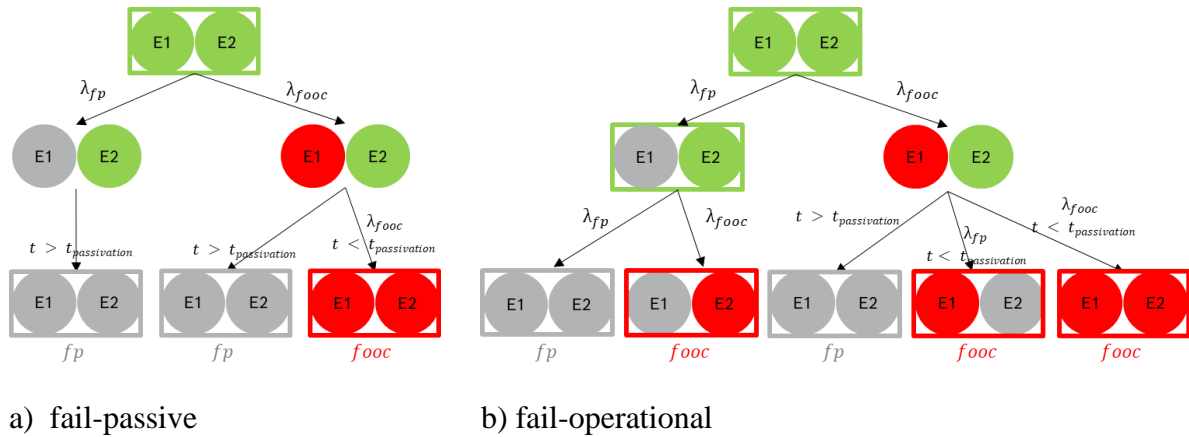


Fig. E.1: Markov-Trees of different ECU operation strategies for duplex architectures

It is defined that the system passivates itself if a discrepancy without majority exists between the ECUs. Different operating principles (*fail-passive* (a) or *fail-operational* (b)) may however be chosen if an ECU fails passively with one ECU continuing to operate normally. In this case, the remaining unit may either passivate itself (a) due to the loss of redundancy / monitoring or continue to provide a *fail-operational* functionality (b). Both operating principles have in common, that a *fooc*-failure of one ECU remains undetected if another ECU fails *fooc* during $t_{passivation}$.

F. Failure Allocation to Failure Effects within the Powertrain System

Tab. F.1 allocates the failure modes (FM) of the components analyzed in section 5.4 to the FE on vehicle level. It, especially, displays the effects onto a vehicle with a single powertrain system. The FE of a vehicle equipped with two powertrain systems (Tab. F.2) are derived by conservatively assuming that one (out of two) powertrain may already provoke a FE.

Tab. F.1: Overview on item definition options

Component	FM	FE1	FE2	FE3	FE4	FE5
		Fail-passive	Fail-degraded	Unintend. Acc. (ua)	Fail-out-of-control	Warning
I-sensor	fp	+ RPS _{fp}	1 st Fault			
RPS	fp	+ I _{fp}	1 st Fault			
	fooc	1 st Fault			+ MCU _{fp}	
WSS	any					x
MCU	fp	1 st Fault			+ ASIC _{fp}	
	fooc			1 st Fault		
Safety-ASIC	fp					x
	fooc	1 st Fault			+ MCU _{fp}	
eDrive	fd		1 st Fault			
	fp	1 st Fault				
Clutch	fp	1 st Fault				

Tab. F.2: State Table for dual PT systems

PT1 \ PT2		No FE	FE1	FE2	FE3	FE4	FE5
		NOP	fp	fd	unint. Acc.	fooc	Warn
NO FE	NOP	NOP	fd	fd	ua	fooc	warn
FE1	fp	fd	fp	fd	ua	fooc	fd
FE2	fd	fd	fd	fd	ua	fooc	fd
FE3	unint. Acc.	ua	ua	ua	ua	fooc	ua
FE4	fooc	fooc	fooc	fooc	fooc	fooc	fooc
FE5	warn	warn	fd	fd	ua	fooc	warn

References

- Audi AG, BMW AG, Daimler AG, Porsche AG, VW AG, 2013. *Standardized E-Gas Monitoring Concept for Gasoline and Diesel Engine Control Units*. unknown: EGAS Workgroup.
- Audi AG, BMW AG, Porsche AG, Volkswagen AG, 2013. *Standardized E-Gas Monitoring Concept for Gasoline and Diesel Engine Control Units - Version 5.5*. s.l.:s.n.
- Audi AG, 2022. *Datasheet Audi Q8 - 50 e-tron quattro 250 kW*, Ingolstadt: Audi AG.
- Auguste (Hitachi ASTEMO), A., 2021. *Autonomous Driving and Safety Requirements for Braking Systems for different automation levels*. Shanghai, China: China Automotive Steering & Braking Summit 2021.
- Bauer, U., Brand, M. & Maucher, T., 2017. Integrated Power Brake – modular set extension for highly automated driving. In: *Proceedings*. s.l.:Springer Fachmedien Wiesbaden, p. 693–710.
- Becker, C., Arthur, D. & Brewer, J., 2018. *Functional safety assessment of a generic, conventional, hydraulic braking system with antilock brakes, traction control, and electronic stability control (Report No. DOT HS 812 574)*, Washington: s.n.
- Becker, C., Yount, L., Arthur, D. & Attioui, F., 2018. *Functional Safety Assessment of a Generic Steer-by-Wire Steering System With ActiveSteering and Four-WheelSteering Features*, Washington: s.n.
- Bei, S. et al., 2017. *Self power supply type double-motor brake execution mechanism of automobile electro-mechanical brake system*. China, Patent No. CN106347339A.
- Bergmiller, P., 2013. Design and Safety Analysis of a Drive-by-Wire Vehicle. In: *Automotive Systems Engineering*. s.l.:Springer Berlin Heidelberg, p. 147–202.
- Birolini, A., 2014. *Reliability Engineering*. s.l.:Springer Berlin Heidelberg.
- BMW AG, 2022. *Technical Data - i7*, Singapore, Singapore: BMW Asia Pte Ltd.
- BMW AG, 2023. *All-Electric Visionary - The BMW iX*. [Online]
Available at: <https://www.bmwusa.com/vehicles/all-electric/ix/sports-activity-vehicle/electric.html#features-and-specifications>
[Accessed 01 02 2023].

BMW AG, 2023. *Find your BMW*. [Online]

Available at: <https://www.bmw.bm/en/all-models/bmw-i/i3/2020/bmw-i3-technical-data.html#tab-0>

[Accessed 01 03 2023].

Bosch Engineering GmbH, 2023. *Speed Sensor Hall-Effect HA-Di*. Abstatt, Germany: Bosch Engineering GmbH.

Bosch Rexroth AG, 2016. *Speed sensor DSM series 10*. Schwieberdingen, Germany: Bosch Rexroth AG.

Boyd, J. & Ingberman, D. E., 1995. *Should 'State of the Art' Safety Be a Defense Against Liability?*, Washington, USA: Resources of the Future.

Boyer, D., Cadoux, D., De-Winter, D. & Lansonneur, M., 2023. *Safety First*. [Online]

Available at: <https://safetyfirst.airbus.com/thrust-reverser-selection-is-a-decision-to-stop/>

[Accessed 21 06 2023].

Bundesamt für die Sicherheit der nuklearen Entsorgung, 2022. *Fukushima am 11. März 2011: Der katastrophale Unfall und seine Folgen*. [Online]

Available at:

https://www.base.bund.de/DE/themen/kt/unfaelle/fukushima/fukushima_node.html

[Accessed 19 06 2023].

Bureau of Indian Standards, 2001. *Automotive Vehicles - Brakes and Braking Systems: Part 2 General Functions and Features*. New Delhi, India: Bureau of Indian Standards.

Bureau of Indian Standards, 2003. *Automotive Vehicles - Brakes and Braking Systems: Requirements for vehicles equipped with Anti-Lock Braking Systems*. New Delhi, India: Bureau of Indian Standards.

Cadwallader, L. C., 2018. *Failure Rate Estimates for Passive Mechanical Components*. Idaho Falls, USA: U.S. Department of Energy.

Calabro, S. R., 1962. *Reliability Principles and Practice*. New York, USA: McGraw-Hill.

Car and Driver, 2023. *2016 Chevrolet Spark EV LT 5dr HB Features And Specs*. [Online]

Available at: <https://www.caranddriver.com/chevrolet/spark-ev/specs>

[Accessed 01 03 2023].

carwow Ltd., 2023. *Volkswagen ID3 Review & Prices*. [Online]

Available at: <https://carwow-uk-wp-1.imgix.net/vw-id3-blue-parked-front-studio-1.jpg?auto=format&cs=tinysrgb&fit=clip&ixlib=rb-1.1.0&q=60&w=1920>

[Accessed 23 06 2023].

- Chen, S., Hao, X., Gao, C. & Jiang, Z., 2023. An Effective Nontransient Active Short-Circuit Method for PMSM in Electric Vehicles. *IEEE Transactions on Industrial Electronics*, April, Volume 70, p. 3571–3580.
- Cheon, J. S., 2010. *Brake By Wire System Configuration and Functions using Front EWB (Electric Wedge Brake) and Rear EMB (Electro-Mechanical Brake) Actuators*. s.l., SAE International.
- Cheon, J. S., Kim, J., Jeon, J. & Lee, S. M., 2011. *Brake By Wire Functional Safety Concept Design for ISO/DIS 26262*. s.l., SAE International.
- Choi, H. R. & Hyun, D. Y., 2021. *Electromechanical Brake System having Suspension Control Function*. USA, Patent No. US2021108692A1.
- Christiaens, S., Ogrzewalla, J. & Pischinger, S., 2012. *Functional Safety for Hybrid and Electric Vehicles*. s.l., SAE International.
- Continental AG, 2022. *Continental Receives Major Award for its Future Brake System Technology Worth Over Two Billion Euros*. Hannover: Continental AG.
- De Luca, S., 2023. *Briefing - EU Legislation in Progress: New Product Liability Directive*, s.l.: European Parliament.
- DIN Deutsches Institut für Normung e.V., 2013. *DIN ISO 8855: Straßenfahrzeuge - Fahrzeugdynamik und Fahrverhalten - Begriffe (ISO 8855:2011)*. Berlin, Germany: DIN Deutsches Institut für Normung e.V..
- Doericht, M. & Schmid, R., 2000. *Elektromechanische Kraftfahrzeug-Bremsvorrichtung*. Germany, Patent No. WO0037818A1.
- Doppelbauer, M., 2020. *Grundlagen der Elektromobilität*. s.l.:Springer Fachmedien Wiesbaden.
- Ebner, C., 2024. *Modellbasierte Optimierung von mechatronischen Systemen für sicherheitsrelevante Fahrzeuganwendungen*. Ilmenau, Germany: s.n.
- Ecomotors Inc., 2023. *Renault Twizy*. [Online]
Available at: https://evcompare.io/cars/renault/renault_twizy/
[Accessed 01 03 2023].
- Edmunds.com, Inc., 2023. *2022 Chevrolet Bolt EUV - Specs & Features*. [Online]
Available at: <https://www.edmunds.com/chevrolet/bolt-euv/2022/features-specs/>
[Accessed 01 03 2023].
- Edmunds.com, Inc., 2023. *2022 Chevrolet Bolt EV - Specs & Features*. [Online]
Available at: <https://www.edmunds.com/chevrolet/bolt-ev/2022/features-specs/>
[Accessed 01 03 2023].

Edmunds.com, Inc., 2023. *2022 GMC HUMMER EV - Specs & Features*. [Online]
Available at: <https://www.edmunds.com/gmc/hummer-ev/2022/features-specs/>
[Accessed 01 03 2023].

Edmunds.com, Inc., 2023. *2022 Mercedes-Benz EQB - Specs & Features*. [Online]
Available at: <https://www.edmunds.com/mercedes-benz/eqb/2022/features-specs/>
[Accessed 01 03 2023].

Edmunds.com, Inc., 2023. *2022 Mercedes-Benz EQS - Specs & Features*. [Online]
Available at: <https://www.edmunds.com/mercedes-benz/eqs/2022/features-specs/>
[Accessed 01 03 2023].

Edmunds.com, Inc., 2023. *2022 MINI Hardtop 2 Door Electric - Specs & Features*. [Online]
Available at: <https://www.edmunds.com/mini/hardtop-2-door/2022/electric/features-specs/>
[Accessed 01 03 2023].

Edmunds.com, Inc., 2023. *Used 2019 Volkswagen e-Golf - Specs & Features*. [Online]
Available at: <https://www.edmunds.com/volkswagen/e-golf/2019/features-specs/>
[Accessed 01 03 2023].

Edmunds.com, Inc., 2023. *2023 Genesis GV60 - Specs & Features*. [Online]
Available at: <https://www.edmunds.com/genesis/gv60/2023/features-specs/>
[Accessed 01 03 2023].

European Aviation Safety Agency, 2011. *Certification Specification (CS) 25: Amendment 11 - AMC 25.1309*. Cologne, Germany: European Aviation Safety Agency.

European Aviation Safety Agency, 2017. *Guidance Material (GM) to Annex I – Definitions for terms used in Annexes II to VIII of Commission Regulation (EU) 965/2012 on air operations*. Cologne, Germany: European Aviation Safety Agency.

European Commission, 2015. *Mobility & Transport - Road Safety*. [Online]
Available at: https://road-safety.transport.ec.europa.eu/index_en
[Accessed 19 06 2023].

European Commission, 2023. *Internal Market, Industry, Entrepreneurship and SMEs*. [Online]
Available at: https://single-market-economy.ec.europa.eu/sectors/automotive-industry/vehicle-safety-and-automatedconnected-vehicles_en
[Accessed 19 06 2023].

European Parliament, 2019. *Parliament approves EU rules requiring life-saving technologies in vehicles*. Brussels: European Parliament.

European Union Aviation Safety Agency, 2007. *Certification Specifications for Large Aeroplanes CS-25: Amendment 3*. Cologne, Germany: European Union Aviation Safety Agency.

- EV Charge +, 2023. *Ford Focus Electric 23 kWh*. [Online]
Available at: <https://evchargeplus.com/ev-specification/ford-focus-electric/>
[Accessed 01 03 2023].
- EV Charge +, 2023. *Lucid Air Pure*. [Online]
Available at: <https://evchargeplus.com/ev-specification/lucid-air/>
[Accessed 01 03 2023].
- EV Compare, 2023. *Mitsubishi i-Miev*. [Online]
Available at: https://evcompare.io/cars/mitsubishi/mitsubishi_i-miev/
[Accessed 01 03 2023].
- EV Database, 2023. *Citroen e-Berlingo M 50 kWh*. [Online]
Available at: <https://ev-database.org/car/1546/Citroen-e-Berlingo-M-50-kWh>
[Accessed 01 03 2023].
- EV Database, 2023. *Citroen e-C4*. [Online]
Available at: <https://ev-database.org/car/1587/Citroen-e-C4>
[Accessed 01 03 2023].
- EV Database, 2023. *Citroen e-C4 X*. [Online]
Available at: <https://ev-database.org/car/1706/Citroen-e-C4-X>
[Accessed 01 03 2023].
- EV Database, 2023. *Citroen e-Jumpy Combi M 75 kWh*. [Online]
Available at: <https://ev-database.org/car/1597/Citroen-e-Jumpy-Combi-M-75-kWh>
[Accessed 01 03 2023].
- EV Database, 2023. *CUPRA Born 150 kW - 58 kWh*. [Online]
Available at: <https://ev-database.org/car/1516/CUPRA-Born-150-kW---58-kWh>
[Accessed 01 03 2023].
- EV Database, 2023. *CUPRA Born 170 kW -77 kWh*. [Online]
Available at: <https://ev-database.org/car/1518/CUPRA-Born-170-kW---77-kWh>
[Accessed 01 03 2023].
- EV Database, 2023. *Dacia Spring Electric 45*. [Online]
Available at: <https://ev-database.org/car/1705/Dacia-Spring-Electric>
[Accessed 01 03 2023].
- EV Database, 2023. *DS 3 E-Tense*. [Online]
Available at: <https://ev-database.org/car/1791/DS-3-E-Tense>
[Accessed 01 03 2023].
- EV Database, 2023. *Electric Vehicle Database*. [Online]
Available at: <https://ev-database.org/car/1490/Audi-Q4-e-tron-40>
[Accessed 01 03 2023].

-
- EV Database, 2023. *Electric Vehicle Database*. [Online]
Available at: <https://ev-database.org/car/1782/BYD-ATTO-3>
[Accessed 01 03 2023].
- EV Database, 2023. *Electric Vehicle Database*. [Online]
Available at: <https://ev-database.org/car/1784/BYD-HAN>
[Accessed 01 03 2023].
- EV Database, 2023. *Electric Vehicle Database*. [Online]
Available at: <https://ev-database.org/car/1783/BYD-TANG>
[Accessed 01 03 2023].
- EV Database, 2023. *Fiat E-Ulysse L2 50 kWh*. [Online]
Available at: <https://ev-database.org/car/1721/Fiat-E-Ulysse-L2-50-kWh>
[Accessed 01 03 2023].
- EV Database, 2023. *Fiat E-Ulysse L3 75 kWh*. [Online]
Available at: <https://ev-database.org/car/1724/Fiat-E-Ulysse-L3-75-kWh>
[Accessed 01 03 2023].
- EV Database, 2023. *Fisker Ocean One*. [Online]
Available at: <https://ev-database.org/car/1712/Fisker-Ocean-One>
[Accessed 01 03 2023].
- EV Database, 2023. *Genesis G80 Electrified Luxury*. [Online]
Available at: <https://ev-database.org/car/1703/Genesis-G80-Electrified-Luxury>
[Accessed 01 03 2023].
- EV Database, 2023. *Honda e*. [Online]
Available at: <https://ev-database.org/car/1233/Honda-e-Advance>
[Accessed 01 03 2023].
- EV Database, 2023. *Jaguar I-Pace EV400*. [Online]
Available at: <https://ev-database.org/car/1287/Jaguar-I-Pace-EV400>
[Accessed 01 03 2023].
- EV Database, 2023. *Lexus RZ 450e*. [Online]
Available at: <https://ev-database.org/car/1677/Lexus-RZ-450e>
[Accessed 01 03 2023].
- EV Database, 2023. *Lexus UX 300e*. [Online]
Available at: <https://ev-database.org/car/1251/Lexus-UX-300e>
[Accessed 01 03 2023].
- EV Database, 2023. *Lightyear 0*. [Online]
Available at: <https://ev-database.org/car/1166/Lightyear-0>
[Accessed 01 03 2023].

EV Database, 2023. *Lotus Eletre*. [Online]

Available at: <https://ev-database.org/car/1767/Lotus-Eletre>

[Accessed 01 03 2023].

EV Database, 2023. *Maserati GranTurismo Folgore*. [Online]

Available at: <https://ev-database.org/car/1803/Maserati-GranTurismo-Folgore>

[Accessed 01 03 2023].

EV Database, 2023. *Mazda MX-30*. [Online]

Available at: <https://ev-database.org/car/1680/Mazda-MX-30>

[Accessed 01 03 2023].

EV Database, 2023. *Mercedes EQC 400 4MATIC*. [Online]

Available at: <https://ev-database.org/car/1337/Mercedes-EQC-400-4MATIC>

[Accessed 01 03 2023].

EV Database, 2023. *Mercedes EQV 300 Long*. [Online]

Available at: <https://ev-database.org/car/1240/Mercedes-EQV-300-Long>

[Accessed 01 03 2023].

EV Database, 2023. *Opel Astra Electric*. [Online]

Available at: <https://ev-database.org/car/1792/Opel-Astra-Electric>

[Accessed 01 03 2023].

EV Database, 2023. *Opel Combo-e Life 50 kWh*. [Online]

Available at: <https://ev-database.org/car/1544/Opel-Combo-e-Life-50-kWh>

[Accessed 01 03 2023].

EV Database, 2023. *Opel Corsa-e*. [Online]

Available at: <https://ev-database.org/car/1585/Opel-Corsa-e>

[Accessed 01 03 2023].

EV Database, 2023. *Opel Mokka-e*. [Online]

Available at: <https://ev-database.org/car/1586/Opel-Mokka-e>

[Accessed 01 03 2023].

EV Database, 2023. *Opel Vivaro-e Combi M 75 kWh*. [Online]

Available at: <https://ev-database.org/car/1602/Opel-Vivaro-e-Combi-M-75-kWh>

[Accessed 01 03 2023].

EV Database, 2023. *Peugeot e-2008 SUV*. [Online]

Available at: <https://ev-database.org/car/1584/Peugeot-e-2008-SUV>

[Accessed 01 03 2023].

EV Database, 2023. *Peugeot e-308*. [Online]

Available at: <https://ev-database.org/car/1744/Peugeot-e-308>

[Accessed 01 03 2023].

EV Database, 2023. *Peugeot e-Expert Combi Standard 75 kWh*. [Online]
Available at: <https://ev-database.org/car/1607/Peugeot-e-Expert-Combi-Standard-75-kWh>
[Accessed 01 03 2023].

EV Database, 2023. *Peugeot e-Rifter Standard 50 kWh*. [Online]
Available at: <https://ev-database.org/car/1522/Peugeot-e-Rifter-Standard-50-kWh>
[Accessed 01 03 2023].

EV Database, 2023. *Peugeot e-Traveller Standard 50 kWh*. [Online]
Available at: <https://ev-database.org/car/1351/Peugeot-e-Traveller-Standard-50-kWh>
[Accessed 01 03 2023].

EV Database, 2023. *Polestar 2*. [Online]
Available at: <https://ev-database.org/car/1170/Polestar-2>
[Accessed 01 03 2023].

EV Database, 2023. *Polestar 3 Long Range Dual Motor*. [Online]
Available at: <https://ev-database.org/car/1758/Polestar-3-Long-Range-Dual-motor>
[Accessed 01 03 2023].

EV Database, 2023. *Porsche Taycan*. [Online]
Available at: <https://ev-database.org/car/1393/Porsche-Taycan>
[Accessed 01 03 2023].

EV Database, 2023. *Renault Kangoo E-Tech Electric*. [Online]
Available at: <https://ev-database.org/car/1802/Renault-Kangoo-E-Tech-Electric>
[Accessed 01 03 2023].

EV Database, 2023. *Renault Megane E-Tech EV60 220hp*. [Online]
Available at: <https://ev-database.org/car/1521/Renault-Megane-E-Tech-EV60-220hp>
[Accessed 01 03 2023].

EV Database, 2023. *Renault Twingo Electric*. [Online]
Available at: <https://ev-database.org/car/1270/Renault-Twingo-Electric>
[Accessed 01 03 2023].

EV Database, 2023. *Renault Zoe ZE50 R110*. [Online]
Available at: <https://ev-database.org/car/1164/Renault-Zoe-ZE50-R110>
[Accessed 01 03 2023].

EV Database, 2023. *Rolls-Royce Spectre*. [Online]
Available at: <https://ev-database.org/car/1765/Rolls-Royce-Spectre>
[Accessed 01 03 2023].

EV Database, 2023. *Skoda Enyaq iV60*. [Online]
Available at: <https://ev-database.org/car/1279/Skoda-Enyaq-iV-60>
[Accessed 01 03 2023].

- EV Database, 2023. *Skoda Enyaq iV80*. [Online]
Available at: <https://ev-database.org/car/1280/Skoda-Enyaq-iV-80>
[Accessed 01 03 2023].
- EV Database, 2023. *Smart #1*. [Online]
Available at: <https://ev-database.org/car/1667/Smart-1>
[Accessed 01 03 2023].
- EV Database, 2023. *Smart EQ fortwo coupe*. [Online]
Available at: <https://ev-database.org/car/1230/Smart-EQ-fortwo-coupe>
[Accessed 01 03 2023].
- EV Database, 2023. *SSangYong Korondo e-Motion*. [Online]
Available at: <https://ev-database.org/car/1589/SsangYong-Korando-e-Motion>
[Accessed 01 03 2023].
- EV Database, 2023. *Subaru Solterra AWD*. [Online]
Available at: <https://ev-database.org/car/1567/Subaru-Solterra-AWD>
[Accessed 01 03 2023].
- EV Database, 2023. *Tesla Model 3*. [Online]
Available at: <https://ev-database.org/car/1555/Tesla-Model-3>
[Accessed 01 03 2023].
- EV Database, 2023. *Tesla Model X Dual Motor*. [Online]
Available at: <https://ev-database.org/car/1407/Tesla-Model-X-Dual-Motor>
[Accessed 01 03 2023].
- EV Database, 2023. *Tesla Model Y*. [Online]
Available at: <https://ev-database.org/car/1743/Tesla-Model-Y>
[Accessed 01 03 2023].
- EV Database, 2023. *Toyota bZ4X FWD*. [Online]
Available at: <https://ev-database.org/car/1564/Toyota-bZ4X-FWD>
[Accessed 01 03 2023].
- EV Database, 2023. *Toyota Proace City Verso Electric L1 50 kWh*. [Online]
Available at: <https://ev-database.org/car/1779/Toyota-Proace-City-Verso-Electric-L1-50-kWh>
[Accessed 01 03 2023].
- EV Database, 2023. *VinFast VF 8 Eco Standard Range*. [Online]
Available at: <https://ev-database.org/car/1806/VinFast-VF-8-Eco-Standard-Range>
[Accessed 01 03 2023].
- EV Database, 2023. *VinFast VF 9 Standard Range*. [Online]
Available at: <https://ev-database.org/car/1810/VinFast-VF-9-Standard-Range>
[Accessed 01 03 2023].

-
- EV Database, 2023. *Volkswagen ID.3 Pro*. [Online]
Available at: <https://ev-database.org/car/1531/Volkswagen-ID3-Pro>
[Accessed 01 03 2023].
- EV Database, 2023. *Volkswagen ID.4 Pro*. [Online]
Available at: <https://ev-database.org/car/1627/Volkswagen-ID4-Pro>
[Accessed 01 03 2023].
- EV Database, 2023. *Volkswagen ID.Buzz Pro*. [Online]
Available at: <https://ev-database.org/car/1651/Volkswagen-ID-Buzz-Pro>
[Accessed 01 03 2023].
- EV Database, 2023. *Volvo XC40 Recharge Single Motor*. [Online]
Available at: <https://ev-database.org/car/1796/Volvo-XC40-Recharge-Single-Motor>
[Accessed 01 03 2023].
- EV Database, 2023. *Volvo XC90 Twin Motor*. [Online]
Available at: <https://ev-database.org/car/1775/Volvo-EX90-Twin-Motor>
[Accessed 01 03 2023].
- evspecifications.com, 2023. *2021 Mercedes-Benz EQA 250 - Specifications*. [Online]
Available at: <https://www.evspecifications.com/en/model/30db155>
[Accessed 01 03 2023].
- evspecifications.com, 2023. *2023 Mercedes-Benz EQE 350 - Specifications*. [Online]
Available at: <https://www.evspecifications.com/en/model/818816b>
[Accessed 01 03 2023].
- Fijalkowski, B. T., 2010. Anti-Lock EFMB or EPMB BBW AWB Dispulsion Mechatronic Control Systems. In: *Automotive Mechatronics: Operational and Practical Issues*. s.l.:Springer Netherlands, p. 463–495.
- Friesen, U., 2005. *Electromechanical brake applying device*. USA, Patent No. US2005006948A1.
- Fu, Y. et al., 2020. *Electromechanical brake device and vehicle with same*. China, Patent No. CN211202695U.
- Gächter, J. et al., 2014. Evaluation of Angular Sensor Systems for Rotor Position Sensing of Automotive Electric Drives. In: *Advanced Microsystems for Automotive Applications 2014*. s.l.:Springer International Publishing, p. 277–286.
- Gates, D. & Baker, M., 2019. *The inside story of MCAS: How Boeing's 737 MAX system gained power and lost safeguards*. [Online]
Available at: <https://www.seattletimes.com/seattle-news/times-watchdog/the-inside-story-of-mcas-how-boeings-737-max-system-gained-power-and-lost-safeguards/>
[Accessed 19 06 2023].

Gehring, O. et al., 2005. *Verfahren und Anordnung zur Regelung einer Bremsanordnung mit redundantem Energiepfad zur Energieversorgung der Regelungseinrichtung*. Germany, Patent No. DE102004014623A1.

General Administration of Quality Supervision, Inspection and Quarantine of People's Republic of China., 2014. *Technical Requirements and Testing Methods for Commercial Vehicles and Trailer Braking Systems GB12676-2014*. Beijing, China: General Administration of Quality Supervision, Inspection and Quarantine of People's Republic of China..

glücksleasing, 2023. *GlücksLeasing*. [Online]
Available at: <https://gluecksleasing.de/images/3563/44d1ae0bc73e6acc/28691-vw-id-4-97a3321371.png>
[Accessed 23 06 2023].

Gohbrandt, J. & Stroschein, J., 2021. *Verfahren zum Erkennen von Schäden an mechanischen Bauteilen einer elektromechanischen Bremse, elektronisch gesteuertes Bremssystem, Computerprogrammprodukt, Steuergerät und Kraftfahrzeug*. Germany, Patent No. DE102019128742A1.

greencarreports, 2023. *200-mph, 520-mile Tesla Model S Plaid available to order, but delayed to late 2021*. [Online]
Available at: https://images.hgmsites.net/hug/tesla-model-s_100762374_h.jpg
[Accessed 23 06 2023].

Harper, D., 2021. *Online Etymology Dictionary*. [Online]
Available at: <https://www.etymonline.com/word/redundancy>
[Accessed 22 05 2023].

Hartmann, H. & Schautt, M., 2004. *Fail-safe concept for an electromechanical brake*. USA, Patent No. US7748793B2.

Hayward, J., 2020. *The History of The Boeing 737*. [Online]
Available at: <https://simpleflying.com/boeing-737/>
[Accessed 19 06 2023].

Hearst Autos, Inc., 2023. *2023 Ford Mustang Mach-E Select RWD Features and Specs*. [Online]
Available at: <https://www.caranddriver.com/ford/mustang-mach-e/specs>
[Accessed 01 03 2023].

HELLA GmbH & Co. KGaA, 2022. *HELLA brings fully electric brake-by-wire pedal into large-scale production worldwide for the first time*, Lippstadt: HELLA GmbH & Co. KGaA.

Hobbs, G. K., 2000. *Accelerated Reliability Engineering*. s.l.:John Wiley & Sons.

-
- Holzwarth, J., 2010. *Electromechanical Brake System with a Failsafe Energy Supply and Method for Failsafe Energy Supply in an Electromechanical Brake System For Vehicles*. USA, Patent No. US2010243388A1.
- Holzwarth, J. & Krausen, L., 2008. *System zur Aktorsteuerung, insbesondere Bremssystem*. Germany, Patent No. DE102006053617A1.
- Hommel, Q. V. E. & Becker, C., 2018. *Functional Safety Assessment of a Generic Accelerator Control System With Electronic Throttle Control in Gasoline-Fueled Vehicles*, Washington: s.n.
- Huang, S. et al., 2016. Transient fault tolerant control for vehicle brake-by-wire systems. *Reliability Engineering & System Safety*, May, Volume 149, p. 148–163.
- Hwan, C. S., 2009. *Fail-Safe Embodiment Device Brake by Wire System in Vehicle*. Korea, Patent No. KR20090061969 A.
- Hwan, C. S., 2009. *Fail-Safe Embodiment Device Brake by Wire System in Vehicle*. Korea, Patent No. KR20090061766 A.
- Hyundai Motor America, 2023. *2023 IONIQ 5*. [Online]
Available at: <https://www.hyundaiusa.com/us/en/vehicles/ioniq-5/compare-specs>
[Accessed 01 03 2023].
- Hyundai Motor America, 2023. *2023 KONA Electric*. [Online]
Available at: <https://www.hyundaiusa.com/us/en/vehicles/kona-electric/compare-specs>
[Accessed 01 03 2023].
- Infogalactic, 2016. *Buddy (electric car)*. [Online]
Available at: [https://infogalactic.com/info/Buddy_\(electric_car\)](https://infogalactic.com/info/Buddy_(electric_car))
[Accessed 01 03 2023].
- Insurance Institute for Highway Safety (IIHS), 2006. *Electronic stability control could prevent nearly one-third of all fatal crashes and reduce rollover risk by as much as 80%; effect is found on single- and multiple-vehicle crashes*. [Online]
Available at:
<https://web.archive.org/web/20130525140543/http://www.iihs.org/news/rss/pr061306.html>
[Accessed 19 06 2023].
- International Organization for Standardization, 2018. *ISO 26262-1, Road vehicles - Functional safety - Part 1: Vocabulary*. Geneva, Switzerland: ISO copyright office.
- International Organization for Standardization, 2018. *ISO 26262-10: Road vehicles - Functional safety - Part 10: Guidelines on ISO 26262*. Geneva, Switzerland: ISO copyright office.

- International Organization for Standardization, 2018. *ISO 26262-3: Road vehicles - Functional safety - Part 3: Concept phase*. Geneva, Switzerland: ISO copyright office.
- International Organization for Standardization, 2018. *ISO 26262-5: Road vehicles - Functional safety - Part 5: Product Development at the hardware level*. Geneva, Switzerland: ISO copyright office.
- International Organization for Standardization, 2018. *ISO 26262-6: Road vehicles - Functional safety - Part 6: Product development at the software level*. Geneva, Switzerland: ISO copyright office.
- International Organization for Standardization, 2018. *ISO 26262-9: Road vehicles - Functional safety - Part 9: Automotive safety integrity level (ASIL)-oriented and safety-oriented analysis*. Geneva, Switzerland: ISO copyright office.
- International Organization for Standardization, 2022. *ISO 21448: Road vehicles - Safety of the intended functionality*. Geneva, Switzerland: s.n.
- International Organization on Standardization, 2021. *ISO/PAS 5101: Road vehicles - Field load specification for brake actuation and modulation systems*. Geneva, Switzerland: ISO copyright office.
- Isermann, R., 2006. *Fault-Diagnosis Systems*. s.l.:Springer Berlin Heidelberg.
- Isermann, R., 2007. Fehlertolerante mechatronische Systeme, Teil 1 (Fault-tolerant Mechatronic Systems, Part 1). *at - Automatisierungstechnik*, April, Volume 55, p. 170–179.
- Isermann, R., 2011. *Fault-Diagnosis Applications*. s.l.:Springer Berlin Heidelberg.
- Isermann, R., Schwarz, R. & Stölzl, S., 2002. Fault-tolerant drive-by-wire systems. *IEEE Control Systems Magazine*, Volume 22, pp. 64–81.
- Isermann, R., Schwarz, R. & Stölzl, S., 2002. Fault-tolerant drive-by-wire systems. *IEEE Control Systems*, October, Volume 22, p. 64–81.
- Jennings, J., Finn, D. & Hunter, T., 2023. Novel Multi-Functional Clutch Technology for EV Drivetrain Disconnects – Next Generation Disconnect with One-Way-Clutch for Automatic, and Non-Blocked Shifting. In: *Dritev 2023*. s.l.:VDI Verlag, p. 325–338.
- Jeong, Y., Sul, S.-K., Schulz, S. E. & Patel, N. R., 2005. Fault Detection and Fault-Tolerant Control of Interior Permanent-Magnet Motor Drive System for Electric Vehicle. *IEEE Transactions on Industry Applications*, January, Volume 41, p. 46–51.
- Jeon, K. et al., 2012. Development of a fail-safe control strategy based on evaluation scenarios for an FCEV electronic brake system. *International Journal of Automotive Technology*, December, Volume 13, p. 1067–1075.
- Kapur, K. C. & Pecht, M. eds., 2014. *Reliability Engineering*. s.l.:John Wiley & Sons, Inc..

-
- Kelling, N. A. & Heck, W., 2002. *The BRAKE Project - Centralized Versus Distributed Redundancy for Brake-by-Wire Systems*. s.l., SAE International.
- Kemmann, S. & Trapp, M., 2011. *SAHARA -A Systematic Approach for Hazard Analysis and Risk Assessment*. s.l., SAE International.
- Keski-Luopa, M., 2007. *Sähkömekaaninen seisontajarrujärjestely*. Finland, Patent No. FI119855B.
- Khastgir, S. et al., 2017. Towards increased reliability by objectification of Hazard Analysis and Risk Assessment (HARA) of automated automotive systems. *Safety Science*, November, Volume 99, p. 166–177.
- KIA Media, 2023. *2022 Kia EV6 Specifications*. [Online]
Available at: <https://www.kiamedia.com/us/en/models/ev6/2022/specifications>
[Accessed 01 03 2023].
- KIA Media, 2023. *2022 Kia Niro EV Specifications*. [Online]
Available at: <https://www.kiamedia.com/us/en/models/niro-ev/2022/specifications>
[Accessed 01 03 2023].
- KIA UK, 2023. *Kia Soul EV Specification*. [Online]
Available at: <https://www.kia.com/uk/new-cars/soul-ev/specification/>
[Accessed 01 03 2023].
- Kilian, P. et al., 2021. Principle Guidelines for Safe Power Supply Systems Development. *IEEE Access*, Volume 9, p. 107751–107766.
- Kilian, P. et al., 2022. Safety-Related Availability in the Power Supply Domain. *IEEE Access*, Volume 10, p. 47869–47880.
- Kim, S., 2009. *Disk Break Apparatus For Electromechanical Brake System*. USA, Patent No. US2009223752A1.
- Knödel, U., Stein, F.-J. & Schlenkermann, H., 2011. Variantenvielfalt der Antriebskonzepte für Elektrofahrzeuge. *ATZ - Automobiltechnische Zeitschrift*, July, Volume 113, p. 552–557.
- Kopetz, H., 2011. *Real-Time Systems*. s.l.:Springer US.
- Koren, I. & Krishna, C. M., 2007. *Fault-Tolerant Systems*. s.l.:Elsevier.
- Kraftfahrtbundesamt, 2023. *Typgenehmigungserteilung*. [Online]
Available at:
https://www.kba.de/DE/Themen/Typgenehmigung/Typgenehmigungserteilung/typgenehmigungserteilung_node.html
[Accessed 19 06 2023].
- Kügeler, C. et al., 2021. Brake-by-Wire Actuator for Electromechanical Disc Brake. In: *Proceedings*. s.l.:Springer Berlin Heidelberg, p. 435–448.

- Laxhuber, T., Baumgartner, H. & Pahle, W., 2004. *Device and method for monitoring a brake-applying electromechanical device for vehicle brakes*. USA, Patent No. US6774595B1.
- Lee, K. J. et al., 2014. Approach to functional safety-compliant ECU design for electro-mechanical brake systems. *International Journal of Automotive Technology*, March, Volume 15, p. 325–332.
- Liu, Q., Qin, C., Fu, Y. L. D. & Liao, K., 2021. *Vehicle electromechanical brake system and vehicle with same*. China, Patent No. CN112550189A.
- Mahindra - Last Mile Mobility, 2023. *Get bigger savings on our Electric, Diesel and CNG vehicles*. [Online]
Available at: <https://www.mahindraelectric.com/vehicles/e2oPlus/>
[Accessed 01 03 2023].
- Martin, S., 2004. *Elektromechanische Bremse zum Abbremsen einer sich drehenden Komponente und Bremsanlage mit einer elektromechanischen Bremse*. Germany, Patent No. DE10319082 B3.
- Maruyama, Y. & Yamazaki, F., 2003. *Automobile Drivers' Responses to Lateral Wind Disturbance Based on Driving Simulator Experiments*. Bali, Indonesia, s.n.
- Mercedes-Benz AG, 2023. *EQS Saloon*. [Online]
Available at: https://www.mercedes-benz.co.za/passengercars/mercedes-benz-cars/models/eqs/saloon-v297/_jcr_content/image.MQ6.2.2x.20210505112527.png
[Accessed 23 06 2023].
- Messnarz, R., Macher, G., Stolfa, J. & Stolfa, S., 2019. Highly Autonomous Vehicle (System) Design Patterns – Achieving Fail Operational and High Level of Safety and Security. In: *Communications in Computer and Information Science*. s.l.:Springer International Publishing, p. 465–477.
- MINI UK, 2023. *MINI Electric Technical Data*. [Online]
Available at: https://www.mini.co.uk/en_GB/home/range/more-mini-electric/mini-electric-tech-specs.html
[Accessed 01 03 2023].
- Mitschke, M. & Wallentowitz, H., 2014. *Dynamik der Kraftfahrzeuge*. s.l.:Springer Fachmedien Wiesbaden.
- Molfetta, D., Ringlstetter, M. & Zelger, C., 2008. *Redundante Übermittlung von Bremsanweisungen*. Germany, Patent No. DE102007001371A1.
- Mosher, D. & Gould, S., 2018. *The odds that a gun will kill the average American may surprise you*. [Online]
Available at: <https://www.businessinsider.com/us-gun-death-murder-risk-statistics-2018->

3?op=1

[Accessed 19 06 2023].

Najm, W. G., Smith, J. D. & Yanagisawa, M., 2007. *Pre-Crash Scenario Typology for Crash Avoidance Research*, s.l.: s.n.

Naval Surface Warfare Center, Carderock Division, 2006. *Handbook of Reliability Prediction Procedures for Mechanical Equipment*. West Bethesda, USA: Naval Surface Warfare Center.

Niedermeier, E., 2001. *Brake system for a motor vehicle*. USA, Patent No. US6189981B1.

Nilsson, A. & Linidqvist, A., 2021. *An Electromechanical Brake System*. China, Patent No. WO2021122214A1.

Nilsson, R., 2002. Evaluation of a combined brake–accelerator pedal. *Accident Analysis & Prevention*, March, Volume 34, p. 175–183.

Nissan USA, 2023. *2023 Nissan Ariya*. [Online]

Available at: <https://www.nissanusa.com/vehicles/electric-cars/ariya/specs/compare-specs.html#modelName=ENGAGE%20FWD|63%20kWh>

[Accessed 01 03 2023].

Nissan USA, 2023. *2024 Nissan Leaf*. [Online]

Available at: <https://www.nissanusa.com/vehicles/electric-cars/leaf/specs/compare-specs.html#modelName=S|40%20kWh%20lithium-ion%20battery>

[Accessed 01 03 2023].

Nuesse, D., 2020. *Elektromechanische Bremsvorrichtung für ein Fahrzeug*. Germany, Patent No. DE102018218472A1.

Our World in Data, 2022. *Probability of dying, by age, World, 2000 to 2019*. [Online]

Available at: <https://ourworldindata.org/grapher/probability-of-dying-by-age?time=2000..2019> from WHO, Global Health Observatory (2022)

[Accessed 19 06 2023].

Our World in Data, 2023. *Death rate due to road traffic injuries, 2000 to 2019*. [Online]

Available at: https://ourworldindata.org/grapher/death-rate-road-traffic-injuries?tab=chart&country=OWID_WRL~USA~DEU~ZWE~DOM~Frau

[Accessed 19 06 2023].

Parker, D., Godof, A., Papadopoulos, Y. & Saintis, L., 2018. *A Study of Automatic Allocation of Automotive Safety Requirements in Two Modes: Components and Failure Modes*. s.l., SAE International.

Pepper, T., 2022. *Product Liability & Safety 2022*. [Online]

Available at: <https://practiceguides.chambers.com/practice-guides/product-liability-safety->

2022/usa

[Accessed 19 06 2023].

Putz, M. H., Seifert, H., Zach, M. & Peternel, J., 2016. *Functional Safety (ASIL-D) for an Electro Mechanical Brake*. s.l., SAE International.

Reuters, 2022. *Passengers in fatal Boeing 737 MAX crashes are 'crime victims', US judge says*. [Online]

Available at: <https://edition.cnn.com/2022/10/22/business/boeing-737-max-crime-victims/index.html>

[Accessed 19 06 2023].

Robert Bosch GmbH, 2013. *iBooster – Vacuum-independent electromechanical brake booster*, Abstatt: Robert Bosch GmbH.

Robert Bosch GmbH, 2020. *25 Jahre ESP® von Bosch: Schluss mit der Schleuderpartie*. [Online]

Available at: <https://www.bosch-presse.de/pressportal/de/de/25-jahre-esp-von-bosch-schluss-mit-der-schleuderpartie-212032.html>

[Accessed 19 06 2022].

Robert Bosch GmbH, 2023. *Electric motors for commercial vehicles*. [Online]

Available at: <https://www.bosch-mobility.com/en/solutions/electric-motors/electric-motors-for-commercial-vehicles/>

[Accessed 31 07 2023].

Robert Bosch GmbH, 2023. *Electronic stability program - System components*. [Online]

Available at: <https://www.bosch-mobility.com/en/solutions/driving-safety/electronic-stability-program/>

[Accessed 29 09 2023].

Robert Bosch GmbH, 2023. *Inertial measurement unit*. [Online]

Available at: <https://www.bosch-mobility.com/en/solutions/sensors/inertial-measurement-unit/>

[Accessed 29 09 2023].

Robert Bosch GmbH, 2023. *Wheel-speed sensor*. [Online]

Available at: <https://www.bosch-mobility.com/en/solutions/sensors/wheel-speed-sensor/>

[Accessed 29 09 2023].

Ross, H.-L., 2016. *Functional Safety for Road Vehicles*. s.l.:Springer International Publishing.

Ross, K. & Dorenkamp, T., 2020. *Product liability and safety in the United States: overview*. [Online]

Available at: <https://uk.practicallaw.thomsonreuters.com/w-012->

[8129?contextData=\(sc.Default\)&transitionType=Default&firstPage=true](#)

[Accessed 19 06 2023].

SAE International, 2021. *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*. Warrendale, USA: SAE International.

Saitner, M. & Keller, R., 2009. *Elektrisch betreibbare Parksperrenvorrichtung für ein Fahrzeuggetriebe*. Germany, Patent No. DE102009028858A1.

Schade, K. & Linhoff, P., 2012. *Elektromechanische Bremse und zugehöriges Betriebsverfahren*. Germany, Patent No. DE102011076424A1.

Schaffer, W., 1999. *Electromechanical Wheel Brake System*. USA, Patent No. US6340077 BA.

Schrade, S., Nowak, X. & Peter, S., 2022. *Betriebsverfahren für eine Betätigungsanordnung für sicherheitskritische Fahrzeugsysteme*. Germany, Patent No. DE102022213119.

Schrade, S., Nowak, X. & Peter, S., 2022. *Betriebsverfahren für eine Pedalanordnung für sicherheitskritische Fahrzeugsysteme*. Germany, Patent No. DE102022213115.

Schrade, S., Nowak, X. & Peter, S., 2022. *Betriebsverfahren für eine Pedalanordnung für sicherheitskritische Fahrzeugsysteme*. Germany, Patent No. DE102022213127.

Schrade, S., Nowak, X., Peter, S. & Boros, L., 2022. *Radbremssmodul, Kraftfahrzeug, Verfahren zum Betreiben des Kraftfahrzeugs*. Germany, Patent No. DE102022211584.

Schrade, S., Nowak, X., Schramm, D. & Verhagen, A., 2023. *Safety Concepts for Brake-by-Wire Pedal Boxes*. s.l., IEEE.

Schrade, S., Nowak, X., Verhagen, A. & Schramm, D., 2022. Short Review of EMB Systems Related to Safety Concepts. *Actuators*, July, Volume 11, p. 214.

Schrade, S., Nowak, X., Verhagen, A. & Schramm, D., 2023. *Generic X-Domain Hazard Analysis and Risk Assessment*. s.l., SAE International.

Schrade, S., Nowak, X. & Walter, R., 2023. *Verfahren zum Betreiben einer Aktuatoranordnung eines Bremssystems eines Kraftfahrzeugs, Aktuatoranordnung, Bremssystem, Kraftfahrzeug*. Germany, Patent No. DE102023209998.

Schrade, S. et al., unpublished yet. Safety Concepts for future Electromechanical Brake Actuators. *SAE International Journal of Passenger Vehicle Systems*, unknown(unknown), p. unknown.

Schrade, S. et al., unpublished yet. Safety Concepts for future EMB-Systems. *SAE International Journal of Passenger Vehicle Systems*, unknown(unknown), p. unknown.

Schröder, T., Bächle, M. & Ullrich, T., 2023. *Sicherheits- und Zuverlässigkeitsanforderungen von EMB-Systemen*. Munich, Germany: ATZ live.

- Schumann, F., 1997. *Elektromechanische Bremsvorrichtung*. Germany, Patent No. WO9736116A1.
- Schumann, F., Blossch, G. & Baehrle, F., 2002. *Verfahren zur Betätigung einer Feststellbremsanlage einer Betriebsbremsanlage und eine Feststellbremsanlage ausweisenden elektromechanischen Bremsanlage und elektromechanische Bremsanlage*. Germany, Patent No. DE 10224688 A 1.
- Schwarz, R. et al., 1999. *Clamping Force Estimation for a Brake-by-Wire Actuator*. s.l., SAE International.
- Semsch, M., Feigel, H.-J. & Hoffmann, J., 2012. Elektromechanisch betätigte Bremse. In: *Bremsenhandbuch*. s.l.:Vieweg Teubner Verlag, p. 439–445.
- Siemens AG, 2004. *Siemens Norm SN 29500-1: Failure rates of component - Expected values, General*. Munich, Germany: Siemens AG.
- Siemens AG, 2004. *Siemens Norm SN 29500-2: Failure rates of components - Part 2: Expected values for integrated components*. Munich, Germany: Siemens AG.
- Sim, G. & Jian, J., 2021. *Electro-Mechanical Brake System and Method for Operating Same*. Korea, Patent No. WO2021158022A1.
- Sinha, P., 2011. Architectural design and reliability analysis of a fail-operational brake-by-wire system from ISO 26262 perspectives. *Reliability Engineering & System Safety*, October, Volume 96, p. 1349–1359.
- SKYbrary, 2023. *Autoland*. [Online]
Available at: <https://skybrary.aero/articles/Autoland>
[Accessed 19 06 2023].
- Sommerville, I., 2004. *Airbus flight control system - The organisation of the Airbus A330/A340 flight control system*. s.l.:s.n.
- Spånberg, H., 2022. Electric Torque Vectoring Disconnect unit, eTVD. In: *Dritev 2022*. s.l.:VDI Verlag, p. 253–266.
- Standardization, I. O. f., 2021. *ISO/PAS5101: Road vehicles - Field load specification for brake actuation and modulation systems*. Geneva, Switzerland: s.n.
- statista, 2023. *Anzahl verkaufter Personenkraftwagen weltweit nach ausgewählten Ländern in den Jahren 2021 und 2022*. [Online]
Available at: <https://de.statista.com/statistik/daten/studie/734067/umfrage/anzahl-verkaufter-automobile-nach-laendern-weltweit/>
[Accessed 19 06 2023].
- Stoelzl, S. et al., 2000. *Electromechanical brake system*. USA, Patent No. US6317675B1.
- Takahashi, H. & Takahashi, K., 2010. *Electric Brake*. USA, Patent No. US7806241B2.

Transport Canada, Motor Vehicle Safety, 2015. *Technical Standards Document No. 105, Revision 5: Hydraulic and Electric Brake Systems*. Ottawa, Canada: Transport Canada, Motor Vehicle Safety.

Triggs, T. J. & Harris, W. G., 1982. *REACTION TIME OF DRIVERS TO ROAD STIMULI*. s.l., s.n.

U.S. Department of Defense, 1991. *MIL-HDBK-217F: Reliability Prediction of Electronic Equipment*. Washington D.C., USA: U.S. Department of Defense.

U.S. Department of Defense, 1998. *MIL-HDBK-338B: Electronic Reliability Design Handbook*. Philadelphia, USA: Standardization Documents Order Desk.

U.S. Department of Energy National Laboratory, 2018. *Failure Rate Estimates for Passive Mechanical Components*. Idaho Falls: Idaho National Laboratory.

U.S. Department of Transportation - National Highway Traffic Safety Administration, 2005. *Laboratory Test Procedure for FMVSS 135 Light Vehicle Brake System*. Washington D.C., USA: Office of Vehicle Safety Compliance.

United Nations ECE, 2015. *Regulation No 13-H of the Economic Commission for Europe of the United Nations (UN/ECE) — Uniform provisions concerning the approval of passenger cars with regard to braking [2015/2364]*. Geneva, Switzerland: United Nations ECE.

Verband der Automobilindustrie e.V., 2015. *VDA 702: Situationskatalog E-Parameter nach ISO 26262-3*. Berlin, Germany: Verband der Automobilindustrie e.V..

Verband der Automobilindustrie, 2016. *VDA 360: Empfehlung zur Umsetzung einer Kommunikationsschnittstelle zwischen einem elektrischen Bremskraftverstärker und einem ESC-Steuergerät*. Berlin, Germany: Verband der Automobilindustrie.

Volkswagen AG, 2019. *News Room: Technical Data of e-up!*. [Online]
Available at: <https://www.volkswagen-newsroom.com/en/the-e-up-taken-to-a-new-level-5583/technical-data-5590>
[Accessed 01 03 2023].

von Alven, W. H., 1964. *Reliability Engineering*. Englewood, USA: ARINC Research Corporation.

WatteV2Buy, 2023. *Bollore Bluecar*. [Online]
Available at: <https://wattv2buy.com/electric-vehicles/bollore/bluecar-ev/>
[Accessed 01 03 2023].

Weiberle, R., 2011. *Elektrisches Bremssystem, insbesondere elektromechanisches Bremssystem*. Germany, Patent No. DE102009046231A1.

Weiberle, R., 2021. *Elektrisches Bremssystem, insbesondere elektromechanisches Bremssystem*. Germany, Patent No. DE102009046238B4.

Weiberle, R., Mueller, B. & Hassdenteufel, F., 2011. *Electric brake system i.e. electromechanical brake system, for motor vehicle, has brake circuits provided with control apparatuses, and rolling dynamics control unit integrated in each control apparatus*. France, Patent No. FR2952011A1.

Weiberle, R., Mueller, B. & Kriso, S., 2011. *Electrical brake system i.e. electromechanical brake system, for motor vehicle, has brake system controlling CPU transmitting signal by communication system of brake circuit, and seizing unit directly connected to controller*. France, Patent No. FR2952886A1.

Wikipedia, 2023. *BMW iX*. [Online]

Available at: https://en.wikipedia.org/wiki/BMW_iX#Battery_and_charging
[Accessed 25 07 2023].

Winkler, J., 2010. *Bordnetz für ein Fahrzeug und Verfahren zur Energieversorgung eines sicherheitsrelevanten Verbrauchers eines Bordnetzes*. Germany, Patent No. DE102006010713B4.

Wolf, P., 2020. *Fiat 500e Specs*. [Online]

Available at: <https://fiatservice.eu/ fiat-500e-specs/>
[Accessed 01 03 2023].

World Nuclear Association, 2023. *Fukushima Daiichi Accident*. [Online]

Available at: <https://world-nuclear.org/information-library/safety-and-security/safety-of-plants/fukushima-daiichi-accident.aspx>
[Accessed 19 06 2023].

Yang, I., Liu, S., Ma, F. & Miao, F., 2020. *Electromechanical brake cylinder with parking function and brake system*. China, Patent No. CN111319596 A.

Yang, S. et al., 2023. *Disconnect Actuator System (DAS) for AWD EV's Driving System*. s.l., SAE International.

Yan, L., Hao, Z. & Sui, Q., 2021. *EMB redundancy control system and method*. China, Patent No. CN113110238A.

Zhang, J. et al., 2016. *Fault diagnosis and fault tolerant control for electrified vehicle torque security*. s.l., IEEE.

Publications of the Author

2022

S. Schrade, X. Nowak, A. Verhagen and D. Schramm, "Short Review of EMB Systems Related to Safety Concepts," *Actuators*, vol. 11, p. 214, July 2022.

2023

S. Schrade, X. Nowak, A. Verhagen and D. Schramm, "Generic X-Domain Hazard Analysis and Risk Assessment," in *SAE Technical Paper Series*, 2023.

S. Schrade, X. Nowak, D. Schramm and A. Verhagen, "Safety Concepts for Brake-by-Wire Pedal Boxes," in *2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, 2023.

2024 (accepted)

S. Schrade, A. Röhler, X. Nowak, A. Verhagen and D. Schramm, "Safety Concepts for future Electromechanical Brake Actuators," *SAE International Journal of Passenger Vehicle Systems*, vol. unknown, no. unknown, p. unknown, unpublished.

S. Schrade, A. Röhler, X. Nowak, A. Verhagen and D. Schramm, "Safety Concepts for future EMB-Systems," *SAE International Journal of Passenger Vehicle Systems*, vol. unknown, no. unknown, p. unknown, unpublished.

Patents of the Author

Title	Inventors	Appl.-Number
Innovative Methode für Hazard Analysis and Risk Assessment	Schrade Simon Nowak Xi	DE102022208936.7
Verfahren zum Bestimmen eines Schweregrads	Schrade Simon Nowak Xi	DE102022208935.9
Radbremssmodul, Kraftfahrzeug, Verfahren zum Betreiben des Kraftfahrzeugs	Schrade Simon Nowak Xi Peter Simon Boros Laszlo	DE102022211584.8
Betriebsverfahren für eine Betätigungsanordnung für sicherheitskritische Fahrzeugsysteme	Schrade Simon Nowak Xi Peter Simon	DE102022213119.3
Betriebsverfahren für eine Pedalanordnung für sicherheitskritische Fahrzeugsysteme	Schrade Simon Nowak Xi Peter Simon	DE102022213115.0
Aktuatoranordnung, Kraftfahrzeug, Verfahren zum Betreiben einer Aktuatoranordnung	Schrade Simon Nowak Xi	DE102023210219.6
Verfahren zum Betreiben des Bremssystems eines Kraftfahrzeugs, Bremssystem	Schrade Simon Nowak Xi Boros Laszlo Peter Simon	DE102023208782.0
Verfahren zum Prüfen einer Funktionsfähigkeit einer elektromechanischen Radbremseinrichtung eines Kraftfahrzeugs, Radbremseinrichtung, Bremssystem	Peter Simon Boros Laszlo Nowak Xi Schrade Simon Walter Rainer	DE102023205887.1
Betriebsverfahren für eine Pedalanordnung für sicherheitskritische Fahrzeugsysteme	Schrade Simon Nowak Xi Peter Simon	DE102022213127.4
Verfahren und Vorrichtung zum Betreiben eines Bremssystems, Bremssystem und Kraftfahrzeug	Schrade Simon Nowak Xi Boros Laszlo Walter Rainer	DE102023211296.5
Verfahren und Steuergerät zum Beeinflussen einer Fahrdynamik eines Fahrzeugs	Haeffner Nicolas Schrade Simon	DE102023205773.5
Verfahren zum Betreiben einer Aktuatoranordnung, Aktuatoranordnung, Kraftfahrzeug	Schrade Simon Nowak Xi Walter Rainer	DE102023211288.4
Verfahren zum Betreiben einer Aktuatoranordnung, Aktuatoranordnung, Kraftfahrzeug	Schrade Simon Mehl Volker	DE102023209209.3

Title	Inventors	Appl.-Number
Verfahren zum Prüfen einer Bremsfunktionalität eines Bremssystems eines Fahrzeugs	Schrade Simon Nowak Xi Walter Rainer	DE102023204718.7
Steuervorrichtung und Traktionsregelverfahren für ein erstes Rad einer zusätzlich mit einem zweiten Rad bestückten Fahrzeugachse eines Fahrzeugs	Loss Tobias Peter Simon Schrade Simon Maier Marcel Boros Laszlo	DE102023210541.1
Verfahren zum Betreiben einer Aktuatoranordnung eines Bremssystems eines Kraftfahrzeugs, Aktuatoranordnung, Bremssystem, Kraftfahrzeug	Schrade Simon Nowak Xi Walter Rainer	DE102023209998.5
Computer-implementiertes Verfahren zur Bestimmung eines Radbremsmoments für eine Bremsvorrichtung in einem Fahrzeug	Peter Simon Comak Mesut Schrade Simon Nowak Xi	DE102023212934.5
Elektromechanischer Bremsaktor (EMB) für eine Reibungsbremse eines Fahrzeugs	Schrade Simon Nowak Xi	DE102023211962.5
Bremssystem für ein Fahrzeug und Verfahren zum Betreiben eines solchen Bremssystems	Schrade Simon Nowak Xi	DE102023212151.4
Verfahren und Vorrichtung zum Steuern eines Systems mit Anforderungen an dessen funktionale Sicherheit	Schrade Simon Verhagen Armin Peter Simon Boros Laszlo Nowak Xi Mehl Volker	DE102024200438.3

Supervised Theses

Type	Name	Title	Duration	
			from	until
M. Sc.	Mesut Comak	Brake Torque Estimation for New Brake Concepts with Deep Learning	01.05. 2022	31.10. 2022
M. Sc.	Oliver Markus	Methode zur Quantifizierung von fahrdynamischen Eigenschaften bei Fahrzeugen im Fehlerbetrieb	15.09. 2022	14.03. 2023
M. Sc.	Pratibha John	Study on the Application of Predictive Maintenance for Future Brake Concepts	01.10. 2022	28.03. 2023
B. Sc.	Jonas Laubis	Bestimmung der fahrdynamischen Eigenschaften von Fahrzeugen im Fehlerbetrieb	15.04. 2023	14.09. 2023
M. Sc.	Jan Pfingsten	Radindividuelle Regelungsstrategie der Fahrzeugverzögerung für neuartige Bremskonzepte	01.10 2023	31.03. 2023