

# Methodological Approach to Identify Automation Risks of Highly Automated Vehicles Using STPA

Methodischer Ansatz zur Identifizierung von Automationsrisiken von hochautomatisierten Fahrzeugen mittels STPA

Scientific work for obtaining the academic degree

Master of Science (M.Sc.)

at the Department of Mechanical Engineering of the Technical University of Munich

**Supervised by** Univ.-Prof. Dr.-Ing. Markus Lienkamp  
Thomas Ponn, M.Sc.  
Chair of Automotive Technology

**Submitted by** Jessica Steck, B.Sc.  
jessica.steck@tum.de

**Submitted on** Garching, October 12, 2018



# Project description

## Methodischer Ansatz zur Identifizierung von Automationsrisiken von hochautomatisierten Fahrzeugen mittels STPA

Revolutionäre Technik wie hochautomatisierte Fahrzeuge erfordern auch in ihrer Risikobeurteilung neue Ansätze. Ein vielversprechender Ansatz hierfür ist die im Jahr 2012 am MIT vorgestellte Methode STPA. Diese bringt der Vorteil, dass nicht mehr nur Fehler einzelner Komponenten als Ursache für Risiken und Unfälle betrachtet werden, sondern auch das Zusammenspiel funktionierender Teilsysteme. Diese Eigenschaft macht die Methode für den Einsatz im komplexen Umfeld von hochautomatisierten Fahrzeugen so interessant. Im Rahmen dieser Arbeit sollen mittels STPA Automationsrisiken – die als Konfliktsituationen definiert sind, die erst aufgrund der Automatisierung der Fahrzeuge auftreten können – bestimmt werden. Ein Beispiel hierfür ist eine Konfliktsituation, bei der ein Fußgänger einen Fußgängerüberweg queren möchte und dabei das Verhalten des hochautomatisierten Fahrzeugs aufgrund des fehlenden Blickkontakts mit dem „Fahrer“ missinterpretiert. Neben diesem Beispiel werden weitere Konfliktsituationen auftreten, die bereits jetzt analysiert werden sollen. Ziel der Arbeit ist es, einen bereits existierenden Ansatz zur Bestimmung von Risiken auf Autobahnen zu optimieren und auf ein Landstraßenszenario zu erweitern. Die Funktionsweise der Methode soll anhand mehrerer Beispiele erläutert werden. In einer theoretischen Masterarbeit sollen neu entstehende Risiken beim hochautomatisierten Fahren durch Anwendung der systematischen Methode STPA gefunden werden.

Folgende Punkte sind durch Frau Jessica Steck zu bearbeiten:

- Einarbeitung ins Themenfeld der Absicherung von hochautomatisierten Fahrzeugen und in die Anwendung von STPA
- Überarbeitung des bereits bestehenden Ansatzes zur Identifizierung von Automationsrisiken auf Autobahnen und anschließender Erweiterung auf ein Landstraßenszenario. Dazu müssen für die Landstraße Basis-Szenarien – in Analogie zu den bereits ansatzweise existierenden Autobahn-Basis-Szenarien wie Einscherer, Ausscherer, etc. – definiert werden.
- Die Funktionsweise des erstellten Risikoanalysemodells muss durch Beispielanalysen erklärt und belegt werden.
- Abschließend sollen die ausgearbeiteten Szenarien in Anlehnung an die ASIL-Bewertung bewertet werden. Dazu müssen die Auftretenswahrscheinlichkeit, die Schwere eines möglichen Unfalls und die Beherrschbarkeit der Situation abgeschätzt werden.
- Dokumentation der Ergebnisse

Die Ausarbeitung soll die einzelnen Arbeitsschritte in übersichtlicher Form dokumentieren. Der Kandidat/Die Kandidatin verpflichtet sich, die Semesterarbeit selbständig durchzuführen und die von ihm verwendeten wissenschaftlichen Hilfsmittel anzugeben.

Die eingereichte Arbeit verbleibt als Prüfungsunterlage im Eigentum des Lehrstuhls und darf Dritten nur unter Zustimmung des Lehrstuhlinhabers zugänglich gemacht werden.

Ausgabe: 12. April 2018

Abgabe: 12. Oktober 2018

---

Univ.-Prof. Dr.-Ing. Markus Lienkamp

---

Thomas Ponn, M.Sc.

# Geheimhaltungsverpflichtung

Frau: **Steck, Jessica**

Gegenstand der Geheimhaltungsverpflichtung sind alle mündlichen, schriftlichen und digitalen Informationen und Materialien die der Unterzeichner vom Lehrstuhl oder von Dritten im Rahmen seiner Tätigkeit am Lehrstuhl erhält. Dazu zählen vor allem Daten, Simulationswerkzeuge und Programmcode sowie Informationen zu Projekten, Prototypen und Produkten.

Der Unterzeichner verpflichtet sich, alle derartigen Informationen und Unterlagen, die ihm während seiner Tätigkeit am Lehrstuhl für Fahrzeugtechnik zugänglich werden, strikt vertraulich zu behandeln.

Er verpflichtet sich insbesondere:

- derartige Informationen betriebsintern zum Zwecke der Diskussion nur dann zu verwenden, wenn ein ihm erteilter Auftrag dies erfordert,
- keine derartigen Informationen ohne die vorherige schriftliche Zustimmung des Betreuers an Dritte weiterzuleiten,
- ohne Zustimmung eines Mitarbeiters keine Fotografien, Zeichnungen oder sonstige Darstellungen von Prototypen oder technischen Unterlagen hierzu anzufertigen,
- auf Anforderung des Lehrstuhls für Fahrzeugtechnik oder unaufgefordert spätestens bei seinem Ausscheiden aus dem Lehrstuhl für Fahrzeugtechnik alle Dokumente und Datenträger, die derartige Informationen enthalten, an den Lehrstuhl für Fahrzeugtechnik zurückzugeben.

Eine besondere Sorgfalt gilt im Umgang mit digitalen Daten:

- Für den Dateiaustausch dürfen keine Dienste verwendet werden, bei denen die Daten über einen Server im Ausland geleitet oder gespeichert werden (Es dürfen nur Dienste des LRZ genutzt werden (Lehrstuhlaufwerke, Sync&Share, GigaMove).
- Vertrauliche Informationen dürfen nur in verschlüsselter Form per E-Mail versendet werden.
- Nachrichten des geschäftlichen E-Mail Kontos, die vertrauliche Informationen enthalten, dürfen nicht an einen externen E-Mail Anbieter weitergeleitet werden.
- Die Kommunikation sollte nach Möglichkeit über die (my)TUM-Mailadresse erfolgen.

Die Verpflichtung zur Geheimhaltung endet nicht mit dem Ausscheiden aus dem Lehrstuhl für Fahrzeugtechnik, sondern bleibt 5 Jahre nach dem Zeitpunkt des Ausscheidens in vollem Umfang bestehen. Die eingereichte schriftliche Ausarbeitung darf der Unterzeichner nach Bekanntgabe der Note frei veröffentlichen.

Der Unterzeichner willigt ein, dass die Inhalte seiner Studienarbeit in darauf aufbauenden Studienarbeiten und Dissertationen mit der nötigen Kennzeichnung verwendet werden dürfen.

Datum: 12. Oktober 2018

Unterschrift: \_\_\_\_\_



## Erklärung

Ich versichere hiermit, dass ich die von mir eingereichte Abschlussarbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Garching, den 12. Oktober 2018

---

Jessica Steck, B. Sc.





# Contents

<b>List of Abbreviations</b> .....	<b>III</b>
<b>Glossary</b> .....	<b>V</b>
<b>1 Introduction</b> .....	<b>1</b>
<b>2 State of the Art</b> .....	<b>3</b>
<b>2.1 Levels of Automation</b> .....	<b>3</b>
<b>2.2 Functional Safety within ISO26262</b> .....	<b>5</b>
2.2.1 Basic Definitions for Hazard Analyses and Risk Assessments .....	6
2.2.2 Risk Assessment .....	6
<b>2.3 Safety Engineering Approaches</b> .....	<b>8</b>
2.3.1 FMEA.....	8
2.3.2 HAZOP.....	9
2.3.3 Systems Theoretic Approach – STPA .....	10
<b>2.4 Research Gap</b> .....	<b>14</b>
2.4.1 Risk of Automation .....	15
2.4.2 PEGASUS .....	15
2.4.3 Related Work.....	16
<b>2.5 Need for Action</b> .....	<b>19</b>
<b>3 Application of STPA to Automation Risks Resulting from AVs</b> .....	<b>21</b>
<b>3.1 Selection of Safety Engineering Approach</b> .....	<b>21</b>
<b>3.2 Preliminaries</b> .....	<b>22</b>
3.2.1 Definition of Fundamentals .....	23
3.2.2 Control Structure Diagram .....	24
3.2.3 Identification of Control Actions.....	25
3.2.4 Scenario Selection .....	26
3.2.5 Determination of Expectations .....	35
<b>3.3 STPA Implementation</b> .....	<b>45</b>
3.3.1 Determination of Unsafe Control Actions .....	45
3.3.2 Hazard Identification .....	47
3.3.3 Causal Factors Analysis .....	49
<b>3.4 Summary of Approach</b> .....	<b>50</b>

<b>3.5 Adaption to Class 1 and Class 3 Risks</b> .....	<b>52</b>
<b>4 Proof of Method Applicability</b> .....	<b>55</b>
<b>4.1 Application to a Category B Highway Scenario</b> .....	<b>55</b>
4.1.1 HW–B03: Control Actions Not Provided .....	56
4.1.2 HW–B03: Control Actions Provided .....	57
4.1.3 HW–B03: Control Actions Provided Instantly .....	59
4.1.4 HW–B03: Control Actions Provided Delayed .....	59
4.1.5 HW–B03: Too Soon Stopped Acceleration .....	63
4.1.6 HW–B03: Too Long Applied Braking .....	63
4.1.7 HW–B03: Discussion of Identified Hazards .....	63
<b>4.2 Applicability to Category A and C Highway Scenarios</b> .....	<b>65</b>
4.2.1 Category A: Cut in with positive relative velocity .....	66
4.2.2 Category C: End of Neighboring Lane .....	66
<b>4.3 Applicability to a Combined Driving Scenario</b> .....	<b>67</b>
<b>4.4 Applicability to a Rural Road Scenario</b> .....	<b>68</b>
4.4.1 RR–A06: Control Actions Not Provided .....	68
4.4.2 RR–A06: Control Actions Provided .....	69
4.4.3 RR–A06: Control Actions Provided Instantly .....	71
4.4.4 RR–A06: Control Actions Provided Delayed .....	71
4.4.5 RR–A06: Too Soon Stopped Acceleration .....	73
4.4.6 RR–A06: Too Long Applied Braking .....	73
4.4.7 RR–A06: Discussion of Identified Hazards .....	75
<b>4.5 Discussion</b> .....	<b>77</b>
<b>5 Summary and Outlook</b> .....	<b>79</b>
<b>List of Figures</b> .....	<b>i</b>
<b>List of Tables</b> .....	<b>iii</b>
<b>Bibliography</b> .....	<b>v</b>
<b>Appendix</b> .....	<b>ix</b>

# List of Abbreviations

A	Accident
ACC	Adaptive Cruise Control
AD	Automated Driving
ASIL	Automated Safety Integrity Level
AV	Automated Vehicle
CA	Control Action
D	Delayed
DMV	Department of Motor Vehicles
ETA	Event Tree Analysis
FCW	Forward Collision Warning
FMEA	Failure Mode and Effect Analysis
FTA	Fault Tree Analysis
GIDAS	German In-Depth Accident Study
H	Hazard
HAZOP	Hazard and Operability Study
I	Instantly
LDW	Lane Departure Warning
LKA	Lane Keeping Assist
OEM	Original Equipment Manufacturer
QM	Quality Management
RPN	Risk Priority Number
SC	Safety Constraint
STAMP	Systems-Theoretic Accident Model and Process
STPA	System-Theoretic Process Analysis
UCA	Unsafe Control Action



# Glossary

A-1	Collision AV with leading vehicle
A-2	Collision AV with following vehicle
A-3	Collision AV with neighboring vehicle
A-4	Collision AV with pedestrian / cyclist / motorcyclist
A-5	Collision AV with obstacles or surrounding
A-6	Collision of other vehicles
CA-1	Keep speed and keep lane
CA-2	Keep speed and change lane
CA-3	Change speed and keep lane
CA-4	Change speed and change lane
CA-5	Abort lane change
CA-6	Emergency brake
CA-7	Emergency stop
Failure	Termination of the ability of an element to perform a function as required
H-1	AV entering safety distance to leading vehicle
H-2	AV entering safety distance to following vehicle
H-3	AV entering safety distance to neighboring vehicle
H-4	AV entering safety distance to pedestrian / cyclist / motorcyclist
H-5	AV entering minimum distance to obstacle or surrounding
H-6	AV behavior startling or confusing other road user(s)
H-7	AV provoking other road user(s) to perform dangerous maneuvers
H-8	AV startling own AV human driver
Harm	Physical injury or damage to the health of persons
Hazard	Potential source of harm caused by malfunctioning behavior of an item
Hazard Analysis	Method to identify and categorize hazardous events
Hazardous Event	Combination of a hazard and an operational situation
HW-A01	Cut in with positive relative velocity on highway (vehicle cutting in is faster than the ego-vehicle)
HW-A02	Cut in with negative relative velocity (vehicle cutting in is slower than the ego-vehicle)
HW-A03	Cut out on highway
HW-A04	Cut through on highway
HW-A05	Slow leading vehicle on highway
HW-A06	Leading vehicle on highway brakes
HW-A07	Leading vehicle on highway accelerates
HW-A08	Slow moving traffic on highway
HW-A09	End of traffic jam ahead on highway

HW-A10	Small static object (can be run over) on highway
HW-A11	Small moving object (can be run over) on highway
HW-A12	Large static object (cannot be run over) on highway
HW-A13	Large moving object (cannot be run over) on highway
HW-A14	Pedestrian / cyclist on highway
HW-A15	Wrong-way driver on highway
HW-A16	Convoy on highway
HW-A17	Heavy-duty transport on highway
HW-A18	Gigaliner on highway
HW-B01	Emergency vehicle on highway
HW-B02	Beginning speed limit on highway
HW-B03	End speed limit on highway
HW-B04	Time frame of temporal speed limit on highway begins
HW-B05	Time frame of temporal speed limit on highway ends
HW-B06	Beginning no passing on highway
HW-B07	End no passing on highway
HW-B08	Opening new lane on highway
HW-B09	Lane ends on highway
HW-B10	Beginning emergency lane clearance on highway
HW-B11	End emergency lane clearance on highway
HW-B12	Red traffic light on highway
HW-B13	Traffic light turns green
HW-B14	Ramp on highway
HW-B15	Exit on highway
HW-B16	Toll station on highway
HW-B17	Customs station on highway
HW-B18	Highway junction on highway
HW-C01	No overtaking on highway
HW-C02	No overtaking one-sided on highway
HW-C03	Missing lane marking on highway
HW-C04	Confusing lane marking on highway
HW-C05	Narrowed lane on highway
HW-C06	Ending of neighboring lane on highway
HW-C07	Ruts on highway
HW-C08	Slippery road surface on highway
HW-C09	Wind on highway
Malfunctioning Behavior	Failure or unintended behavior of an item with respect to its design intent
Operational Situation	Scenario that can occur during a vehicle's life
Risk	Combination of the probability of occurrence of harm and the severity of that harm
Risk Assessment	Method to specify safety goals and ASILs related to the prevention or mitigation of the associated hazards in order to avoid unreasonable risk
RR-A01	Cut in with positive relative velocity on rural road (vehicle cutting in is faster than the ego-vehicle)
RR-A02	Cut in with negative relative velocity on rural road (vehicle cutting in is slower than the ego-vehicle)

RR-A03	Cut out on rural road
RR-A04	Cut through on rural road
RR-A05	Overtaking vehicle from oncoming traffic in ego-vehicle's lane on rural road
RR-A06	Oncoming vehicle turning left on rural road
RR-A07	Slow leading vehicle on rural road
RR-A08	Very slow leading vehicle on rural road
RR-A09	No more neighboring vehicle on rural road
RR-A10	End of traffic jam on rural road
RR-A11	Leading vehicle on rural road brakes
RR-A12	Leading vehicle on rural road accelerates
RR-A13	Small static object (can be run over) on rural road
RR-A14	Small moving object (can be run over) on rural road
RR-A15	Large static object on entire lane (cannot be run over) on rural road
RR-A16	Large moving object (cannot be run over) on rural road
RR-A17	Pedestrian / cyclist on rural road
RR-A18	Convoy ahead on rural road
RR-A19	Heavy-duty transport ahead on rural road
RR-A20	Gigaliner ahead on rural road
RR-A21	Large static object on right half of lane on rural road
RR-B01	Emergency vehicle on rural road
RR-B02	Beginning speed limit on rural road
RR-B03	End speed limit on rural road
RR-B04	Time frame of temporal speed limit on rural road begins
RR-B05	Time frame of temporal speed limit on rural road begins
RR-B06	Beginning no passing on rural road
RR-B07	End no passing on rural road
RR-B08	Opening new lane on rural road
RR-B09	Lane ends on rural road
RR-B10	Red traffic light on rural road
RR-B11	Stop sign on rural road
RR-B12	Yield sign on rural road
RR-B13	Traffic light turns green on rural road
RR-B14	Entry of roundabout on rural road
RR-B15	Exit of roundabout on rural road
RR-B16	Approaching intersection on rural road
RR-B17	Entry of intersection on rural road
RR-C01	No overtaking on rural road
RR-C02	No overtaking one-sided on rural road
RR-C03	Missing lane marking on rural road
RR-C04	Confusing lane marking on rural road
RR-C05	Narrowed lane on rural road
RR-C06	Ruts on rural road
RR-C07	Slippery road surface on rural road
RR-C08	Wind on rural road

RR-C09	Construction site with one-sided traffic on rural road
RR-C10	Traffic island on rural road
Safety	Absence of unreasonable risk
SC-1	AV must always maintain safety distances
SC-2	AV must never startle or confuse others
SC-3	AV must never block traffic
SC-4	AV must never provoke others to dangerous maneuvers
SC-5	AV must never startle own AV human driver
SC-6	AV must always work properly



# 1 Introduction

The automotive industry currently faces big development trends, among others are the development of electric driving and automated driving [1, p. 8]. A few electric vehicles are already on the market, automated vehicles do currently not exist and customers have to wait for the first vehicles to come on the market. In all the research and development around automated driving, one question is still to be answered:

## **Will automated vehicles really reduce the amount of accidents as everybody expects?**

The development of automated vehicles aims to reduce the amount of accidents on public roads, but these vehicles do not only prevent accidents, they also create new types of accidents. These new types can reduce the trust of humans in automated systems extremely. A consultant for self-driving car companies, Dr. Phil Koopman, identifies the general problem to be that automated vehicles drive different than humans and humans do not expect the different automated driving behavior of other road users [2]. The discrepancy between automated vehicle behavior and the human expectations in the surrounding vehicles is the cause of arising accidents on public roads that would not have occurred without automated systems.

The following accident description is an extract from the accident report of a test vehicle from Apple Inc. released by the Department of Motor Vehicles (DMV) and happened recently in California, due to a misunderstanding of an automated vehicle and a human driver. "On August 24<sup>th</sup> [2018] at 2:58 PM, an Apple test vehicle in autonomous mode was rear-ended while preparing to merge onto Lawrence Expressway South from Kifer Road. The Apple test vehicle was traveling less than 1 mph waiting for a safe gap to complete the merge when a 2016 Nissan Leaf contacted the Apple test vehicle at approximately 15 mph."

[3, p. 2]

The automated vehicle was about to merge into another lane, but drives over-carefully and very slow trying to find a gap in the oncoming traffic. The human driver following the automated vehicle probably expected that the vehicle would slip into the oncoming traffic and merge immediately. Because it did not do so, the human bumped into the automated vehicle. This accident brought back the public discussion about the safety of automated vehicles. The BBC comments that these types of accidents occur because "the self-driving cars would stop abruptly in scenarios where humans might zip through" [4].

The accident triggered a high amount of press reports which shows the importance of preventing accidents that are caused by different driving styles compared to human driving. In order to prevent these accidents, risks of automated vehicles must be identified and analyzed. Knowing about possible risks is necessary to develop safe systems. Besides the risks due to malfunctions, also the ones due to different driving behavior have to be identified. The objective of this work is to develop a method which can be used to identify risks of automated driving systems which occur due to different driving patterns of these systems compared to human driving.

This thesis is structured into three main parts: the state of the art, the application of the System-Theoretic Process Analysis (STPA) to automation risks of automated vehicles, and the proof of the method applicability to highway and rural road scenarios. It is concluded with a summary and outlook. The structure is visualized in Figure 1.1.

In the state of the art (Chapter 2), the differentiation of levels of automated driving systems are explained according to the standard SAE J3016 [5]. Furthermore, the process for functional safety development in the international standard ISO26262 [6] is described. The definitions necessary for this work are reproduced and the proposed risk assessment method ASIL is outlined. It is followed by the introduction of three safety engineering approaches that can be used for a hazard analysis within ISO26262 [6]: FMEA, HAZOP, and STPA. The research gap is drafted based on the definition of automation risks, the project PEGASUS and related work. The problem addressed with this thesis is concluded in a need for action.

Chapter 3 focuses on the adaption of the System-Theoretic Process Analysis (STPA) to automation risks which arise for road users due to the different driving behavior of automated driving systems. At the beginning, the use of STPA is justified and some preliminaries are defined that are necessary for the following STPA implementation. Next, the concept of the newly developed method is summarized. The chapter ultimately discusses adapting the method to other types of automation risks in automated driving.

The applicability of the proposed hazard analysis method is proven in Chapter 4. Example analyses are carried out for typical highway driving scenarios and one typical rural road scenario.

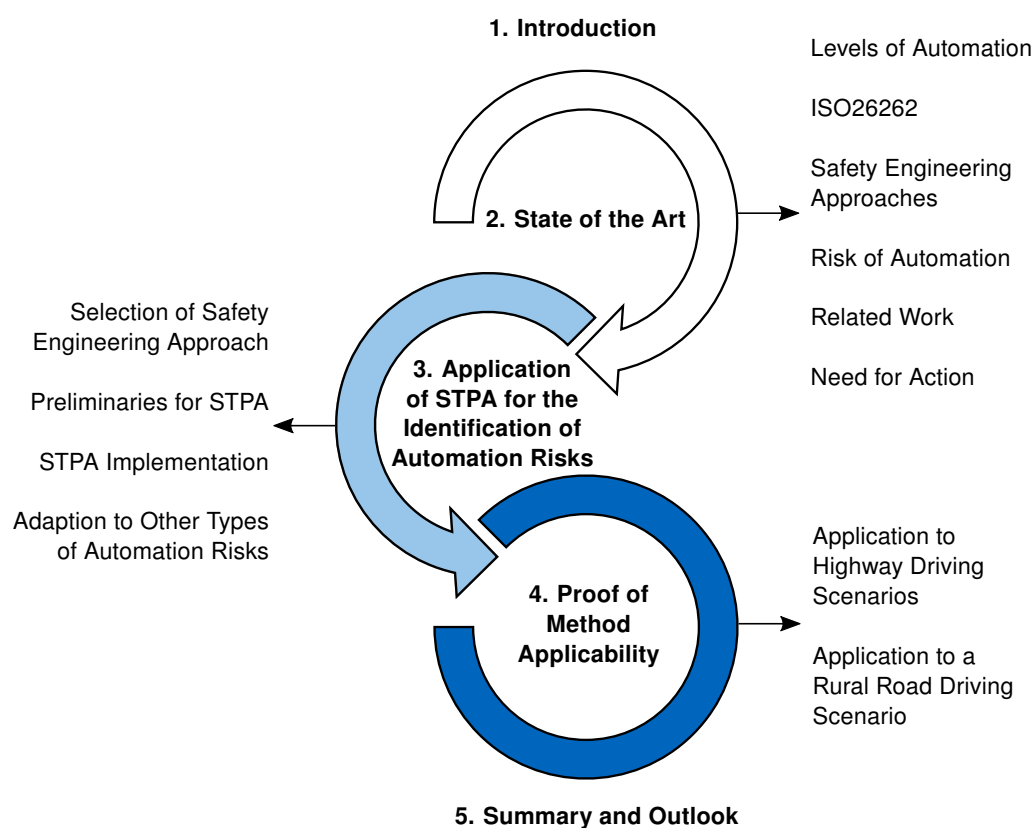


Figure 1.1: Structure of this thesis.

## 2 State of the Art

Many companies are working on the development of Automated Vehicles (AVs) as the amount of companies that are registered for testing AVs at the DMV ([7]) shows. The risks that can arise with these new types of vehicles are though mostly unknown and are required to be able design AVs at a high safety level and to make people trust them.

This chapter introduces and explains the levels of automation of Automated Driving (AD) systems and gives an overview of the functional safety determination of today's systems. The determination of a functional safety concept requires a hazard analysis and safety assessment. For both parts, some basic definitions are given and the determination of ASILs for safety assessment is explained. Three hazard identification and analysis techniques are presented: FMEA, HAZOP, and STPA. Finally, the research gap in the risk determination of AVs and the intention of this thesis are developed.

### 2.1 Levels of Automation

The SAE standard J3016 [5] categorizes different types of AD into six levels of automation. Figure 2.1 illustrates and describes these levels and the distribution of the driving tasks between driver and system.

Level	Name	Lateral and longitudinal vehicle control	Object and event detection and response	Dynamic Driving Task fallback	Operational design domain
Driver performs part or all of the Dynamic Driving Task					
0	No Automation	Driver	Driver	Driver	n/a
1	Driver Assistance	Driver and System	Driver	Driver	Limited
2	Partial Automation	System	Driver	Driver	Limited
AD System performs the entire Dynamic Driving Task (while engaged)					
3	Conditional Automation	System	System	Fallback-ready user	Limited
4	High Automation	System	System	System	Limited
5	Full Automation	System	System	System	Unlimited

Figure 2.1: Levels of automation according to SAE J3016 [5, p. 17].

In the first three groups, level 0 to 2, the human driver performs a part or all of the dynamic driving task. From level 3 onward, the AD system performs the entire dynamic driving task. The following explanation of each level is extracted from [5, pp. 19-21]:

**Level 0: No Automation** – At this level of automation, the human driver performs all dynamic driving tasks throughout the entire driving time. Warning or support systems, such as emergency intervention, can exist to improve the driving performance. Lane Departure Warning (LDW) and Forward Collision Warning (FCW) systems belong to this level [8, p. 39].

**Level 1: Driver Assistance** – A driver assistance system and a human driver share the driving task. The assistance system takes over either acceleration / deceleration or steering, not both. All remaining tasks are left for the human driver, who must also supervise all AD tasks and represent the fallback level for the automation. Currently available systems at this level are the Adaptive Cruise Control (ACC) and the Lane Keeping Assist (LKA) [8, p. 40]. ACC controls the longitudinal vehicle speed; LKA the lateral vehicle movement [8, p. 50].

**Level 2: Partial Automation** – This mode requires at least one driver assistance system, which executes both longitudinal (acceleration / deceleration) and lateral (steering) control. The human driver remains in the loop to monitor the automated tasks and to execute all remaining tasks. Systems at this level are for example traffic jam or highway assistance systems [8, p. 9]. These systems follow the leading vehicle at a safe distance in the center of the lane [8, p. 51,52]. Traffic jam assistance systems operate at speeds up to 60 km/h; highway assistance systems up to 130 km/h [8, p. 51,52]. Highway assistance systems are additionally capable of overtaking maneuvers, which are initiated by the driver [8, p. 52]. Key parking systems also belong to this level [8, p. 9]. These are parking systems where the vehicle parks itself while the driver can be outside of the vehicle but has to be pressing a key button [8, p. 52].

**Level 3: Conditional Automation** – The AD system performs all dynamic driving tasks (lateral and longitudinal) within certain use cases. The human driver has to determine appropriate situations and to activate the system. At this level, humans do not have to monitor the driving and can focus on not driving related tasks while the system is activated. Nevertheless, if the system requires an intervention, the driver has a limited period of time to take over. Systems at level 3 include traffic jam chauffeur and highway chauffeur [8, p. 9]. The functions of both are similar to the assistance systems of level 2, however the human driver is not required to constantly supervise the system [8, pp. 52,53]. Compared to the highway assistance system, the highway chauffeur is additionally capable of overtaking maneuvers and driving in highway junctions [8, p. 53].

**Level 4: High Automation** – At level 4, an AD system fulfills the same tasks as a level 3 one, except that driver does not exist as fallback anymore. The human driver will not respond to any request for intervention. An AD system at this level is for example a driverless valet parking system [8, p. 43]. The vehicle finds open parking spots in parking garages by itself and does not require human observation [8, p. 53].

**Level 5: Full Automation** – Here, a human driver is not obligatory anymore. An AD system at this level performs all aspects of the dynamic driving task when activated. The system is capable of handling all roadway and environmental conditions that a human driver can manage, not only in certain use cases but throughout the entire driving time. BARTELS et al. [8, p. 43] describe an universal robot taxis at this level. These taxis would fulfill all tasks of today's vehicles without the need for a human [8, p. 55].

In this work, an AD system and an AV refer to levels 3 and higher.

## 2.2 Functional Safety within ISO26262

ISO26262 [6] is a guideline to determine functional safety for the entire product life cycle of systems within road vehicles [9, p. V]. Functional safety herein means the "absence of an unreasonable risk due to hazards caused by malfunctioning behavior of [Electrical / Electronic] systems" [9, p. 8].

The guideline describes the procedure to identify the requirements necessary for a safe development of safety critical components and systems [10, p. 86]. Expressions and conceptual definitions are given which are relevant for the development of a functional safety concept.

Figure 2.2 is a reduced visualization of the guideline's structure which is oriented on the V-model for product development [10, p. 86]. ISO26262 [6] provides the users a procedure for every product phase: concept phase, product development, and production and operation phase. This work is located within the concept phase of AV. The concept phase contains four steps, from item definition to the definition of the functional safety concept. This phase includes a hazard analysis and risk assessment, which is the foundation for the functional safety concept.

The first part of this section summarizes some basic definitions necessary for a hazard analysis and risk assessment given in the standard ISO26262 [6]. In the second part, the proposed risk assessment method Automated Safety Integrity Level (ASIL) is outlined.

Section 2.3 introduces hazard analysis methods recommended in the standard and one not explicitly recommended. Hazards and their risks need to be defined as early as in the concept phase of the V-model [10, p. 86]. These definitions are used to identify top-level safety requirements to create a functional safety concept [11, p. 12]. The result is further used for the development of the system [10, p. 86], which is split into the development at system level, at hardware level, and software level. All three levels are connected throughout the development.

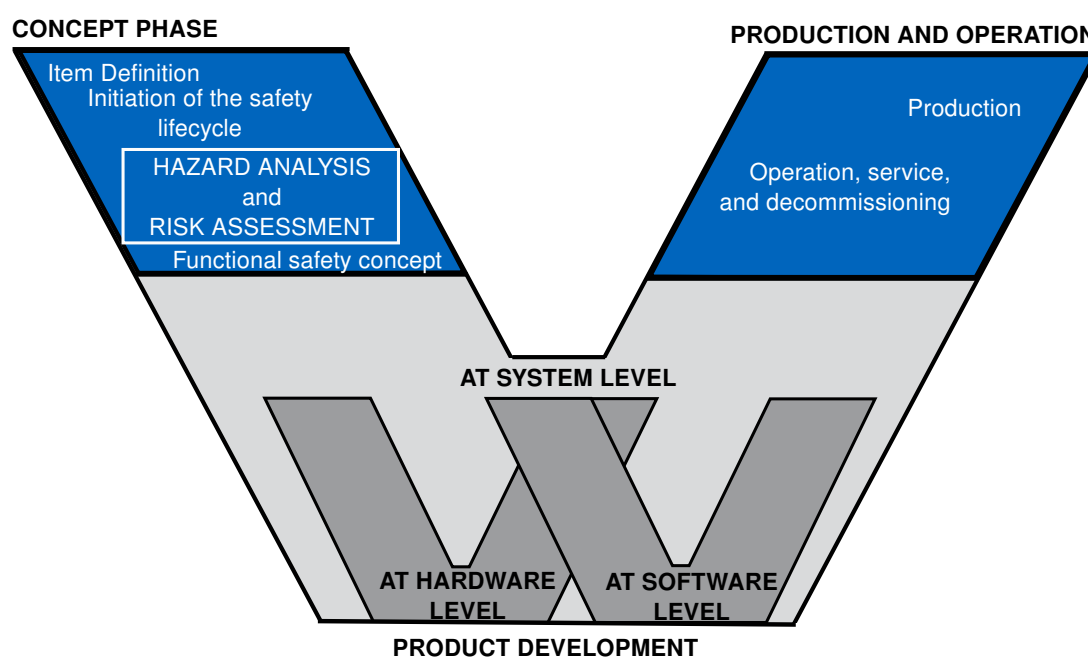


Figure 2.2: Structure of the product life cycle in the ISO26262 [6].

### 2.2.1 Basic Definitions for Hazard Analyses and Risk Assessments

Hazard analysis and risk assessment require a definition of the used terminology. The following explanations are given according to their specification in ISO26262-Part 1 [9].

**Hazard Analysis:** A hazard analysis is a "method to identify and categorize hazardous events" [9, p. 9].

**Hazardous Event:** A hazardous event identified through a hazard analysis is a "combination of a hazard and an operational situation" [9, p. 9].

**Operational Situation:** An operational situation is a "scenario that can occur during a vehicle's life" [9, p. 11]. In this thesis these situations are also called driving scenarios.

**Hazard:** A hazard means the "potential source of harm caused by malfunctioning behavior of [an] item" [9, p. 9]

**Malfunctioning Behavior:** Malfunctioning behavior describes a "failure or unintended behavior of an item with respect to its design intent" [9, p. 10].

**Failure:** A failure is the "termination of the ability of an element to perform a function as required" [9, p. 7].

**Harm:** A "physical injury or damage to the health of persons" [9, p. 9] is called harm.

**Risk Assessment:** After a hazard analysis is carried out, a risk assessment can follow. Risk assessments define "safety goals and ASILs related to the prevention or mitigation of the associated hazards in order to avoid unreasonable risk" [9, p. 9]. The determination of ASILs is explained in Section 2.2.2.

**Risk:** The "combination of the probability of occurrence of harm and the severity of that harm" [9, p. 13] is called risk.

**Safety:** Safety is the "absence of unreasonable risk" [9, p. 14].

All definitions are used in the same manner in this thesis.

### 2.2.2 Risk Assessment

Hazardous events need to be classified by their relevance in order to determine how much time and money are reasonably invested to solve them. A method for this is called ASIL, which is defined in ISO26262 [11]. According to it, hazardous events need to be analyzed by three parameters: probability of exposure, controllability, and severity [11, p. 7].

The probability of exposure defines the frequency of a driving situation in which the hazard can occur [10, p. 89]. ASIL therefore provides five classes: E0, E1, E2, E3, E4, ranging from incredibility to high probability, respectively. This grading including can be seen in Table 2.1. The table also includes two suggested classifications of the exposure classes in [11] due to the duration in operational situations and the frequency of a specific situation. In this work, all classifications are performed using the classification by the duration of operational situations.

Table 2.1: Classes of exposure and their duration in operational situations according to [11, pp. 9,22,23].

	<b>E0</b>	<b>E1</b>	<b>E2</b>	<b>E3</b>	<b>E4</b>
<b>Description</b>	Incredible	Very low probability	Low probability	Medium probability	High probability
<b>Duration</b>	Not specified	Not specified	< 1 % of average operating time	1 % - 10 % of average operating time	> 10 % of average operating time
<b>Frequency of situation</b>	Not specified	Occurs less often than once a year for the great majority of drivers	Occurs a few times a year for the great majority of drivers	Occurs once a month or more often for an average driver	Occurs during almost every drive on average

The controllability rates the chance of a driver or of other road participants to react to a hazardous situation and bringing it under control, an action necessary to avoid harm [10, p. 89]. For this parameter four categories are defined: C0,C1,C2,C3; ranging from generally controllable to uncontrollable. Table 2.2 shows each of the four classes' definitions.

Table 2.2: Classes of controllability according to [11, p. 10].

	<b>C0</b>	<b>C1</b>	<b>C2</b>	<b>C3</b>
<b>Description</b>	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

Severity refers to a potential harm, which results from the respective hazard [10, p. 89]. This parameter consists of four severity classes: S0, S1, S2, and S3. All driving situations where a failure would not lead to an injury are classified as S0. All driving situations where a failure could lead to a life-threatening or fatal injury are classified as S3. The grading of all classes can be found in Table 2.3.

Table 2.3: Classes of severity according to [11, p. 9].

	<b>S0</b>	<b>S1</b>	<b>S2</b>	<b>S3</b>
<b>Description</b>	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

A determination of these three parameters, exposure, controllability, and severity, for a driving situation allows to identify the respective ASIL, according to Table 2.4. Five levels exist, which are Quality Management (QM), ASIL A, ASIL B, ASIL C, and ASIL D. ASIL A corresponds to the lowest risk potential and ASIL D to the highest. The higher the ranking, the more intervention required to prevent the situation from occurring [10, p. 90]. If a driving situation is rated to the

level QM, only some quality management improvements need to be carried out [10, p. 91]. The severity level S0 and exposure level E0 are not listed in the table because all their hazards are classified QM, independently of its controllability and exposure or controllability and severity respectively. For every determined ASIL, a corresponding safety goal has to be defined [11, p. 11].

Table 2.4: Table for the ASIL determination according to [11, p. 10].

Severity class	Probability class	Controllability class		
		C1	C2	C3
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

## 2.3 Safety Engineering Approaches

This section introduces three different safety engineering approaches: FMEA, HAZOP, and STPA, from which FMEA and HAZOP are recommended in the standard ISO26262 [6]. All three approaches are different system safety analysis techniques. STPA differs from the other two by its causality model based on which hazards are identified.

### 2.3.1 FMEA

Failure Mode and Effect Analysis (FMEA) is an analysis technique that underlies the assumption that failures are the only cause of a hazard, as defined in Section 2.2. The method has three main objectives. The first one is to identify all possible failure modes of a product or process, their causes, and their effects on the entire system [12, p. 21]. Secondly, the analysts assess the risk for each identified failure mode and create a prioritized list with corrective actions [12, p. 21]. Finally, they select corrective actions which prevent most severe consequences [12, p. 21].

The analyst team should contain cross-functional team members who are subject matter experts [12, p. 21]. They should start with their analysis as early as in the design phase of the product life cycle [13, p. 119]. FMEA can be continued throughout the entire product life cycle considering failure elements resulting from system changes or aging [13, p. 119].

At the beginning, an FMEA team collects as much information as available about the system to be analyzed. This information can include design drawings, system schematics, functional diagrams, previous analytical data, system descriptions, lessons learned data, manufacturer's component data / specifications, preliminary hazard list, preliminary hazard analysis, and other system analyses which were previously performed [13, pp. 120,121]. This information structures a system into subsystems down to the component level. Analysts can then identify failures



of each individual component and conclude these effects on a system level [13, p. 119]. This evaluation starts at the lowest level element, where the detected failures could cause failure modes on higher level elements [14, p. 16].

Figure 2.3 gives an example for an FMEA worksheet. In the first column, the experts list all the components, subsystems, and the system itself [12, p. 26]. For each item, the design intent is collected in the column 'function' [12, p. 27]. In the following column, the failure mode is inserted. It describes the manner in which the item may fail [12, p. 28]. The consequences of the respective failure are listed in the column 'effect' [12, p. 32]. Severity is characterized by a ranking number describing the most serious effect for the detected failure modes [12, pp. 34]. Similarly, occurrence is characterized by a ranking number describing the likelihood for the detected failure modes and its causes [12, pp. 38]. Causes are detected by looking at the specific reasons for failures [12, p. 36]. Existing design controls can be created for either failure prevention or failure detection. Both should be noted in their respective cells on the worksheet. The column 'detection' links a ranking number, which associates the best detection control [12, p. 43]. Risk Priority Number (RPN) ranks each failure mode by the severity of the effect, likelihood of occurrence of the cause, and likelihood of detection of the cause [12, p. 44]. The final column is for an advice of actions that reduce or eliminate risks for each potential failure [12, p. 45]

Item	Function	Potential Failure Mode	Potential Effect(s) of Failure	Severity	Potential Cause(s) of Failure	Occurrence	Current Design Controls – Prevention	Current Design Controls – Detection	Detection	RPN	Recommended Action(s)

Figure 2.3: Generic FMEA worksheet according to [12, p. 26].

### 2.3.2 HAZOP

Hazard and Operability Study (HAZOP) is one of the mostly used hazard identification and analysis methods [15, p. 1]. The purpose of the hazard identification is to systematically determine all hazards preventing a system's efficient operation [16, p. 9]; the purpose of the hazard analysis part is to investigate the hazards' possible causes and consequences [15, p. 4]. HAZOP can be applied to many different systems, especially when there is a flow of materials, of people or of information [17, p. 14]. The entire study is carried out under the guidance of an experienced study leader with multiple specialists from different disciplines [17, p. 10].

The premise of HAZOP is that deviations from the design intent cause hazards [15, p. 4], analogous to FMEA. Therefore, all deviations have to be analyzed and the respective hazards revealed. The deviations also need to be inspected for their possible causes and consequences [15, p. 25]. Every consequence must be considered, no matter if it is an immediate or long-term hazard and whether consequences always follow exposure or not [16, p. 6].

The HAZOP is divided into two parts. In Part 1, the entire system is split into all its components,

which should be as precise as necessary to represent its function and design adequately. The HAZOP team identifies discrete properties of each component [17, p. 12]. The level of refinement depends on the complexity of the system and the magnitude and relevance of the consequences [17, p. 11]. Part 2 consists of a guide-word-driven analysis for every single component. Table 2.5 and 2.6 show two sample sets of guide words and their meanings. The selected guide words must cover all possible deviations of the component's properties [17, p. 12]. This step is usually performed by the study leader [17, p. 12]. Once the guide words are identified, the HAZOP team carries out an analysis with each of them for every property of every component [15, p. 33]. Through this process, every component deviation is derived. In the next step, the problem cause and consequence is detected for every theoretically possible deviation [15, pp. 33,34]. This information is necessary to determine the required actions to prevent the deviation. Similar to FMEA, a tabular representation is possible.

Table 2.5: Guide words for HAZOP with their meanings: example set 1 according to [17, p. 12].

Guide Word	Meaning
NO OR NOT	Complete negation of the design intent
MORE	Quantitative increase
LESS	Quantitative decrease
AS WELL AS	Qualitative modification / increase
PART OF	Qualitative modification / decrease
REVERSE	Logical opposite of the design intent
OTHER THAN	Complete substitution

Table 2.6: Guide words for HAZOP with their meanings: example set 2 according to [17, p. 12].

Guide Word	Meaning
EARLY	Relative to the clock time
LATE	Relative to the clock time
BEFORE	Relating to order or sequence
AFTER	Relating to order or sequence

HAZOP is equally to FMEA, Fault Tree Analysis (FTA), and Event Tree Analysis (ETA) a hazard analysis technique which is recommended in the standard ISO26262 [6] [11, p. 12]. Although is it recommended, the hazard and operability study has one main disadvantage, similarly to FMEA: the analysis only reveals hazards occurring from a single deviation. Hazards caused by multiple deviations cannot be identified [18, p. 8].

### 2.3.3 Systems Theoretic Approach – STPA

In *Engineering a Safer World: Systems Thinking Applied to Safety*, LEVESON [19] suggests a different approach for creating safer systems: the System-Theoretic Process Analysis (STPA). She proposes this new method because traditional safety engineering approaches such as HAZOP and FMEA only work well for simple systems [19, p. 3]. Today's systems are much more complex than they used to be, thus requiring new hazard identification methods [19, p. 3]. LEVESON [19, pp. 3-6] identifies nine reasons why these traditional simple models are no longer sufficient:

1. Lessons learned from predecessors cannot be recorded anymore, as technology is changing more quickly. These lessons learned used to be a reliable source for identifying hazards.

2. Product life cycles are decreasing due to rapid technological advancements and therefore systems are tested merely briefly.
3. New technology leads to new causes of accidents.
4. New hazards occur due to advances in science and societal changes.
5. System complexity is increasing as system components are interacting or due to dynamic changes.
6. It is becoming less acceptable that accidents occur in the first place. This is due to systems becoming more complex and therefore more expensive and labor-intensive in their development.
7. The pressure on developers increases with tight budget limitations for complex systems. Shortcuts need to be made, which may compromise safety.
8. Systems that allow a complex interaction between humans and automation are booming. The shared control creates new causes for human errors.
9. People expect the government to take responsibility for public safety as they cannot control the risks around them anymore. Innovative design strategies for regulation are required.

All these difficulties can be handled with LEVESON's STPA model and its underlying expanded accident causality model: Systems-Theoretic Accident Model and Process (STAMP) [19, p. 73].

## STAMP

Traditional causality models such as HAZOP assume that chains of failures lead to accidents and that these failures need to be prevented [19, p. 75]. In contrast, STAMP works top-down [20, p. 12]: the focus is set towards enforcing behavioral safety constraints. Accidents are not only to be caused by individual component failures, but also by component interaction failure [19, p. 73]. An accident is herein defined as "an undesired and unplanned event that results in a loss (including loss of human life or injury, property damage, environmental pollution, and so on)" [19, p. 467]. This defines a hazard as follows: "A system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident (loss)" [19, p. 467].

STAMP contains three design elements: (1) safety constraints, (2) hierarchical safety control structures, and (3) process models.

1. Safety constraints specify the requirements for a system or component and have to meet the safety level that society currently demands [19, p. 80]. Within the development process, the constraints are refined from the system level down to the component level [19, p. 80]. All safety constraints have to be complied throughout the entire development process, otherwise a hazard occurs.
2. Systems can be grouped into hierarchical structures. Each level imposes new safety constraints on the subjacent level. In between them, control processes enforce the underlying safety constraints. If the control process does not guarantee sufficient control or safety constraints are violated, accidents occur [19, pp. 80-81]. Loss events are the consequences of component failures, external disturbances,

poor interaction among system components, or a malfunction of a system component that creates a hazardous system status [19, p. 75]. Each hierarchical level contains a controller that controls a subjacent level and receives feedback from it. A diagram of different levels and their interactions is called a control structure diagram. Through these diagrams, not only are physical aspects represented, but also social and logical aspects, operations and management aspects and information [21, p. 34]

3. A process model is required for every controller [19, p. 87]. These models help to identify the causal factors for a hazard in a process effectively. Automated and human controller models consist of information defining the relationship among the system variables, the current state, and information about how states can change [19, p. 87]. This information helps to identify the performed Control Actions (CAs) [19, p. 88]. After a CA is executed, feedback is returned to the higher level [19, p. 88]. Figure 2.4 visualizes the interaction of a controller with the controlled process. The process model is pictured inside of the controller. Each arrow pointing downwards symbolizes a message conveyed to the next level. The message includes information that enforces safety constraints. Each arrow pointing upwards reflects the feedback on how well these constraints were fulfilled. Every hierarchical level has a controller and therefore needs a defined process model [19, p. 89]. Figure 2.4 visualizes the interaction between controller, controlled process and the object transported between these elements.

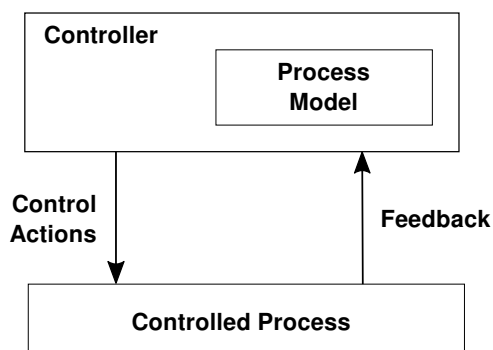


Figure 2.4: Control structure according to [19, p. 88].

The combination of these three elements sets the foundation for a hazard analysis of a system: hazardous system states can arise either by inadequate control or by inadequate enforcement of safety constraints as pictured in Figure 2.5.

The causes for accidents at each level can be grouped into four categories [19, p. 92]. Accidents occur, if

- necessary CAs are not provided
- necessary CAs are provided at the wrong time (too early or too late) or stopped too soon
- unsafe CAs are provided
- appropriate CAs are provided, but not executed.

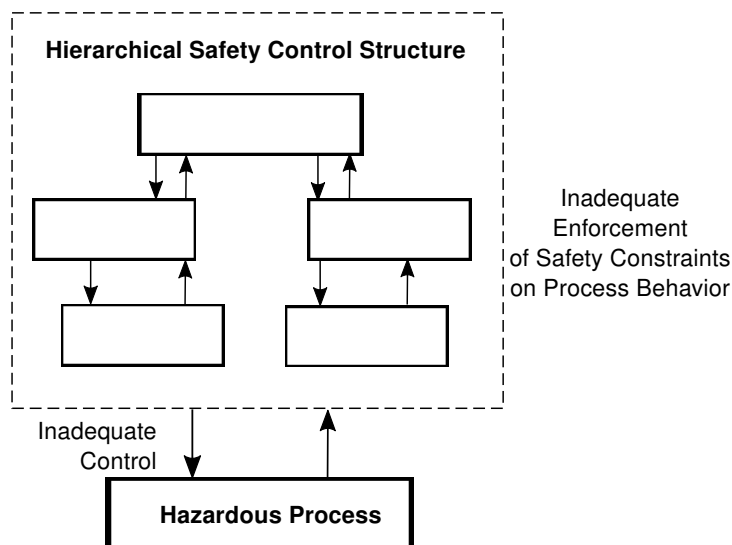


Figure 2.5: Schematic representation of the causality model in STAMP according to [19, p. 91].

## STPA

STPA is a hazard analysis technique, which uses the causality model STAMP. Before starting with the hazard analysis, the three design elements of STAMP – safety constraints, control structure diagram, and process model – are to be established [19, p. 213]. In this design process, system accidents and system hazards are also specified.

The hazard analysis technique STPA consists of two main steps. In step 1, a guide-word-driven hazard analysis is carried out [19, p. 213]. Four categories (a to d) describe the causes of hazards [19, p. 213]. These categories are derived from the causes of accidents defined in STAMP:

- a Control action is not provided or not followed,
- b Control actions are provided that are unsafe,
- c Control actions is provided at the wrong time or sequence (too early or too late),
- d Control action is stopped too soon or applied too long.

The STPA user inserts every identified CA into each category and checks whether the system state is hazardous or not and under which circumstance [19, p. 217]. Every CA that leads to a hazardous system state is called Unsafe Control Action (UCA). For every identified UCA, a controller constraint needs to be specified [20, p. 41]. It is useful to visualize this process in a table.

Step 2 determines the causes of each UCA [19, p. 213], which are analyzed by the respective control loop in order to determine the part inside the loop that is responsible for the UCA. Figure 2.6 is a useful template for this analysis showing the causal factors leading to hazards. Following this guideline, the potential cause can be determined for every UCA. The analyst identifies which entities and / or transitions cause the UCA. For example, accidents involving the controller can have six sources of causes. A controller receives (1) wrong or missing external information and therefore instructs wrong information to an actuator. It contains (2) inadequately implemented control algorithms or (3) its process model is inconsistent. It sends

(4) inappropriate, ineffective or no instruction to the actuator. The sensor returns the feedback to the controller (5) delayed, inadequately or not at all. An interaction with another controller that is (6) missing or wrong can lead to accidents as well. Analogously, this breakdown needs to be done at actuators, controlled processes, and sensors.

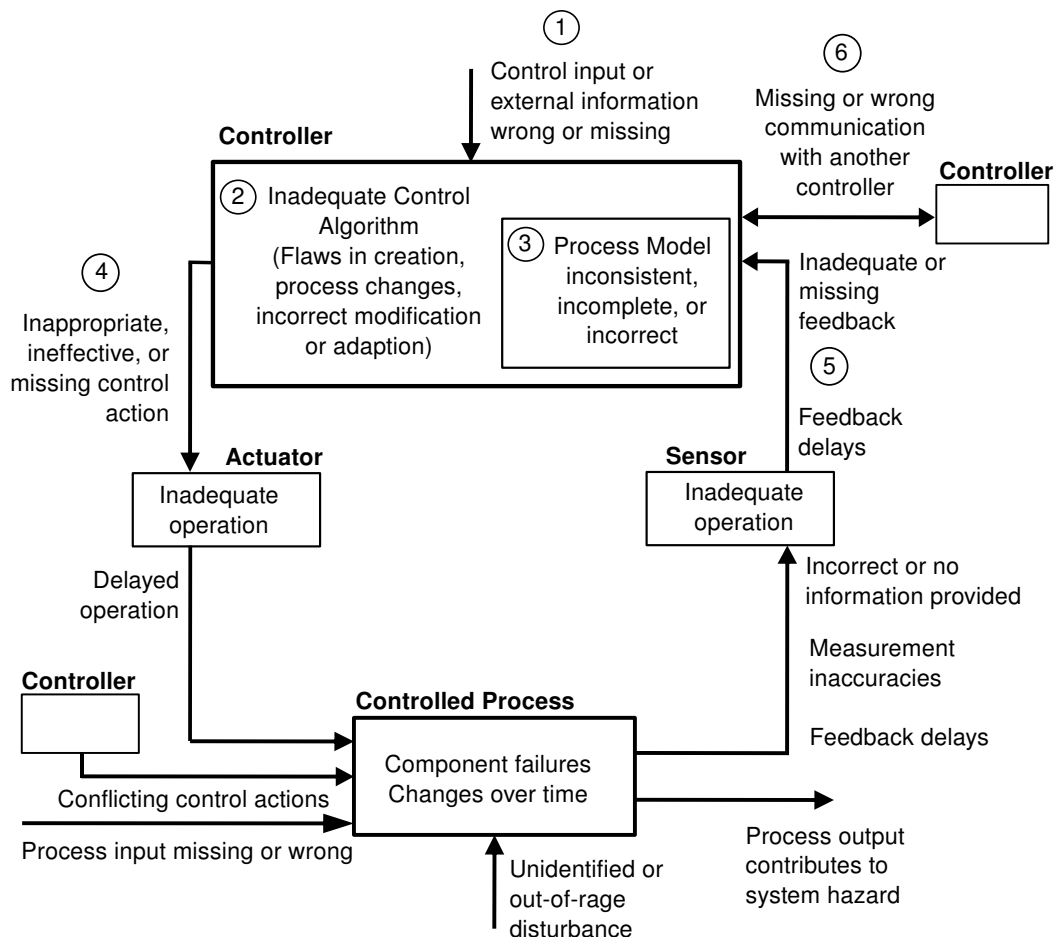


Figure 2.6: Causal factors within a control process according to [22, p. 30].

A hands-on tutorial on STAMP and STPA including two examples from the aviation industry can be found in [22].

## 2.4 Research Gap

Human drivers have high expectations of AD functions. These functions should increase safety, hence failures are not accepted. At SAE levels 0 to 2, automation failures can be fixed by the driver. At SAE levels 3 to 5, vehicles operate without supervision and the driver cannot intervene urgently (3-4) or at all (5). This lack of human intervention requires a development of a new safety assessment process. Currently available methods are insufficient, costly, and laborious for these levels [23, p. 6].

This section describes in detail the need for a new safety assessment process. The project called PEGASUS refers to a project currently focusing on developing mechanisms for safety assessments of AV. At the end of this section, a literature review is conducted to describe current research in this area.

### 2.4.1 Risk of Automation

Today, 94 % of all vehicle accidents are caused by humans [24, p. 1]. Typical causes are inattentiveness or violation of safety regulations such as speed limits or time gaps [25, p. 22]. Automated systems reduce human action, avoiding therefore these accidents. At the same time, automated systems cause new types of accidents [26, p. 1].

In Figure 2.7, both causes of accidents are represented through overlapping circles. Many accident causes result from conventional guidance; a smaller amount by AV guidance. The overlapping area shows the causes for accidents that cannot be reduced through automation. The crescent area on the right represents the newly arising causes through automation.

The advantage of automated systems for their users is indisputable, but the new accident causes create an acceptance gap for humans [26, p. 1]. A failure of the system that leads to an accident, which a human would have avoided, creates this gap. The corresponding risk to the new accident causes is called risk of automation. During the development of AD systems, a strong focus needs to be set towards diminishing this risk to a minimum tolerated level.

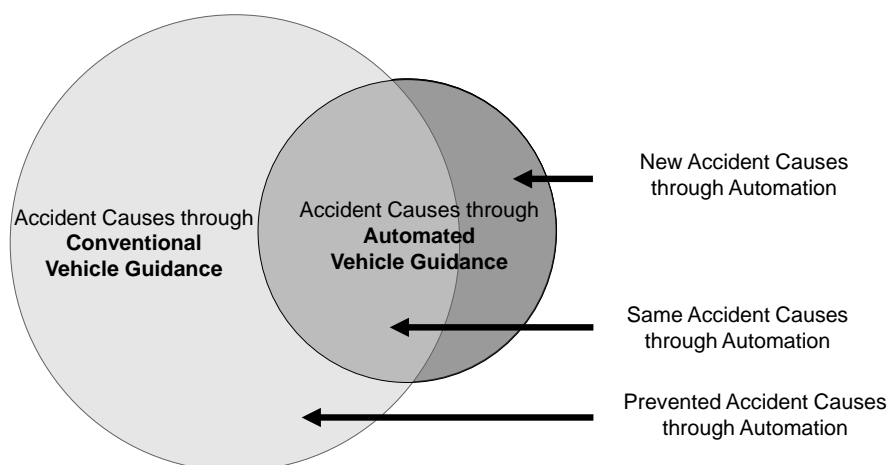


Figure 2.7: New, prevented, and same accident causes through automation compared to conventional driving according to [26, p. 1].

### 2.4.2 PEGASUS

The acronym PEGASUS stands for "Project for the Establishment of Generally Accepted quality criteria, tools and methods as well as Scenarios and Situations" [27]. This project is a collaboration of 17 partners funded by the German Federal Ministry for Economic Affairs and Energy and aims to establish the insurance of AD [28, p. 1]. All German Original Equipment Manufacturers (OEMs) are involved, as well as Tier 1 suppliers, a vehicle test lab, and scientific institutes. This large-scale involvement displays the high demand for such a method. Present state is that many OEMs have developed prototypes with AD functions and tested them in real traffic situations [23, p. 7]. To transform these prototypes into series vehicles, they need a safety assessment guideline permitting safety release [29, p. 7]. Such a standard guideline does currently not exist for SAE automation levels 3 and higher.

One sub-goal is to capture critical scenarios arising for and through AVs [26, p. 2]. These scenarios are derived from identified automation risks. Critical scenarios are then joined in a database for test specifications [26, p. 2].

For an explicit risk identification, automation risks are split into three classes, and their boundaries are illustrated in Figure 2.8. Class 1 looks at the risks that are caused by the environment on automation. These risks can result from incorrect environmental perception, false interpretation of a situation or faulty trajectory prediction of other road users [26, p. 2]. A example of an incorrect situation interpretation is an AV that follows yellow lane markings, although they are left-overs from a former construction site. This creates a risk of a lateral collision with other vehicles.

Class 2 considers the impact of automation on other road users. Causes can be misinterpretation of AD behavior or not-predictable AD behavior [26, p. 2]. A typical hazard of this class results of emergency braking of an AV due to a vehicle cutting through the AV's lane. The AV performs this reaction because its safety distance was undercut. The following traffic is not expecting this behavior and crashes into the AV.

The scope of Class 3 covers the interaction of the human driver of an AV with automation and environment. This interaction can lead to mode confusion, loss of confidence or misuse of the functionality [26, p. 2]. Mode confusion can occur when an AV requests the human driver to take over and assumes that the human actually did, whereas the driver believes the automation is still active. During this time, neither automation nor a human control the vehicle. Within this thesis, the same classification for automation risks is used.

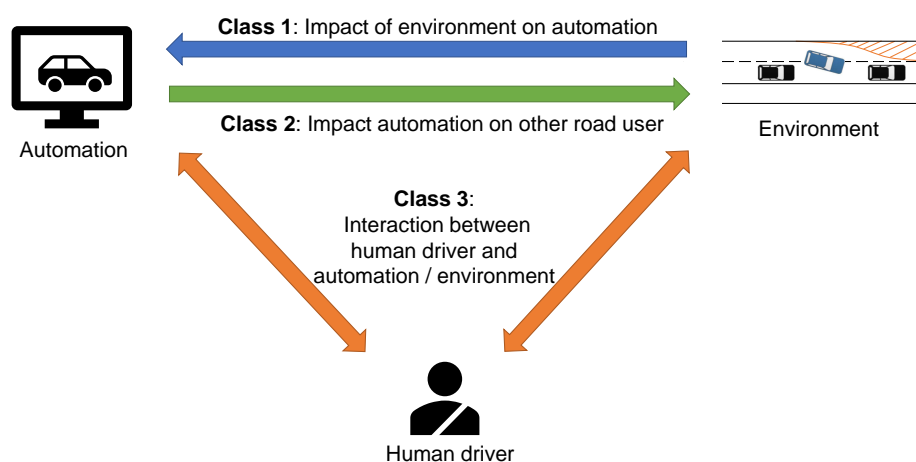


Figure 2.8: Classification of new accident causes at SAE level 3 according to [26, p. 2].

### 2.4.3 Related Work

A lot of research is going on in the field of hazard analysis for AD systems and in the application of STPA in the automotive industry. The International Risk Governance Center [30] outlines the significance of the identification of automation risks for law makers and insurance companies. This identification proves the need for the identification of arising risks for many industries and to be the key parameter for the social acceptance of AVs.

WOTAWA et al. [31] point out that an AD system cannot be assured by testing all possible road scenarios, which is the common procedure for standard vehicles [31, p. 323]. For AVs, test cycles of more than 275 million miles are required to be tested. The amount can be reduced by only testing specific scenarios in a simulation. This requires meaningful test scenarios which cover all relevant hazardous corner cases for AD [31, p. 324]. The detection of hazardous situations is therefore not only necessary during the concept phase, but also for quality assurance.



KRUPPA [32] analyzed in his Bachelor Thesis inter alia the accidents of AVs that happened to the development vehicles tested in California based on the accident reports collected by the DMV. He found out that most rear-end collisions occurred because human drivers in the following vehicles did expect different driving behavior than the one actually performed [32, p. 48]. The main cause for accidents are therefore not malfunctioning or falsely implemented AD system, although the most research is done to identify these Class 1 hazards.

IVANOV and SHADRIN [33] describe possible types of automation risks which arise with automated and autonomous vehicles and define requirements of these vehicles prior getting legal permissions to drive on public roads. Their work focuses on the negative technical and social problems, which do not include the problems arising with the different driving behavior of AVs compared to human driving.

In [34], WESSEL et al. focus on the risks arising through human machine cooperation and presents recommendations for the design of the cooperation in AVs. Besides WESSEL et al. [34], also HERZBERGER et al. [35] work on minimizing the risks through human machine cooperation. HERZBERGER et al. [35] develop an explanatory model which can be used to describe potential concepts of cooperation. In both papers, the aim is to minimize Class 3 risks.

In [36], MALLYA proves that STPA can be used within the ISO262622 [6] hazard analysis and risk assessment for software systems. This is analysis conducted by applying STPA to a battery management system.

Many analyses within the ISO262622 [6] that use STPA have been carried out for driver assistance systems at SAE levels 0 to 2. SULAMAN et al. [37] successfully apply STPA to a collision avoidance system. They conclude that the analysis technique is effective and efficient and requires a moderate level of effort. By applying STPA to an ACC system, ABDULKHALEQ and WAGNER [38] classify the method as powerful and useful for software-intensive systems in the automotive industry.

In [39], the aim is to identify unsafe combinations of CAs from one or more automotive control systems using STPA. This is done by using an example of three independent controllers that are active in parallel: Auto-Hold, Engine Stop-Start, and an ACC system with stop-go functionality. PLACKE et al. [39] found out that the hazards caused through interactions among these systems can be easily identified.

STPA also constitutes a useful tool to carry out a retrospective analysis. HOSSE et al. [40] use STPA to identify causes for system failure on a Tesla Model S crash in Florida in 2016, where the vehicle operated with an activated SAE level 2 highway assistance system. The control structure diagram is based on the assumption that the accident was caused by a Class 1 hazard. The control structure diagram is visualized in Figure 2.9.

Since 2017, STPA has also been applied to AD systems, SAE levels 3 and higher. BAGSCHIK et al. [41] successfully apply STPA to an unmanned protective vehicle, which should reduce the risk of injuries for road workers due to crashes on German highways. They follow the standard ISO262622 [6] in their product development process. The modeling of control structures for AD causes difficulties due to a high number of possible events and combinations. It is concluded that more context information about operational scenarios is necessary to identify hazardous situations. [41] only focuses on the identification of Class 1 automation risks.

ABDULKHALEQ et al. [42] create an architecture (control structure diagram) that can be used for an STPA for fully AVs (SAE level 5). This diagram also includes safety requirements regarding different attributes at different levels. The suggested architecture can be applied to Class 1 and

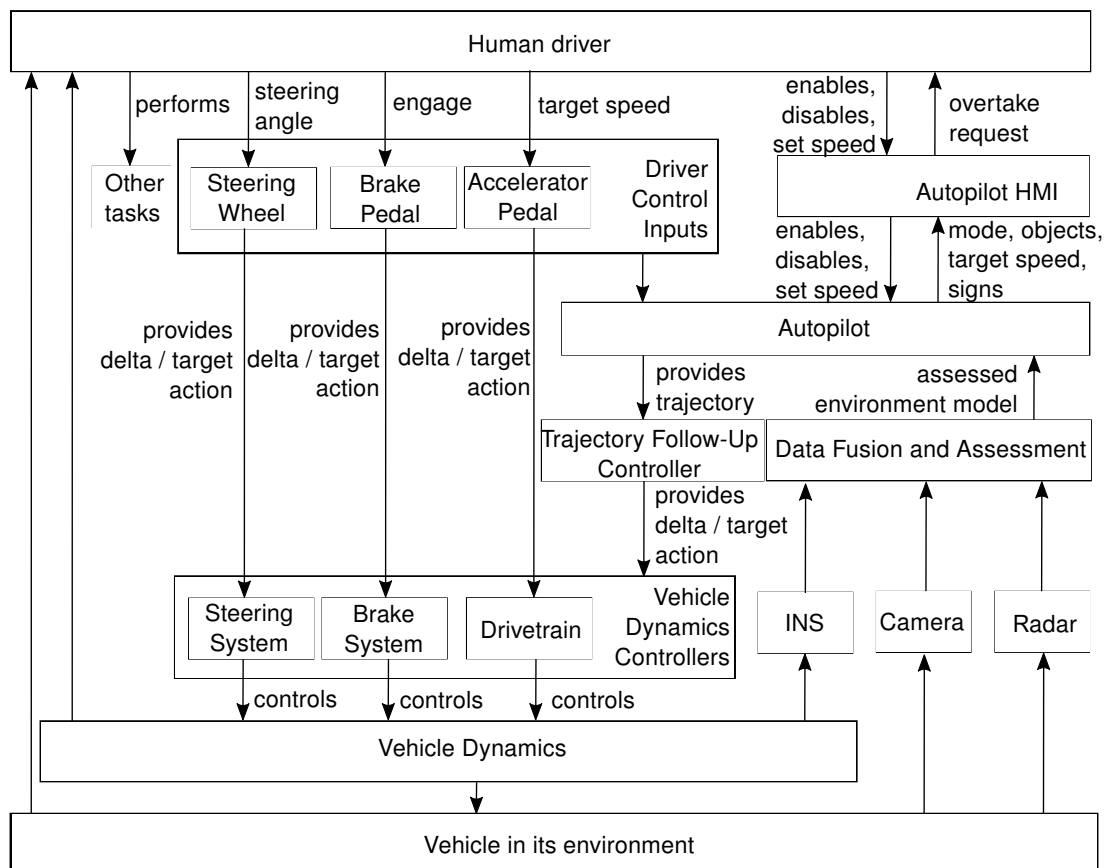


Figure 2.9: Control structure diagram for automation risks of Class 1 according to [40].

Class 3 automation risks, but Class 2 automation risks are not included in the control structure diagram and can therefore not be determined with this method.

In [43], ABDULKHALEQ et al. carry out an STPA for automation risks for SAE level 4 due to hazardous interactions of AD systems in the absence of system malfunctions. This approach should lead to the identification of Class 2 and Class 3 automation risks. By comparing the identified hazards with the results of a brain-storming method, ABDULKHALEQ et al. [43] observe difficulties with identifying all possible hazards. They suggest an extension of their approach using a traffic situation analysis at the beginning of the STPA process or in the causal factors analysis.

In her term paper [44], BOURDON traces two methods for the identification of hazardous Class 2 situations associated with a highway chauffeur system: a brain-storming method based on the accident causality model of REASON [45] and an STPA approach. The identified issues with Reason's causality model are the incompleteness of identified hazards, due to brain-storming and the missing interaction of components, as the analysis is only performed on system level. Additionally, an analysis can only be traced back to the causes, when concrete hazards or accidents are known. To overcome these issues, BOURDON [44] creates an STPA for a highway chauffeur system. The identified CAs are steering and braking. This level of refinement leads to a low level of safety constraints, so that no conclusions for hazardous situations for test purposes can be drawn. For example, an identified unsafe CA is that no braking is executed, when another vehicle wants to merge into lane.

## 2.5 Need for Action

It seems obvious that AD systems will prevent many accidents which happen due to inattentiveness or long reaction times of humans. By now, every higher level of automation that was developed resulted in safer systems, but it is unclear if this development trend continuous with the accomplishment of SAE level 3 systems as automation also causes new types of accidents. These types are currently unknown because only a limited accident database for this level exists. A reduced risk potential and information about new types of accidents are required to enhance trust of humans in new AD systems, who have high safety expectations.

A lot of research covers the identification of Class 1 and Class 3 hazards, but no method for the identification of Class 2 hazards currently exists. It is not proven or known that even if AVs are designed without any malfunctions and with clear human-machine interaction, AVs of SAE levels 3 and higher would create more or less accidents.

Current safety assurance and its hazard identification methods are no longer sufficient. With the standard ISO262622 [6] and the herein proposed hazard identification tools, hazards occurring through object misinterpretation or complex traffic situations are not detected because only functional safety of single Electrical / Electronic systems are covered and not the functional safety of multiple components or interactions [29, p. 13].

A lot of research has been done on hazard identification of component and system failures (Class 1) and human-machine interaction (Class 3) inter alia by using STPA. STPA is proven to be an effective method for hazard identification and analysis in the automotive industry. No research team successfully identified the Class 2 automation risks. Until today, there is no broad understanding of risks resulting from AV interaction with the environment and other road users arising from SAE automation levels 3 and higher.

This thesis focuses on a method to identify Class 2 automation risks – the impact of automation on the environment – for SAE levels 3 and higher. Additionally, a recommendation for the extension to Class 1 automation risks – impact of environment on automation – is given. A hazard identification and analysis for highway and rural road scenarios is proposed using the STPA, as the causality model of traditional analysis techniques does not hold for Class 2 problems. Each identified hazardous scenario is classified using ASIL, as defined in ISO262622 [6]. It is assumed that the correct coefficient of friction is always available to the system, otherwise it is assumed to be a Class 1 problem.

Selected hazardous scenarios can then be used for simulations or real tests to validate and insure new AD systems.



# 3 Application of STPA to Automation Risks Resulting from AVs

Determining a functional safety concept requires the identification of system hazards and the assessment of their risks as part of the concept phase defined in ISO26262 [6]. A method for this analysis on AVs of SAE levels 3 and higher is suggested in this chapter. In the beginning, the selection of the hazard identification and analysis method STPA is constituted for Class 2 automation risks of AVs. The selected STPA method is adapted to Class 2 risks and it is finally evaluated if and how the suggested method can be transferred to Class 1 and Class 3 automation risks.

## 3.1 Selection of Safety Engineering Approach

Before a hazard analysis can be carried out, the best fitting safety engineering approach has to be carefully selected, since an approach which identifies all possible automation risks at once does not exist. Each class of automation risks is based on different interactions and subsystems to be analyzed. Class 1 risks indicate when the environment creates a situation which the system cannot detect properly or which leads to software miscalculations. All risks arise through a malfunction of the AD system or one of its subsystems. Detailed information about each subsystem (hardware and software components) and their interactions must be provided.

In contrast, Class 2 risks indicate that the AD system detects the environment accurately at all times. The AD system does not make an error, drives defensively, and always abides by the law [46, pp. 560,561]. Nevertheless, this correct behavior can cause hazardous situations if people are not used to it. Most humans usually drive more offensively and do not in all cases follow the road laws [46, pp. 560,561]. Automation risks of Class 2 are identified using a method that can evaluate risks through the interaction of an AD system with other road users and does not require information of all subsystems.

To detect Class 3 automation risks, the system's interaction between the human driver inside the AV and the AD system has to be examined. The risks occur due to the interaction between two parties, similar to Class 2, but both classes have different interaction parties which require different foci in the analysis. The focus in Class 2 is set on happenings outside of the vehicle; Class 3 on happenings inside the vehicle.

To select the appropriate safety engineering approach, it has to be identified first how accidents in the system can occur to build an identical causality model on top. For this work, only Class 2 automation risks are considered. Traditional hazard identification and analysis techniques, such as FMEA and HAZOP, contemplate the malfunction of a component as the cause of failure. This is not a valid approach for automation risks of Class 2. It is not useful to split the system to be evaluated, the AV, into its components or subsystems because failure does not occur

through actions within or between them. They occur through the interaction with other road users. Nevertheless, traditional techniques should not be generally excluded as they might be reasonable for an analysis of Class 1 and Class 3 risks.

BOURDON [44] creates a hazard analysis using REASON's barrier causality model for identifying automation risks of Class 2. This model interprets accidents as a combination of failures [45]. BOURDON [44] defines four categories of barriers: management (such as traffic infrastructure, OEMs, and test organizations), traffic monitoring (such as camera monitoring, traffic checks), environment (such as weather / light conditions and traffic flow), and possible hazard defense (on the part of the driver, other road users, or Car-to-x communication). An accident occurs if a failure exists in every barrier and a trajectory passes through the failures in all of these barriers. The model makes it possible to trace back specific accidents through every barrier by determining the causes of failure in each barrier. This retrospective analysis would be ideal if a large accident database for AD systems existed, but it does not because no AD systems are on the market yet that could cause accidents.

The causality model in STPA (STAMP) can be used for a prospective analysis. It does not require an accident database and is additionally not based on the principle that only malfunctions lead to failure. STPA only requires all possible accidents types as a foundation. Accident types are for vehicles crash types. They are essential to derive system Safety Constraints (SCs) which are used for differentiate between hazardous and non-hazardous situations. A top-down approach can be carried out solely based on the identified SCs.

## 3.2 Preliminaries

The STPA is divided into two steps, the hazard analysis and causal factors analysis. Before starting with step 1, some preliminaries have to be defined in order to create an appropriate causality model. Section 3.2.1 to Section 3.2.3 characterize the fundamentals which are introduced in the STPA concept by LEVESON [19]. Section 3.2.4 and 3.2.5 describe preliminaries that are especially necessary for automation risks of Class 2. The linking between the sections is visualized in Figure 3.1. Based on the preliminaries defined in this section, the STPA steps 1 and 2 are adapted in Section 3.3.

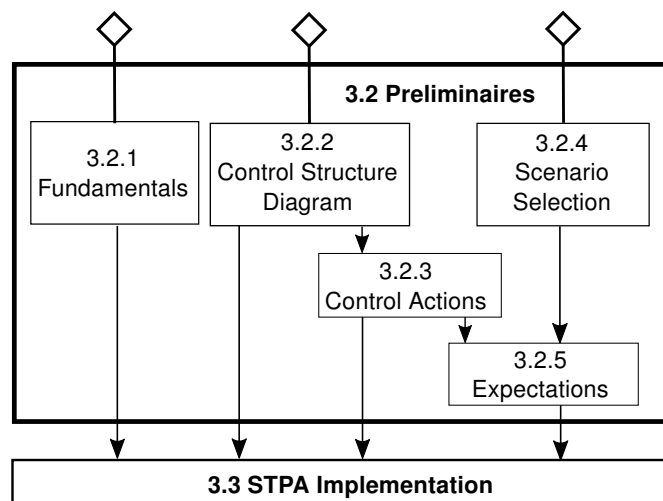


Figure 3.1: Flow chart diagram for the determination of the preliminaries leading to the STPA implementation.

### 3.2.1 Definition of Fundamentals

As a prerequisite to the hazard analysis, STPA requires defined system SCs. If one of these predefined SCs is violated, the AV causes a Hazard (H) to other road users. System SCs are derived from system hazards, that are concluded from system Accidents (As).

Table 3.1 shows a list of all possible accident types that can occur to a(n) (automated) vehicle. The accidents are oriented on the ones identified by BOURDON in [44]. These six accident

Table 3.1: Potential accidents through AVs.

Number	Description
A-1	Collision AV with leading vehicle
A-2	Collision AV with following vehicle
A-3	Collision AV with neighboring vehicle
A-4	Collision AV with pedestrian / cyclist / motorcyclist
A-5	Collision AV with obstacle or surrounding
A-6	Collision of other vehicles

types are determined as follows: collision with (A-1) a leading, (A-2) a following, or (A-3) a neighboring vehicle, with (A-4) a pedestrian or cyclist or motorcyclist, with (A-5) an obstacle or the surrounding, and a collision (A-6) between other vehicles. A-1 to A-5 involve the AV in the collision, whereas A-6 is an accident of at least on other road user which is caused by the AV.

Changes from BOURDON's [44] accidents are made for A-4. Her accident classification defines separate accidents for different collision partners. For this work it is sufficient to group all collision partners, pedestrians, cyclists, and motorcyclists, into one group. BOURDON's [44] approach also requires the accident "Injury or death of people", which is not necessary for this analysis, as a separate ASIL determination follows the hazard identification in the proposed method.

Table 3.2 lists the hazards derived from the accidents A-1 to A-6 (Table 3.1) and links them. One accident leads at least to one new hazard definition, but each defined hazard can be linked to multiple accidents that could result from it.

The only hazard that leads to a collision of the AV with the leading vehicle (A-1) is through entering its safety distance (H-1). A collision with the following vehicle (A-2) can occur, if the safety distance to the following vehicle is entered (H-2). Entering this safety distance (H-2) can also cause a collision of other vehicles (A-6), for example through an emergency brake of the following vehicle leading to a collision of following traffic. H-3 and the linked accidents are analogously determined to H-2; H-4 and H-5 analogously to H-1.

The occurrence of the hazards H-1 to H-5 is easily determined through a measurable variable: the safety distance in front of or behind the vehicle or the safety distance on the sides of the vehicle. Whether a hazard of H-6 to H-8 exists, cannot be measured and depends on the individual human involved. Some humans are startled easily, some less. The hazards cannot be directly derived from the accidents A-1 to A-6. A startled or confused road user (H-6) can collide with other road users (A-3) or pedestrians / cyclists / motorcyclists (A-4). The same reason exists for the linked accidents to H-7, provoking other road user(s) to perform dangerous maneuvers, A-4 and A-6. In cases where the human driver in the AV is startled (H-8), all types of accidents can occur by falsely steering, accelerating or braking.

The identified hazards lead to the definition of safety constraints on the system level, which are shown in Table 3.3. H-1, H-2, H-3, H-4, and H-5 can be combined to safety constraint SC-1, AV must always maintain safety distances. AV must never startle others (SC-2), results from

Table 3.2: Derived hazards and linked accidents.

Number	Description	Linked Accident(s)
H-1	AV entering safety distance to leading vehicle	A-1
H-2	AV entering safety distance to following vehicle	A-2, A-6
H-3	AV entering safety distance to neighboring vehicle	A-3, A-6
H-4	AV entering safety distance to pedestrian /cyclist / motorcyclist	A-4
H-5	AV entering minimum distance to obstacle or surrounding	A-5
H-6	AV behavior startling or confusing other road user(s)	A-4, A-6
H-7	AV provoking other road user(s) to perform dangerous maneuvers	A-4, A-6
H-8	AV startling own AV human driver	A-1 to A-6

H-6. Both, SC-3 (AV must never block traffic) and SC-4 (AV must never provoke others to dangerous maneuvers), are derived from H-7. A blocked lane can provoke other road users to perform dangerous maneuvers to take over the AV. All other situations that provoke others to perform dangerous maneuvers should be prevented. H-8 (AV startles own human driver), leads to SC-5, AV must never startle own human driver. SC-6 cannot be derived from the system hazards, but is a constraint that needs to be added to differentiate between Class 1 and Class 2 hazards. Every malfunction of the system causes a risk in Class 1. These risks are excluded with the constraint that the AV must always work properly (SC-6).

Table 3.3: Derived safety constraints and linked hazards.

Number	Description	Linked Hazard(s)
SC-1	AV must always maintain safety distances	H-1 to H-5
SC-2	AV must never startle or confuse others	H-6
SC-3	AV must never block traffic	H-7
SC-4	AV must never provoke others to dangerous maneuvers	H-7
SC-5	AV must never startle own AV human driver	H-8
SC-6	AV must always work properly	-

Every situation identified in the hazard analysis described further down in Section 3.3 causes a hazard to the entire system, if one of the defined SCs in Section 3.3 is not met.

### 3.2.2 Control Structure Diagram

The STPA proposed by LEVESON [19] requires the creation of a control structure diagram, besides the definition of SCs within the preliminaries. A control structure diagram assists in determining the interactions between systems and in localizing the root which performs the CAs. Figure 3.2 illustrates the control structure diagram for the interaction of an AV with a human road user who is affected by the AV's behavior. The AV is the designated ego-vehicle. The human affected by it is in this thesis from now on called challenger.

The identification of interactions that cause hazards requires a modification of the classical control structure diagram in STPA. Firstly, the interaction between the ego-vehicle and the challenger is defined to be the controlled process instead of a hardware or software system. Secondly, CAs that lead to a hazard result from the different expectation that the challenger has of the AV's CA compared to the actual CA. In the unmodified STPA, wrong executed control actions can directly lead to a hazard, which is not applicable for the Class 2 hazard identification. The issue for Class 2 hazards is, that the challenger does not know whether the ego-vehicle is automated or not, and even if, the human does not know in which situations an AV can act differently from a human-steered vehicle. The challenger always expects human driving behavior.



The interaction between the vehicles is determined to be the controlled process relevant for the analysis of Class 2 automation risks. It is controlled through the behavior of the AV and the human-driven vehicle (the challenger). The AV receives instructions from the AD system, executes them, and sends the perceived information about the environment back. The only remaining task of the human driver inside the AV is to turn on and off the automation mode.

The challenger reacts to the actions of other vehicles, inter alia of the AV, and has an expectation of what the other drivers might do and does not anticipate other actions. The executed instructions by the AD system are therefore influenced by the expectations of the human driver. In situations where the driver is startled by the AV, they might also perform uncontrolled and unwanted actions.

Unexpected defensive driving and strictly following the laws are typical behavior patterns for AD systems and less likely for human drivers. This over-cautious driving is a high potential risk for other road users [4]. The discrepancy between human and AD can be well depict with the given representation.

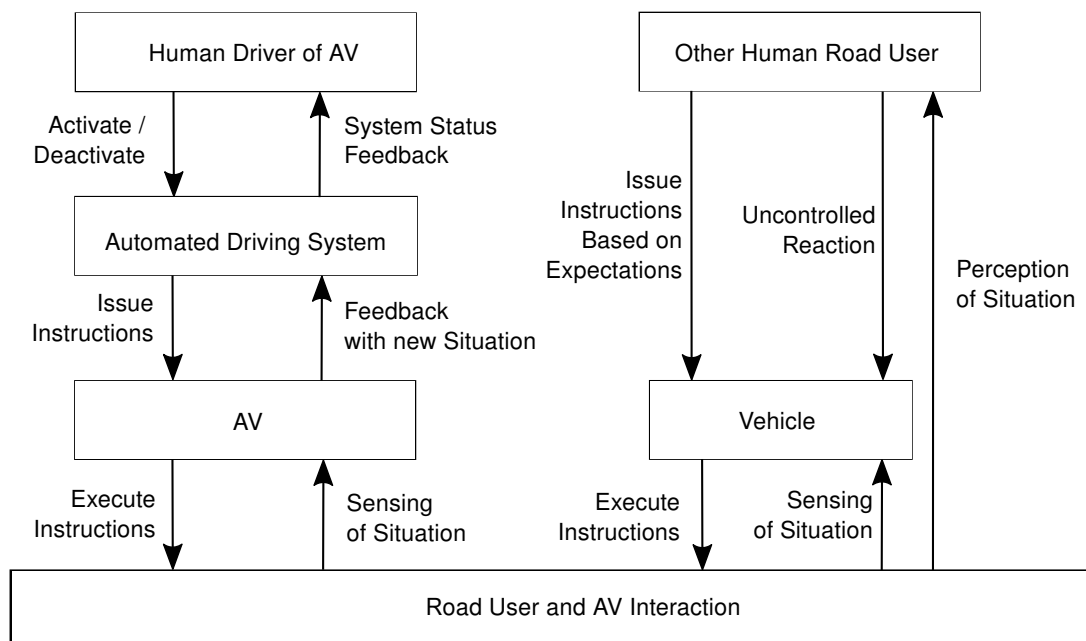


Figure 3.2: Control structure diagram for the identification of Class 2 automation risks.

### 3.2.3 Identification of Control Actions

The relevant CAs in the control structure diagram (Figure 3.2) for the intended hazard identification are the ones executed by the AV that control the interaction between the vehicles. Similar to a not-automated vehicle, it can control longitudinal and lateral movements: acceleration, deceleration and steering. These are actions a vehicle can perform, but are not the ones of humans expectations. They expect more broader defined actions such as lane changes and changes in speed. The steering maneuver itself due to a curvature is a necessary maneuver to follow a lane, but is not relevant for a vehicle interaction. A human only has the expectancy that the vehicle remains in that lane or not. This high level of refinements leads to the CAs listed in Table 3.4.

Additionally to the combinations of keeping or changing speed and keeping or changing lane (CA-1 to CA-5), a vehicle can also abort an already initiated lane change (CA-6) and can

Table 3.4: Identified CAs for automation risks of Class 2.

Number	Control Action
CA-1	Keep speed and keep lane
CA-2	Keep speed and change lane
CA-3	Change speed and keep lane
CA-4	Change speed and change lane
CA-5	Abort lane change
CA-6	Emergency brake
CA-7	Emergency stop

perform an emergency brake (CA-7) or stop (CA-8). The differentiation between CA-6, an emergency stop, and CA-7, an emergency brake, is that in a stop the vehicle brakes until it stands still, i.e. the wheels are not turning at all; in an emergency brake on the other hand is a strong braking that does not lead to a complete stop.

All CAs are applicable for highway and rural road analyses. The action change lane has different interpretations for the different road types. For highways, the CA of changing a lane can be performed by changing to the right lane for example in order to take an exit or to follow the rule to keep right. Changes to the left lane can be performed for example to merge from a ramp onto the highway, or to take over a slow vehicle.

For rural roads, the lane change maneuver can refer to a pull out or pull back in within an overtaking maneuver, similarly to the maneuver on highways. Lane change can also refer to the action of turning at an intersection or leaving a roundabout. Rural roads are considered to have one lane in each direction in order not to double the hazard analysis for multiple lanes which is already covered in the highway analysis.

#### 3.2.4 Scenario Selection

A not provided CA or delayed CA does not directly create a hazardous situation because it is not a malfunction of the system by definition. Nevertheless, if one of these CAs is performed in a situation in which the challenger does not expect it, a hazardous situation might arise. The combination of CAs and guide-words (a-d, Section 2.3.3) with different driving scenarios builds a method to systematically identify UCA. A similar proposal is made in [43], where ABDULKHALEQ et al. suggest including a traffic situation analysis at the beginning of the STPA or in the causal factors analysis.

This section suggests a method used to define the required driving situations, followed by the actual determination of highway and rural road situations. Defined situations found in literature are inadequate for this problem. Databases with situations for specific road types, such as German In-Depth Accident Study (GIDAS), only contain situations that caused an accident with injured persons [47]. This excludes all fender benders, hazardous situations in which an accident was prevented in the last second, and standard situations that can create new hazardous situations for AVs. Even though the situation catalog VDA702 [48] lists basic situations with their exposure specifically for hazard analyses, they are improper for the analysis of Class 2 hazards. Specific situations while driving, standing, and others are given. For these situations, the exposure is given for a certain number of passengers, activated and deactivated systems, loading weights, and so on is specified. The level of refinement is too small for the determination of automations risks and relevant situations such as cut ins or cut outs are not included. If once a catalog for driving scenarios on different road types including their exposure is created, this

one can be used for the analysis instead of the proposed procedure for the driving scenario identification.

To this point, there was no need for research identifying common driving scenarios, especially of those that never caused an accident – if no accident occurs due to them, there is no need to analyze them. The development of AD systems creates nowadays the need for a catalog with these scenarios in order to create systems that do not cause more accidents than humans already do. Current research focuses on Class 1 and Class 3 automation risks, which do not require these catalogs. Methods are proposed which for example define the uniform requirements necessary of representing test scenarios and the resulting levels of refinement [49]. Zhou et al. [50] suggest a method to parametrize test scenarios for maneuvers which are supposed to be existent using Field-Operational-Test measurements [50].

## Method

As previously described, no scenario catalog exists that would fulfill the demands for the Class 2 hazard determination. Following, a method is described which can be used to systematically create such a catalog.

No hazardous events of Class 2 can arise, if the AV follows a vehicle and maintains its lane and speed. A drive without a leading vehicle at constant speed in the same lane is similarly hazard-less. If a hazard occurs in one of these standard situations, they are Class 1 hazards. Hazardous situations of Class 2 only result from changes in the environment that require an action from the AV.

Environmental changes can be categorized into three groups: changes within the field of view (Category A), direct calls to action (Category B), and deviations from standard road surface (Category C). These definitions are shown in Table 3.5.

The proposed classification covers all possibilities a vehicle could react to. Category A contains all stationary and moving obstacles within the field of view, such as vehicles cutting in or out, or a plastic bag blowing over the road. Direct calls to actions (Category B) are for example road signs that are relevant for the AV, such as speed limit or no passing signs. Category C covers all deviations on the road surface level which could be for example an icy road or a missing lane marking.

For each road type and each country, the driving scenarios differ in each category and have to be determined individually. This thesis only focuses on highways and rural roads in Germany.

Table 3.5: Categories of scenarios that potentially provoke a vehicle for a change of its driving behavior.

Category	Description
Category A	Change within field of view
Category B	Direct call for action
Category C	Deviation from standard road surface

A hazard analysis should to be carried out for each driving scenario separately and additionally for all reasonable double or triple combinations of the scenarios in order to detect as many hazards as possible. This creates a big amount of scenarios to be analyzed and needs to be reduced to the most important ones to start with. To identify those, a reduction can be done by determining the parameters for the ASIL (controllability, exposure, and severity) for each uncombined scenario and selecting the highest rated one in each parameter.

The controllability class can be rated as **C3** for all driving scenarios, firstly because no human is in charge of the driving task in an AV and therefore cannot prevent an accident in a hazardous situation. Secondly, an accident prevented by other road users would not fulfill the requirements for a safe design of AVs. It would generally expect other road users to react to the AV's hazardous causing behavior.

The exposure of a driving scenario cannot be precisely determined as no database for their frequency of occurrence exists, but a qualified assumption can be made, whether the exposure is rare (**E0**, **E1**, or **E2**) and occurs in less than 1 % of the average operating driving time or it is frequent (**E3** or **E4**) and occurs in more than 1 % of the average operating driving time. The exposure is in this work only defined by the occurrence of the average operating driving time and not by the frequency, which is also suggested in the ISO26262 [11] because no source for the exact exposure exists and none of the both parameters can be determined with certainty.

The severity of an accident cannot directly be determined by only knowing the driving scenario as many other factors influence the severity. Nevertheless, it is relevant to include all scenarios which have a higher likelihood of being life-threatening or causing fatal injuries (**S3**). Every situation with severity potential **S3** has a high ASIL independently of its exposure and must therefore be analyzed additionally to driving scenarios at **S1** combined with **E3** / **E4** and **S2** with **E3** / **E4**. The severity level of a driving scenario can be determined by looking at the total weight of the conflicting partner, the magnitude of the absolute velocity, or the magnitude of the negative relative velocity between the ego-vehicle and an object, pedestrian, or other vehicle. Chances of fatal injuries are much higher at high absolute or at highly negative relative velocities than with low velocities and with heavy conflict partners. The determination of the severity at this point is only used to include possibly severe situations and does not determine the severity of a specific hazardous situation. The exact level of severity has to be identified within the hazard analysis for every hazardous situation individually.

The ASILs addressed with the previously described method are highlighted in Table 3.6. It is the same table as used for the explanation of ASIL in Section 2.2.2. The method covers all ASILs of level B to D.

Table 3.6: ASIL determination according to [11, p. 10] with highlighted levels that are considered in the scenario selection method.

Severity class	Probability class	Controllability class		
		C1	C2	C3
<b>S1</b>	E1	QM	QM	QM
	E2	QM	QM	QM
	<b>E3</b>	QM	QM	<b>A</b>
	<b>E4</b>	QM	A	<b>B</b>
<b>S2</b>	E1	QM	QM	QM
	E2	QM	QM	A
	<b>E3</b>	QM	A	<b>B</b>
	<b>E4</b>	A	B	<b>C</b>
<b>S3</b>	E1	QM	QM	<b>A</b>
	E2	QM	A	<b>B</b>
	<b>E3</b>	A	B	<b>C</b>
	<b>E4</b>	B	C	<b>D</b>

## Highway Scenarios

A standard situation must be defined to be able to apply the previously described method to highway driving. The standard situation on a highway has two or more lanes which are all properly marked with white lane markings, overtaking is allowed, driving on the hard-shoulder is prohibited a speed limit of 120 km/h exists. The AV, which is a motor vehicle with up to 3.500 kg, either follows another vehicle at constant speed or does not have a leading vehicle. Neither wind nor icy or wet conditions exist. If none of these parameters changes, no Class 2 risk will arise.

In the following tables, situations of high exposure (**E3** and **E4**) are assigned to **1**, low exposure (**E0**, **E1**, **E2**) to **0**. Analogously, high severity (**S3**) is classified as **1** and low severity (**S0**, **S1**, **S2**) is assigned to **0**.

18 scenarios are that describe changes within the field of view of the AV (Category A). These scenarios are listed in Table 3.7.

Table 3.7: Category A scenarios for highway driving – Changes within field of view – including their severity and exposure. Exposure levels of **E0** / **E1** / **E2** are classified as 0; exposure levels of **E3** / **E4** as 1. Severities **S0** / **S1** / **S2** are classified as 0; **S3** as 1.

Number	Event	Exposure	Severity
HW-A01	Cut in with positive relative velocity	1	1
HW-A02	Cut in with negative relative velocity	1	1
HW-A03	Cut out	1	1
HW-A04	Cut through	1	1
HW-A05	Slow leading vehicle	1	1
HW-A06	Leading vehicle brakes	1	1
HW-A07	Leading vehicle accelerates	1	1
HW-A08	Slow moving traffic	1	1
HW-A09	End of traffic jam ahead	0	1
HW-A10	Small static object (can be run over)	0	0
HW-A11	Small moving object (can be run over)	0	0
HW-A12	Large static object (cannot be run over)	0	1
HW-A13	Large moving object (cannot be run over)	0	1
HW-A14	Pedestrian / Cyclist	0	1
HW-A15	Wrong-way driver	0	1
HW-A16	Convoy	0	1
HW-A17	Heavy-duty transport	0	1
HW-A18	Gigaliner	1	1

A vehicle can cut in, which means change lanes into the ego-vehicle's lane, in front of the AV with a positive (HW-A01) or negative (HW-A02) relative velocity. The relative velocity is calculated by subtracting the ego-velocity from the velocity of the vehicle cutting in. Both scenarios are common driving scenarios on highways and occur in more than 1 % of the driving time; their exposure is determined to 1. In both scenarios, a somehow created accident will probably cause fatal injuries because the cutting in vehicles usually have high absolute velocities; the severity is set to 1.

The opposite scenario can also occur: the leading vehicle leaves the ego-vehicle's lane. This scenario of a vehicle cutting out (HW-A03) happens similarly often as HW-A01 and HW-A02 and has similarly severe consequences.

A vehicle cutting through represents a separate scenario (HW-A04). Vehicles cutting through also occur often on highways (more than in 1 % of the driving), especially when vehicles on the left lane intend to reach an exit and therefore cross multiple lanes at once. The severity of a potential accident is high as the absolute velocities of such a maneuver is typically high.

The leading vehicle can either be slower than the actual or intended velocity of the AV (HW–A05), brake (HW–A06), or accelerate (HW–A07). All three scenarios are daily scenarios on highways and usually occur at high speeds: exposure 1, severity 1.

A slow moving traffic (HW–A08) differs from the slow leading vehicle (HW–A05) therein that all vehicles in all lanes are moving slowly, not only the leading vehicle. A lane change in this case is not useful. HW–A08 is very common, especially on highways around bigger cities (exposure 1) and dangerous due to the highly negative relative velocity when approaching the end of the slow moving traffic (severity 1). Chances of running into the end of a traffic jam (HW–A09) (vehicles are not moving at all) are rare, but in those cases an inappropriate behavior easily causes fatal injuries due to highly negative relative velocities.

HW–A10 to HW–A13 describe scenarios in which an object is in the ego-vehicle's lane. Objects can be small or large, static or moving. Small static objects (HW–A10), such as bits of tires, and small moving objects (HW–A11), such as plastic bags blown by the wind, are neither often on German highways, nor is a collision dangerous due to their small size and low weight. Small objects define all objects that can occur on a highway and that can be run over.

In contrast, large objects cannot or should not be run over. Large static objects that cannot be run over (HW–A12) such as vehicles with a breakdown in driving lane are rare, but a crash into one with high speed can have severe consequences. Large moving objects that cannot be run over (HW–A13), such as wild animals or tarpaulins blown by the wind, are rare and can also cause severe injuries depending on their weight. Besides objects, pedestrians or cyclists can be present on highways (HW–A14). They create a separate scenario as a collision with one of them is usually directly life-threatening and their moving behavior differs. Pedestrians could be on the road after an accident, cyclists could be on the highway by accident. These scenarios do not occur often (exposure 0), but an accident would have a high probability for fatal injuries (severity 1).

Even more uncommon are wrong-way drivers (HW–A15), but their absolute value of the negative relative velocity compared to the AV is very high, causing fatal injuries in case of an accident.

Special types of vehicles which drive ahead of the AV in the right neighboring lane must be included as they require or permit the AV to perform certain maneuvers, which common vehicles do not. A convoy (HW–A16) consisting of multiple vehicles should not be interrupted, i.e. a vehicle should only merge into its lane at the beginning of the convoy or at the end. Convoys are rare (exposure 0), but are driven at high speeds and accidents would have severe consequences (severity 1). Heavy-duty transport vehicles (HW–A17) and gigaliners (HW–A18) are extra wide or extra long compared to normal trucks and therefore represent two separate scenarios. Heavy-duty transport trucks are rare, gigaliner will soon be common, but independently from that a crash with one of them has fatal consequences due to their high amount of mass.

For Category B, 18 highway scenarios are found and listed in Table 3.8 including their probabilities of exposure. The severity level is not given in the table. No collisions with direct calls to action signs should be analyzed, only the behavior resulting from it. Not following the calls for action does not directly lead to an accident. In Category A, the AV might need to change its behavior directly to avoid an accident.

A direct call for action can be initiated by an emergency vehicle (HW–B01) approaching from behind through its siren or flash lights. The emergency vehicle thereby requests the vehicles to clear the lane or if it is not possible to create an emergency lane. This call for action does happen in less than 1 % of and the average operating time, the exposure is therefore 0.

Table 3.8: Category B scenarios for highway driving – Direct calls to action – including their exposure. Exposure levels of **E0** / **E1** / **E2** are classified as 0; exposure levels of **E3** / **E4** as 1.

Number	Event	Exposure
HW–B01	Emergency vehicle	0
HW–B02	Beginning speed limit	1
HW–B03	End speed limit	1
HW–B04	Time frame of temporal speed limit begins	1
HW–B05	Time frame of temporal speed limit ends	1
HW–B06	Beginning no passing	0
HW–B07	End no passing	0
HW–B08	Opening new lane	1
HW–B09	Lane ends	1
HW–B10	Beginning emergency lane clearance	0
HW–B11	End emergency lane clearance	0
HW–B12	Red traffic light	0
HW–B13	Traffic light turns green	0
HW–B14	Ramp	1
HW–B15	Exit	1
HW–B16	Toll station	0
HW–B17	Customs station	0
HW–B18	Highway junction	0

Scenarios HW–B02 to HW–B07 are road signs that call for action. Speed limit signs are usual on highways, so their exposure is 1. Speed limit signs can be divided into those marking the beginning (HW–B02) and those marking the end (HW–B03) of a certain speed limit. Furthermore, specific speed limits exist which are only valid at a certain day time (HW–B04 and HW–B05). Another type of road signs are no passing signs. Usually, no passing signs only appear at the beginning and at the end of construction sites and they do not occur in more than 1 % of the driving time on a highway. The exposure of the signs at the beginning of a no passing area (HW–B06) and at the end of a no passing area (HW–B07) are classified 0.

A new lane opening (HW–B08) or a lane closing (HW–B09) are very common driving scenarios on highways (exposure 1). In some situations, emergency lanes can be used as driving lanes (HW–B10) or can be closed for traffic (HW–B11). Normally, they are kept closed and are rarely opened for traffic which leads to exposure 0. In this category (Category B) a closing lane means that the lane of the ego-vehicles closes and the AV has to change lanes; an opening lane is a lane that opens and the ego-vehicle take or not for example due to the law of driving on the right lane or because it wants to take over the leading vehicle.

HW–B12 to HW–B18 are scenarios of infrastructure installations. Traffic lights do not only exist off highways, but also for example at the entrance of highway tunnels. They are most of the time green or turned off, only in some occasions they turn red. Chances being on a highway and being confronted with a red traffic light (HW–B12) are low. Similarly low are the chances of being on the highway in the first row of vehicles when the traffic lights turn green (HW–B13). Ramps (HW–B14) and exits (HW–B15) are the only possibility to enter and exit the highway, so every vehicle faces them every time when driving on a highway. These two scenarios do not include all ramps and exits a vehicle passes, but only those the AV wants to take. All others are included in lane ends (HW–B09) or lane opens (HW–B08). Toll stations (HW–B16) do not exist on German highways and customs stations (HW–B17) only exist at the borders of the country. Both exposures are 0. Highway junctions (HW–B18) are more common, but still occur fewer than in 1 % of highway roads. Junctions might occur in more than 1 % of highways around larger cities, but they are especially rare in rural areas. The overall occurrence is less than 1 %.

Table 3.9 lists the 9 identified scenarios for Category C, the deviation from the standard road surface, on highways. Similar to Category B, no severity is determined as they only describe changes of the road surface; no accidents directly result from them when not reacting adequately.

Table 3.9: Category C scenarios for highway driving – Deviation from standard road surface – including their exposure. Exposure levels of **E0** / **E1** / **E2** are classified as 0; exposure levels of **E3** / **E4** as 1.

Number	Event	Exposure
HW-C01	No overtaking	0
HW-C02	No overtaking one-sided	0
HW-C03	Missing lane marking	0
HW-C04	Confusing lane marking	0
HW-C05	Narrowed lane	0
HW-C06	Ending neighboring lane	1
HW-C07	Ruts	1
HW-C08	Slippery road	0
HW-C09	Wind	0

HW-C01 to HW-C05 are lane marking deviations from the standard. The "No overtaking" lane markings (HW-C01) differ from the no passing sign (HW-B06) in the way that the sign is a brief call for action and the lane marking shows the duration of the prohibition to change lanes. HW-C02 is a continuous lane marking prohibiting a lane change for the ego-vehicle, but allowing other to merge into the AV's lane. The similar scenario with reversed lane markings is irrelevant because it does not constrain the ego-vehicle and having no vehicle that merge into the ego-vehicle's lane does not cause hazards. Missing (HW-C03) and confusing lane markings (HW-C04) are accidentally created at current or former construction sites. Narrowed lanes (HW-C05) also only exist in construction sites. All these lane markings are uncommon on highways since they only occur at construction sites or highway junctions which leads to exposure 0.

If the lane next to the ego-vehicle closes (HW-C06), it does not represent a direct call for action (not Category B), but it indirectly asks to make space for others to zip merge into lane. This situation is common on highways: every ramp is an end of a neighboring lane.

The road surface deviations HW-C07 to HW-C09 are all grip related. A road can have ruts (HW-C07) or be slippery due to rain or ice (HW-C08). Wind (HW-C09) can also reduce the grip. Slippery and windy driving conditions are rare in most of the driving in Germany. Ruts are much more common due to aging roads.

## Rural Road Scenarios

Rural roads differ from highways especially in three aspects: rural roads are not separated from oncoming traffic through infrastructural barriers, usually just have one lane for each direction, so overtaking maneuvers are performed in the lane of the oncoming traffic, and rural roads cross intersections and towns. These completely different conditions need to be evaluated in an individual hazard analysis for rural roads.

All deviations from the standard scenario are listed in Table 3.10 - 3.12. The standard scenario on rural roads contains a two-lane road, one lane for each direction, which are delimited by lane markings and the road boundaries are delimited by reflector posts; no specific speed



limit is given and the AV either follows a vehicle of constant speed or does not have a leading vehicle; the AV is outside of a town (no traffic lights) and is not currently passing a roundabout or intersection; no wild life crosses the road and the road is neither windy nor slippery due to ice or puddles.

In Table 3.10, the 21 identified changes within the field of view (Category A) with their severity and exposure levels are listed. Many scenarios are identical to the ones identified for highways; the newly identified scenarios are highlighted in bold.

Table 3.10: Category A for rural road driving – Changes within field of view – including their severity and exposure. Scenarios which do not occur on highways are printed bold. Exposure levels of **E0** / **E1** / **E2** are classified as 0; exposure levels of **E3** / **E4** as 1. Severities **S0** / **S1** / **S2** are classified as 0; **S3** as 1.

Number	Event	Exposure	Severity
RR–A01	Cut in with positive relative velocity	1	1
RR–A02	Cut in with negative relative velocity	1	1
RR–A03	Cut out	1	1
RR–A04	Cut through	1	1
<b>RR–A05</b>	<b>Overtaking vehicle from oncoming traffic</b>	1	1
RR–A06	Oncoming vehicle turning left	1	1
RR–A07	Slow leading vehicle	1	1
RR–A08	Very slow leading vehicle	0	1
<b>RR–A09</b>	<b>No more neighboring vehicle</b>	1	0
RR–A10	End of traffic jam	1	0
RR–A11	Leading vehicle brakes	1	1
RR–A12	Leading vehicle accelerates	1	1
RR–A13	Small static object (can be run over)	0	0
RR–A14	Small moving object (can be run over)	1	0
RR–A15	Large static object on entire lane (cannot be run over)	0	1
RR–A16	Large moving object (cannot be run over)	0	1
RR–A17	Pedestrian / Cyclist	1	1
RR–A18	Convoy ahead	0	1
RR–A19	Heavy-duty transport ahead	0	1
RR–A20	Gigaliner ahead	1	1
<b>RR–A21</b>	<b>Large static object on right half of lane (cannot be run over)</b>	1	1

A vehicle merging from an intersection into the AV's lane is a vehicle cutting into the ego-vehicle's lane. It can either have a positive (RR–A01) or negative (RR–A02) relative velocity. A cut out is a vehicle that leaves the rural road for example at an intersection (RR–A03). These are standard maneuvers on rural roads (exposure 1) and the relative negative velocity between the vehicles is usually high (severity 1). A vehicle cutting through does not occur on rural roads as the assumption is, that only one lane exists in each direction to avoid redundancy. A vehicle cutting through (RR–A04) on rural roads can only occur at intersections. The vehicle crosses the intersection perpendicular to the ego-vehicle's lane. This situation is a common scenario at intersections which leads to exposure 1. The severity of an accident with a perpendicularly moving vehicle is high (S3) as the relative velocity is highly negative.

When an oncoming vehicle takes over a vehicle, it enters the lane of the ego-vehicle (RR–A05). An accident with oncoming traffic is severe (severity 1), but it happens rarely, less than 1 % of the driving. Either the oncoming traffic passes a vehicle only when there is a long space between itself and oncoming traffic, or no passing is performed at all. This scenario implies that the oncoming vehicle merges back into its original lane in time. Furthermore, oncoming vehicles may also enter the ego-vehicle's lane while turning left for example at intersections (RR–A06). This is much more likely and similarly severe (exposure and severity 1).

If the AV has a leading vehicle, it can be either slow (RR–A07) or extremely slow (RR–A08), such as tractors. Vehicles that are slower than the ego-vehicle intends to be (RR–A07) occur very often on rural roads (exposure 1); very slow vehicles are much rarer and occur in less than 1 % of the driving (exposure 0). In both scenarios, an accident with the vehicle ahead can lead to severe consequences (severity 1).

In an overtaking maneuver, the ego-vehicle has a neighboring vehicle until it successfully passed it in order to merge back into its original lane or until the driver decides to merge back into its previous spot. This driving scenario described with RR–A09, no more neighboring vehicle. This scenario is very common (exposure 1) as it always happens, once an overtaking maneuver is initiated. The severity in this situation is low (severity 0) as no direct conflicting partner exists due to the empty neighboring lane.

Reaching the end of a traffic jam (RR–A10) does not only exist on highways, but also on rural roads where it is similarly hazardous. It is much more common on rural roads because it can easily be caused by red traffic lights or other priority rules at intersections further ahead of the ego-vehicle.

Similar scenarios with similar exposure and severity for changes within the field of view exist for rural roads, as they do for highways. HW–A03 - HW–A08, HW–A10 to HW–A14, and HW–A16 to HW–A18 correspond to RR–A11 to RR–A20. HW–A12 is split into two scenarios for rural roads: RR–A15 and RR–A21. On a rural road, vehicles can either stop on the entire lane (RR–A21) for example due to a flat tire or be pushed to right side of the lane (RR–A21), so that the following traffic take over more easily. It is also common that vehicles park on the side of the road, usually in towns or for some special events where no other parking spots are available. Both situations should be analyzed separately. Looking at the exposure and severity column, just small static objects and convoy driving can be neglected for a first analysis.

Oncoming vehicles in the neighboring lane do not represent an individual scenario as this is not a scenario that forces the AV to change its behavior. The information of oncoming traffic is not neglected though as the expectancies of other road users varies if vehicles are oncoming in the neighboring lane or not.

17 scenarios are found for direct calls to action on rural roads, Category B. Nine of them are similar scenarios as on highways. HW–B02 to HW–B10 correspond with RR–B01 to RR–B10. The exposure differs from the ones on highways. Temporal speed limits are much more common on rural roads as for example passing schools often have lowered speed limits during the day.

Seven additional calls to action exist on rural roads compared to highways exist. These are highlighted in Table 3.11 RR–B10 to RR–B12 are priority rules that require the ego-vehicle to stop: red traffic lights, stop signs, and yield signs. When the traffic light turns green (RR–B13), the vehicle is requested to continue driving. Entering and exiting of roundabouts (RR–B14 and RR–B15) and approaching intersections (RR–B16) can also be interpreted as calls to action. The vehicle is called to enter, remain, or leave a roundabout, to turn or pass an intersection. These cases are RR–B14 to RR–B17. The exposure is for all of them 1, as those are typical infrastructural scenarios on rural roads.

The scenarios for Category C on rural roads can be seen in Table 3.12. 10 scenarios are found for the deviations from the standard road surface. RR–C01 to RR–C08 are identical to HW–C02 to HW–C09.

RR–C09 only exists on rural roads. One lane is blocked due to construction work and only the one remaining lane is available for both traffic directions. Traffic islands (RR–C10) for

Table 3.11: Category B scenarios for rural road driving – Direct calls to action – including their exposure. Scenarios which do not occur on highways are printed bold. Exposure levels of **E0** / **E1** / **E2** are classified as 0; exposure levels of **E3** / **E4** as 1.

Number	Event	Exposure
RR-B01	Emergency vehicle	0
RR-B02	Beginning speed limit	1
RR-B03	End speed limit	1
RR-B04	Time frame of temporal speed limit begins	0
RR-B05	Time frame of temporal speed limit ends	0
RR-B06	Beginning no passing	0
RR-B07	End no passing	0
RR-B08	Opening new lane	0
RR-B09	Lane ends	1
RR-B10	Red traffic light	1
<b>RR-B11</b>	<b>Stop sign</b>	1
<b>RR-B12</b>	<b>Yield sign</b>	1
<b>RR-B13</b>	<b>Traffic light turns green</b>	1
<b>RR-B14</b>	<b>Entry of roundabout</b>	1
<b>RR-B15</b>	<b>Exit of roundabout</b>	1
<b>RR-B16</b>	<b>Approaching intersection</b>	1
<b>RR-B17</b>	<b>Entry of intersection</b>	1

pedestrians exist on rural roads, mostly in towns. RR-C10 describes the situation when a pedestrian is at the traffic island and intends to cross the road.

The exposure of construction sites which have wrong lane markings or one-sided traffic is lower than the other normal driving scenarios. Most common for changes in the road surface are ruts, narrowed lanes and lane markings prohibiting overtaking.

Table 3.12: Category C scenarios for rural road driving – Deviation from standard road surface – including their exposure. Scenarios which do not occur on highways are printed bold. Exposure levels of **E0** / **E1** / **E2** are classified as 0; exposure levels of **E3** / **E4** as 1.

Number	Event	Exposure
RR-C01	No overtaking	1
RR-C02	No overtaking one-sided	0
RR-C03	Missing lane marking	0
RR-C04	Confusing lane marking	0
RR-C05	Narrowed lane	1
RR-C06	Ruts	1
RR-C07	Slippery road	0
RR-C08	Wind	0
<b>RR-C09</b>	<b>Construction site with one-sided traffic</b>	0
<b>RR-C10</b>	<b>Traffic island</b>	0


### 3.2.5 Determination of Expectations

The STPA for AV is based on the assumption that a hazard can occur if the driving maneuver of the AV is not expected by the challenger. Of course, a human driver always has to assume that everything can happen and has to be able to react in every situation appropriately, but driving with this assumption would not be possible. A driver for example will not expect another vehicle to turn around on a highway, although it would be possible. This example shows that a human reduces the possibilities to a few assumptions so it is possible to drive. This reduced assumption is used for the analysis and can be determined independently from the AV's behavior.

For every previously defined driving scenario the expectancy of the challenger is determined. The challenger expects the same behavior from human driver in a manually steered vehicle and it can therefore be looked at the intended and most often performed human actions in every driving scenario. Human misbehavior due to inattentiveness, heart attacks, or else, are not intended CA and considered to unexpected behavior. CA-6 and CA-7 are excluded from this analysis as no emergency braking or emergency stopping can ever be expected and CA-1 and CA-5 can only be executed instantly. Keeping speed and keeping lane (CA-1) does not represent a change in behavior and can therefore not be delayed; a lane change cannot be aborted delayed because an AV continues to perform an already started lane change until there is a reason to abort a lane change. If it does not abort the lane change instantly, it executes the change completely.

A human can react to a changing driving situation by performing an action Instantly (I), a little Delayed (D), or not at all. Table 3.13 shows the legend that is used to mark the respective behavior in the following three tables for highway scenarios and within the hazard identification process.

Table 3.13: Labeling for the classification of expectations.

Description	Symbol
Instant action expected	I
Delayed action expected	D
Both actions expected (instant and delayed)	B
Unexpected	

The exemplarily carried out analyses in Chapter 4 are performed for the driving scenarios HW-A01, HW-B03, HW-C06, and RR-A06. The expectations of other road users are determined in the next two paragraphs among others.

## Expectations of Highway Driving Scenarios

In Table 3.14 - 3.16 the actions a human would perform can be seen for all uncombined driving scenarios on highways. These expectations are also the one of a challenger. Grey shaded cells show that the respective CA is not expected in the specific driving scenario; a white cell with an "I" represents the expectation of instant action; a cell with a D represents the expectation of delayed action and a B represents that the challenger anticipates with both actions – delayed and instant, as defined in Table 3.13. Whether a human would perform CA-7 and CA-8 is not determined because they are always surprising for the following vehicle as they happen out of the sudden without any indicators and always require instant actions when necessary.

If a vehicle cuts in with a positive relative velocity (HW-A01) in front of a human-driven vehicle, a human driver would not brake or change lanes as it does not influence its driving. It is obvious that the vehicle soon leaves the safety distance and therefore a human would keep the current speed and lane (CA-1). In cases when the driver was about to change lanes and simultaneously another vehicle merges into the same lane, a human driver would abort the lane change instantly (CA-5).

If the vehicle cuts in with a negative relative velocity (HW-A02), it is necessary to either change lanes, brake or abort the lane change maneuver in order to avoid an accident. Usually this is not performed instantly when the vehicle enters the safety distance but with a little delay.

Table 3.14: Expectations of Category A highway driving scenarios for CA-1 to CA-5. The definitions of abbreviations of driving scenarios, categories, and CAs are in the glossary.

Number	Event	CA-1	CA-2	CA-3	CA-4	CA-5
HW-A01	Cut in with positive relative velocity	I				I
HW-A02	Cut in with negative relative velocity		D	D	D	D
HW-A03	Cut out	I		B		
HW-A04	Cut through	I				I
HW-A05	Slow leading vehicle		I	I	I	I
HW-A06	Leading vehicle brakes		I	D	D	I
HW-A07	Leading vehicle accelerates	I		I		
HW-A08	Slow moving traffic	I				
HW-A09	End of traffic jam ahead			I	I	
HW-A10	Small static object (can be run over)		I			I
HW-A11	Small moving object (can be run over)		I			I
HW-A12	Large static object (cannot be run over)		I		I	I
HW-A13	Large moving object (cannot be run over)	B	B	B	B	I
HW-A14	Pedestrian / Cyclist		I	I	I	I
HW-A15	Wrong-way driver		B	B	B	I
HW-A16	Convoy	I	B	B	B	I
HW-A17	Heavy-duty transport		I	I	I	I
HW-A18	Gigaliner	I				

The reaction of a vehicle cutting out (HW–A03) is similarly insignificant for a driver as (HW–A01) if the driver does not want to accelerate. If the vehicle cutting out slowed the other driver down, he / she would (instantly or delayed) accelerate. In cases when the vehicle is cutting out into the same lane into which the ego-vehicle started to move, nobody would abort the maneuver as the lane change was either to pass (lane change to the left) or to take right-hand lane.

When a vehicle cuts through the lane of a human-driver vehicle (HW-A04), the driver does not brake, accelerate, or change lanes; the only action is to keep speed and lane. The driver can see the intentions of the vehicle cutting through and does not need to reduce speed to increase the distance between the vehicles to the by law required safety distance. An already initiated lane change maneuver is aborted when the vehicle cutting through aims the same lane as the ego-vehicle.

A human has to choose between changing the lane or slowing down (CA–2 to CA–4) when approaching a slow leading vehicle (HW–A05). If the vehicle is about to change lane and the vehicle on the lane is slower, would also abort the lane change. All actions are performed as soon as possible (instantly).

When the leading vehicle brakes (HW–A06) the human has three options to brake, to change lanes and keep the current speed, or to change lanes and accelerate. A lane change would usually be done immediately, braking would be executed delayed (while already within the safety distance). If the leading vehicle that brakes is on the lane the ego-vehicle wants to merge into, the human would most likely abort the lane change immediately.

The reaction to an accelerating vehicle in the front (HW–A07) of a human is either to instantly accelerate as well or to do not perform any different action (keep speed and keep lane).

In slow moving traffic (HW–A08), the average driver does not change its lane as he / she knows that the driving speed of all lanes is almost the same and adapts its speed to the leading vehicle. An already started lane change maneuver will not be aborted.

When a human driver detects the end of a traffic jam (HW–A09), he / she reacts by immediately braking moderately combined or not with a lane change. An already started lane change would not be aborted.

When a human driver detects small static (HW–A10) or small moving (HW–A11) objects, the driver would not change speed or lane, but just bypass or run over the object. If the driver detects the object while changing lane, chances are high that he / she aborts the lane change.

Large static objects that cannot be run over (HW–A12) force the human to change its lane or to stop in front of them. Human drivers normally react as soon as they see that their lane is blocked with a lane change and perhaps additionally with slowing down. A lane change into a lane that is blocked is directly aborted.

A reaction to a large moving object (HW–A13) such as deer or tarpaulins cannot be predicted. Every human reacts differently in such an unusual scenario.

If there is a pedestrian or cyclist on right-hand side the highway (HW–A14), a driver would immediately perform a lane change to increase the distance, slow down or both. An initiated lane change would be aborted.

The behavior of a human when he / she is confronted with a wrong-way driver (HW–A15) is similarly unpredictable as the reaction to HW–A13. An initiated lane change into the lane of the wrong-way driver would be instantly aborted.

A lane change into a convoy (HW–A16) is not allowed, but often performed anyways. All CA are instantly or delayed possible to be performed because the situation occurs so rarely that just a few people realize a convoy and do not know how to react.

Passing by a heavy-duty transport vehicle (HW–A17) normally requires slowing down or changing the lane instantly and a lane change maneuver is aborted. In contrast to the heavy-duty truck, a gigaliner (HW–A18) on the right-hand side or ahead does not make a human change the behavior.

Analog to Table 3.14 of Category A, Table 3.15 shows the derived expectations for Category B driving scenarios.

When an emergency vehicle approaches from behind (HW–B01), the human is supposed to immediately clear the lane or if not possible, move to the edge of the lane and slow down. An initialized change of lane is aborted to keep the lane clear for the emergency vehicle.

At the beginning of speed limits (HW–B02), humans usually roll out and do not brake instantly, whereas at the end of a speed limit (HW–B03), humans usually start accelerating before even passing the road sign. A change in speed and lane can be performed either to start and overtaking maneuver or to finish an overtaking maneuver. When starting, the vehicle merges to the left and accelerates. When finishing an overtaking maneuver, the vehicle merges back to the right and can continue accelerating as no leading vehicle exists.

Table 3.15: Expectations of Category B highway driving scenarios for CA–1 to CA–5. The definitions of abbreviations of driving scenarios, categories, and CAs are in the glossary.

Number	Event	CA–1	CA–2	CA–3	CA–4	CA–5
HW–B01	Emergency vehicle	■	I	I	I	I
HW–B02	Beginning speed limit	■	■	D	D	■
HW–B03	End speed limit	■	■	I	I	■
HW–B04	Time frame of temporal speed limit begins	I	■	■	■	■
HW–B05	Time frame of temporal speed limit ends	I	■	■	■	■
HW–B06	Beginning no passing	I	■	■	■	■
HW–B07	End no passing	I	■	■	■	■
HW–B08	Opening new lane	I	B	I	B	■
HW–B09	Lane ends	■	B	■	B	I
HW–B10	Beginning emergency lane clearance	I	B	I	B	■
HW–B11	End emergency lane clearance	■	B	■	B	I
HW–B12	Red traffic light	■	■	I	■	■
HW–B13	Traffic light turns green	■	■	B	■	■
HW–B14	Ramp	■	■	■	B	■
HW–B15	Exit	■	■	■	I	■
HW–B16	Toll station	■	■	B	B	■
HW–B17	Customs station	■	■	B	B	■
HW–B18	Highway junction	B	B	B	B	B

Once passed the beginning of a temporal speed limit sign (HW-B04) when the specified time period is not reached, a human will not slow down even if he / she reaches the time period while driving in the specified area. When the end of the defined time period is reached (HW-B05), a human does usually not remember and does not change its behavior.

At the beginning of a no passing area (HW-B06), a human driver usually keeps in its lane and keeps speed. If the driver already initiated a lane change, he / she does complete it.

It is common not to change lanes before the road sign indicating the end of no passing (HW-B07) or the respective lane markings.

When a new lane opens (HW-B08) on the left hand-side, a human driver might take it to take over the leading vehicle or keeps at its speed and in its lane. When a new lane opens on the right-hand side, a human is either taking it because of the law to drive on the right-handed lane or keeps in its lane at the same speed.

If the lane of the human-driven vehicle ends (HW-B09), a human tries to change lanes either instantly or at the actual end of the lane (delayed). If the lane the vehicle was about to merge into, ends, the vehicle aborts the lane change immediately. The actions are identically to the end of a hard shoulder release (HW-B11).

At the beginning of an emergency lane clearance (HW-B10) a vehicle can either turn into the upcoming lane or remain in its lane accelerating or not. A lane change is usually not combined with a change of speed.

In Germany it is strictly forbidden to pass a red traffic light (HW-B12). Most human drivers stick to that law and stop within their lane immediately. An already initiated lane change can be completed when stopping in front of the traffic light. When the traffic light turns green (HW-B13), human drivers accelerate in their lane. This is usually done instantly, but it is also common that humans do not instantly notice the changing lights and start accelerating delayed.

At ramps (HW-B14) a human changes lanes as soon as possible (immediately or delayed), at exits (HW-B15) humans change into the lane at the beginning.

Actions are similar on toll stations (HW-B16) and customs stations (HW-B17). Vehicles remain in lane or change lanes, but always reduce their speed; a started lane change is completed.

Highway junctions (HW-B18) are complex infrastructural facilities where many lane changes take place at reduced velocities. Initiated lane changes can be completed or aborted.

Table 3.16 shows the classification of human behavior in Category C.

When lane marking indicates that overtaking is not allowed (HW-C01) a human does not cross lanes or changes speed, just in cases when the lane is blocked and there is no other chance to avoid an accident. In the uncombined driving situation of HW-C01, there is no slow leading vehicle and no blocked lane. A lane change cannot be aborted, as no lane change takes place when overtaking is prohibited. The identical actions are performed by a human when only one-sided overtaking is allowed (HW-C02)

Missing lane marking (HW-C03) or confusing lane marking (HW-C04) does not influence the driving of a human. It remains in its lane at the same speed. An initiated lane change can be completed independently of existing or correct lane markings. When the lane is narrowed (HW-C05) a human keeps its speed and lane (CA-1), if it is still wide enough to be passed with the current speed. If the lane is not wide enough and the drivers feel uncomfortable, they might change lanes at the same or reduced speed (CA-2, CA-4) or remain in lane with reduced speed



Table 3.16: Expectations of Category C highway driving scenarios for CA-1 to CA-5. The definitions of abbreviations of driving scenarios, categories, and CAs are in the glossary.

Number	Event	CA-1	CA-2	CA-3	CA-4	CA-5
HW-C01	No overtaking	I				
HW-C02	No overtaking one-sided	I				
HW-C03	Missing lane marking	I				
HW-C04	Confusing lane marking	I				
HW-C05	Narrowed lane	I	B	B	B	
HW-C06	Ending neighboring lane		I	I	I	I
HW-C07	Ruts	I				
HW-C08	Slippery road		D	D	D	
HW-C09	Wind	I				

(CA-3). The actions CA-2, CA-4, and CA-3 can all be performed either instantly or delayed as a human can start to feel uncomfortable within a narrowed lane at every time. A human would not abort a lane change (CA-5) into a narrowed lane as humans can foresee the situation and know that the lane is narrowed before initiating a lane change.

When a neighboring lane ends (HW-C06), humans intentionally create a gap to let vehicles from that lane merge into. Therefore, they slow down or change lane.

Humans usually maintain their speed and lane when ruts (HW-C07) exist or windy (HW-C09) as they do not have sensors to detect those in advance. When the entire road it is slippery (HW-C08), drivers slow down and might perform a lane change to the right. As it takes time to realize that it is slippery, the actions are performed delayed.

### Expectations of Rural Road Driving Scenarios

In Table 3.18 - 3.19 the expected and unexpected control actions are shown for each rural road driving scenario. The expectations for Category A scenarios are listed in Table 3.18.

A vehicle cutting in with a positive relative velocity (RR-A01) is a vehicle that has passed the ego-vehicle or that merges into the AV's lane at an intersection. It is common to slow down or at least not to accelerate while the other vehicle is merging. When a vehicle with negative relative velocity cuts in (RR-A02), the human driver has to slow down within its lane. Usually this action is not performed instantly, but with a little delay. If a vehicle cuts out (RR-A03) to take over another vehicle, the ego-vehicle is not influenced in its behavior and continues driving at the same speed.

If a vehicle crosses an intersection perpendicular to the ego-vehicle (RR-A04), the ego-vehicle slows down instantly in order to let the crossing vehicle leave the intersection before it enters it itself. If the ego-vehicles intends to turn at the intersection too, it not only slows down instantly, but also makes a turn (change lane).

The overtaking maneuver from a vehicle of the oncoming traffic (RR-A05) does provoke a human driver to keep its lane and speed or to slow down, but not to accelerate in order to give the overtaking vehicle enough time to merge back into its lane after passing a vehicle. An already initiated lane change is instantly aborted.

### 3 Application of STPA to Automation Risks Resulting from AVs

Table 3.17: Expectations of Category A rural road driving scenarios for CA-1 to CA-5. The definitions of abbreviations of driving scenarios, categories, and CAs are in the glossary.

Number	Event	CA-1	CA-2	CA-3	CA-4	CA-5
RR-A01	Cut in with positive relative velocity	■	■	I	■	I
RR-A02	Cut in with negative relative velocity	■	■	D	■	■
RR-A03	Cut out	I	■	■	■	■
RR-A04	Cut through	■	■	I	I	■
RR-A05	Overtaking vehicle from oncoming traffic	I	■	I	■	I
RR-A06	Oncoming vehicle turning left	■	■	I	I	■
RR-A07	Slow leading vehicle	■	■	I	B	■
RR-A08	Very slow leading vehicle	■	■	I	B	■
RR-A09	No more neighboring vehicle	■	B	■	B	■
RR-A10	End of traffic jam	■	■	I	■	I
RR-A11	Leading vehicle brakes	■	■	B	■	■
RR-A12	Leading vehicle accelerates	I	■	I	■	■
RR-A13	Small static object (can be run over)	I	■	■	■	■
RR-A14	Small moving object (can be run over)	I	■	■	■	I
RR-A15	Large static object on entire lane (cannot be run over)	■	■	■	I	I
RR-A16	Large moving object (cannot be run over)	■	■	I	I	I
RR-A17	Pedestrian / Cyclist	■	■	I	■	I
RR-A18	Convoy ahead	■	■	I	B	■
RR-A19	Heavy-duty transport ahead	■	■	I	B	■
RR-A20	Gigaliner ahead	■	■	I	B	■
RR-A21	Large static object on right half of lane (cannot be run over)	■	I	I	I	I

A left turning vehicle at an intersection (RR–A06) provokes the following vehicle to slow down instantly. The human driver can also turn at the intersection, which requires to brake (change speed) and make a turn (lane change). Similar to HW–A05, people tend to take over a (very) slow leading vehicle (RR–A07, RR–A08), which requires a lane change and accelerating. When humans decide to follow the slow vehicle, they slow down within their lane. Very slow vehicles are most of the times overtaken, assumed there is no oncoming traffic.

If a humans do not have a neighboring vehicle anymore (RR–A09) in an overtaking maneuver, they move back into their original lane at the same speed or accelerate even more. When a traffic jam (RR–A10) exists, an overtaking maneuver cannot be performed and the vehicle must remain in its original lane and start to slow down instantly, as taking over is not useful when more vehicles than the leading vehicle is stuck. An already initiated lane change maneuver is aborted.

When the leading vehicle brakes (RR–A11), a human brakes too and does not start an overtaking maneuver. The braking of the leading vehicle is usually caused by another vehicle braking ahead, a blocked road, or caused by traffic guidance instructions. Overtaking is not reasonable. If the leading vehicle accelerates (RR–A12), the following vehicle can either accelerate too or keep its current speed. There is no need for a lane change. When a lane change maneuver was already initiated, the maneuver is aborted and the acceleration can be continued in the original lane.

Small static and moving objects which can be run over (RR–A13, RR–A14) are passed at constant speed and lane. Nevertheless, it is common to interrupt an already initiated lane change maneuver to avoid running over the object and to start the lane change maneuver again after passing the object.

If a large static object (RR–A15) which cannot be run over blocks the lane, the human driver slows down and changes lanes to pass the object. An already initiated lane change maneuver is aborted, if the lane the vehicle intended to change into is blocked. When a large moving object is ahead (RR–A16) of the vehicle, the safest option is to brake entirely, but also lane changes are likely to be performed by humans as a spontaneous reaction. A started lane change maneuver is instantly aborted, if a large moving object crosses the lanes.

Pedestrians and cyclists RR–A17 on the right-hand side of the lane are avoided by changing lanes instantly. The speed is usually not reduced. When a lane change maneuver was already initiated and pedestrians or cyclists appear in the target lane, the lane change maneuver is aborted.

It is the safest option not to take over convoys (RR–A18), heavy-duty transports (RR–A19), and giganliners (RR–A20), to remain in the current lane, and to slow down to their speed. Humans do not always pursue the safest option and therefore it is also common to start a take over maneuver by changing speed and lanes delayed or instantly.

Vehicles parking on the right-hand side of the lane (RR–A21) can be easily passed by changing the lane. The speed can be either reduced or kept at the current level. If there is oncoming traffic, the ego-vehicle can also slow down in its own lane and even stop. An already started lane change maneuver is not aborted instantly.

Table 3.18 lists the expectations for Category B driving scenarios on rural roads. When an emergency vehicle approaches from behind (RR–B01), a human slows down immediately and moves to the right-hand side of the lane. An initiated lane change for example to turn left at an intersection or to initiate a take over maneuver is aborted until the emergency vehicle itself turned or passed the intersection or passed the ego-vehicle.

### 3 Application of STPA to Automation Risks Resulting from AVs

The human behavior at the beginning of the end of a speed limit (RR–B02, RR–B03, RR–B04, RR–B05) is similar to the one on highways, except that no lane change is possible. At the beginning and end of a no passing area (RR–B06, RR–B07) and when a new lane opens or closes (RR–B08, RR–B09), a human behaves also similar on rural roads to highway driving.

Table 3.18: Expectations of Category B rural road driving scenarios for CA–1 to CA–5. The definitions of abbreviations of driving scenarios, categories, and CAs are in the glossary.

Number	Event	CA–1	CA–2	CA–3	CA–4	CA–5
RR–B01	Emergency vehicle		I			I
RR–B02	Beginning speed limit			D	D	
RR–B03	End speed limit			I	I	
RR–B04	Time frame of temporal speed limit begins	I				
RR–B05	Time frame of temporal speed limit ends	I				
RR–B06	Beginning no passing	I				
RR–B07	End no passing	I				
RR–B08	Opening new lane	I	B	I	B	
RR–B09	Lane ends		B		B	I
RR–B10	Red traffic light			I		
RR–B11	Stop sign				I	
RR–B12	Yield sign			I		
RR–B13	Traffic light turns green			B		
RR–B14	Entry of roundabout			I		
RR–B15	Exit of roundabout		B	B		
RR–B16	Approaching of intersection	I		I		
RR–B17	Entry of intersection	I			I	

In front of a red traffic light (RR–B10) and a stop sign (RR–B11), the vehicle instantly stops entirely and a lane change is completed before reaching the respective road infrastructural sign. The executed actions are similar when approaching a yield sign (RR–B12), except that no entire stop is required, if the intersection is empty.

When traffic lights turn green (RR–B13), the human drivers instantly start to accelerate in their own lane; if drivers is not vigilant, they might start to accelerate delayed. A lane change maneuver does not have to be aborted, if the vehicle just approached the traffic light without stopping entirely.

The behavior when entering a roundabout (RR–B14) and approaching an intersection (RR–B16) are identically: in both cases the vehicle remains in its lane and slows down instantly. No lane change is executed. To exit a roundabout (RR–B15), the vehicle turns right (change lane) at current speed or reduced speed. This can be instantly be the first exit or delayed at a different exit.

When entering an intersection with priority (RR–B17), the vehicle keeps speed and lane. A lane change maneuver in this case means a turning maneuver at the intersection. To perform this maneuver, the vehicle has to slow down instantly.

In Table 3.19 the expectations of Category C scenarios on rural roads are given. RR–C01 to RR–C08 are similar scenarios to highway driving and humans behave in the same manner. The only difference is that in rural road driving a lane change is never possible, as only one lane for each direction exists.

When a construction site blocks one's lane (RR–C09), the vehicle changes the lane and passes the construction site at reduced speed. An already started lane change maneuver into the blocked lane is instantly aborted.

Table 3.19: Expectations of Category C rural road driving scenarios for CA–1 to CA–5. The definitions of abbreviations of driving scenarios, categories, and CAs are in the glossary.

Number	Event	CA–1	CA–2	CA–3	CA–4	CA–5
RR–C01	No overtaking	I				
RR–C02	No overtaking one-sided	I				
RR–C03	Missing lane marking	I				
RR–C04	Confusing lane marking	I				
RR–C05	Narrowed lane	I	B	B	B	
RR–C06	Ruts	I				
RR–C07	Slippery road		D	D	D	D
RR–C08	Wind	I				
RR–C09	Construction site with one-sided traffic				I	I
RR–C10	Traffic island	I		I		I

At traffic islands from which a human wants to cross the road (RR–C10), sometimes humans let them cross, sometimes they pass the island without stopping. An initiated lane change is aborted in order to pass the traffic island on the right-hand side.

The expectations for combined driving scenarios are not determined in this work. For the analysis of those scenarios, the respective expectations have to be determined using the same strategy as used for the determination of expectations for the uncombined scenarios. These expectations are not determined in this thesis. An example for a combined scenario is given in Section 4.3.

### 3.3 STPA Implementation

All previously defined elements are required for the implementation of the STPA, described in this section. The first part gives an overview in which situation a CA can be hazardous in relation to the expectations. It is followed by the adaption to the STPA step 1, the actual hazard identification, and to step 2, the causal factors analysis. Figure 3.3 visualizes the linking between the process steps described in this section.

#### 3.3.1 Determination of Unsafe Control Actions

The STPA uses the four categories **a-d** described in Section 2.3.3 for the determination of UCAs. Two categories have to be specified for the AD control actions, category **c** and **d**. CAs executed at the wrong time or in the wrong order (**c**) can be executed delayed or instantly. CAs that are

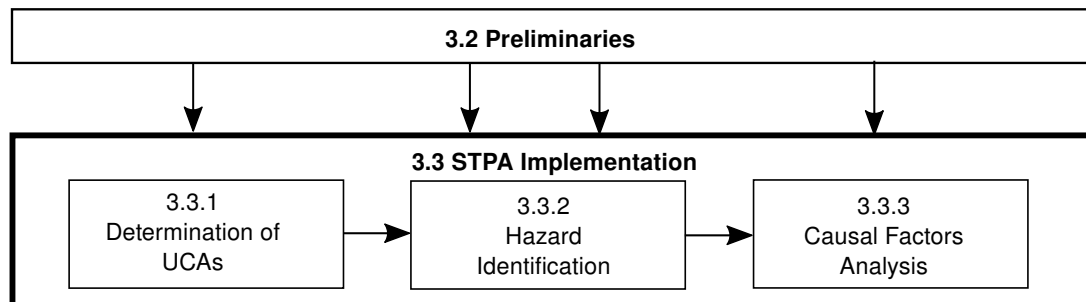


Figure 3.3: Flow chart diagram for the STPA implementation including the previously defined preliminaries.

stopped too soon or applied too long (**d**) can either be an acceleration that was stopped too soon or a braking maneuver that was executed too long. A lane change cannot at all be stopped too soon as lane changes are either completed entirely or aborted, which is defined in a separate control action, CA-5.

Table 3.20 gives an overview of these categories combined with the principle that an executed CA can only be hazardous if it is not expected.

Table 3.20: Overview of possibly UCAs.

Expected Control Action	Executed Control Action			
	(a) Not Provided Causes Hazard	(b) Provided Causes Hazard	(c) At Wrong Time or in Wrong Order Causes Hazard	(d) Stopped Too Soon or Applied Too Long
(CA-1) Keep speed & keep lane	CA-1	CA-2, CA-3, CA-4, CA-5, CA-6, CA-7		
(CA-2) Keep speed & change lane	CA-2	CA-1, CA-3, CA-4, CA-5, CA-6, CA-7	delayed, instantly	
(CA-3) Change speed & keep lane	CA-3	CA-1, CA-2, CA-4, CA-5, CA-6, CA-7	delayed, instantly	too soon stopped acceleration, too long applied braking
(CA-4) Change speed & change lane	CA-4	CA-1, CA-2, CA-3, CA-5, CA-6, CA-7	delayed, instantly	too soon stopped acceleration, too long applied braking
(CA-5) Abort lane change	CA-5	CA-1, CA-2, CA-3, CA-4, CA-6, CA-7	delayed, instantly	

Not every combination is reasonable and can therefore not all combinations are listed in the respective cells. The AV can execute seven CAs, but the challenger will only expect five. An emergency brake and emergency stop are unforeseen actions for the AV, otherwise it would brake sooner and less abrupt, so the challenger cannot expect these actions. A not provided action (**a**) is only hazardous, if there is one situation in which only the not provided action is expected by the challenger. If multiple CAs are expected in one driving situation, it does not represent a hazardous situation as this depends on the actually executed CA. Reversely, providing a CA (**b**) is only hazardous, if it is not expected. Wrong timing of a CA (**c**) for an AV can only be a delayed action or an instant action when the opposite is expected. The only possible CAs that stopped too soon or was applied too long (**d**) for the here identified CAs are if

an acceleration stopped too soon or if braking is applied too long. If a lane change is aborted too soon, it implies that the action was expected delayed and the situation is therefore covered with the classification of delayed and instantly expected CAs.

For CA–1, possible UCAs arise if the AV executes the CA to keep the lane and to keep the speed, but CA–2, CA–3, CA–4, or CA–5 are expected. It can also be unsafe not to provide CA–1, although it is expected that the AV keeps its lane and keeps its speed. Possibly unsafe CAs for (a) and (b) can similarly determined for CA–2, CA–3, CA–4, and CA–5.

For CA–1, an instant or a delayed action can neither be expected nor executed. The keep lane and keep speed action is an action that does not change the current status of the vehicle. If nothing should happen, nothing can be delayed or not be executed instantly. Changing speed or lane can either be delayed or executed instantly. Each CA of CA–2, CA–3, CA–4, and CA–5 contains a lane change, a change of speed or even both.

A stopped too soon or applied too long action **d** is impossible for CAs, where no change in speed takes place. This is the case for CA–1, CA–2, and CA–5. An emergency brake (CA–6) or emergency stop (CA–7) also cannot be applied too long or stopped too soon as in their definition an entire stop is determined or not. Only CA–3 and CA–4 can theoretically be UCAs if they were stopped too soon or applied too long.

To determine precise UCA for AVs, every possible unsafe CA from this table (Table 3.20) must be combined with every driving scenario and must be evaluated regarding its hazard potential.

### 3.3.2 Hazard Identification

Step 1 of the STPA (hazard identification) is performed with six separate tables for every driving scenario to be analyzed: for not provided CAs (1), provided CAs (2), delayed provided CAs (3), instantly provided CAs (4), CAs in which the accelerations stopped too soon (5), and CAs in which braking was applied too long (6). Table 3.21 represents the template of all of them. In the first column, the legend for the meaning of the rows can be seen. The first row is the legend for the CAs that are not provided, delayed provided, instantly provided, stopped too soon or applied to long, depending on the table viewed.

Table 3.21: Template for the identification of UCAs.




Legend	CA–1	CA–2	CA–3	CA–4	CA–5	CA–6	CA–7
Classification							
Reason for AV action							
Violated system SC							
Reason for classification							
Severity							
ASIL							
UCA							
Refined SC							

First, every CA has to be analyzed, if the action is plausible and why an AV would act so. The identified reason is filled in row "Reason for AV action". Next, it is identified, if a system SC is violated or not. If not, no further analysis is necessary and the cell "hazard classification" can be marked according to Table 3.22 green. If a SC is violated, it can be determined if the

### 3 Application of STPA to Automation Risks Resulting from AVs

action represents a malfunction of the system (Class 1) or not (Class 2), and the cell "hazard classification" is colored respectively using the colors defined in Table 3.22. For traceability, the reason for the classification should be captured in a separate cell.

Table 3.22: Labeling colors for (not) hazardous situations and situations caused by a malfunction of the system.

Description	Color
Not hazardous	
Hazardous (Class 2)	
Malfunction of system (Class 1)	

Hazards according to Class 1 are not further analyzed in this work. For Class 2 hazards, the severity is determined to conclude the ASIL by using the exposure for every driving situation and the highest controllability level **C3** according to Subsection 3.2.4. The ASIL is not the only rating that should be used to conclude the importance in preventing the respective hazard. It is most important to reduce the hazards which are most unlikely performed by humans. This leads to an additional hazard classification: likelihood that a human driver would perform the same action. Table 3.23 shows the legend of how the "hazard classification" cells should be marked.

Table 3.23: Labeling categories for the likelihood of hazardous situations that human-driven vehicles would cause the hazard.


Description	Label
Almost never happens to human driver	
Unlikely happens to human driver	
Likely happens to human driver	

Table 3.24 shows an example how a filled hazard analysis table a delayed provided control action could look like.

Table 3.24: Exemplary filled hazard analysis table for a delayed provided control action.


Legend	CA-4
Classification	
Reason for AV action	AV starts accelerating and initiating a take over maneuver delayed, after passing the road sign
Violated system SC	SC-3
Reason for classification	Challenger wants to take over the AV and starts the maneuver as soon as he / she detects the road sign. If AV initiates a take over delayed, it might block the challenger who is forced to brake
Severity	S3
ASIL	D
UCA	AV starts an overtaking maneuver right behind the end of speed limit road sign
Refined SC	AV should only start an overtaking maneuver if the challenger did just start to take over AV

Table 3.25-3.27 are the tables for the hazard categories **a**, **c**, and **d**. Category **b** can be analyzed using the template Table 3.21. Table 3.26 and 3.27 have to be created twice for instant and delayed CAs and the CAs "too soon stopped acceleration" and "too long applied braking".



Each table can be minimized with the information collected in Table 3.20. Table 3.25 can be reduced by the last two columns because an emergency brake and an emergency stop are never expected and a not providing cannot cause an error. If the system detects the need for emergency braking, it brakes, else it does not. All impossible or irrelevant actions are blacked in the following tables.

Table 3.26 can be reduced according to Table 3.20 to only four remaining columns (four CAs) and Table 3.27 to only two remaining CAs.

Table 3.25: Template for the hazard identification of are not provided CAs although they are expected.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification						■	■
Reason for AV action						■	■
Violated system SC						■	■
Reason for classification						■	■
Severity						■	■
ASIL						■	■
UCA						■	■
Refined SC						■	■

Table 3.26: Template for the hazard identification of delayed / instantly executed CAs although the opposite is expected.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification	■					■	■
Reason for AV action	■					■	■
Violated system SC	■					■	■
Reason for classification	■					■	■
Severity	■					■	■
ASIL	■					■	■
UCA	■					■	■
Refined SC	■					■	■

Another reduction of CAs to be analyzed can be done for each driving scenario independently by including the previously determined expectancy. Only every CA that is expected needs to be evaluated in the table "not providing"; provided actions are hazardous, if they were not expected at all. Delayed action only has to be evaluated, if instant action is expected and reverse. The table for "Too soon stopped acceleration" and "Too long applied braking" cannot be reduced with the determined expectancy, but the word "too" implies, that the action was not expected as it was performed.

### 3.3.3 Causal Factors Analysis

Step 2 in the STPA identifies the causes for the hazards determined in step 1. Usually this is done using the template of Figure 2.6. For Class 2 hazards, this template is not applicable

Table 3.27: Template for the hazard identification of too soon stopped or too long applied CAs.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification	■	■			■	■	■
Reason for AV action	■	■			■	■	■
Violated system SC	■	■			■	■	■
Reason for classification	■	■			■	■	■
Severity	■	■			■	■	■
ASIL	■	■			■	■	■
UCA	■	■			■	■	■
Refined SC	■	■			■	■	■

though, as hazards are not caused by the malfunction of a system or component and therefore cannot be determined within a control cycle that has a process model, actuators, and sensors.

The primary cause for Class 2 is known through the definition of the adapted STPA described in this chapter: the expected behavior from the challenger does not correlate with the actual behavior of the AV. Nevertheless, a more specific cause should be found for each scenario describing why this mismatch exists. This will help to give the system developer later on in the product development cycle a global understanding of how the system should be designed.

An additional row is therefore required in each of the six tables defined in Section 3.3.2. A reduced representation of the extended hazard identification template of UCAs is shown in Table 3.28 to emphasize the changes within the tables.

Table 3.28: Additional row for the causal factors analysis to the template for the identification of UCAs

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
...							
Refined SC							
Causal factors							

## 3.4 Summary of Approach

The previous sections explained in detail each step of the process to develop and apply STPA for the identification of the risks that occur due to the interaction of AVs with other road users. All process steps can be summarized in a flow chart diagram, shown in Figure 3.4.

The process is split into two parts: the identification of preliminaries and the actual implementation of the STPA. Three out of the five preliminaries can be developed separately from one another: the fundamental definitions (Section 3.2.1), the control structure diagram (Section 3.2.2), and the scenario selection (Section 3.2.4). The other two preliminaries, scenario identification and determination of expectations (Section 3.2.4 and 3.2.5) are specially developed for automation risks of Class 2.

In Section 3.2.1, the system safety constraints SC-1 to SC-6 (Table 3.3) are determined. If one of these is violated in the hazard analysis described in Section 3.3, a hazard occurs.

A control structure diagram is created which to visualize the interaction between the AV and other human road users (Section 3.2.2). The diagram sets the basis for the identification of seven control actions (Table 3.4). A vehicle can keep or change its speed, can keep or changes lanes or perform a combination of them. Additionally, emergency brakes and emergency stops can be necessary actions to prevent an accident.

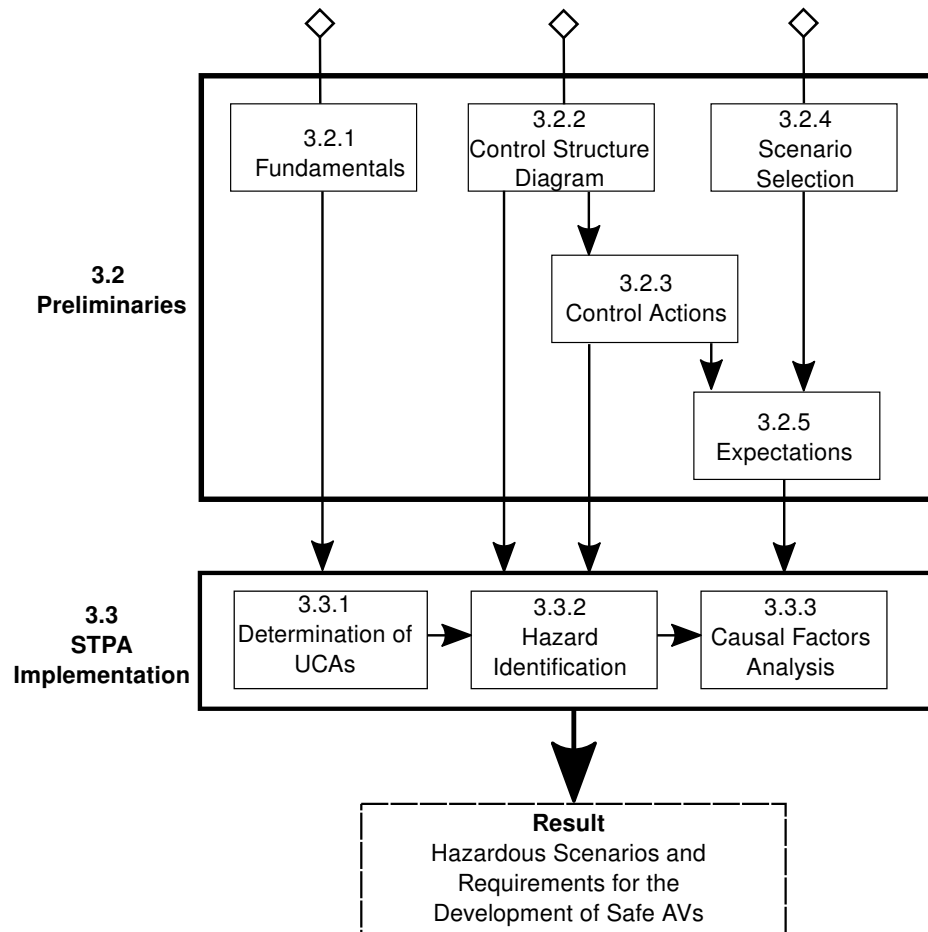


Figure 3.4: Flow chart diagram representing the process of the proposed hazard identification method.

The third independent preliminary is the scenario selection step described in Section 3.2.4. The execution of any control action is never hazardous by itself because they are standard driving maneuvers, but if these actions are performed in the wrong situation they can lead to hazardous situations. These hazardous situations can either result from a malfunctioning driving system in the AV (Class 1 automation risks) or from a correct behavior which does not resemble usual human driving behavior (Class 2 automation risks). A potential Class 2 hazard results from anything that happens on the road that could lead to a change in the behavior of a human or automated vehicle. The relevant situations are identified using three groups that describe calls for changes in the driving behavior: changes within the field of view, direct calls to action, and deviations from the standard road surface (Table 3.5). Each road type has different characteristics which requires separate determinations of driving scenarios. In Section 3.2.4, they are defined for highways and rural roads.

In the next preliminary step, the expected control actions for each scenario must be determined. Three categories are defined to represent immediately expected actions, delayed expected actions and unexpected actions (Table 3.13).

The preliminaries are used for the actual STPA implementation, which is divided into three parts (Section 3.3). In a first step, UCAs which an AV executes are determined for each CA a human expects from another vehicle (Section 3.3.1), under the assumption that hazards of Class 2 only occur when the expected behavior diverges from the performed actions.

The UCAs are used in the hazard identification step to identify in which situations the UCA actually leads to a hazardous situation (Section 3.3.2). The hazardous situations are further analyzed whether they are Class 1 or Class 2 automation risks. Combinations where an incorrect AD behavior occurs that is caused by a system's malfunction are not further evaluated. The other hazardous scenarios, Class 2 scenarios, are classified by the likelihood of occurrence in human driving. The resulting hazardous scenarios least likely to occur are the most important ones to investigate in order to prevent them and to maintain the trust of humans into AD systems.

The last part of the STPA implementation is a causal factors analysis. The classical STPA analysis is not applicable to the driving behavior that is analyzed. A technical explanation for the uncommon driving behavior is specified instead. This process for the hazard analysis identifies hazardous scenarios for Class 2 automation risks and additionally determines requirements that are necessary in the product development process of AVs to avoid these hazards.

A template for the determination of Class 2 hazards with the proposed method is created in addition to this thesis; it automatically creates the required tables for the scenarios to be analyzed. All scenarios can be evaluated separately or in combination with each other.

## 3.5 Adaption to Class 1 and Class 3 Risks

The here proposed method is a special modification of STPA to automation risks of Class 2. For Class 1 and Class 3 automation risks, the same method would not lead to the desired results as the expectations of other road users are not relevant to detect UCAs. Their hazards result from malfunctions which systematically can be identified using the STPA with an adequate control structure diagram for each class. Class 1 hazards result from malfunctioning systems that do not react properly to their environment. Class 3 hazards result from a malfunctioning interaction between the human driver inside the ego-vehicle and the automation.

As described in Section 2.4.3, ABDULKHALEQ et al. [43] introduced a control structure diagram for Class 1 risks of AVs (Figure 2.9). For a Class 1 analysis, the execution of vehicle guidance commands can be assumed to be always correct as they are also existent for manually-driven vehicles. Only the new subsystems and components of AVs compared to manual vehicles need to be analyzed. The hazard analysis can be carried out exactly how LEVESON [19] defined it, no further modifications are necessary such as predefined scenarios. Weather or road conditions that influence the perception of sensors or require different driving behavior can be described within the process model of the AD system controller. As the proposed Class 2 analysis also identifies a few Class 1 hazards, they should be used to cross-validate the Class 1 analysis in order to check the completeness of the method.

Class 3 automation risks also do not depend on specific driving scenarios, the scenarios just determine the severity of an accident. In all situations the human must know whether the AD system is activated or not. The interaction itself between the system and the human driver has to be analyzed for potential hazards. The hazards do not diminish or occur in different driving situations.

The STPA proposed in literature could be useful to determine mode confusion and other Class 3 risks, especially by identifying the causes using Figure 2.6. A control structure diagram could look like Figure 3.5.

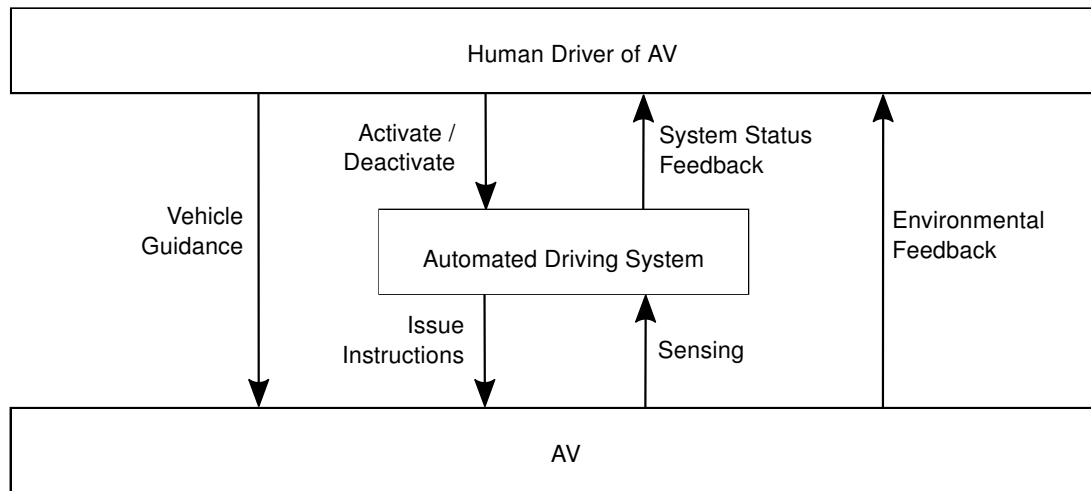


Figure 3.5: Control structure diagram for automation risks of Class 3.

All three control structure diagrams of the Classes 1 to 3 can be combined into one where every class of automation risks covers a different part of the interaction partners. The hazard identification and analysis has to be performed individually for all classes according to the previously mentioned reasons.



## 4 Proof of Method Applicability

In this chapter, the previously method derived is applied to four driving scenarios in order to prove its usefulness to identify hazardous situations. Initially, the applicability of a highway driving scenario of Category B is proven with a detailed description of all steps and the identified hazards are discussed. The example scenario is a call for action (Category B) that is performed through a road sign indicating the end of a speed limit. Further, the applicability of Category A and C scenarios is demonstrated on two highway driving examples. For Category A, a vehicle cutting in in front of the AV with a positive relative velocity is selected; for Category C, the end of a neighboring lane is used. An outlook is given of how an analysis with combined driving scenarios of Category A, B, and C can be carried out on the example of HW–A06 (Category A), HW–B07 (Category B), and HW–C04 (Category C). This is followed by a detailed presentation and discussion of the applicability to rural roads. This is discussed on the example of an oncoming vehicle turning left at an intersection (RR–A06, Category A). Finally, the merits and limitations of the proposed method are discussed.

### 4.1 Application to a Category B Highway Scenario

In this section, a step by step hazard identification and analysis is carried out for an example scenario of Category B, the end of a speed limit (HW–B03), in order to illustrate the process of the proposed method. The highway scenario HW–B03 is selected to demonstrate the method on a very common call for action.

At the beginning, six empty hazard analysis tables are created for the UCA categories **a-d** described in Table 3.20. This is done using the templates Table 3.21, Table 3.25, Table 3.26, and Table 3.27 including an extra row for the causal factors analysis described in Section 3.3.3. Table 3.26 and Table 3.27 must both be created twice to evaluate instant and delayed actions separately, and to evaluate too soon stopped acceleration and too long applied braking separately.

The hazard analysis tables of the situation when the AV is passes the road sign indicating the end of a speed limit (HW–B03) are given in Table 4.1 - 4.5. The reason why there are only five tables instead of six is given in Section 4.1.6.

The first step of the analysis is to insert the expected behavior determined in Section 3.2.5 into the first row of each table. For evaluating combined scenarios of the ones presented, the expectations are not defined and have to be determined analogously to the expectations of uncombined scenarios in Section 3.3.1. The hazard identification and analysis is performed for every table individually.

### 4.1.1 HW–B03: Control Actions Not Provided

Table 4.1 shows the results for the analysis of not provided control actions. Hazardous situations only occur, if a control action that is not provided is actually expected. That means for HW–B03 that CA–1, CA–2, and CA–6 can be excluded from the analysis, additionally to CA–6 and CA–7 which are always excluded for a "not providing" analysis. The respective columns are blacked in Table 4.1. Only the remaining two control actions CA–3 and CA–4 must be evaluated. To analyze hazards due to a not provided control action, the analyst has to create a situation in which the challenger only expects one action: the control action which is not provided.

#### CA–3: Change Speed and Keep Lane

A challenger expects the ego-vehicle to change speed and remain in its lane, if the ego-vehicle speed is below the new maximum allowed driving speed and if there is no need for a take over maneuver as the ego-vehicle is not following a slow vehicle. A reason why the AV stays in its lane and does not change speed (CA–3) in the situation when passing the road sign canceling the speed limit can be that the AV is already driving at its maximum capable driving speed. Therefore, it maintains its speed and does not start a take over maneuver with a lane change to the left. The ego-vehicle does not have a leading vehicle, otherwise the challenger would not expect the ego-vehicle to accelerate in its lane. The ego-vehicle does not change lanes to the right, as this would mean that it has not already used the most right lane. The most right lane possible to drive on has to be taken according to the driving regulations. A short summary of why the AV would act in the certain manner should be inserted in the respective cell of Table 4.1.

The next step is to check whether the behavior violates one of the defined system safety constraints in Table 3.3. The challenger expects the AV only to change speed and not to change lanes. This implies that the challenger can take over on the left-hand side or accepts that there is no chance for the AV to merge to the right, otherwise it would expect a lane change. Not accelerating when passing the end of a speed limit road sign, but it is still not uncommon when humans steer a vehicle. The challenger therefore can react appropriately by taking over or by waiting until the AV leaves the lane and merges to the right. Not providing CA–3 therefore does not violate any system SC and the CA is classified to be not hazardous. The respective "Classification" cell is colored green according to Table 3.22 and a short summary of the reason for classification is written in the respective "Reason for classification" cell.

#### CA–4: Change Speed and Change Lane

The challenger expects the ego-vehicle to instantly change speed and change lanes, but the ego-vehicle does not perform this action (CA–4). The cause of not providing this action could be that the AV already reached its maximum driving speed it is capable of in the automated mode and cannot merge to the right as the vehicles on the right start accelerating. The accelerating neighboring vehicles do not leave a gap large enough for the AV to merge into.

This action might provoke challengers to take over from the right as the left lane is blocked by the ego-vehicle. The safety constraint SC–4 is violated. The hazard classification cell is colored yellow indicating a hazardous situation due to the behavior of the automated vehicle. Additionally the cell is not further marked with any symbol that would indicate a likelihood of occurring in human driving. Humans can adapt quicker to changing driving situations and would consider slowing down to be able to merge back to the right lane or could merge into the neighboring lane using the small gap between vehicles, if they do not feel comfortable with accelerating.



The driving behavior of the AV can cause life-threatening or fatal injuries (**S3**) when other vehicles do not expect the challengers to pass on the right-hand side of the AV at high velocities. Life-threatening injuries (**S3**), a high exposure (**E3** or **E4**), combined with no controllability (**C3**) leads to a ASIL rating of **C** or **D**. As the highest possible level is decisive, level **D** is inserted into the respective cell. The exposure and controllability classes result from the classifications defined in Subsection 3.2.4.

The danger of not providing CA–4 although it is expected is summarized in the row UCA. In this specific case it is unsafe not to merge into the right lane when the speed limit is canceled and the AV on the left lane cannot further accelerate. The UCA leads to a newly defined safety constraint, which is that the AV requires a high relative velocity compared to the leading vehicle in order to quickly merge back into the right lane.

Finally, the cause for the hazard is identified. The possible cause in this scenario could be that the AV is restricted to a maximum velocity which is lower than the one from human-driven vehicles.

#### 4.1.2 HW–B03: Control Actions Provided

In the next step, the control actions are analyzed which are provided, but not expected. Table 4.2 shows the result of this analysis. Reverse to the analysis of not provided control actions, the actions CA–3 and CA–4 are not analyzed as they are expected by the challenger.

##### CA–1: Keep Speed and Keep Lane

Providing CA–1, keep speed and keep lane, is identically to not providing CA–3, where other road users expect a change in velocity, but the AV does not provide this action. The AV already reached its maximum capable driving speed and does not intend to accelerate further. The control action is classified as not hazardous, due to the same reasons, as described in paragraph CA–3: Change Speed and Keep Lane, in Table 4.1.

##### CA–2: Keep Speed and Change Lane

With the cancellation of a speed limit, no acceleration is obligatory. If the AV already reached its maximum capable driving speed it would maintain that speed and not accelerate. Keeping the current speed and performing a lane change can be considered to be a malfunction of the system. The AV should always drive on the rightest possible lane. If it initiates a lane change to the right-hand side due to a canceled speed limit, it would mean that it had not used the most right lane before. The change lane action cannot be a change to the left-hand side as the only reason to do so is a slow leading vehicle. The analyzed driving scenario does not include a slow leading vehicle and a performed lane change to the left would therefore be caused by a malfunction of the system. This violates system safety constraint SC–6; the AV does not always work properly. These derivations of the classification are inserted into the respective cells and the hazard classification cell is colored red, symbolizing a malfunction of the system. The analysis of the provided CA–2 ends here because the focus of the analysis is on Class 2 hazards.

Table 4. 1 : Hazard analysis table for not provided control actions at the driving scenario HW-B03.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification							
Reason for AV action			AV already reached maximum capable driving speed in automated mode.	AV wants to finish an overtaking maneuver with merging back into the right lane, but does not detect a gap between vehicles that is big enough as they started accelerating and AV already reached maximum capable driving speed in automated mode.			
Violated system SC			-	SC-4			
Reason for classification			Also human drivers do not always accelerate when a certain speed limit is canceled; challengers are aware of that behavior and pass on the left-hand side or wait until vehicle merges to the right.	Might provoke people to take over from the right which can create a hazard for the overtaking vehicle itself and other road users due to high speed and sudden actions.			
Severity				S-3			
ASIL				D			
UCA				Not merging into the right lane when speed limit is canceled and vehicle is unable to accelerate.			
Refined SC				AV must have a high relative velocity to the leading vehicle when taking over so that it can merge back in quickly.			
Causal factors				AV is restricted to a maximum velocity that is lower than the one from human-driven vehicles.			

## CA–5: Abort Lane Change

For the abort lane change control action, no reason can be found that would justify this action. A cancellation of a speed limit does not require to abort an already started lane change maneuver. The system can complete the lane change and decide on the next action after accomplishing the change. The next action could triggered by a slow leading vehicle that does not accelerate up to the new allowed speed. The AV would then initiate a new lane change maneuver. The next action is independent from the end of the speed limit and only depends other driving situations.

If an AV does abort a lane change nonetheless, it must be due to a malfunction of the system. SC–6 is violated and the hazard classification cell is colored red.

## CA–6: Emergency Braking and CA–7: Emergency Stop

The end of a speed limit does not require an emergency brake (CA–6) or emergency stop (CA–7). If one of these actions is performed nonetheless, there must be a malfunction in the driving system, similar to CA–5. SC–6 is violated and the respective hazard classification is colored red due to the malfunction of the system.

### 4.1.3 HW–B03: Control Actions Provided Instantly

For the evaluation of hazardous situations due to instantly provided control actions, only the ones where instant actions are not expected have to be evaluated. CA–3 and CA–4 are expected to be executed instantly, which is exactly what the AV does. Both, actions and expectations are congruent and no analysis is required. CA–1, CA–2, CA–5, CA–6 and CA–7 are control actions that are not expected and therefore instant action can be hazardous by definition. As these control actions are already analyzed in the table for providing control actions (Table 4.2), they do not be analyzed again. The respective table (Table 4.3) is blacked entirely.

### 4.1.4 HW–B03: Control Actions Provided Delayed

The analysis of delayed provided actions focuses on the actions that are expected to be executed instantly, but executed delayed. These are CA–3 and CA–4. The corresponding table for the analysis is Table 4.4.

## CA–3: Change Speed and Keep Lane

The AV changes its speed later than a human might do. Humans start accelerating as soon as they detect the road sign of a canceled speed limit even before passing it. An AV does not start accelerating as soon as it detects the road sign, but as soon as it passes the sign. This violates the safety constraint, that the AV must maintain the safety distance as the following traffic might enter this distance through accelerating in advance.

Nevertheless, the action is classified as not hazardous. The following vehicle (challenger) might enter the safety distance, but also leaves it quickly again by either starting a take over maneuver or by releasing the accelerator pedal until the AV started to accelerate too. No active braking is necessary. The respective cell is colored green and the analysis can be stopped at this point.

Table 4.2: Hazard analysis table for provided control actions at the driving scenario HW-B03.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification							
Reason for AV action	AV already reached maximum capable driving speed in automated mode	Malfunctioning system			Malfunctioning system	Malfunctioning system	Malfunctioning system
Violated system SC	-	SC-6			SC-6	SC-6	SC-6
Reason for classification	Also human driver do not always accelerate when a certain speed limit is canceled; challengers are aware of that behavior and pass on the left-hand side or wait until vehicle merges to the right.	If right lane were empty, AV would have taken it even before passing the road sign. A lane change to the left without accelerating is also a malfunction as there is no need to do so (no slow vehicle ahead).			Canceled speed limit does not require to abort a lane change, if the AV does, it is because of a malfunction of the system.	Canceled speed limit does not require emergency braking, if the AV does, it is because of a malfunction of the system.	Canceled speed limit does not require an emergency stop, if the AV does, it is because of a malfunction of the system.
Severity							
ASIL							
UCA							
Refined SC							
Causal factors							

Table 4.3: Hazard analysis table for instantly provided control actions at the driving scenario HW-B03.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification							
Reason for AV action							
Violated system SC							
Reason for classification							
Severity							
ASIL							
UCA							
Refined SC							
Causal factors							

### CA-4: Change Speed and Change Lane

In the first step, the reason why an AV could change its speed and lane delayed has to be identified. The AV could be following a vehicle at a certain speed while passing the road sign of canceled speed limit. The leading vehicle does not accelerate after having passed the road sign and the AV starts a take over maneuver as the leading vehicle turned into a slow leading vehicle. The action is performed delayed because the AV requires time to notice that the leading vehicle will not accelerate at all. This action could violate SC-3: The AV blocks oncoming traffic, when following traffic was about to take over the AV when the AV suddenly starts to leave its lane.

The following vehicle (challenger) could start a take over maneuver as soon as it detects the road sign, which is sooner than the performed actions by AV. The challenger realizes therefore sooner that its leading vehicles does not accelerate. While changing to the left lane, the AV also starts to change its lane without expecting the challenger to be accelerating. The challenger must switch immediately from accelerating to actively braking in order to avoid a collision. The delayed provided CA-4 is therefore classified as hazardous (yellow). The identified hazard does not occur in human driving as humans either accelerate sooner or are more aware of possible driving action of the following vehicles. This likelihood of occurring does not have to be marked in the table, according to Table 3.23.

An accident that could result from this control action would have life-threatening or fatal injuries (**S3**). The ASIL is concluded to be at level **C** or **D**, as the exposure is **E3 / E4** and the controllability is **C3** (defined in Section 3.2.4). The highest rating is inserted into the table (**D**).

In the next step, the unsafe control action is defined. It is unsafe that the vehicle starts a take over maneuver combined with an acceleration right behind the end of a speed limit road sign when its following vehicle just started the same maneuver. The refined safety constraint can be derived from the UCA. An AV should avoid a take over maneuver after passing a road sign if its following vehicle already started to change its lane to the left-hand side and to accelerate. The cause for the AV behavior is that it only starts to accelerate after having passed the road sign due to the law.

Table 4.4: Hazard analysis table for delayed provided control actions at the driving scenario HW-B03.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification							
Reason for AV action			AV starts accelerating after passing the sign (humans would start accelerating in advance)	AV starts accelerating and initiating a take over maneuver delayed, after passing the road sign			
Violated system SC			SC-1	SC-3			
Reason for classification			The following vehicle might enter the safety distance to the AV but leaves it quickly by not further accelerating	Challenger wants to take over the AV and starts the maneuver as soon as he / she detects the road sign. If AV initiates a take over delayed, it might block the challenger who is forced to brake			
Severity				S3			
ASIL				D			
UCA				AV starts an overtaking maneuver right behind the end of speed limit road sign			
Refined SC				AV should only start an overtaking maneuver if the challenger did not just start to take over AV			
Causal factors				AV always follows the law			

### 4.1.5 HW–B03: Too Soon Stopped Acceleration

Table 4.5 shows the results of the analysis of a too soon stopped acceleration. Only CA–3 and CA–4 need to be evaluated, as the other control actions do not include a change in velocity at all and therefore an acceleration cannot be stopped too soon.

#### CA–3: Change Speed and Keep Lane

Humans usually drive at higher speed than the one defined by speed limit sign. The same expectations have most people about the driving speed of other road users. When a speed limit is canceled, humans also accelerate to higher speeds than the recommended speed of 130 km/h on highways if no speed limit exists at all or to higher speeds than the speed defined by the new speed limit sign.

The violated system safety constraint is SC–3. The AV blocks following traffic by stopping to accelerate at the exact newly given speed. Although this safety constraint is violated, the control action is not classified to be hazardous and the respective cell is colored green. The challenger can react instantly to the stopped acceleration of the ego-vehicle by releasing the accelerator pedal without having to brake actively and no injuries have to be expected.

#### CA–4: Change Speed and Change Lane

The AV can initiate a lane change maneuver as it intends to take over a vehicle which did not accelerate after passing the road sign. During the lane change, the AV starts accelerating exactly up to the new given speed limit or to the maximum capable driving speed. Following traffic on the new lane might expect that the ego-vehicle to continue accelerating even above the limit and itself does not stop accelerating. The AV therefore blocks following traffic (SC–3).

Although a safety constraint that is violated is identified, the control action is not hazardous, because challengers can instantly react when they detect that the ego-vehicle stopped accelerating. The challenger does not have to brake actively and only has to release the accelerator pedal until the safety distance is adhered again.

### 4.1.6 HW–B03: Too Long Applied Braking

For the analysis of hazardous situations due to too long applied braking, only control actions that include a braking maneuver have to be evaluated. The remaining two control actions are CA–3 and CA–4. In the chosen highway scenario of passing the road sign that cancels a speed limit, only control actions for an acceleration are expected, no control action for a braking maneuver. If no braking is expected at all, no too long braking can be executed. That the AV brakes at all is excluded in the assumption of Class 2 risks that the AV always performs correct actions. Malfunctions are evaluated in a separate analysis for Class 1 hazards. The resulting table is identically to Table 4.3.

### 4.1.7 HW–B03: Discussion of Identified Hazards

The previous sections prove that the proposed method in Chapter 3 can be successfully applied to the specific driving scenario of a canceled speed limit. Two hazardous situations are identified, one results from not providing a change of speed and lane, the other one from providing a change of speed and lane delayed. For the hazard due to a delayed lane change and acceleration,

Table 4.5: Hazard analysis table for too soon stopped acceleration at the driving scenario HW-B03.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification							
Reason for AV action			AV accelerates exactly up to the given speed limit (humans would accelerate above that limit)	AV intends to take over with adapting the speed to the new speed limit, AV accelerates exactly up to the given speed limit (humans would accelerate above that limit)			
Violated system SC			SC-3	SC-3			
Reason for classification			The challenger can react instantly when acceleration stopped with releasing the accelerator pedal, no active braking required	The challenger can react instantly when acceleration stopped with releasing the accelerator pedal, no active braking required			
Severity							
ASIL							
UCA							
Refined SC							
Causal factors							



it is arguable whether current systems can already handle cases where the following traffic simultaneously changes the lane. Nevertheless, all these types of hazards for which it is unclear whether the current design of AD systems covers them, should be recorded in the hazard analysis and validated with specialists later on. This example scenario also proves the importance of including the time factor (delayed or instantly) of expectations and executed actions into the analysis, as one hazard could only be detected through this classification.

The second identified hazard, might turn out to become a serious problem of AVs when they get stuck on the left lane and do not find a gap on their neighboring right lane which is large enough to merge into. This hazard has to be investigated further and checked if it is reasonable to intentionally slow down the AV when a take over maneuver failed. The identified hazard also justifies the importance of analyzing not provided actions. For many control action analyzes, not providing one CA is not hazardous by itself, but depends on the actually executed control action. In this example, not providing a change in speed and of lane although it is expected makes the analyst think of a concrete scenario where the expectations could be valid and hazardous, independently from what the AV actually does. A schematic representation of both identified hazardous situation can be seen in Figure 4.1(a) and 4.1(b).

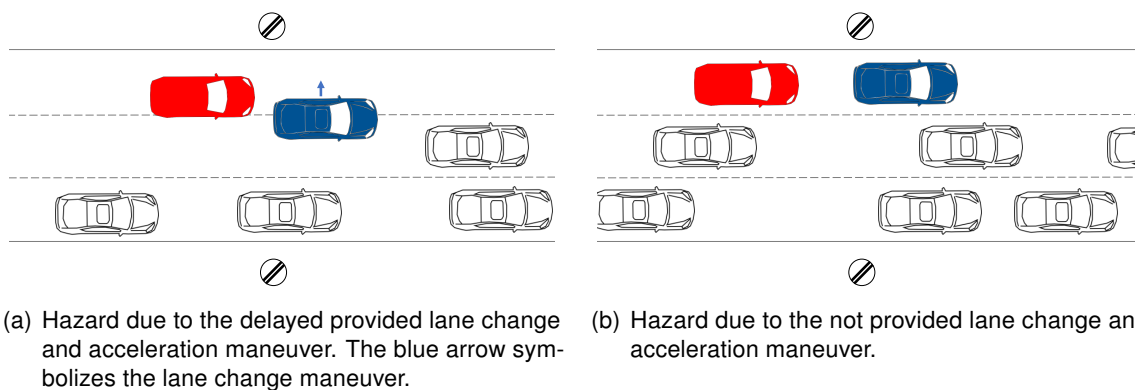


Figure 4.1: Visualization of the detected hazards in the driving scenario HW-B03. The AV is colored blue; the challenger red.

Additionally, four Class 1 hazards are identified. They should be used to cross-validate the selected Class 1 hazard identification method. A top-down approach can be started with the identified hazards.

The example scenario HW-B03 also shows that the effort for one scenario analysis is tolerable as many control action–guide-word combinations do not have to be analyzed and can be ignored from the beginning. In this example only eleven control action combinations have to be explicitly analyzed, the others are excluded systematically.

## 4.2 Applicability to Category A and C Highway Scenarios

With the previously analyzed driving scenario HW-B03, an analysis for a highway driving scenario of Category B, direct call for action, is conducted. In this section, a hazard analysis is carried out for the two other categories to prove the applicability of the method to all categories of driving scenarios.

For Category A, a positive cut in (HW–A01) is chosen; for Category C, the end of a neighboring lane (HW–C06) is analyzed. The corresponding tables can be found in the the appendix (Chapters A and B).

### 4.2.1 Category A: Cut in with positive relative velocity

A vehicle cutting in with a positive relative velocity (HW–A01) leads to four identified hazards. Three of them result from the AV providing a braking maneuver which is not expected by its following vehicle; the other one results from providing a lane change maneuver at constant speed which surprises an oncoming vehicle in the new lane with higher velocities. All these hazards only occur, because the vehicle cutting in enters the AV's safety distance and the AV reacts to it by braking.

The hazards can be prevented with an AD system implementation which includes the relative velocities of other vehicles into the maneuver calculations. The two hazardous situation are visualized in Figure 4.2.

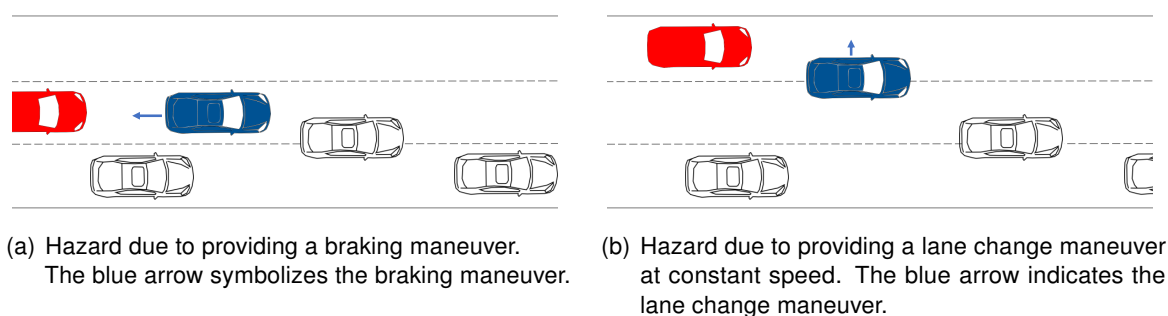


Figure 4.2: Visualization of the detected hazards in the driving scenario HW–A01. The AV is colored blue; the challenger red.

### 4.2.2 Category C: End of Neighboring Lane

The analysis of the end of a neighboring lane (HW–C06) reveals three hazardous classified control actions from which two lead to the same hazardous situation. The identical hazards occur because the AV does not perceive the end of the neighboring lane in advance and therefore does not provide a change of speed, but maintains its speed and lane. A vehicle from the ending lane intends to merge into the AV's lane and expects the AV to slow down or change lanes. This action can happen at high velocities and could result in a fatal accident. The hazardous situation is caused by an AD system that does not follow the happenings of the road infrastructure in its neighboring lanes.

The other hazardous situation occurs, if the neighboring lane ends and the AV brakes too long to let a vehicle merge into its lane. It creates a gap that is larger than necessary and its following vehicle does not expect this strong braking maneuver. This hazard is similar to the hazard identified in Section 4.2.1 for a vehicle cutting in, except that in this situation the AV creates the safety distance intentionally in advance and not as a reaction of a violated safety distance. The cause is identically though: the AV maintains safety distances at all times. The three hazardous situations are visualized in Figure 4.3; the two identical situations are represented in Figure 4.3(a), the other one is represented in Figure 4.3(b).

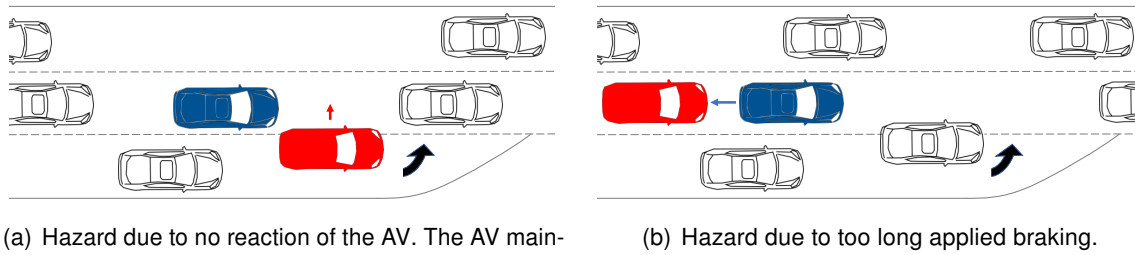


Figure 4.3: Visualization of the detected hazards in the driving scenario HW-C06. The AV is colored blue; the challenger red.

### 4.3 Applicability to a Combined Driving Scenario

The proposed method is also applicable to a combined driving scenario. This is shown using driving scenarios of all three categories: Category A, B, and C. For Category A, HW-A06 is selected. The slow leading vehicle is a very common scenario on highways. The road sign indicating the end of a no overtaking area (HW-B07) is analyzed for Category B, and confusing lane markings (HW-C04) are analyzed for Category C. The probability of occurrence for a combination of these three scenarios is very low. Not only are the scenarios of Categories B and C unlikely according to Table 3.8 and 3.9, but also a combination of three situations that are likely to occur by themselves, unlikely occur all together.

At the beginning of this hazard analysis, the expectations must be determined, as they are not determined for combined scenarios in Section 3.2.5. The only expected action is an instant lane change while accelerating for the situation where the no overtaking area ends and a slow vehicle is ahead of the ego-vehicle is. The confusing lane markings do not change the expectations as humans can also follow lanes without having precise lane markings.

With these defined expectations, one hazard can be identified for the described combined driving scenario. The corresponding hazard analysis tables can be found in the appendix in Chapter C. The identified hazard results from a too soon stopped acceleration, when the AV changes lanes and accelerates in order to take over the slow leading vehicle. As soon as the no passing sign occurs, the AV changes lanes to take over the slow leading vehicle and starts accelerating. The AV stops accelerating when it approaches the new lane due to confusing lane markings, which the AV cannot allocate correctly. Following vehicles that also intend to take over the slow vehicle do not expect the ego-vehicle to stop accelerating and must brake in order not to run into the AV. Only releasing the accelerator pedal is not sufficient as the stop of acceleration suddenly happens during the acceleration maneuver. The hazardous situation does not occur with human drivers as they can handle confusing lane markings and would continue accelerating. The hazardous situation is visualized in Figure 4.4. The situation can be prevented by an AD system that has enough foresight to interpolate missing lane markings and is able to differentiate between correct and false lane markings.

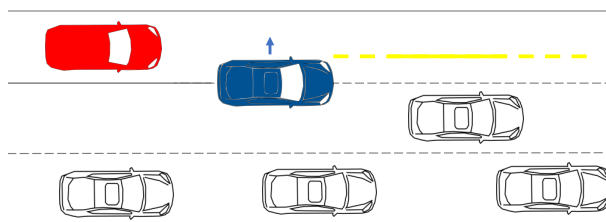


Figure 4.4: Visualization of the detected hazards in the combined driving scenario of HW-A06, HW-B07, and HW-C04. The AV is colored blue; the challenger red.

## 4.4 Applicability to a Rural Road Scenario

Besides the applicability for highway, the suggested method can also be used for the analysis of rural road driving scenarios. This section proves the applicability of the analysis for the rural road driving scenario RR-A06 from Category A (changes within the field of view). It is a very common driving situation that oncoming vehicle makes a left turn and thereby crosses the lane of the AV (RR-A06). The change lane control actions are, for this case, interpreted as turning of the AV at the intersection, as described in Section 3.2.3.

The structure of the analysis is identical to the one described in Section 4.1 and the corresponding tables can be seen in Table 4.6 - 4.10. Human expectations are defined according to Table 3.17 of Chapter 3.

### 4.4.1 RR-A06: Control Actions Not Provided

Only the expected actions have to be evaluated for the analysis of not provided but expected control actions, which are CA-1, CA-3, and CA-4. All three control actions are expected to be executed instantly.

#### CA-1: Keep Speed and Keep Lane

Not maintaining the current driving speed and lane (CA-1) does not necessarily result in a hazardous situation as the challenger cannot exclusively expect a vehicle to maintain its speed and to pass the intersection. Every vehicle can either cross an intersection or turn at an intersection. The AV could intend to turn at the intersection or to brake in order to let the vehicle complete its turn. These performed actions need to be analyzed in order to detect hazards. Not to provide the control action CA-1 does not directly lead to a hazardous situation. It might indirectly result in hazardous situations though through providing different actions. The corresponding classification cell is colored green.

#### CA-3: Change Speed and Keep Lane

The identically reasoning of not providing CA-1 applies to not providing CA-3. A hazardous situation does not directly result from the AV not changing its speed and keeping lane (CA-3). Depending on the provided actions a hazard might occur and the corresponding classification cell is colored green.

## CA–4: Change Speed and Change Lane

The lane change action combined with a change of speed can be interpreted as the AV slowing down and makes a turn. A reason why the AV would not perform this action at an intersection is that it does not intend to do so and continues traveling on the same road. Nobody must make turns at intersections if they do not want to. Not providing this action is therefore not hazardous and colored green in the corresponding cell of Table 4.6.

### 4.4.2 RR–A06: Control Actions Provided

Provided control actions are only hazardous if they are not expected. CA–1, CA–3, and CA–4 are expected and therefore must not be analyzed in Table 4.7.

## CA–2: Keep Speed and Change Lane

Keep speed and change lane is unexpected as it is physically impossible. Driving on a rural road is usually performed on high speeds between 50 km/h to 100 km/h provided that no traffic jam or slow moving traffic exists as they are excluded in this driving scenario. Turning at an intersection without braking is highly dangerous and should not be implemented in AD systems. Providing this control action is only possible if there is a malfunction in the AD system. SC–6 is violated and the hazard classification cell is colored red.

## CA–5: Abort Lane Change

If the AV intends to make a turn at the upcoming intersection, it should be able to do so independently from oncoming vehicles that also intend to make a turn. Aborting a turning maneuver (CA–5) due to a turn of an oncoming vehicle can only occur due to a malfunction in the AD system. SC–6, AV must always work properly, is violated and the hazard classification cell for CA–5 is colored red.

## CA–6: Emergency Braking

The reason why an AV would perform an emergency brake when an oncoming vehicle makes a turn, could be that the AD system detects the turning vehicles as a large object within its safety distance. The AV intends to avoid hitting the object by performing an emergency stop as this is the only possible action a vehicle can perform on an one lane road to avoid hitting objects. After the vehicle finished its turn, the AV notices that it is not necessary to stop and starts accelerating before making an entire stop. The intended emergency stop turns into an emergency brake. Human drivers would react differently in this situation. They can perceive the situation better, realize that the vehicle immediately leaves the driving area, and would not perform an emergency brake. They might brake softly to let the vehicle pass safely, but would not perform an emergency brake.

The challenger following the AV does not expect an emergency brake. Due to the unexpected emergency brake the challenger enters the safety distance of the AV. This leads to a violation of SC–1. A resulting accident could be life-threatening or fatal for all passengers of both vehicles (**S3**). Combined with the high exposure of the driving situation (**E3/E4**) and the uncontrollability of AVs (C3), the ASIL is rated **D**. The hazard classification cell is colored yellow and not further marked as this situation almost never happens in human driving.

Table 4.6: Hazard analysis table for not provided control actions at the driving scenario RR-A06.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification	High	Medium	High	High	Medium	Medium	Medium
Reason for AV action	AV intends other actions, e.g. turning at intersection	██████████	AV intends other actions, e.g. turning at intersection	AV does not intend to make a turn	██████████	██████████	██████████
Violated system SC	-	██████████	-	-	██████████	██████████	██████████
Reason for classification	not keeping speed and keeping lane does not directly cause any hazards	██████████	not changing speed and keeping lane does not directly cause any hazards	Normal action	██████████	██████████	██████████
Severity	High	High	High	High	High	High	High
ASIL	High	High	High	High	High	High	High
UCA	High	High	High	High	High	High	High
Refined SC	High	High	High	High	High	High	High
Causal factors	██████████	██████████	██████████	██████████	██████████	██████████	██████████

The UCA can be summarized into an AV performing an emergency brake when an oncoming vehicle makes a left turn and the refined safety constraint into an AV that must not perform an emergency brake for a left turning vehicle at an intersection that would leave the lane before the AV passes the intersection.

The general cause of that hazard is that the AV does not detect the driving intentions of oncoming traffic. If an AD system can include driving directions and intentions of oncoming traffic, it would not perform an emergency brake.

### **CA–7: Emergency Stop**

The reason for an emergency stop of an AV are identical to the ones for an emergency stop. The only difference is that the emergency stop is executed completely. This does not change the violated safety constraint (SC–1), the hazard classification, level of severity and resulting ASIL.

The UCA is that the AV performs an emergency stop when an oncoming vehicle makes a left turn. Similar to the refined SC for the emergency brake, the refined SC for providing an emergency stop is that the AV must not perform an emergency stop for oncoming vehicles that make a left turn and leave the intersection before the AV enters it.

The cause for the AV's driving behavior is identical to the one for an emergency stop: AV does not detect the driving directions and intentions of oncoming traffic.

#### **4.4.3 RR–A06: Control Actions Provided Instantly**

All delayed actions have to be evaluated in the analysis of hazardous situations due to instantly provided actions. The expectations of other road users for the turning maneuver of an oncoming vehicle does not include any delayed actions and therefore no control action needs to be analyzed. All cells are blacked, as it can be seen in Table 4.8.

#### **4.4.4 RR–A06: Control Actions Provided Delayed**

Delayed actions are only hazardous if they are expected instantly. CA–1, CA–3, and CA–4 are expected instantly, but only CA–3 and CA–4 have to be evaluated as keeping ones lane and speed cannot be delayed. Table 4.9 shows the results of the analysis.

### **CA–3: Change Speed and Keep Lane**

When performing the control action CA–3, the AV intends to cross the intersection and slows down to allow the turning vehicle to finish the crossing of the intersection safely. It only starts to slow down when the turning vehicle already is within the AV's safety distance. Human drivers would brake sooner in order to signal the driver in the turning vehicle to cross the intersection.

The delayed braking performed by the AV might startle the human driver of the turning vehicle who feels pushed to quickly finish crossing the intersection. This might not be a pleasant situation for the human driver in the turning vehicle, but finishing a crossing of an intersection quickly does not create any hazards. The vehicle instantly leaves the safety distance of the AV and no accident can occur. Executing CA–3 when an oncoming vehicle is turning to its left is therefore no unsafe control action.

Table 4.7: Hazard analysis table for provided control actions at the driving scenario RR-A06.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification	I	I	I	I	I	I	I
Reason for AV action	[REDACTED]	Malfunctioning system	[REDACTED]	[REDACTED]	Malfunctioning system	Vehicle enters safety distance	Vehicle enters safety distance
Violated system SC	[REDACTED]	SC-6	[REDACTED]	[REDACTED]	SC-6	SC-1	SC-1
Reason for classification	[REDACTED]	No turning maneuver without braking possible	[REDACTED]	[REDACTED]	[REDACTED]	Following vehicle cannot react to an emergency braking and runs into AV	Following vehicle cannot react to an emergency stop and runs into AV
Severity	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	S3	S3
ASIL	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	D	D
UCA	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	AV performs an emergency brake when an oncoming vehicle makes a left turn	AV performs an emergency stop when an oncoming vehicle makes a left turn
Refined SC	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	AV must not perform an emergency brake for turning vehicles that will leave the lane before the AV passes the intersection	AV must not perform an emergency stop for turning vehicles that will leave the lane before the AV passes the intersection
Causal factors	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	AV does not detect the driving intentions of oncoming traffic	AV does not detect the driving intentions of oncoming traffic



Table 4.8: Hazard analysis table for instantly provided control actions at the driving scenario RR–A06.

Legend	CA–1	CA–2	CA–3	CA–4	CA–5	CA–6	CA–7
Classification	■	■	■	■	■	■	■
Reason for AV action	■	■	■	■	■	■	■
Violated system SC	■	■	■	■	■	■	■
Reason for classification	■	■	■	■	■	■	■
Severity	■	■	■	■	■	■	■
ASIL	■	■	■	■	■	■	■
UCA	■	■	■	■	■	■	■
Refined SC	■	■	■	■	■	■	■
Causal factors	■	■	■	■	■	■	■

### CA–4: Change Speed and Change Lane

Changing speed and changing lane (CA–4) is the appropriate control action when an AV intends to make a turn. A delayed execution implies an intensive braking to be able to reduce the speed fast enough before entering the intersection. Intensive braking is not a driving style generated for AVs as they are usually implemented to drive defensively. If an AV performs this action anyways, it is due to a malfunction in the system. SC–6 is violated and the corresponding cell in Table 4.9 is colored red. This situation is hazardous and if the AD system does this action intentionally to copy a more aggressive behavior from humans, this situation could be classified to a Class 2 hazard.

The analyst can classify these indifferent scenarios directly to Class 2 although the aggressive driving style is currently not commonly implemented or they classify it as a Class 1 hazard. The Class 1 hazard must be added to the Class 1 hazard list of identified hazards which uses a specific Class 1 hazard identification method.

#### 4.4.5 RR–A06: Too Soon Stopped Acceleration

A too soon stop of acceleration can only exist, if a human driver expects the AV to accelerate at all. In this driving scenario, the only expectations are to keep the speed or to slow down. Therefore, no control action has to be analyzed for the driving scenario of an oncoming vehicle making a turn. The corresponding table is identically to the one to Table 4.8.

#### 4.4.6 RR–A06: Too Long Applied Braking

Only control actions CA–3 and CA–4 have to be evaluated for the too long applied braking analysis. All other actions do not include braking at all or their intensity of braking is included in their definition and cannot be applied longer (CA–6 and CA–7). Table 4.10 shows the results of this analysis.

### CA–3: Change Speed and Keep Lane

Applying too long braking within CA–3 can be described with the following scenario. The AV brakes due to an object within its safety distance, which is the oncoming vehicle making a turn.

Table 4.9: Hazard analysis table for delayed control actions at the driving scenario RR-A06.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification	I		I	I			
Reason for AV action			Large moving object within lane and AV slows down	Malfunctioning system			
Violated system SC			SC-5	SC-6			
Reason for classification			AV might startle the turning vehicle with braking delayed; as the vehicle is already crossing the intersection it will not stop crossing and leave the lane, no hazard results	AV knows in advance if it wants to take a turn and where the intersection starts; Avs are designed to brake smoothly when making a turn			
Severity							
ASIL							
UCA							
Refined SC							
Causal factors							

To avoid hitting the object the AV starts to brake. Even when the turning vehicle already left the intersection, the AV continues braking.

A properly working AD system would not continue braking, but start accelerating again when no object is in the AV's lane anymore. Performing this action represents therefore a malfunction. SC-6 is violated and the corresponding hazard classification cell is colored red.

### CA-4: Change Speed and Change Lane

The AV can stop entirely at an intersection when it intends to make a turn. This action is represented in applying CA-4 too long. A human driver might understand sooner that the oncoming vehicle intends to make a turn and therefore it is also for the ego-vehicle possible to make its turn to the left instantly without stopping entirely.

This behavior might be unexpected for the vehicle following the AV, but as it can never be sure that its driver sees everything happening in the intersection, the driver in this vehicle (challenger) is always ready to brake. No hazardous situation occurs and the respective cell in Table 4.9 is colored green.

#### 4.4.7 RR-A06: Discussion of Identified Hazards

The analysis of the situation of an oncoming vehicle turning left reveals two similar hazards that result from different driving behavior of the AV and human driving behavior. In both scenarios, the cause of the hazard is that the intentions and actions of other road users cannot be foreseen.

If there is no technical method available to predict the driving intentions of other road users, no AD system should be allowed on rural roads as the hazard is ASIL D rated. Figure 4.5 visualizes the detected hazardous situation which occurs due to an executed (emergency) braking.

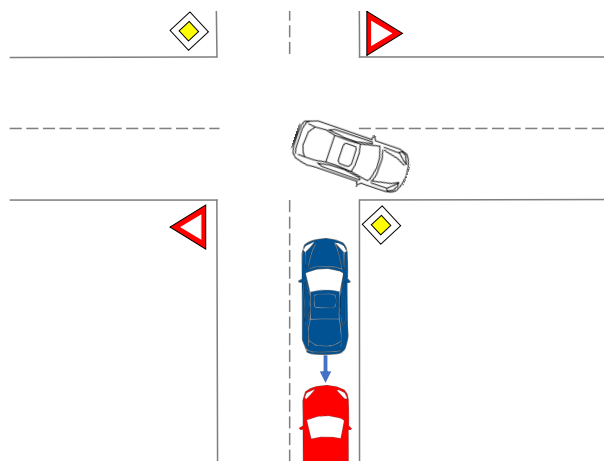


Figure 4.5: Visualization of the detected hazards in the driving scenario RR-A06. The AV is colored blue; the challenger red. The blue arrow indicates the braking maneuver.

Table 4.10: Hazard analysis table for too long applied braking at the driving scenario RR-A06.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification							
Reason for AV action			Starts to brake to avoid hitting the turning vehicle; AV does not stop braking after the vehicle left the intersection	AV stops entirely although no oncoming traffic blocks its maneuver as the vehicle intends to turn			
Violated system SC			SC-3	-			
Reason for classification			Malfunction of system not to detect that no vehicle is within lane anymore	Stopping at an intersection to wait until the oncoming traffic does not only show its intention, but also performs it; is a maneuver to provide safety; stopping entirely is a common maneuver in human driving			
Severity							
ASIL							
UCA							
Refined SC							
Causal factors							

## 4.5 Discussion

The hazard analyses and risk assessments carried out in this chapter prove that the suggested method is a helpful tool for systematic identification of Class 2 risks, but it also has its limitations. The suggested method divides the driving scenarios into three categories that potentially provoke the AV to change its current behavior. This allows a systematic analysis process without having to know predefined accident scenarios for AVs. An analysis can be performed for individual driving scenarios, as well as for combined scenarios. In the previous sections it can be seen that an analysis of individual and combined scenarios already reveal many hazardous situations, which are not easily detected through brainstorming. The method is equally applicable to highway driving scenarios as to rural road driving scenarios by changing the meaning of the control action "change lane" from a take over maneuver into a turning action at intersections. Similar modifications can be made for expanding the method to other road types. With the analyses of the example scenarios in previous sections, it can already be seen how some hazards might arise with AVs in simple driving situations due to the different driving behavior of AVs to humans. This reveals the importance of working on the identification of Class 2 risks.

Despite these merits, the method has some limitations. A successful application of this method requires an analyst who knows the current state of the art of AD systems. This allows them to identify reasons why an AV could perform certain control actions in certain situations. This knowledge is also required to be able to differentiate between Class 1 and Class 2 risks. As this might not always be easy to do, it is important to check whether the identified hazards which arise due to malfunctions (Class 1) are covered within the separately carried out Class 1 hazard analysis. Along with this knowledge, the hazard analyst should be willing to identify hazards. It is less effort to simply classify situations as not hazardous than to think about possible vehicle constellations that could lead to a hazard.

Even if there is an analyst who has the required knowledge and the willingness to identify hazards, it is not easy to identify all possible hazards. For both road types that are analyzed in this work, more than 40 driving scenarios were identified and depending on the level of refinement, many more could be identified. All of them have to be analyzed and combined with each other to achieve the best possible results for a catalog of Class 2 risks. This is a huge amount of work, therefore the analysis process should begin with the most common and most severe situations. The resulting hazard catalog based on the more than 40 driving scenarios mostly considers driving scenarios which focus on correct human behavior. Nonetheless, incorrect human behavior can be represented in a new category and can similarly be analyzed.

It is also difficult for the analyst to differentiate between hazards that also occur in human driving and the ones that are actually new automation hazards. If a human creates a hazard once in a lifetime and an AV creates it frequently, it is per definition no automation hazard, but should be seen as one. The intention in this work is to identify all possible hazards and rate them on the likelihood of occurrence in human driving. Reductions of hazards can be done with this rating in following steps.

Even if all possible hazards on German roads would be identified with the proposed method, an AD system that avoids all of them would only be suited for German roads. The defined driving scenarios and expected actions in this work were determined for German roads and driving culture in Germany. An AD system that is only implemented based on German driving behavior might not reduce hazards in other countries or might even provoke more hazards as other countries have different road infrastructures and expectations on the driving behavior.

Separate analyses have to be carried out that start with the identification of the driving behavior and expectations in every country and / or culture.

All these limitations have to be considered when performing the hazard analysis and assessment for Class 2. Even if an analyst carries out the analysis who has the necessary knowledge about AVs and the willingness to identify hazards only analyzes a few driving scenarios, it already reveals many hazardous situations. The gained information is helpful for the development of AVs, even though not all possible hazards are identified. The proposed method is a helpful tool to guide an analyst in order to identify hazards systematically.

## 5 Summary and Outlook

This thesis investigates and develops a method to identify and analyze risks of automation that are caused by the different driving behaviors of an automated vehicle compared to human driving. Automated driving systems do not only create risks if the system is malfunctioning or the interaction between the automated system and the human driver fails, but also if the automated vehicle works correctly and other human road users do not expect that certain behavior. This is for example the case when AVs strictly follow all road laws or drive too defensively.

At the beginning of this work, the state of the art is outlined in order to explain current procedures and developments in safety determination for AVs. The hazard analysis and risk assessment are part of the safety determination within the concept phase of the product development described in the international standard ISO26262. Two of the herein suggested hazard analysis techniques are FMEA and HAZOP. Both are based on the causality model that a malfunction of a system causes a hazard. A newer method called STPA creates a causality model based on the assumption that accidents occur, when a system safety constraint is violated. The method is additionally able to model interactions, for example between system components. STPA is already used in many applications, among others in the hazard identification for automation risks of AVs which arise due to a malfunctioning system interaction.

Literature shows that the STPA can be used within the safety determination of ISO26262 and that analyses using STPA were successful for automation risks caused by a malfunctioning system. No research has been successful on identifying the risks of automation caused by the unexpected driving behavior of AVs because no method has been developed that includes driving scenarios at the beginning of the analysis.

The method for the identification of hazards due to this unexpected behavior is outlined in Chapter 3. It is based on the hazard identification and analysis technique STPA and is modified in order to model the interaction between an automated vehicle and a human-driven vehicle.

Two steps are added to the standard STPA. First, driving scenarios are identified that could cause an action of the AV. Three categories for driving scenarios are determined: a change in the field of view of the AV, a direct call for action for the AV, and a deviation from the standard road surface. Secondly, the driving behavior of human road users in those cases is determined using seven possible control actions. The identified behavior is used as the expected driving behavior that other road users will expect from the AV.

The expectations are used to identify the possible hazards that could occur if the AV behaves differently. Three groups for a classification are possible: not hazardous, hazardous, or malfunctioning. The identification of the hazardous control actions in specific scenarios is the actual objective of this work. A malfunctioning system might also be hazardous, but it is out of the scope of this work. Nonetheless, identified hazards due to system malfunctions should not be neglected, they should be cross-validated with the results of a specific hazard analysis for malfunctioning systems.

At the end of this work, the method is applied to five driving scenarios to demonstrate and prove its applicability. The derived method is exemplarily conducted for the highway driving scenario when the AV passes a road sign indicating the end of a certain speed limit. Already for this simple and common driving scenario two hazardous situations are identified that result from the AV's different driving behavior compared to humans'.

Other scenarios analyzed for different driving scenarios on highways and a rural road driving scenarios also reveal hazardous situations due to the differently expected driving behavior. The chosen examples often occur during the driving time and do not require rare traffic constellation, but also these scenarios can turn out to be hazardous for AVs if the AD systems are not designed to react appropriately.

The example analyzes prove that the method can be successfully used for all possible highway and rural road scenarios that it is a beneficial tool to guide the analyst through the hazard analysis process. The proposed method is additionally helpful to determine hazards in a structured and systematic manner.

With the derived method, the hazard that existed in the Apple accident in California [3, p. 2], described in Chapter 1, could have been identified because the expectations of the vehicle following are included. The Apple test vehicle could be modeled as the ego-vehicle taking a ramp. Its following vehicle expects the ego-vehicle to slip into a small gap in the oncoming traffic as human drivers would do. The ego-vehicle does not perform that action of a lane change as the distance between oncoming vehicles is not large enough to merge without entering the safety distances. The AV stops entirely and blocks traffic. The consequence is that an oncoming vehicle enters the AV's safety distance and rear-ends the ego-vehicle. An identification of more such risks of AVs can help to prevent accidents and to create safer systems.

Further work should be done in evaluating if a chronological combination of the determined driving scenarios is necessary. A human driver can foresee more situations and react accordingly, which an automated vehicle cannot. If the leading vehicle changes lanes because the road ends and the AV vehicle is suddenly confronted with a lane change, it could cause an accident because others made space for the vehicle to merge into. Human drivers would have foreseen the end of the blocked lane and might have acted differently.

Another research field to investigate is the determination of expectations. In this work, the expectations are derived for driving behavior on German roads. For systems that should be able to drive worldwide, different driving behavior exists and has to be analyzed and integrated into the hazard identification. The question needs to be discussed, if there can exist one implemented driving system for the entire world or if every driving culture requires different setups. Combining all setups is not expedient because the vehicles would be unable to drive at all in order to avoid all detected hazards.



# List of Figures

Figure 1.1:	Structure of this thesis. ....	2
Figure 2.1:	Levels of automation according to SAE J3016. ....	3
Figure 2.2:	Structure of the product life cycle in the ISO26262. ....	5
Figure 2.3:	Generic FMEA worksheet.....	9
Figure 2.4:	Control structure. ....	12
Figure 2.5:	Schematic representation of the causality model in STAMP. ....	13
Figure 2.6:	Causal factors within a control process. ....	14
Figure 2.7:	New, prevented, and same accident causes through automation compared to conventional driving. ....	15
Figure 2.8:	Classification of new accident causes at SAE level 3. ....	16
Figure 2.9:	Control structure diagram for automation risks of Class 1.....	18
Figure 3.1:	Flow chart diagram for the determination of the preliminaries leading to the STPA implementation. ....	22
Figure 3.2:	Control structure diagram for the identification of Class 2 automation risks. ....	25
Figure 3.3:	Flow chart diagram for the STPA implementation including the previously defined preliminaries. ....	46
Figure 3.4:	Flow chart diagram representing the process of the proposed hazard identification method.....	51
Figure 3.5:	Control structure diagram for automation risks of Class 3.....	53
Figure 4.1:	Visualization of the detected hazards in HW-B03. ....	65
Figure 4.2:	Visualization of the detected hazards in HW-A01. ....	66
Figure 4.3:	Visualization of the detected hazards in HW-C06. ....	67
Figure 4.4:	Visualization of the detected hazards in the combined driving scenario of HW-A06, HW-B07, and HW-C04. ....	68
Figure 4.5:	Visualization of the detected hazards in RR-A06.....	75



# List of Tables

Table 2.1:	Classes of exposure and their duration in operational situations. ....	7
Table 2.2:	Classes of controllability.....	7
Table 2.3:	Classes of severity. ....	7
Table 2.4:	Table for the ASIL determination. ....	8
Table 2.5:	Guide words for HAZOP: example set 1. ....	10
Table 2.6:	Guide words for HAZOP: example set 2. ....	10
Table 3.1:	Potential accidents through AVs. ....	23
Table 3.2:	Derived hazards and linked accidents. ....	24
Table 3.3:	Derived safety constraints and linked hazards. ....	24
Table 3.4:	Identified CAs for automation risks of Class 2. ....	26
Table 3.5:	Categories of scenarios that potentially provoke a vehicle for a change of its driving behavior. ....	27
Table 3.6:	ASIL determination with highlighted levels which are considered in the scenario selection method.....	28
Table 3.7:	Category A scenarios for highway driving – Changes within field of view. ....	29
Table 3.8:	Category B scenarios for highway driving – Direct calls to action. ....	31
Table 3.9:	Category C scenarios for highway driving – Deviation from standard road surface. ....	32
Table 3.10:	Category A for rural road driving – Changes within field of view. ....	33
Table 3.11:	Category B scenarios for rural road driving – Direct calls to action. ....	35
Table 3.12:	Category C scenarios for rural road driving – Deviation from standard road surface. ....	35
Table 3.13:	Labeling for the classification of expectations. ....	36
Table 3.14:	Expectations of Category A highway driving scenarios.....	37
Table 3.15:	Expectations of Category B highway driving scenarios.....	39
Table 3.16:	Expectations of Category C highway driving scenarios.....	41
Table 3.17:	Expectations of Category A rural road driving scenarios.....	42
Table 3.18:	Expectations of Category B rural road driving scenarios.....	44
Table 3.19:	Expectations of Category C rural road driving scenarios.....	45
Table 3.20:	Overview of possibly UCAs. ....	46
Table 3.21:	Template for the identification of UCAs. ....	47
Table 3.22:	Labeling colors for (not) hazardous situations and situations caused by a malfunction of the system.....	48
Table 3.23:	Labeling categories for the likelihood of hazardous situations that human-driven vehicles would cause the hazard.....	48
Table 3.24:	Exemplary filled hazard analysis table for a delayed provided control action. ....	48
Table 3.25:	Template for the hazard identification of are not provided CAs although they are expected. ....	49
Table 3.26:	Template for the hazard identification of delayed / instantly executed CAs although the opposite is expected.....	49

---

Table 3.27:	Template for the hazard identification of too soon stopped or too long applied CAs. ....	50
Table 3.28:	Additional row for the causal factors analysis to the template for the identification of UCAs .....	50
Table 4.1:	Hazard analysis table for not provided control actions at HW–B03. ....	58
Table 4.2:	Hazard analysis table for provided control actions at HW–B03. ....	60
Table 4.3:	Hazard analysis table for instantly provided control actions at HW–B03. ....	61
Table 4.4:	Hazard analysis table for delayed provided control actions at HW–B03. ....	62
Table 4.5:	Hazard analysis table for too soon stopped acceleration at HW–B03. ....	64
Table 4.6:	Hazard analysis table for not provided control actions at RR–A06. ....	70
Table 4.7:	Hazard analysis table for provided control actions at RR–A06. ....	72
Table 4.8:	Hazard analysis table for instantly provided control actions at RR–A06. ....	73
Table 4.9:	Hazard analysis table for delayed control actions at RR–A06. ....	74
Table 4.10:	Hazard analysis table for too long applied braking at RR–A06. ....	76
Table A.1:	Hazard analysis table for not provided control actions at HW–A01. ....	xi
Table A.2:	Hazard analysis table for provided control actions at HW–A01. ....	xii
Table A.3:	Hazard analysis table for delayed provided control actions at HW–A01. ....	xiii
Table A.4:	Hazard analysis table for instantly applied control actions, too soon stopped acceleration, and too long applied braking at HW–A01. ....	xiv
Table B.1:	Hazard analysis table for not provided control actions at HW–C06. ....	xv
Table B.2:	Hazard analysis table for provided control actions at HW–C06. ....	xvi
Table B.3:	Hazard analysis table for instantly applied control actions at HW–C06. ....	xvii
Table B.4:	Hazard analysis table for delayed provided control actions at HW–C06. ....	xviii
Table B.5:	Hazard analysis table for too soon stopped acceleration at HW–C06. ....	xix
Table B.6:	Hazard analysis table for too long applied braking at HW–C06. ....	xx
Table C.1:	Hazard analysis table for not provided control actions at the combined driving scenario of HW–A06, HW–B07, and HW–C04. ....	xxi
Table C.2:	Hazard analysis table for provided control actions at the combined driving scenario of HW–A06, HW–B07, and HW–C04. ....	xxii
Table C.3:	Hazard analysis table for instantly applied control actions at the combined driving scenario of HW–A06, HW–B07, and HW–C04. ....	xxiii
Table C.4:	Hazard analysis table for delayed provided control actions at the combined driving scenario of HW–A06, HW–B07, and HW–C04. ....	xxiv
Table C.5:	Hazard analysis table for too soon stopped acceleration at the combined driving scenario of HW–A06, HW–B07, and HW–C04. ....	xxv
Table C.6:	Hazard analysis table for too long applied braking at the combined driving scenario of HW–A06, HW–B07, and HW–C04. ....	xxvi

# Bibliography

- [1] Kuhnert, F. et al.: *Five trends transforming the Automotive Industry*. URL: <https://eu-smart-cities.eu/sites/default/files/2018-03/pwc-five-trends-transforming-the-automotive-industry.compressed.pdf>, visited on: September 24, 2018.
- [2] Martyn, A.: *Autonomous car companies report getting rear-ended in most crashes, blame driver error*. URL: <https://www.consumeraffairs.com/news/autonomous-car-companies-report-getting-rear-ended-in-most-crashes-blame-driver-error-102017.html>, visited on: September 15, 2018.
- [3] *DMV - State of California: Report of traffic collision involving an autonomous vehicle: Accident: Apple 08/24/2018*. URL: [https://www.dmv.ca.gov/portal/wcm/connect/36a7cf14-592c-4197-9226-fa40bb652c62/Apple\\_082418.pdf?MOD=AJPERES&CVID=](https://www.dmv.ca.gov/portal/wcm/connect/36a7cf14-592c-4197-9226-fa40bb652c62/Apple_082418.pdf?MOD=AJPERES&CVID=), visited on: September 14, 2018.
- [4] Lee, D.: *BBC: Apple self-driving car in minor crash*. URL: <https://www.bbc.com/news/technology-45380373>, visited on: September 15, 2018.
- [5] *SAE J3016: Surface Vehicle Recommended Practice*, 2016.
- [6] *ISO 26262: Road vehicles - Functional safety*, 2011.
- [7] *DMV - State of California: Report of Traffic Collision Involving an Autonomous Vehicle*. URL: [https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/autonomousveh\\_ol316](https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/autonomousveh_ol316).
- [8] Bartels, A. et al.: *System Classification and Glossary: Deliverable D2.1*, 2015.
- [9] *ISO 26262: Road vehicles - Functional safety - Part 1: Vocabulary*, 2011.
- [10] Winner, H. et al.: *Handbuch Fahrerassistenzsysteme: Grundlagen, Komponenten und Systeme für aktive Sicherheit und Komfort*, Springer Vieweg, 3rd edition, ISBN: 978-3-658-05734-3, 2015.
- [11] *ISO 26262: Road vehicles - Functional safety - Part 3: Concept phase*, 2011.
- [12] Carlson, C.: *Effective FMEAs: Achieving Safe, Reliable, and Economical Products and Processes Using Failure Mode and Effects Analysis*, Wiley, ISBN: 978-1-118-31258-2, 2012.
- [13] Vincoli, J. W.: *Basic Guide to System Safety*, Wiley, 3rd edition, ISBN: 978-1-118-90486-2, 2014.
- [14] *IEC 60812: Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)*, 2006.
- [15] Redmill, F. et al.: *System safety: HAZOP and software HAZOP*, Wiley, ISBN: 0471982806, 1999.
- [16] *Hazop and Hazan: Identifying and Assessing Process Industry Hazards*, Taylor & Francis Group, 4th edition, ISBN: 1560328584, 1999.
- [17] *IEC 61882: Hazard and operability studies (HAZOP studies) - Application guide*, 2016.

- [18] Gould, J. et al.: *Review of Hazard Identification Techniques*. URL: [http://www.hse.gov.uk/research/hsl\\_pdf/2005/hsl0558.pdf](http://www.hse.gov.uk/research/hsl_pdf/2005/hsl0558.pdf), visited on: August 15, 2018.
- [19] Leveson, N. G.: *Engineering a Safer World: Systems Thinking Applied to Safety*, The MIT Press, ISBN: 978-0262016629, 2011.
- [20] Leveson, N. G., Thomas, J. P.: *STPA Handbook*. URL: [http://psas.scripts.mit.edu/home/get\\_file.php?name=STPA\\_handbook.pdf](http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf), visited on: August 22, 2018.
- [21] Young, W., Leveson, N. G.: *An Integrated Approach to Safety and Security Based on Systems Theory*. In: *Commun. ACM*, vol. 57, DOI: 10.1145/2556938, pp. 31–35, 2014.
- [22] Thomas, J.: *Systems Theoretic Process Analysis (STPA): Tutorial*. URL: <http://psas.scripts.mit.edu/home/wp-content/uploads/2014/03/Systems-Theoretic-Process-Analysis-STPA-v9-v2-san.pdf>, visited on: August 22, 2018.
- [23] Form, T.: *PEGASUS: Ziele und Arbeitsinhalte*. URL: <https://www.pegasusprojekt.de/de/pegasus-halbzeitveranstaltung>.
- [24] Singh, S.: *Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey: Traffic Safety Facts Crash: Stats. Report No. DOT HS 812 115*, 2015.
- [25] Winner, H. et al.: *(How) to Address the Approval Trap for Autonomous Vehicles A survey of the challenge on safety validation and releasing the autonomous vehicle*. URL: [https://www.fzd.tu-darmstadt.de/media/fachgebiet\\_fzd/publikationen\\_3/2016\\_5/2016\\_Wi\\_Wf\\_Ju\\_ViV-Symposium\\_Graz.pdf](https://www.fzd.tu-darmstadt.de/media/fachgebiet_fzd/publikationen_3/2016_5/2016_Wi_Wf_Ju_ViV-Symposium_Graz.pdf), visited on: August 25, 2018.
- [26] *Kritische Szenarien für und durch die HAF (L3): Halbzeitveranstaltung: Stand 6 - Anforderungen & Rahmenbedingung*. URL: <https://www.pegasusprojekt.de/de/pegasus-halbzeitveranstaltung>.
- [27] *PEGASUS - Project Info: About PEGASUS*. URL: <https://www.pegasusprojekt.de/en/about-PEGASUS>, visited on: August 24, 2018.
- [28] Zlocki, A.: *Research project PEGASUS: Effectively Ensuring Automated Driving: Goals and work contents of PEGASUS*. URL: [https://www.pegasusprojekt.de/files/tmpl/pdf/1st\\_European\\_CCAD\\_Side\\_Event\\_Folien.pdf](https://www.pegasusprojekt.de/files/tmpl/pdf/1st_European_CCAD_Side_Event_Folien.pdf).
- [29] Steininger, U. et al.: *Validation of assisted and automated driving systems*. URL: <https://www.pegasusprojekt.de/en/lectures-publications>, visited on: August 10, 2018.
- [30] International Risk Governance Center: *Risk and Opportunity Governance of Autonomous Cars: Background Paper: Expert Workshop*. URL: [https://www.irgc.org/wp-content/uploads/2016/06/IRGC-workshop-Autonomous-Cars\\_15-16June-Background-Paper-13June.pdf](https://www.irgc.org/wp-content/uploads/2016/06/IRGC-workshop-Autonomous-Cars_15-16June-Background-Paper-13June.pdf).
- [31] Wotawa, F. et al.: *Quality assurance methodologies for automated driving*. In: *e & i Elektrotechnik und Informationstechnik*, vol. 135, DOI: 10.1007/s00502-018-0630-7, pp. 322–327, 2018.
- [32] Kruppa, S.: *Evaluierung gefährlicher Situationen im Straßenverkehr und Beurteilung der Gefährlichkeit für hochautomatisierte Fahrzeuge: Bachelorarbeit zur Erlangung des Grades B. Sc. an der Fakultät für Maschinenwesen der Technischen Universität München*.
- [33] Ivanov, A., Shadrin, S.: *Development of autonomous vehicles' testing system*. In: IOP Conference Series: Materials Science and Engineering 1, 2018.
- [34] Wessel, G. et al.: *Cooperation and the role of autonomy in automated driving*. In: *Lecture Notes in Control and Information Sciences*, vol. 476, DOI: 10.1007/978-3-319-91569-2\_1, pp. 1–27, 2019.

- [35] Herzberger, N. D. et al.: *Derivation of a Model of Safety Critical Transitions between Driver and Vehicle in Automated Driving*. In: *Advances in Intelligent Systems and Computing*, DOI: 10.1007/978-3-319-93885-1\_38, pp. 421–433, 2019.
- [36] Mallya, A.: *Thesis: Using STPA in an ISO 26262 Compliant Process*, 2015.
- [37] Sulaman, S. M. et al.: *Hazard Analysis of Collision Avoidance System using STPA*. In: 11th International Conference on Information Systems volume 11.
- [38] Abdulkhaleq, A., Wagner, S.: *STAMP Workshop: Experiences with Applying STPA to Software-Intensive Systems in the Automotive Domain*. URL: [http://psas.scripts.mit.edu/home/wp-content/uploads/2013/04/04\\_Abdulkhaleq\\_STAMP\\_2013.pdf](http://psas.scripts.mit.edu/home/wp-content/uploads/2013/04/04_Abdulkhaleq_STAMP_2013.pdf).
- [39] Placke, S. et al.: *Integration of Multiple Active Safety Systems using STPA*. In: *SAE International*, vol. SAE Technical Paper Series, DOI: 4271/2015-01-0277, 2015.
- [40] Hosse, R. et al.: *Evolution Issues of Automated Driving Functions by Application of Systemic Accident Analysis: On the Example of the Tesla Model S Fatality*, 2017.
- [41] Bagschik, G. et al.: *Safety Analysis Based on Systems Theory Applied to an Unmanned Protective Vehicle*. In: *Procedia Engineering*, vol. 179, DOI: 10.1016/j.proeng.2017.03.096, pp. 61–71, 2017.
- [42] Abdulkhaleq, A. et al.: *A Systematic Approach Based on STPA for Developing a Dependable Architecture for Fully Automated Driving Vehicles*. In: *Procedia Engineering*, vol. 179, DOI: 10.1016/j.proeng.2017.03.094, pp. 41–51, 2017.
- [43] Abdulkhaleq, A. et al.: *Missing no Interaction - Using STPA for Identifying Hazardous Interactions of Automated Driving Systems*. In: *International Journal of Safety Science*, vol. 2, DOI: 10.24900/ijss/0201115124.2018.0301, pp. 115–125, 2018.
- [44] Bourdon, L.: *Identifizierung von Automatisierungsrisiken durch die Interaktion von hochautomatisierten Fahrzeugen mit anderen Verkehrsteilnehmern: Semesterarbeit an der Technische Universität München - Lehrstuhl für Fahrzeugtechnik*, 2018.
- [45] Reason, J. T.: *Human error*, Cambridge Univ. Press, 1st, ISBN: 978-0-521-31419-0, 2009.
- [46] Maurer, M. et al.: *Autonomes Fahren: Technische, rechtliche und gesellschaftliche Aspekte*, Springer, ISBN: 978-3-662-45854-9, 2015.
- [47] *Methodik: Interesse der Gesetzgeber und Forscher*. URL: <https://www.gidas.org/ueber-gidas/gidas-methodik/>, visited on: September 5, 2018.
- [48] *VDA 702: Situationskatalog E-Parameter nach ISO26262-3*, 2015.
- [49] Bagschik, G. et al.: *Szenarien für Entwicklung, Absicherung und Test von automatisierten Fahrzeugen*. In: *Vandenhoeck & Ruprecht*, DOI: 10.13109/9783666252884.17, pp. 17–124, 2012.
- [50] Jinwei Zhou, Luigi Del Re: *2017 Asian Control Conference Gold Coast, Australia: Gold Coast Convention and Exhibition Centre, 17th-20th December 2017*, IEEE, ISBN: 9781509015740, 2017.





# Appendix

<b>A</b>	<b>Hazard Analysis Tables for HW–A01</b> .....	<b>xi</b>
<b>B</b>	<b>Hazard Analysis Tables for HW–C06</b> .....	<b>xv</b>
<b>C</b>	<b>Hazard Analysis Tables for Combined HW–A06, HW–B07, HW–C04</b> .....	<b>xxi</b>



# A Hazard Analysis Tables for HW-A01

Table A.1: Hazard analysis table for not provided control actions at the driving scenario HW-A01.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification	I				I		
Reason for AV action	Cut in enters safety distance				Both vehicles merging into the same lane; AV does not detect vehicle cutting in or is not ready to move back to original lane		
Violated system SC	SC-1				SC-6		
Reason for classification	Not hazardous by itself, it depends on provided actions				Malfunctioning system		
Severity							
ASIL							
UCA							
Refined SC							
Causal factors							

Table A.2: Hazard analysis table for provided control actions at the driving scenario HW-A01.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification	1				1		
Reason for AV action		Cut in enters safety distance	Cut in enters safety distance	Cut in enters safety distance; Vehicle changes lane to the left and brakes		Cut in enters safety distance	Cut in enters safety distance
Violated system SC		SC-3	SC-1	SC-6		SC-1	SC-1
Reason for classification		Hazardous if AV changes lane and oncoming traffic in this lane has highly negative relative velocity and is forced to brake	Hazardous if AV brakes and following traffic is forced to suddenly brake too	Braking although no slow leading vehicle is in new lane, can only be caused by a malfunction of the system		Hazardous if AV performs an emergency brake and following traffic is forced to suddenly stop too	Hazardous if AV performs an emergency stop and following traffic is forced to suddenly brake too
Severity		S3	S2			S3	S3
ASIL		D	C			D	D
UCA		AV changes lane due to a vehicle cutting with positive relative velocity	AV brakes due to a vehicle cutting in with positive relative velocities			AV performs an emergency brake due to a vehicle cutting in with positive relative velocities	AV performs an emergency stop due to a vehicle cutting in with positive relative velocities
Refined SC		AV should not change its lane due to a vehicle cutting in	AV must not brake due to a vehicle cutting in with positive relative velocity			AV must not perform an emergency brake due to a vehicle cutting in with positive relative velocity	AV must not perform an emergency stop due to a vehicle cutting in with positive relative velocity
Causal factors		AV does not include the relative velocity of vehicles cutting in into the determination of executed actions	AV does not include the relative velocity of vehicles cutting in into the determination of executed actions			AV does not include the relative velocity of vehicles cutting in into the determination of executed actions	AV does not include the relative velocity of vehicles cutting in into the determination of executed actions

Table A.3: Hazard analysis table for delayed provided control actions at the driving scenario HW-A01.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification	I				I		
Reason for AV action					Malfunctioning system		
Violated system SC					SC-6		
Reason for classification					Not aborting a lane change although the cut in vehicle enters the safety distance of the AV; hazardous if other vehicles start moving into the original AV's lane		
Severity							
ASIL							
UCA							
Refined SC							
Causal factors							

Table A.4: Hazard analysis table for instantly applied control actions, too soon stopped acceleration, and too long applied braking at the driving scenario of HW–A01.

<b>Legend</b>	<b>CA-1</b>	<b>CA-2</b>	<b>CA-3</b>	<b>CA-4</b>	<b>CA-5</b>	<b>CA-6</b>	<b>CA-7</b>
Classification	■	■	■	■	■	■	■
Reason for AV action	■	■	■	■	■	■	■
Violated system SC	■	■	■	■	■	■	■
Reason for classification	■	■	■	■	■	■	■
Severity	■	■	■	■	■	■	■
ASIL	■	■	■	■	■	■	■
UCA	■	■	■	■	■	■	■
Refined SC	■	■	■	■	■	■	■
Causal factors	■	■	■	■	■	■	■

## B Hazard Analysis Tables for HW-C06

Table B.1: Hazard analysis table for not provided control actions at the driving scenario HW-C06.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification	■	I	I	I	I	■	■
Reason for AV action	■	AV does not notice end lane	AV does not notice end lane	AV does not notice end lane	AV does not notice end	■	■
Violated system SC	■	-	SC-3	-	-	■	■
Reason for classification	■	Hazard depends on provided actions	Merging vehicle (challenger) expects AV to make space by slowing down and merges into lane	Hazard depends on provided actions	AV only changes lane if there is enough space to merge into, following vehicles might take the opening spot	■	■
Severity	■	■	S3	■	■	■	■
ASIL	■	■	D	■	■	■	■
UCA	■	■	AV does not slow down when neighboring lane ends	■	■	■	■
Refined SC	■	■	AV must slow down when neighboring lane ends and cannot change lanes	■	■	■	■
Causal factors	■	■	AV does not follow happenings outside of own lane	■	■	■	■

Table B.2: Hazard analysis table for provided control actions at the driving scenario HW-C06.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification							
Reason for AV action	AV does not notice the end of its neighboring lane					AV detects end of neighboring lane and makes space by performing an emergency brake	AV detects end of neighboring lane and makes space by performing an emergency stop
Violated system SC	SC-3					SC-6	SC-6
Reason for classification	Merging vehicle (challenger) expects AV to make space					Emergency brake due to an ending neighboring lane is performed by a malfunctioning system	Emergency brake due to an ending neighboring lane is performed by a malfunctioning system
Severity	S3						
ASIL	D						
UCA	AV does not slow down when neighboring lane ends						
Refined SC	AV must slow down when neighboring lane ends and it cannot change lanes						
Causal factors	AV does not follow happenings outside of own lane						



Table B.3: Hazard analysis table for instantly applied control actions at the driving scenario of HW-C06.

<b>Legend</b>	<b>CA-1</b>	<b>CA-2</b>	<b>CA-3</b>	<b>CA-4</b>	<b>CA-5</b>	<b>CA-6</b>	<b>CA-7</b>
Classification	■	■	■	■	■	■	■
Reason for AV action	■	■	■	■	■	■	■
Violated system SC	■	■	■	■	■	■	■
Reason for classification	■	■	■	■	■	■	■
Severity	■	■	■	■	■	■	■
ASIL	■	■	■	■	■	■	■
UCA	■	■	■	■	■	■	■
Refined SC	■	■	■	■	■	■	■
Causal factors	■	■	■	■	■	■	■

Table B.4: Hazard analysis table for delayed provided control actions at the driving scenario HW-C06.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification	█	█	█	█	█	█	█
Reason for AV action	█	AV does not find immediately a gap that is large enough to merge into	AV detects too late that neighboring lane ends	AV does not find immediately a gap that is large enough to merge into	AV detects too late that neighboring lane ends	█	█
Violated system SC	█	SC-6	SC-6	SC-6	-	█	█
Reason for classification	█	AV starts changing lanes right before the neighboring lane ends; this does not help any vehicle to merge into; AV needs to change lanes instantly or not at all, if it does anyways, it must be a malfunction of the system	AV starts braking right before the neighboring lane ends; this does not help any vehicle to merge into; AV needs to brake instantly or not at all, if it does anyways, it must be a malfunction of the system	AV starts changing lanes right before the neighboring lane ends; this does not help any vehicle to merge into; AV needs to change lanes instantly or not at all, if it does anyways, it must be a malfunction of the system	AV aborts lane change right before the end of the neighboring lane and merges back into its original lane; not hazardous because no other vehicle expected the AV to perform a lane change as they foresaw the end of the lane	█	█
Severity	█	█	█	█	█	█	█
ASIL	█	█	█	█	█	█	█
UCA	█	█	█	█	█	█	█
Refined SC	█	█	█	█	█	█	█
Causal factors	█	█	█	█	█	█	█

Table B.5: Hazard analysis table for too soon stopped acceleration at the driving scenario HW-C06.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification	■	I	■	■	I	■	■
Reason for AV action	■	■	AV starts accelerating to the speed limit when neighboring lane ends	AV makes space for vehicle to merge in by changing lane and accelerating up to the allowed speed limit	■	■	■
Violated system SC	■	■	SC-6	SC-6	■	■	■
Reason for classification	■	■	Malfunctioning system: AV should be driving maximum possible speed independently from the end of the neighboring lane	Malfunctioning system: AV should be driving maximum possible speed or perform a take over maneuver independently from the end of the neighboring lane	■	■	■
Severity	■	■	■	■	■	■	■
ASIL	■	■	■	■	■	■	■
UCA	■	■	■	■	■	■	■
Refined SC	■	■	■	■	■	■	■
Causal factors	■	■	■	■	■	■	■

Table B.6: Hazard analysis table for too long applied braking at the driving scenario HW-C06.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification		I	I	I	I		
Reason for AV action			AV slows down until safety distance is large enough that the vehicle can merge in safely	Malfunctioning system			
Violated system SC			SC-3	SC-6			
Reason for classification			Following vehicle does not expect the AV to brake that long as it is not necessary to instantly fulfill safety distances	No braking required /expected when changing lane			
Severity			S3				
ASIL			D				
UCA			AV slows down until safety distance is large enough when neighboring lane ends				
Refined SC			AV should not force to maintain the safety distances when neighboring vehicle merges due to the end of its lane				
Causal factors			AV always maintains safety distances				

# C Hazard Analysis Tables for Combined HW-A06, HW-B07, HW-C04

Table C.1: Hazard analysis table for not provided control actions at the combined driving scenario of HW-A06, HW-B07, and HW-C04.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification							
Reason for AV action				AV is confused by lane markings and remains in lane			
Violated system SC				-			
Reason for classification				Remaining in lane and continuing to follow a slowly leading vehicle is not hazardous, other vehicles can pass if they intend to accelerate; hazardous situation depends on actually provided control action			
Severity							
ASIL							
UCA							
Refined SC							
Causal factors							

Table C.2: Hazard analysis table for provided control actions at the combined driving scenario of HW-A06, HW-B07, and HW-C04.

Legend		CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification					I			
Reason for AV action	AV cannot handle confusing lane markings and follows the leading vehicle	AV does not detect lane markings properly	AV does not detect lane markings properly		Malfunctioning system	AV does not detect lane markings properly	AV does not detect lane markings properly	AV does not detect lane markings properly
Violated system SC	-	SC-6	SC-6		SC-6	SC-6	SC-6	SC-6
Reason for classification	Following vehicles can take over AV if they intend to accelerate; does not create a hazardous situation	It is not necessary to change lanes to the left if AV does not accelerate; a lane change to the right can be performed without causing harm to other road users	Accelerating in same lane cannot be performed due to the slow leading vehicle, braking is not necessary as the leading vehicle maintains its speed; if AV does accelerate or brake within its lane, it is due to a malfunction of the system		AV cannot abort a lane change as it was restricted not to change lanes, if AV does anyways it is due to a malfunction of the system	An emergency braking is not necessary as the leading vehicle maintains its speed; if AV performs an emergency brake within its lane, it is due to a malfunction of the system	An emergency stop is not necessary as the leading vehicle maintains its speed; if AV performs an emergency stop within its lane, it is due to a malfunction of the system	An emergency stop is not necessary as the leading vehicle maintains its speed; if AV performs an emergency stop within its lane, it is due to a malfunction of the system
Severity								
ASIL								
UCA								
Refined SC								
Causal factors								

Table C.3: Hazard analysis table for instantly applied control actions at the combined driving scenario of HW–A06, HW–B07, and HW–C04.

<b>Legend</b>	<b>CA-1</b>	<b>CA-2</b>	<b>CA-3</b>	<b>CA-4</b>	<b>CA-5</b>	<b>CA-6</b>	<b>CA-7</b>
Classification	■	■	■	■	■	■	■
Reason for AV action	■	■	■	■	■	■	■
Violated system SC	■	■	■	■	■	■	■
Reason for classification	■	■	■	■	■	■	■
Severity	■	■	■	■	■	■	■
ASIL	■	■	■	■	■	■	■
UCA	■	■	■	■	■	■	■
Refined SC	■	■	■	■	■	■	■
Causal factors	■	■	■	■	■	■	■

Table C.4: Hazard analysis table for delayed provided control actions at the combined driving scenario of HW–A06, HW–B07, and HW–C04.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification				1			
Reason for AV action				AV is confused by lane markings and needs some time to adjust to confusing lane markings			
Violated system SC				SC-1			
Reason for classification				Vehicle following AV (challenger) starts take over maneuver before AV does; challenger has to release accelerator pedal not to run into AV; Challenger must not brake actively as AV also accelerates, therefore it is not hazardous			
Severity							
ASIL							
UCA							
Refined SC							
Causal factors							



Table C.5: Hazard analysis table for too soon stopped acceleration at the combined driving scenario of HW-A06, HW-B07, and HW-C04.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification				I			
Reason for AV action				AV changes lanes and is confused by lane markings and stops acceleration			
Violated system SC				SC-3			
Reason for classification				A following vehicle in the new lane has to brake actively in order to not run into AV (not just release accelerator pedal)			
Severity				S3			
ASIL				B			
UCA				AV starts a take over maneuver of a slow leading vehicle after the no passing rule was canceled and stops accelerating due to confusing lane markings			
Refined SC				AV must not stop accelerating when it is confused by the lane markings			
Causal factors				AV does not detect the course of its lane properly			

Table C.6: Hazard analysis table for too long applied braking at the combined driving scenario of HW-A06, HW-B07, and HW-C04.

Legend	CA-1	CA-2	CA-3	CA-4	CA-5	CA-6	CA-7
Classification							
Reason for AV action				AV is confused by lane markings			
Violated system SC				SC-6			
Reason for classification				Acceleration expected; If AV brakes due to confusing lane markings, it must be due to a malfunction of the system			
Severity							
ASIL							
UCA							
Refined SC							
Causal factors							