Masterarbeit

Human Factor Analyse eines zukünftigen Systems zum automatisierten Fahren mittels STPA und Evaluation des Mehrwerts ggü. traditionellen Verfahren

Lukas Balzer

Studiengang: Softwaretechnik

Prüfer/in: Prof. Dr. Stefan Wagner
Betreuer/in: Herr Wolfgang Fechner, Herr Pierre Blüher

Beginn am: May 2, 2018
Beendet am: November 2, 2018
Kurzfassung

Danksagung

## Inhaltsverzeichnis

1. **Einleitung** ........................................... 19
   1.1. Problemstellung .................................. 19
   1.2. Ziel der Arbeit .................................. 20
   1.3. Struktur der Arbeit .............................. 20

2. **Literaturrecherche** ................................. 21
   2.1. Betrachtung des *Human Factor* in der Sicherheitsanalyse .......... 21
   2.2. Betrachtung des *Human Factor* in der Domäne des automatisierten Fahrens ... 24
   2.3. Traditioneller Ansatz zur Analyse des *Human Factors* ................ 25
   2.4. Anwendung der System Theorie in der Gefahrenanalyse ............... 28

3. **Methodik** ........................................... 33
   3.1. Human Error Analysis (HEA) ........................ 33
   3.2. STPA Guideline zur Durchführung einer *Human Factor* Analyse ........ 34

4. **Evaluation des Mehrwerts von STPA ggü. traditionellen Verfahren** ........ 43
   4.1. Design der durchgeführten Fallstudie .......................... 43
   4.2. Beispielsystem .................................. 47
   4.3. STPA des Beispielsystems ........................... 48
   4.4. Human Error Analysis des Beispielsystems .................... 52
   4.5. Überdeckungsmatrix und Abdeckungsanalyse ...................... 54
   4.6. Vor- und Nachteile der STPA ggü. traditionellen Methoden .......... 59
   4.7. Validität der Fallstudie ................................ 63

5. **Zusammenfassung und Schlussfolgerung** ................. 65
   5.1. Schlussfolgerung .................................. 65
   5.2. Ausblick ........................................ 66

**Anhang** ........................................... 67

**A.** STPA eines zukünftigen Systems zum automatisierten Fahren .................. 67

**B.** Human Error Analysis eines zukünftigen Systems zum automatisierten Fahren .... 91

**Literaturverzeichnis** .......................... 95
Abbildungsverzeichnis

2.1. Das 1990 vorgestellte Modell eines Produktiv-Systems von James Reason[Rea90], welches in jeder Stufe des Systems Beispiele für menschliches Versagen (kursiv dargestellt) definiert (angelehnt an die Darstellung des ICAO (International Civil Aviation Organisation) Circular 240-AN144[Shea]) ........................................... 22

2.2. Das in ICAO(International Civil Aviation Organisation) Circular 216-AN31[Sheb] vorgestellte Shell Modell (Software, Hardware, Environment and Liveware) welches die Beziehung zwischen dem Menschen mit Software, Hardware, seiner Umwelt und Mitmenschen darstellt ........................................................................................................ 23

2.3. Multidisziplinares Modell des HRA (Human Risk Assesment) Frameworks[Coo+96] .................................................................................................................. 26


2.5. Das Engineering for Humans Modell zur Beschreibung der mentalen Prozesse des Menschen (Quelle: France[Fra17]) ................................................................................................................. 29

2.6. Wickens' Human Information-Processing Model[Wic02][Wic+15] ................................................................................................................................. 31


3.2. Die Regelschleife zwischen HMI (Human Maschine Interface) und Driver im betrachteten Beispielsystems .............................................................................. 38

3.3. Die verfeinerte Regelschleife zwischen HMI (Human Maschine Interface) und Driver im betrachteten Beispielsystem .............................................................................. 38

3.4. Die unterschiedlichen Causal Factors die zu UCAs (Unsafe Control Actions) führen können [Lev11][Fra17][LT14] ............................................................................ 42

4.1. Die einzelnen Schritte der Evaluation ........................................................................ 46

4.2. Die fünf Level autonomen Fahrens der SAE (Society of Automotive Engineers) J3016[Int16] ........................................................................................................... 47

4.3. Die initiale Control Structure des Beispielsystems ..................................................... 49

4.4. Die finale Control Structure der in Anhang A zu findenden STPA eines ADS (Automated Driving System) ................................................................................. 50

4.5. Process Model des Drivers in der STPA des Breispielsystems mit den Mental Models, dem Input und der Sensory Perception .............................................. 51

4.6. Überdeckungsmatrix der Safety Constraints(SC) aus der STPA und der Control Strategies(CS) aus der HEA .............................................................................. 54
4.7. Absolute (a) und prozentuale (b) Verteilung der STPA Safety Constraints (in Orange) auf die drei Ebenen der STPA und die Abdeckung der jeweiligen Safety Constraints durch entsprechende Control Strategies der HEA (in Grün)  

4.8. Absolute Verteilung der STPA Safety Constraints (in Orange) und der Control Strategies der HEA (in Blau) auf die drei Ebenen der STPA  

4.9. Themenüberdeckung der Safety Constraints aus der STPA und HEA  

4.10. Visualisierung der Themenüberdeckung der HEA im Vergleich zur STPA des Beispielsystems
Tabellenverzeichnis

2.1. Die Fehler Kategorien die in der PHEA entnommen aus [Emb+94] .......................... 27
3.1. Die Tabelle einer HEA wie sie in [Rudgu] vorgeschlagen wird .............................. 33
3.2. Eine Bewertung der Wahrscheinlichkeit der Auftretens des Fehlers, die von der Ford Motor Company in [Mod11] auf Seite 135 vorgeschlagen wurde ........................ 33
3.4. Tabelle zur Unterstützung der Analyse von UCAs (Unsafe Control Actions) für CAs (Control Actions) .......................................................... 39
4.1. Beschreibung der Systemfunktionen des ADS, die in der Beispielanalyse in Anhang A und B analysiert wurden ................................................................. 44
4.2. Kategorisierung der Severity nach ISO 26262 [Sch11] ........................................ 49
4.3. Tabelle nach [Rudgu] der Einflussfaktoren die in der HEA des Beispielsystems verwendet wurde um die PSF (Performance Shaping Factors) aufzustellen ........... 52
4.4. Die Tabelle der Fehlermodi die in einem ADS (Automated Driving System) zur Analyse der Operator Tasks berücksichtigt werden müssen entnommen und angepasst aus der Guideline von Rudolph[Rudgu] ............................................ 53
4.5. Die drei Analyseebenen, die in STPA Schritt eins, drei und vier betrachtet werden. 57
Abkürzungsverzeichnis

AD Automated Driving. 45
ADS Automated Driving System. 24
FMEA Failure Mode and Effect Analysis. 59
HEA Human Error Analysis. 20
HEM Human Error Mode. 33
HFE Human Failure Event. 62
HMI Human Maschine Interface. 37
HRA Human Risk Assessment. 25
ICAO International Civil Aviation Organisation. 22
ODD Operational Design Domain. 48
PHEA Predictive Human Error Analysis. 25
PIF Performance Inducing Factor. 25
PRA Probabilistic Risk Assessment. 26
PSF Performance Shaping Factor. 25
SAE Society of Automotive Engineers. 47
Shell-Modell Software, Hardware, Environment, Liveware, Liveware Model. 22
SHERPA Systematic Human Error Reduction and Prediction Approach. 26
STAMP Systems-Theoretic Accident Model and Processes. 21
STPA Systems-Theoretic Process Analysis. 19
UCA Unsafe Control Action. 34
# Begriffslexikon


<table>
<thead>
<tr>
<th>Begriff</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control Action</strong></td>
<td>Eine Regelungsaktion, die den Zustand des regulierten Prozesses durch triggern eines Actuators verändert und durch die ein Controller die identifizierten Safety Constraints umsetzen kann.[LT18]</td>
</tr>
<tr>
<td><strong>Control Action Selection</strong></td>
<td>Der Entscheidungsprozess des Menschen für eine bestimmte Control Action basierend auf den Informationen aus den Mental Models.[Fra17]</td>
</tr>
<tr>
<td><strong>Control Algorithm</strong></td>
<td>Der Algorithmus eines automatisierten Controllers zur Selektion einer Control Action basierend auf den Process Models des Controllers.[LT18]</td>
</tr>
<tr>
<td><strong>Control Strategy</strong></td>
<td>Ergebnis einer HEA (Human Error Analysis) welches die Ausführung von Systemaufgaben mittels Strategien und Maßnahmen reglementiert, im Gegensatz zu einem Safety Constraint aber keine konkreten Forderungen an das Design des Systems stellt.</td>
</tr>
<tr>
<td><strong>Control Structure</strong></td>
<td>Eine hierarchische Darstellung des funktionalen Modells des betrachteten Systems, die schon durch die Aufstellung einer Systemhierarchie den Anwender unterstützt, Fehler in der Feedbackschleife zu finden.[LT18]</td>
</tr>
<tr>
<td><strong>Controlled Process</strong></td>
<td>Der vom Controller regulierte Prozess, bspw. ein Fahrzeug welches von einem Human Controller gesteuert wird.</td>
</tr>
<tr>
<td>Begriff</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Controller</td>
<td>Eine Komponente die mittels Control Actions und Feedback einen Controlled Process reguliert. Man kann generell zwischen zwei Arten von Controllern unterscheiden:</td>
</tr>
<tr>
<td></td>
<td><em>Human Controller</em> Ein Mensch der mit vier Komponenten modelliert wird; der Control Action Selection, der Mental Models, dem Mental Model Update und einer Sensory Perception.</td>
</tr>
<tr>
<td></td>
<td><em>Automated Controller</em> Ein automatisierter Controller besteht aus einem Process Model sowie einem Control Algorithm.</td>
</tr>
<tr>
<td>Dynamic Driving Task (DDT)</td>
<td>Alle Fahrzeugfunktionen die zur Erfüllung der Fahraufgabe im Straßenverkehr und zum Treffen taktischer Entscheidungen wie Fahrbahnwechsel oder sonstiger Steuereingriffe benötigt werden. Nicht eingeschlossen sind dabei Funktionen wie Navigation, Zeitplanung oder andere strategische Planungsfunktionen.[Int16]</td>
</tr>
<tr>
<td>DDT-Fallback</td>
<td>Die Antwort des Benutzers eines Automated Driving Systems (ADS), entweder die DDT zu übernehmen oder das Erreichen einer MRC sicherzustellen, nachdem ein DDT-leistungsrelevanter Systemfehler aufgetreten ist oder nachdem die ODD verlassen wurde.[Int16]</td>
</tr>
<tr>
<td>Hazard</td>
<td>Eine Gefährdung (engl. Hazard) ist ein Systemzustand oder eine Reihe von Bedingungen, die zusammen mit einer bestimmten Menge von Worst-Case-Bedingungen zu einem Verlust führen können.[LT18]</td>
</tr>
<tr>
<td>Mental Models</td>
<td>Ein Mental Model enthält alle sicherheits-relevanten Informationen und Annahmen, die ein Human Controller über einen Prozess und dessen Verhalten sowie seine Umwelt besitzt. In Engineering for Humans werden drei Arten von Mental Models vorgestellt:</td>
</tr>
<tr>
<td></td>
<td>- Das Mental Model des Prozesszustandes</td>
</tr>
<tr>
<td></td>
<td>- Das Mental Model des Prozessverhaltens</td>
</tr>
<tr>
<td></td>
<td>- Das Mental Model der Umwelt (des Prozesses)</td>
</tr>
<tr>
<td></td>
<td>[Fra17]</td>
</tr>
<tr>
<td>Mental Model Update</td>
<td>Der Prozess durch den Feedback oder Informationen über äußere Faktoren in die Mental Models integriert werden.[Fra17]</td>
</tr>
<tr>
<td>Begriff</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Minimal Risk Condition (MRC)</td>
<td>Ein Zustand oder eine Position, in den ein Benutzer oder ein Automated Driving System (ADS) das Fahrzeug nach Durchführung des DDT-Fallbacks bringen kann. Durch das Erreichen einer MRC soll das Risiko eines Unfalls minimal gehalten werden, wenn die momentane Fahrt abgebrochen werden muss. [Int16]</td>
</tr>
<tr>
<td>Operational Design Domain (ODD)</td>
<td>Anforderungen an die Umgebung und die Bedingungen unter denen autonomes Fahren erlaubt ist und bildet damit eine Limitierung der Level 1 bis 4 auf bestimmte Anwendungsbereiche, wie bspw. die Autobahn bzw. klar gekennzeichnete Fahrbahnen aber auch bestimmte Geschwindigkeiten. [Int16]</td>
</tr>
<tr>
<td>Sensory Perception</td>
<td>Das unverarbeitete Feedback welches der Mensch durch visuelle, tiefen sensible oder vestibuläre Wahrnehmung empfängt und welches nicht Teil des Systemdesigns ist. [LT14]</td>
</tr>
<tr>
<td>Sicherheit (Safety)</td>
<td>Die Freiheit von Accidents. [LT18]</td>
</tr>
<tr>
<td>Unsafe Control Action</td>
<td>Eine Control Action, die in einem bestimmten Kontext und unter Worst-Case-Bedingungen zu einem Hazard führt. [LT18]</td>
</tr>
</tbody>
</table>
1. Einleitung


1.1. Problemstellung

1. Einleitung

1.2. Ziel der Arbeit


1.3. Struktur der Arbeit

2. Literaturrecherche

In diesem Kapitel wird das für diese Arbeit benötigte Hintergrundwissen aus der Literatur zusammengefasst und die wichtigen Punkte werden herausgearbeitet. Die Literaturrecherche beschäftigt sich mit der Betrachtung des Human Factor in der Domäne des automatisierten Fahrens und den Unterschieden zwischen der STPA und traditionellen Verfahren. Abschnitt 2.1 beschreibt zunächst die generelle Betrachtung des Menschen und die historische Entwicklung dieser in der Sicherheitsanalyse. Danach wird auf den Spezialfall des Human Factors in automatisierten Fahrsystemen anhand aktueller Literatur in Abschnitt 2.2 eingegangen. In Abschnitt 2.3 und Abschnitt 2.4 werden dann nacheinander die traditionelle Analyse und die Analyse mittels Systems-Theoretic Accident Model and Processes (STAMP) unter Berücksichtigung des Human Factor betrachtet, um eine Grundlage für die im Verlauf der Arbeit durchgeführten Analysen zu bilden.

2.1. Betrachtung des Human Factor in der Sicherheitsanalyse

2. Literaturrecherche

Abbildung 2.1.: Das 1990 vorgestellte Modell eines Produktiv-Systems von James Reason[Rea90], welches in jeder Stufe des Systems Beispiele für menschliches Versagen (kursiv dargestellt) definiert (angelehnt an die Darstellung des ICAO (International Civil Aviation Organisation) Circular 240-AN/144[Shea])

2.1. Betrachtung des *Human Factor* in der Sicherheitsanalyse

**Abbildung 2.2.:** Das in ICAO (International Civil Aviation Organisation) Circular 216-AN31 [Sheb] vorgestellte Shell Modell (Software, Hardware, Environment and Liveware) welches die Beziehung zwischen dem Menschen mit Software, Hardware, seiner Umwelt und Mitmenschen darstellt.

In Abbildung 2.2 ist das Shell-Modell mit seinen fünf Komponenten und vier Schnittstellen abgebildet. Das Zentrum des Modells bildet der menschliche Operator, welcher auch das Zentrum der Analyse bildet. Der Pilot eines Flugzeugs oder der Fahrer eines Fahrzeugs der äußeren Einflüssen ausgesetzt ist sind Beispiele Hierfür. Im Folgenden werden die einzelnen Schnittstellen, die zur Aufdeckung möglicher Schwachstellen im System berücksichtigt werden kurz erläutert:

**Liveware-Software**


**Liveware-Hardware**


**Liveware-Liveware**

Liveware-Environment

Die letzte Schnittstelle ist die zur Umwelt des Operators, d.h. zu dessen direkter Umgebung wie der Fahrerkabine oder dem Sitz auf dem er sitzt sowie zum Umfeld des Systems wie z.B. der Straße, der Verkehrssituation oder dem Wetter. Durch die Analyse dieser Schnittstelle werden Fragen zur Beeinflussung des Operators durch seine Umgebung, z.B. räumliche Faktoren wie Größe der Kabine oder Temperatur im Fahrzeug, beantwortet. Außerdem können Umwelteinflüsse wie Luftqualität oder Tageszeit/Licht auch Einfluss auf die Psyche des Operators nehmen wie Stress, Beklommenheit oder Müdigkeit.

2.2. Betrachtung des Human Factor in der Domäne des automatisierten Fahrens

Die Betrachtung des Menschen in Fahrsystemen erfährt mit der Einführung von automatisierten Fahrzeugen einen Rollenwechsel vom Menschen als aktivem Fahrer zum passiven Beobachter [Rad+16]. Dadurch ergibt sich insbesondere bei der Analyse von hochautomatisierten Fahrsystemen, die eine situationsbedingte komplettene Übernahme der Fahrfunktionen durch das Fahrzeug anbieten, eine Reihe an vollkommen neuen Anforderungen an die Gefahrenanalyse. In solchen Systemen wechselt der Mensch zwischen der klassischen Rolle des Fahrers und der eines Beifahrers, der nur noch als Rückfallebene gebraucht wird, hin und her [Rad+16]. In dieser Arbeit spielt dieses Szenario eine wichtige Rolle, da die Übernahme von Fahrfunktionen (engl. take-over) eine sicherheitskritische Aktion in einem hochautomatisierten Fahrsystem darstellt [Göl+16].


2.3. Traditioneller Ansatz zur Analyse des Human Factors


Eine Variable in der Implementierung einer Übernahmesituation, die sich ganz selbstverständlich auf die Übernahmequalität auswirkt, ist die zur Verfügung stehende Zeit. Hier zeigen Dambock et al. [Dam+12], dass in bestimmten Situationen ein Zeitfenster von sechs Sekunden zur Sicherstellung einer fehlerfreien Übernahme notwendig ist. 2014 wies Radlmayr et al. [Rad+14] jedoch nach, dass selbst bei einer Übernahmezeit von sieben Sekunden erhebliche Einschränkungen wie Kollisionswahrscheinlichkeit und Bremsbeschleunigung im Vergleich zum konstanten manuellen Fahrbetrieb existieren.

Ebenfalls wurde in durch Young et al. [YS07] und Merat et al. [MJ09] eine Steigerung der Bremsreaktion beim automatisierten Fahren um ca. zwei bis drei Sekunden nachgewiesen, was eine signifikante Steigerung der Time to Collision (TTC)(auch Time to Collision)[MJ09] darstellt.

2.3. Traditioneller Ansatz zur Analyse des Human Factors


Ein Beispiel einer Analyse die Performance Inducing Factors nutzt, ist Predictive Human Error Analysis (PEHA) welche 1994 von Embery et al. für die CENTER FOR CHEMICAL PROCESS SAFETY beschrieben wurde[Emb+94]. In der Analyse werden die Bedienaufgaben eines Systems systematisch auf mögliche gefährdende Aktivitäten (siehe Tabelle 2.1) hin untersucht, die abhängig von den wirkenden PSFs auftreten können.

25
Abbildung 2.3.: Multidisziplinäres Modell des HRA (Human Risk Assessment) Frameworks [Coo+96]


### 2.3. Traditioneller Ansatz zur Analyse des Human Factors

<table>
<thead>
<tr>
<th>Action Errors</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Action too long/short</td>
</tr>
<tr>
<td>A2</td>
<td>Action mistimed</td>
</tr>
<tr>
<td>A3</td>
<td>Action in wrong direction</td>
</tr>
<tr>
<td>A4</td>
<td>Action too little/too much</td>
</tr>
<tr>
<td>A5</td>
<td>Misalign</td>
</tr>
<tr>
<td>A6</td>
<td>Right action on wrong object</td>
</tr>
<tr>
<td>A7</td>
<td>Wrong action on right object</td>
</tr>
<tr>
<td>A8</td>
<td>Action omitte</td>
</tr>
<tr>
<td>A9</td>
<td>Action incomplete</td>
</tr>
<tr>
<td>A10</td>
<td>Wrong action on wrong object</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Checking Errors</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1</td>
<td>Checking omitted</td>
</tr>
<tr>
<td>C2</td>
<td>Check incomplete</td>
</tr>
<tr>
<td>C3</td>
<td>Right check on wrong object</td>
</tr>
<tr>
<td>C4</td>
<td>Wrong check on right object</td>
</tr>
<tr>
<td>C5</td>
<td>Check mistimed</td>
</tr>
<tr>
<td>C6</td>
<td>Wrong check on wrong object</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Retrieval Errors</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>Information not obtained</td>
</tr>
<tr>
<td>R2</td>
<td>Wrong information obtained</td>
</tr>
<tr>
<td>R3</td>
<td>Information retrieval incomplete</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transmission Errors</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>Information not transmitted</td>
</tr>
<tr>
<td>T2</td>
<td>Wrong information transmitted</td>
</tr>
<tr>
<td>T3</td>
<td>Information transmission incomplete</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Selection Errors</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>Selection omitted</td>
</tr>
<tr>
<td>S2</td>
<td>Wrong selection made</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Plan Errors</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>Plan preconditions ignored</td>
</tr>
<tr>
<td>P2</td>
<td>Incorrect plan executed</td>
</tr>
</tbody>
</table>

*Tabelle 2.1.*: Die Fehler Kategorien die in der PHEA entnommen aus [Emb+94]
2.4. Anwendung der System Theorie in der Gefahrenanalyse

"the whole is more than the sum of its parts"

Aristoteles


Abbildung 2.4.: Control Stucture eines mechanischen Systems, in dem der Human Controller durch die notwendige räumliche Nähe, um den Prozess steuern zu können z.B. ein konventionelles Fahrzeug welches durch unmittelbar verbundene mechanische Instrumente betrieben wird [Lev11]
2.4. Anwendung der System Theorie in der Gefahrenanalyse


<table>
<thead>
<tr>
<th>Safety Constraints</th>
<th>Das Konzept der Safety Constraints ist, Reglementierungen zu formulieren, die jegliche Hazards im System durch Forderungen an Design und Zustand des Systems verhindern.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Structure</td>
<td>Eine hierarchische Darstellung des funktionalen Modells des betrachteten Systems, die schon durch die Aufstellung einer Systemhierarchie den Anwender unterstützt, Fehler in der Feedbackschleife zu finden [LT18].</td>
</tr>
</tbody>
</table>


![Human Controller Diagram](image)

**Abbildung 2.5.**: Das Engineering for Humans Modell zur Beschreibung der mentalen Prozesse des Menschen (Quelle: France[Fra17])

Das Engineering for Humans Modell erweitert die Definition des Process Models auf die Mental Models und den Mental Model Updates und ersetzt den automatisierten Control Algorithm durch die Control Action Selection. Hierzu werden einem menschlichen Controller zusätzlich zu einem Process Model, welches hier als Mental Model des Prozesszustandes bezeichnet wird, noch zwei weitere Modelle zur Seite gestellt. Das Mental Model des Prozessverhaltens beschreibt die erwartete Reaktion auf Control Actions; beispielsweise erwartet ein Autofahrer, der am Lenkrad dreht, dass sich das Fahrzeug dementsprechend mit dreht. Ein drittes Mental Model bildet das Modell der Umwelt, welches den Fokus sowohl auf äußere Einflüsse wie sozialen Kontext, Training in den


1. Regel-basiert

Entscheidungen, die Anhand von Schlussfolgerungen aus den Mental Models getroffen wurden, bspw. aufgrund von wenn-dann Regeln.

2. Fähigkeits-basiert

Entscheidungen, die instinktiv anhand in einer bekannten Situation getroffen werden; Fähigkeits-basierte Aktionen beziehen sich auf die Fähigkeit des Menschen schnell und ohne weitere Überlegung zu reagieren.

3. Wissens-basiert

Entscheidungen die auf dem Wissen über das System basieren, welches in den Mental Models abgebildet ist. Zu dieser Kategorie gehören Aktionen die sich auf den aktuellen Zustand des Controlled Process beziehen und für die eine korrekte Abbildung dessen essentiell ist.


that has not been designed into the system“ ([LT14], Seite 37). Die Filterung des auf den Menschen einwirkenden Informationsstroms wurde von Wickens *Wickens’ Human Information-Processing Model*[Wic02][Wic+15] mit der *Sensory Processing* beschrieben.

**Abbildung 2.6.: Wickens’ Human Information-Processing Model*[Wic02][Wic+15]*

Das Modell beschreibt die *Sensory Perception* als Zusammenspiel zwischen den menschlichen Sensoren, des momentanen Zentrums der Aufmerksamkeit und der im Langzeitgedächtnis gespeicherten Informationen über die observierbare Welt. Ein Beispiel ist ein Vogelzwitschern, welches unterschiedlich wahrgenommen werden kann, je nachdem ob der Mensch seine Aufmerksamkeit auf den Vogel gerichtet hat und ob er zuvor schon mal ein Vogelzwitschern gehört hat.
3. Methodik

In diesem Abschnitt werden die beiden angewendeten Gefahrenanalysen STPA und HEA kurz vorgestellt und die Vorgehensweise der STPA in Form einer Guideline mit besonderer Berücksichtigung der Einbeziehung des menschlichen Faktors in die Analyse skizziert.

3.1. Human Error Analysis (HEA)


<table>
<thead>
<tr>
<th>Operator Task</th>
<th>Description</th>
<th>Goal</th>
<th>Actions</th>
<th>Plans</th>
<th>Performance shaping factors</th>
<th>Human error mode</th>
<th>Occurrence Probability</th>
<th>Human error effect</th>
<th>Control Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>≥ 1 in 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>1 in 20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate</td>
<td>1 in 500 bis 1 in 2000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>1 in 10.000 bis 1.000.000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Very Low</td>
<td>Auftreten des Fehlers wird durch andere Maßnahmen verhindert</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Tabelle 3.1.*: Die Tabelle einer HEA wie sie in [Rudgu] vorgeschlagen wird

<table>
<thead>
<tr>
<th>Bewertung</th>
<th>Wahrscheinlichkeit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very High</td>
<td>≥ 1 in 10</td>
</tr>
<tr>
<td>High</td>
<td>1 in 20</td>
</tr>
<tr>
<td>Moderate</td>
<td>1 in 500 bis 1 in 2000</td>
</tr>
<tr>
<td>Low</td>
<td>1 in 10.000 bis 1.000.000</td>
</tr>
<tr>
<td>Very Low</td>
<td>Auftreten des Fehlers wird durch andere Maßnahmen verhindert</td>
</tr>
</tbody>
</table>

*Tabelle 3.2.*: Eine Bewertung der Wahrscheinlichkeit der Auftretens des Fehlers, die von der Ford Motor Company in [Mod11] auf Seite 135 vorgeschlagen wurde

Auftretenswahrscheinlichkeit, die dem HEM und dem PSF anhand der Tabelle 3.2 zugeordnet wird, kann dann anschließend genutzt werden um die Control Strategien zu priorisieren.

1Die Guideline für die durchgeführte HEA ist ein internes Dokument der Continental Teves AG & Co. oHG und ist u.U. nicht verfügbar
3. Methodik

3.2. STPA Guideline zur Durchführung einer Human Factor Analyse


Schritt 1: Definition des Systems und des Analyseumfangs

Schritt 2: Modellierung der Control Structure

Schritt 3: Analyse der Unsafe Control Actions (UCAs)

Schritt 4: Analyse der Causal Factors

Schritt 1: Definition des Systems und des Analyseumfangs

1. Identifikation der Ziele, die durch das System erreicht werden sollen, dabei sollten alle funktionalen Anforderungen an das System berücksichtigt werden. Ein Ziel kann hierbei sowohl qualitativ wie auch quantitativ formuliert sein (Die Autofahrt soll gemäßlich sein vs. der Benzinverbrauch muss unter 10l/km liegen) um den Fortschritt in der Erstellung eines Systems oder Erreichung angestrebter Sicherheitsziele messbar zu machen. Durch eine gezielte Auswahl der Ziele des Systems kann schon hier beeinflusst werden, welche Aspekte betrachtet werden sollen. Beispiele für Ziele wären hier funktionale Anforderungen wie z.B.:

SG-1 Das System S soll den Anwender bei der Erfüllung der Aufgabe A unterstützen


Leveson et al [LT18] definiert einen Hazard wie folgt:

„A Hazard is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss.“

Ein „loss“ stellt dabei eine Verallgemeinerung eines Accidents dar und ist wie folgt definiert:

„A loss involves something of value to stakeholders. Losses may include a loss of human life or human injury, property damage, environmental pollution, loss of mission, loss of reputation, loss or leak of sensitive information, or any other loss that is unacceptable to the stakeholders.“
Accidents können je nach Einsatz der Analyse anhand verschiedener Merkmale priorisiert werden, als Beispiel wurde in der STPA Beispielanalyse jeder identifizierte Accident nach seiner Severity (siehe Tabelle 4.2) priorisiert.

3. Den Abschluss des ersten Schrittes bildet die Ableitung entsprechender Safety Constraints für alle gefundenen Hazards, dieser Schritt ist eine simple Übersetzung der Hazards in entsprechende Regeln zu deren Verhinderung z.B.:

A-1 Verlust oder Verletzung von menschlichem Leben.
H-1 Das Fahrzeug verletzt den Sicherheitsabstand zu Verkehrsteilnehmern.[A-1]
SC0.1 Das Fahrzeug darf den Sicherheitsabstand zu Verkehrsteilnehmern zu keiner Zeit verletzen.

Schritt 2: Modellierung der Control Structure

Der zweite Schritt der Analyse beschäftigt sich mit der Control Structure des Systems d.h. den (abstrakten) System Komponenten sowie deren Kommunikationspfaden. Eine Control Structure kann sechs verschiedene Komponententypen beinhalten:

- Controller
- Controls
- Displays
- Sensors
- Actuators
- Controlled Processes


- Control Actions
- Feedback
- Sonstiger Input und Output, die keiner der beiden Kategorien zugeordnet werden können

Ein automatisierter Controller kann Input durch einen übergeordneten Prozess bspw. einen menschlichen Operator erhalten, oder es können Umwelteinflüsse wie z.B. Wetterdaten, von für die Analyse ausgeblendeten externen Systemen, geliefert werden. Bei einem menschlichen Controller muss man allerdings eine Reihe von Inputs beachten, die die Fähigkeiten Feedback in entsprechende Control Actions umzuwandeln, beeinflussen [LT14]. Um diesen Input vollständig zu erfassen, schlägt Thornberry in [LT14] vor, folgende Kategorien zu beachten:

Systemverständnis gibt Auskunft über die erlernten oder durch Dokumentation verfügbar gemachten Funktionen und Methoden des Fahrzeugs.

Umwelteinflüsse Einflüsse die nicht in die Kategorie der sensorischen Wahrnehmung fallen, also nicht direkten Einfluss auf die Verarbeitung von Feedback nehmen, aber die Selektion einer Control Action trotzdem beeinflussen können. Umwelteinflüsse können Faktoren wie fahrfremde Ereignisse oder Wetter (sonnig, nebelig, etc.) sein aber auch Einflüsse wie Verkehrsteilnehmer oder schlechte Straßenbedingungen.


Sozialer Kontext Eine Entscheidung wird immer auch vom sozialen Kontext, z.B. dem beruflichen Umfeld, Mitfahrern (soziale Verantwortung) etc. beeinflusst.

Psychologische Faktoren Sind eng mit den anderen Kategorien verbunden, da psychische Reaktionen wie Stress stets als Symptome von sozialem Druck, kulturellen oder Umwelteinflüssen auftreten können.

Außerdem besitzt jeder Mensch eine unterschiedliche Sensory Perception was heißt, dass noch vor der Verarbeitung des Feedbacks und der Ableitung nötiger Control Actions seine individuelle Wahrnehmung analysiert werden muss. Hierzu müssen Veränderung der Wahrnehmung durch...

... Umwelteinflüsse wie extreme Wetterbedingungen (z.B. verschwommene Sicht wegen Hitze, Lärm durch Starkregen)

... gesundheitliche Faktoren wie Schwindel, Fieber, Atemnot oder Sehschwäche etc.
berücksichtigt werden.


Abbildung 3.2.: Die Regelschleife zwischen HMI (Human Machine Interface) und Driver im betrachteten Beispielsystem

In Abbildung 3.2 ist die initiale Struktur der beiden Komponenten zu sehen, die sämtliche Controls oder Actuators ausblendet und nur die konzeptionelle Kommunikation der Komponenten über die Control Actions modelliert. Abbildung 3.3 beinhaltet den gleichen Teil des Systems, aber in einer späteren Iteration.

Abbildung 3.3.: Die verfeinerte Regelschleife zwischen HMI (Human Machine Interface) und Driver im betrachteten Beispielsystem

Schritt 3: Analyse der UCAs


Eine Control Action kann potenziell unsicher sein, wenn sie in einem definierten Kontext:

- nicht ausgeführt wird.
- ausgeführt wird.
• zu früh, zu spät oder nicht in der richtigen Reihenfolge ausgeführt wird.
• zu lange angewendet wird oder zu früh abgebrochen wird.

Hierbei ist der Kontext von entscheidender Rolle, da eine präzise Formulierung dessen Grundlage für einen effizienten Safety Constraint zur Verhinderung der UCA ist. In Tabelle 3.3 werden die konkreten Bausteine, aus denen eine UCA aufgebaut sein sollte, beschrieben. Jede UCA beschreibt

1. **Quelle** Name des **Controllers**, der die **Control Action** ausgeführt hat
2. **Typ** Eine der vier oben definierten Kategorien
3. **Control Action** Name der **Control Action**
4. **Kontext** Die Situation in der die **Control Action** ausgeführt wurde, bspw. bei zu hohem Tempo (wobei hier genauer definiert werden sollte was „zu hoch“ heißt)
5. **Hazard Link** Damit eine **Control Action** zur UCA wird, muss sie in einem bestimmten Kontext einen oder mehrere **Hazards** auslösen

Tabelle 3.3.: Der Aufbau einer UCA nach dem STPA Handbook von Nanacy Leveson[LT18]

eine **Control Action**, die in einem bestimmten Szenario/Kontext zu einem, in Schritt 1 definierten, **Hazard** führen kann. Beispielhaft wäre das Beschleunigen in einem Fahrzeug:

**UCA-1:** Der Fahrer gibt Gas in stehendem Verkehr

**UCA-2:** Der Fahrer gibt kein Gas in fließendem Verkehr

**UCA-3:** Der Fahrer gibt zu früh Gas in stockendem Verkehr

**UCA-4:** Der Fahrer gibt zu lange Gas in stockendem Verkehr

Zur Analyse der **Unsafe Control Actions** kann eine Tabelle angelegt werden, wie sie in Tabelle 3.4 dargestellt wird, die zur Sortierung und Übersicht über die Einträge dient. Für jede, zu einem

<table>
<thead>
<tr>
<th><strong>Control Action</strong></th>
<th>Nicht ausführen der CA führt zur Hazard</th>
<th>Ausführung der CA führt zur Hazard</th>
<th>Falsches Timing der CA führt zur Hazard</th>
<th>Zu lange oder kurze Ausführung führt zur Hazard</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA-1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Tabelle 3.4.: Tabelle zur Unterstützung der Analyse von UCAs (Unsafe Control Actions) für CAs (Control Actions)

**Hazard** führende **Unsafe Control Actions** muss ein Safety Constraint auf Funktionsebene erstellt werden, welcher die Kombination aus Kontext und **Control Action** verhindern soll.

Ein Nebenprodukt von Schritt 2 können hierbei auch Verfeinerungen bzw. bisher unberücksichtigte **Hazards** sein. Hierbei kann eine anschließende Wiederholung der ersten beiden Schritte von Vorteil sein, um das System auf neue identifizierte Hazards hin zu analysieren und so eventuell benötigte neue Sicherheitsmechanismen in Schritt 4 einzubeziehen.
3. Methodik

Schritt 4: Analyse der Causal Factors

Im vierten Schritt werden die Causal Factors, die zu Unsafe Control Actions führen können, mithilfe der in Schritt 2 aufgestellten Zustandsmodelle der Controller aus der Feedbackschleife analysiert. Für eine komplettete Analyse aller Faktoren in einem System nach dem Shell-Modell müssen menschliche Controller zusätzlich um die von France et al. in [Fra17] vorgeschlagenen Mental Models erweitert werden. Ein Mental Model abstrahiert die Sicht des Menschen auf seine Umwelt; so wird zwischen drei Typen unterschieden:

- Das Mental Model des Prozesszustandes
- Das Mental Model des Prozessverhaltens
- Das Mental Model der Umwelt


Unsicheres Verhalten des Human Controller als Ursache für Unsafe Control Actions

In der Analyse möglicher Ursachen für Unsafe Control Actions, die durch unsicheres Verhalten des Menschen ausgelöst werden, müssen das Mental Model und die Control Action Selection, die anhand des Prozesszustandes eine der verfügbaren Control Actions auswählen, aus Abbildung 3.1, betrachtet werden. Hierzu sollten drei Kategorien möglicher Ursachen berücksichtigt werden:

- Unvollständige, inkorrekte oder inkonsistente Mental Models
  Während Fehlinformationen der Mental Models des Human Controller eine Vielzahl an Ursachen haben können, die im nächsten Paragraphen beschrieben werden, wird hier auf die Vollständigkeit, Angemessenheit und Akkurateit der Mental Models eingegangen. Das Modell sollte alle für die Regelung des Prozesses wichtigen Variablen beinhalten (auch nicht mehr). Das heißt, es muss vermieden werden, dem Menschen zu viele, unnötige oder
falsche, aber auch zu wenig notwendige Informationen zur Verfügung zu stellen. Beispiele für Szenarien, die Unsafe Control Actions auslösen können, sind fehlende Informationen über den aktuellen Modus eines Systems oder zu viele Informationen über den Zustand eines Prozesses, die dazu führen können, dass die richtige Information nicht rechtzeitig identifiziert werden kann.

• Fehler in der Selektion einer Control Action

Ein Fehler in der Selektion der richtigen Control Action kann mehrere Ursachen haben, wie unzureichendes Training in den Funktionen des Systems oder kann durch vorhandene Fähigkeiten oder Vorwissen beeinflusst werden [Ras82]. Ein Beispiel für ein Ursachenszenario für UCA-1 ist:

**Szenario-1:** Der Fahrer geht aufgrund von früheren Erfahrungen im stockenden Verkehr davon aus, dass das vorausschreitende Fahrzeug Gas geben wird, und gibt Gas, ohne auf die Situation zu achten.

• Fehler in der Ausführung einer Control Action durch den Human Controller


**Unzureichendes Feedback oder Informationen als Ursache für Unsafe Control Actions**

Abbildung 3.4.: Die unterschiedlichen Causal Factors die zu UCAs (Unsafe Control Actions) führen können [Lev11][Fra17][LT14]
4. Evaluation des Mehrwerts von STPA ggü. traditionellen Verfahren


4.1. Design der durchgeführten Fallstudie

4.1.1. Forschungsziel

Das Ziel der Fallstudie deckt sich mit dem Ziel der Arbeit, welches in Abschnitt 1.2 definiert wurde.

4.1.2. Fragestellung

Um das definierte Forschungsziel zu erreichen wurden zwei Forschungsfragen aufgestellt:

RQ1: Bietet STPA einen Mehrwert bei der Analyse des Human Factor in Software-intensiven Systemen verglichen mit traditionellen Verfahren?

RQ2: Was sind die Vor- und Nachteile einer STPA im Vergleich zu traditionellen Verfahren?

In dieser Arbeit wird der Mehrwert der Analyse durch die Abdeckung verschiedener sicherheitskritischer Bereiche definiert. Ein Beispiel für einen höheren Mehrwert wäre, wenn die Analyse eines Systems mit einer anderen Methode Safety Constraints liefert, die eine breitere Abdeckung sicherheitskritischer Bereiche dieses Systems, wie bspw. der Umwelt des Systems, ermöglicht. Aufgrund dieser Definition wird RQ1 in Abschnitt 4.5 durch einen Vergleich der Analyseergebnisse von STPA und HEA beantwortet. Hierbei wird die Frage nach dem Mehrwert, sowohl mittels
der Größe der Schnittmenge der Ergebnisse, als auch anhand der jeweiligen Abdeckung der in Abbildung 4.9 definierten sicherheitskritischen Bereiche im Beispielsystem, beantwortet. Um die in RQ2 geforderten Vor- und Nachteile aufzustellen, werden sowohl die subjektive Wahrnehmung der Durchführung beider Analysen als auch der ermittelte Mehrwert und die objektiven Argumente aus der Literatur verwertet, um eine möglichst neutrale Bewertung der Methoden zu erreichen.

4.1.3. Fall und Einheit der Analyse


4.1.4. Forschungs Methodik


<table>
<thead>
<tr>
<th>Spurwechselanforderung (an das ADS) (engl. Lane Change Request)</th>
<th>Während das ADS aktiv ist kann der Nutzer des Fahrzeuges einen Spurwechsel, zu einer verfügbaren Fahrspur, über das HMI beantragen.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geschwindigkeitseingabe (engl. Set Speed)</td>
<td>Während das ADS aktiv ist, kann der Nutzer des Fahrzeuges eine Änderung der Geschwindigkeit auf einen definierten Wert über das HMI beantragen.</td>
</tr>
</tbody>
</table>

Tabelle 4.1.: Beschreibung der Systemfunktionen des ADS, die in der Beispielenalyse in Anhang A und B analysiert wurden

Da eine vollständige Analyse des Funktionsumfangs des Beispielsystems den Rahmen dieser Arbeit überschreiten würde, und auch für die Beantwortung der Forschungsfragen nicht notwendig ist, wurde der Umfang der Analysen auf eine Teilmenge der Funktionen beschränkt. Um ein aussagekräftiges Ergebnis für eine Aussage über die Vor- und Nachteile der STPA zu erhalten, wurden die oben aufgeführten Funktionen anhand der nachfolgenden Kriterien ausgewählt:
• **High-Level Aktionen** zwischen Fahrer und HMI, um eine gute Vergleichbarkeit mit der traditionellen Human Error Analysis zu erzielen.

• **Funktionen, die nur im automatisierten Fahrbetrieb möglich sind:**
  Mit der *Geschwindigkeitseingabe* und der *Spurwechselanforderung* wurden zwei Aktionen ausgewählt, die nur über ein *Automated Driving (AD)* exklusives Bedienelement eingegeben werden und nur im Bereich des automatisierten Fahrens eingesetzt werden.

• **Funktionen die sowohl während des automatisierten Fahrens als auch während des manuellen Fahrens verfügbar sind:**

4.1.5. Sammlung der Daten


4.2. Beispielsystem

Zur Durchführung der Evaluation wurde ein System zum hochautomatisierten Fahren nach der Society of Automotive Engineers (SAE) J3016 Level 4 [Int16] in Hinblick auf die, auf den Human Factor bezogenen, Hazards analysiert.

<table>
<thead>
<tr>
<th>Operational Design Domain (ODD)</th>
<th>n/a</th>
<th>Limitiert</th>
<th>Limitiert</th>
<th>Limitiert</th>
<th>Limitiert</th>
<th>Unlimitiert</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rückfallstrategie im Fall eines Undefinierten Ereignisses</td>
<td>Limitiert</td>
<td>Limitiert</td>
<td>Limitiert</td>
<td>Limitiert</td>
<td>Unlimitiert</td>
<td></td>
</tr>
<tr>
<td>Erkennung von Objekten und Ereignissen</td>
<td>Limitiert</td>
<td>Limitiert</td>
<td>Limitiert</td>
<td>Limitiert</td>
<td>Unlimitiert</td>
<td></td>
</tr>
<tr>
<td>Beschleunigung und Lenkung des Fahrzeugs</td>
<td>Unterstützung durch das System</td>
<td>Level 0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Fahrer führt die Fahraufgabe teilweise oder ganz aus</td>
<td>Während das AD System eingeschaltet ist wird die Fahraufgabe automatisiert ausgeführt</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Abbildung 4.2.: Die fünf Level autonomen Fahrens der SAE (Society of Automotive Engineers) J3016[Int16]

In dem oben dargestellten Diagramm sind die fünf verschiedenen Level des automatisierten Fahrens und die Ebene des manuellen Fahrens (Level 0), dargestellt. Dabei beschreibt Level 0 komplett manuelles Fahren und Level 5 eine komplette Automatisierung der Fahraufgaben. Das Diagramm ist
in zwei Bereiche unterteilt: der orange gefärbte Bereich umfasst die Level 0 bis 2, in denen der Fahrer durch das System unterstützt wird, allerdings noch konstant in die Fahraufgabe eingebunden ist. Der zweite Bereich umfasst die Level 3 bis 5 und markiert den Übergang vom Fahrrassistenzsystem, welches den Fahrer bei der Fahraufgabe unterstützt, zum autonomen Fahrsystem, welches die Fahraufgabe innerhalb einer Operational Design Domain (ODD) übernimmt. Hierbei stellt die ODD eines ADS Anforderungen an die Umgebung und die Rahmenbedingungen, unter denen autonomes Fahren erlaubt ist, und bildet damit eine Limitierung der Automatisierung in Level 1 bis 4 auf bestimmte Anwendungsbereiche wie bspw. die Autobahn bzw. klar gekennzeichnete Fahrbahnen. Das untersuchte System soll der SAE Level 4 Spezifikation genügen, was bedeutet, dass der Fahrer in, durch die ODD beschränkten Situationen, die Fahraufgabe komplett an das ADS übergeben kann. Hauptunterschied zu Level 3 ist hierbei, dass die Aufmerksamkeit des Fahrers erwartet wird, aber nicht sicherheitskritisch ist. Konkret heißt das, dass beim Verlassen der ODD der Fahrer zwar aufgefordert wird die Fahraufgabe zu übernehmen, aber, wenn dies nicht geschieht, das Fahrzeug trotzdem zu einem sicheren Halt kommt.

Level 4 stellt außerdem einen zusätzlichen Anspruch an die Human Factor Analyse, auf den in der Literaturrecherche in Abschnitt 2.2 eingegangen wird. Durch die Übernahme der vollständigen Fahraufgabe durch das ADS übernimmt der Fahrer, während des autonomen Fahrens, eine passive Rolle, in der er sich mit fahrfernenden Tätigkeiten beschäftigen kann. Im Falle einer unerwarteten Übernahmesituation kann es zu Gefährdungen kommen, die durch den Übergang vom passiven Fahrer zum aktiven Fahrer hervorgerufen werden.

4.3. STPA des Beispielsystems


Schritt 1: Definition des Systems und des Analyseumfangs

Zu Beginn der Analyse wurde das System in der Systembeschreibung als Interaktion zwischen einem Operator, dem ADS, sowie des gesteuerten Fahrzeuges in der Rolle des Controlled Process beschrieben. Aus Gründen der besseren Anschaulichkeit wurde der Operator in zwei menschliche

\(^1\)https://github.com/SE-Stuttgart/XSTAMPP
4.3. STPA des Beispielsystems

<table>
<thead>
<tr>
<th>Severity Beschreibung</th>
<th>SO</th>
<th>S1</th>
<th>S2</th>
<th>S3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keine Verletzungen</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Leichte/moderat-</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verletzungen</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Schwere/lebensbedroh-</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>liche Verletzungen</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Überleben unwiss)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>oder tödliche</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verletzungen</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Tabelle 4.2.: Kategorisierung der Severity nach ISO 26262 [Sch11]

Der Controller aufgeteilt, den Driver und den Mission Controller. Um die Schnittstelle zwischen Mensch und Maschine, die hier eine zentrale Rolle spielt, herauszuheben, wurde außerdem das HMI des ADS separat eingefügt.

Abbildung 4.3.: Die initiale Control Structure des Beispielsystems


Schritt 2: Modellierung der Control Structure

Die Control Structure wurde mit Unterstützung von Continental erstellt und beinhaltet alle in Schritt 1 erörterten Komponenten sowie Feedback und Control Actions. Die Control Structure in Abbildung 4.4 beinhaltet genau die drei Systemfunktionen, die in Tabelle 4.1 beschrieben werden, und in der weiteren Analyse Grundlage weiterer Safety Constraints sind. Eine nicht ganz offensichtliche Annahme, die hier getroffen wurde, ist dass die Control Actions alle vom HMI des ADS verarbeitet werden, bevor sie an das System bzw. die tatsächlichen Aktuatoren des Fahrzeuges weitergeleitet werden. Während dies bei Set Speed und Lane Change Request offensichtlich ist, ist der manuelle
Eingriff in das Fahrgeschehen über *Manual Steering* eine klassische Fahraufgabe und wird in der Regel an einen *Controller* zur Übertragung der Lenkung auf die Aktuatoren gesendet. In dem hier betrachteten System kann das HMI aber direkt auf einen Lenkeingriff reagieren, ohne dass dieser zuvor durch den *Controlled Process* gemeldet wurde. Aufgrund dessen ergeben sich allerdings auch zusätzliche *Safety Constraints* in Schritt drei und vier, die dafür sorgen müssen, dass ein Eingriff wie in SC0.1 gefordert, weiter möglich ist.
Neben dem systeminternen Feedback welches Zustandsupdates, ausgelöst von Control Actions, an

Abbildung 4.4.: Die finale *Control Structure* der in Anhang A zu findenden STPA eines ADS (Automated Driving System)

die *Controller* weiterleitet, beinhaltet die *Control Structure* auch das eingehende Feedback und die *Sensory Perception* die in Kapitel 3 erklärt werden.

**Schritt 3: Analyse der UCAs**

Schritt 3 wurde wie in Abschnitt 3.2 beschrieben durchgeführt, mit dem Unterschied, dass hier jede UCA mit einer *Severity*, die sich an der höchsten *Severity* der verlinkten *Hazards* richtet, belegt wurde. Des Weiteren wurden die *Unsafe Control Actions* wie in Tabelle 3.3 beschrieben, mit dem Zusatz der Severity dokumentiert und in einem zweiten Schritt in entsprechende *Safety Constraints*
umgewandelt, die hier als Corresponding Safety Constraints bezeichnet werden. Der Schritt wurde ebenfalls in mehreren Iterationen durchgeführt, wobei darauf geachtet wurde die Ergebnisliste durch den Gebrauch von Verlinkungen minimal zu halten.

**Schritt 4: Analyse der Causal Factors**


![Diagramm zur Analyse der Causal Factors](image)

**Abbildung 4.5.: Process Model des Drivers in der STPA des Beispielsystems mit den Mental Models, dem Input und der Sensory Perception**

Die Mental Models des Drivers spiegeln das Wissen über die gesamte Situation wieder, d.h. alle Informationen die der Driver, über das Fahrzeug und die Umwelt, verarbeiten konnte. Zusätzlich beinhaltet Abbildung 4.5 auch noch die, in Schritt 2 abgeleiteten, Informationen, die aus der Umwelt
auf den Driver einfließen, welche zur Modellierung des *Mental Models* der Umwelt genutzt wurden. Unterstützt wird die Aufstellung der *Causal Factors* zusätzlich noch durch die *Sensory Perception*, die als zusätzlicher Inputkanal dem Driver hinzugefügt wurde. Ein Beispiel für einen, mithilfe dieser Modelle erstellten, *Causal Factor* ist CF-1:

**CF-1:** Driver issues a set speed command based on experience without considering dynamic factors like wet road or sudden traffic changes

Hier wurde das, in Abschnitt 2.4 der Literaturrecherche, beschriebene Modell von Rasmussen [Ras83] zur Beschreibung des Fähigkeits-basierten Handelns verwendet und mit der Annahme über den Zustand der Fahrbahn kombiniert.

### 4.4. Human Error Analysis des Beispielsystems


<table>
<thead>
<tr>
<th>Umwelt-/Physische Einflüsse</th>
<th>Temperatur, Wetter (Trocken, Nass, Eisglätte), Lärmm/Stille, Frequenz von Störeinflüssen, Physische Einwirkung durch Mitfahrer oder Verkehrsteilnehmer, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Soziootechnische Einflüsse</td>
<td>Fahrtdauer, Zeitdruck</td>
</tr>
<tr>
<td>Menschliche Einflüsse</td>
<td>Wut, Stress, (übermäßige) Freude, gesundheitliche Faktoren</td>
</tr>
<tr>
<td>Systemdesign</td>
<td>Zeit zur Ausführung zeitkritischer Aufgaben, Änderung/-Rücknahme von HMI Anfragen, parallele Ausführung von Aufgaben, Abhängigkeiten von Aufgaben</td>
</tr>
<tr>
<td>Individuelle Faktoren (Des Führers)</td>
<td>schlechtes Training, ungenügende Erfahrung mit dem ADS, Falsche Eingabe von Interaktionen mit dem ADS, Verwirrung über Verantwortungen</td>
</tr>
<tr>
<td>Software/Hardware</td>
<td>Schlechter Layout des Displays, Schlechte/Unverständliche Design des AD Input Devices, Anzeige von zu viel/zu wenig Information, zu viel/wenig Feedback</td>
</tr>
<tr>
<td>Dokumentation, Materialien und Support</td>
<td>Unvollständige Anleitungen/Handbücher, Schlechte/Keine Wartung, veraltete Materialien</td>
</tr>
</tbody>
</table>

*Tabelle 4.3.:* Tabelle nach [Rudgu] der Einflussfaktoren die in der HEA des Beispielsystems verwendet wurde um die PSF (Performance Shaping Factors) aufzustellen

von Tabelle 4.3 erstellt wobei hier die Tabelle der PSF die in [Rudgu] vorgestellt wurde um die menschlichen Faktoren im Umgang mit dem Beispielsystem erweitert wurde um den *Human Factor* besser analysieren zu können. Mit der Tabelle 4.3 der *Performance Shaping Factors* wurden die Operator Tasks dann auf die Auftretenswahrscheinlichkeit der in Tabelle 4.4 definierten Fehlermodi hin analysiert.
• Aktivierung/Wahrnehmung von Feedback
  – Feedback missachtet
  – Feedback nur teilweise wahrgenommen
  – Signal nicht wahrgenommen
  – Signal falsch wahrgenommen
• Verarbeitung und Analyse der Informationen
  – Unzureichende Informationen extrahiert
  – Unwichtige Informationen extrahiert
  – Widersprüchliche Informationen extrahiert
• Identifikation der Systemzustandes
  – Falsche Identifikation der Systemzustandes
  – Unvollständige Identifikation der Systemzustandes
  – Identifikation eines veralteten Systemzustandes
• Interpretation der Situation
  – Falsche Interpretation der Situation
  – Unvollständige Interpretation der Situation
• Definition des erweiterten Ziels
  – Erstrebung eines inkorrekt en Ziels (moralisch, gesetzlich, sozial)
  – Definition eines Unvollständigen Ziels (Teillösung).
  – Widersprüchliche Ziele
• Procedure selection
  – wrong procedure selected,
  – formulation of procedure incomplete (will not fulfill goal).
• Ausführung von Operator Tasks
  – Ausführung zu früh/zu spät
  – Operator Task nicht ausgeführt
  – Ausführung zu viel/wenig
  – Zu lange/curz angewendet
  – In die falsche Richtung ausgeführt
  – Richte Aktion auf falschem Objekt
  – Falsche Aktion auf richtigem Objekt
  – Flache Reihenfolge
• Überprüfung des Ergebnisses
  – Überprüfung ausgelassen
  – Falsche Stelle/Objekt geprüft
  – Falsche Prüfmethode
  – Falsches Timing
  – Keine Informationen erhalten
  – Falsche Informationen erhalten

Tabelle 4.4: Die Tabelle der Fehlermodi die in einem ADS (Automated Driving System) zur Analyse der Operator Tasks berücksichtigt werden müssen entnommen und angepasst aus der Guideline von Rudolph[124]
4.5. Überdeckungsmatrix und Abdeckungsanalyse

In einem ersten Schritt wurde ein Mapping zwischen den in Anhang A und B aufgestellten, Safety Constraints erstellt, in welchem die Beziehungen der Einträge untereinander dargestellt sind.

<table>
<thead>
<tr>
<th></th>
<th>C1</th>
<th>C2</th>
<th>C3</th>
<th>C4</th>
<th>C5</th>
<th>C6</th>
<th>C7</th>
<th>C8</th>
<th>C9</th>
<th>C10</th>
<th>C11</th>
<th>C12</th>
<th>C13</th>
<th>C14</th>
<th>C15</th>
<th>C16</th>
<th>C17</th>
<th>C18</th>
<th>C19</th>
<th>C20</th>
<th>C21</th>
<th>C22</th>
<th>C23</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CS 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CS 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CS 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CS 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CS 6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CS 7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CS 8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Abbildung 4.6.: Überdeckungsmatrix der Safety Constraints (SC) aus der STPA und der Control Strategies (CS) aus der HEA**

Die in Abbildung 4.6 dargestellte Matrix beschreibt die Überdeckung der STPA Safety Constraints (in den Spalten) durch eine oder mehrere Control Strategies (in den Zeilen), aus der HEA, mit den folgenden farblichen Markierungen:

**Weiβ**  Ein weißes Feld bedeutet, dass die Safety Constraints in keinerlei Bezug zueinander stehen  
**Gelb**  Die Control Strategy reglementiert dieselbe Funktion, ist aber ungenauer formuliert als der STPA Safety Constraint  
**Grün**  Die Reglementierungen der Control Strategy und des Safety Constraint sind wirkungsgleich


In der Matrix wurden teilweise mehrere Safety Constraints durch dieselbe Control Strategy abgedeckt. Dabei ist die Überdeckung in diesen Fällen meist ungenau, da die Control Strategies im allgemeinen grober formuliert wurden oder nur eine teilweise Überdeckung des Safety Constraints
4.5. Überdeckungsmatrix und Abdeckungsanalyse

durch die Control Strategy der HEA gegeben ist. Beispielhaft dafür ist das Feld [CS-8, SC1.4], welches die Überdeckung des Safety Constraints 1.4 mit der Control Strategy 8 zeigt:

SC1.4 The AD system must always assume a correct speed according to the traffic regulations and situation

CS-8 The AD vehicle must prevent undesired high/low speed changes


Abbildung 4.7.: Absolute (a) und prozentuale (b) Verteilung der STPA Safety Constraints (in Orange) auf die drei Ebenen der STPA und die Abdeckung der jeweiligen Safety Constraints durch entsprechende Control Strategies der HEA (in Grün)


Abbildung 4.7(a) visualisiert die Verteilung der STPA Safety Constraints auf die in Tabelle 4.5 dargestellten Ebenen, wobei der orangene Balken jeweils die absolute Zahl darstellt und der grüne die Anzahl an Constraints, die inhaltlich von einer Control Strategy in der HEA abgedeckt werden. Durch diese Analyse wird deutlich, dass in der STPA mehr Safety Constraints, deren Inhalt von keiner Control Strategy abgedeckt wird, entdeckt wurden als Safety Constraints, die auch in der
Abbildung 4.8.: Absolute Verteilung der STPA Safety Constraints (in Orange) und der Control Strategies der HEA (in Blau) auf die drei Ebenen der STPA

HEA vertreten sind. Auch zeigt die Verteilung der Abdeckung, die in Abbildung 4.7(b) in Prozent dargestellt ist, dass die Ergebnisse der HEA die größte Abdeckung auf funktionaler und kausaler Ebene haben und die Systemebene nur spärlich abgedeckt wird. Im Vergleich mit Abbildung 4.8 fällt hier auf, dass die absolute Anzahl an Control Strategies der HEA auf Funktions- und Kausalitätsebene deutlich geringer ist, als deren Überdeckung von STPA Safety Constraints (Abdeckung von 16 Safety Constraints durch 10 Control Strategies auf Kausalitätsebene). Durch die Abdeckung mehrerer Safety Constraints bestätigt sich die höhere Allgemeingültigkeit der Control Strategies und damit auch eine genauere Formulierung der STPA Safety Constraints. Dieser Mehrwert der STPA wird noch deutlicher durch die Visualisierung der abgedeckten sicherheitsrelevanten Kategorien eines ADS, welche im nächsten Absatz vorgestellt werden.

In Abbildung 4.9 wurden die Safety Constraints der Übersichtlichkeit wegen in zwanzig Kategorien unterteilt, um die Unterschiede der beiden Analysen noch deutlicher herauszustellen und die gemeinsame Menge an überdeckten Kategorien klar zu betiteln. Die insgesamt zwanzig Kategorien wurden, in Absprache mit Experten von Continental, in fünf Bereiche des Systems aufgestellt:

1. **Einbeziehung äußerer Regularien und Bedingungen**
   Dieser Bereich umfasst die Interaktion des Systems mit der Umwelt, was auch Verkehrsgesetze miteinbezieht. Dies ist damit die Schnittstelle zwischen Maschine und äußeren Faktoren, die beachtet werden muss, um sicherzustellen, dass das Fahrzeug im Stande ist, den Menschen zuverlässig zu unterstützen bzw. die Fahraufgabe auszuführen.

2. **Wartung und Instandhaltung**
4.5. Überdeckungsmatrix und Abdeckungsanalyse

Systemebene Hier werden Safety Constraints, zur Vermeidung oder Mitigation von Hazards auf Systemebene, abgeleitet. In STPA geschieht dies in Schritt 1 der Analyse.


Kausalitätsebene Dies ist der Teil der Analyse, der sich auf die ursächlichen Faktoren bezieht, also die Faktoren die zu den Unsafe Control Actions führen. In STPA wird damit, in Schritt 4, versucht das Auftreten von Causal Factors zu verhindern. Ein Beispiel für diese Ebene wäre eine Ursache für die Lenkbewegung, die z.B. durch die Ablenkung des Fahrers durch einen Passagier hervorgerufen wurde.

Tabelle 4.5.: Die drei Analyseebenen, die in STPA Schritt eins, drei und vier betrachtet werden.

3. Sicherstellung der Rahmenbedingungen und Definitionen
Definitionen wie Funktionsumfang, Operationsmodi und operative Domäne werden durch die Kategorien in diesem Bereich abgedeckt.

4. Kommunikation mit dem Fahrer

5. Übernahme und Steuerung des Fahrzeugs durch den Nutzer
Der letzte Bereich umfasst Kategorien zur Kommunikation des Fahrers mit dem ADS und damit die Schnittstellen des Shell-Modells zwischen Mensch und Hardware sowie Mensch und Software.
4. Evaluation des Mehrwerts von STPA ggü. traditionellen Verfahren

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Thema</th>
<th>HEA</th>
<th>STPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sicherstellung der Einhaltung von Gesetzen</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>Sicherstellung der Kontrollierbarkeit (durch ADS oder Fahrer) des Fahrzeugs</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>Sicherheitsabstand zu Verkehrsteilnehmern/Hindernissen</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>Regeimäßige Instandhaltung des Systems</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>Sicherstellung von Sicherheitskritischen Funktionen</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>6</td>
<td>Automatisierte Funktionskontrolle des Systems</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>Sicherstellung eines &quot;fail operational&quot;</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>Verhinderung von Verlassen des Fahrbereiches</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>9</td>
<td>Verhinderung von undefinierten Zustandsänderungen</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>Verhinderung von illegalen/gefährdenden Interaktionen durch den Nutzer</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>Dynamische Anpassung des Displays</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>12</td>
<td>Feedback durch das AD System</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>13</td>
<td>Benachrichtigung des Fahrers über RTI by the System</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>14</td>
<td>Steuerungseingriffe über das HMI während des Autonomes Fahrers</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>15</td>
<td>Dokumentation der Fahrfunktionen</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>Aufmerksamkeitsüberprüfung</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>17</td>
<td>Mechanismus um versehenheitliche interaktion mit dem &quot;AD Input Device&quot; zu verhindern</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>18</td>
<td>Manuelles Eingreifen durch den Fahrer während AD</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>19</td>
<td>Kontrollübergabe von AD zum Fahrer</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>20</td>
<td>Design des &quot;AD Input Device&quot;</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

| Einbeziehung äußerer Regularien und Bedingungen                      |
| Wartung und Instandhaltung                                           |
| Sicherstellung der Rahmenbedingungen und Definitionen               |
| Kommunikation mit dem Fahrer                                         |
| Übernahme und Steuerung des Fahrzeugs durch den Nutzer              |

Abbildung 4.9.: Themenüberdeckung der Safety Constraints aus der STPA und HEA

Zur weiteren Visualisierung stellt Abbildung 4.10 die Abdeckung der, in Abbildung 4.9 aufgelisteten Kategorien, durch die Ergebnisse der Analysen, dar. Die Graphik zeigt die Abdeckung der oberen 6 Bereiche durch die Ergebnisse der HEA (in orange). Hier fällt auf, dass diese vor allem auf die beiden grün hinterlegten Bereiche des Diagramms (Kategorien 11 - 20), welche die Interaktionen zwischen Fahrer und Fahrzeug beschreiben, beschränkt sind. Diese Beobachtung deckt sich mit der Definition der HEA in Abschnitt 3.1 als steuerungsorientierte Analyse die, ausgehend von konkreten Aufgaben des Fahrers, nach Ursachen für Fehler sucht. Hier ist deutlich zu sehen, dass die STPA fast doppelt so viele sicherheitskritische Bereiche des Systems abdeckt, als die HEA. Bei Analyse der Grafik fällt allerdings auch auf, dass die HEA ein Themengebiet im linken Bereich abdeckt, welches die STPA nicht erreicht. Dies kann allerdings als Ausreißer vernachlässigt werden, da beide Analysen, wie in Abschnitt 4.1.4 beschrieben, auf die, für die Beantwortung der Forschungsfrage notwendige, Tiefe beschränkt wurden, wodurch kleinere Diskrepanzen in den Ergebnissen zu erklären sind.

4.6. Vor- und Nachteile der STPA g gü. traditionellen Methoden

4.6.1. Vorteile der STPA g gü. der HEA

STPA unterstützt eine gesamthetlische Betrachtung des Systems

Bezug zum Gesamtsystem vernachlässigt wird. Dies wird deutlich wenn man Safety Constraints SC0.1 - SC0.9 betrachtet, die in STPA Schritt 1 aufgestellt wurden und die durch die HEA nur teilweise abgedeckt werden (siehe 4.6).

Betrachtung des Regelkreises versus Betrachtung der Steuerung

Ein großer Vorteil der STPA ist die systematische Betrachtung des Regelkreises eines Systems [Lev11], was bedeutet, dass zur Analyse einer einzelnen Mensch-Maschinen Interaktion der gesamte Lebenszyklus der jeweiligen Control Action betrachtet wird. Im Gegensatz dazu beschränkt sich eine HEA auf die direkte Kommunikation zwischen Mensch und Maschine, ohne eine tiefergehende Analyse der beteiligten Komponenten wie Aktuatoren oder Sensoren, vorzunehmen. Durch diesen Ansatz unterstützt STPA den Analysten bei der Erkennung von Hazards im Regelkreis, die durch eine Beschränkung auf die Steuerungsaaktionen rein von dessen Wissen um die Schwachstellen im System abhängig wäre. Beispielhaft ist SC2.16, der die regelmäßige interne Überprüfung der Systemzustandsinformationen fordert, um Verwirrung zu vermeiden. Dieser Safety Constraint bezieht sich auf interne Komponenten, die in einer HEA nicht abgedeckt werden. Des Weiteren werden durch diese Betrachtung, vor allem in komplexen Systemen, Ebenen der Control Structure mit auf die Analyse einbezogen, die nicht direkt durch die Interaktion tangiert werden aber trotzdem zu einem Hazard führen können. In Safety Constraint SC2.40 ist der Fall abgebildet, dass die Anzeigen des Fahrzeuges einwandfrei funktionieren, aber eine Störung in den Sensoren des Fahrzeuges dafür sorgt, dass die angezeigten Informationen veraltet sind oder fehlen.

STPA fordert eine top-down Vorgehensweise durch einen iterativen Prozess


STPA erlaubt die Entwicklung eines sicherheitsgetrieben Designs

Systematische Betrachtung des Human Factors durch die Mental Models


Berücksichtigung des Human Factor in allen Phasen der System Entwicklung


Übersichtlichere Dokumentation und angeleitete Analyse durch größeren Tool Support


Formulierung von präziseren Safety Constraints durch genauere Kontextinformationen


4.6.2. Nachteile der STPA ggü. der HEA

STPA hat aufgrund ihrer Komplexität einen deutlich höheren Zeitbedarf

Aufgrund des system-basierten Ansatzes erfordert STPA deutlich mehr Zeit, sowohl für die Einarbeitung als auch für die Durchführung. Diese These wird gestützt durch die Anzahl an Schlüsselwörtern, die in den jeweiligen Methoden zum Einsatz kommen. Während eine HEA mit lediglich sieben Schlüsselwörtern auskommt, werden von Leveson et. al. [Fra17], [LT18] bereits über zwanzig verschiedene Begriffe für eine STPA aufgeführt. Auch in den Analysen die in Kapitel
4. Evaluation des Mehrwerts von STPA ggü. traditionellen Verfahren

4.3 und 4.4 durchgeführt wurden, konnte dies nachgewiesen werden. Die STPA mit ca. 220 Stunden (20 Stunden x 9 + 40 Stunden x 1) Aufwand bedeutet gegenüber der HEA mit ca. 75 Stunden (15 Stunden x 5) fast den dreifachen Aufwand. Aufgrund der schwierigen Einschätzbarkeit ist die Zeitspanniss, durch die teilweise von Continental vordefinierten Hazards und System Goals, nicht in den angegebenen Zeitaufwand miteinbezogen.

Erhöhte Anforderungen an den Analysten durch Komplexe Modellierung

Wie schon im letzten Punkt erwähnt, bedarf die Analyse mittels STPA sehr viel mehr Einarbeitung und fordert einen wesentlich größeren analytischen Aufwand durch den Analysten. Eine STPA erfordert sowohl die erwähnte Einarbeitung in die Methode, als auch die richtige Definition der nötigen Mental Models sowie der Process Models, die die Grundlage für die Analyse der kausalen Faktoren bilden und deren vollständige, aber auch minimale Definition essentiell für den Wert der Analysergebnisse ist. Dabei bedeutet vollständig und minimal, dass das Modell genau die für die Aufgabe des Controllers nötigen Informationen beinhaltet.

Fehlende Prioritätskennzahlen in STPA


Redundante Safety Constraints durch den iterativen Ansatz der STPA

Der letzte Punkt ist ein weit verbreitetes Problem und hängt auch mit der generellen Usability listenbasiertter Analysen zusammen, weshalb dieser Nachteil teilweise in den Ausblick dieser Arbeit übergeht. Dieser letzte Nachteil der STPA, den aber auch viele traditionelle Verfahren teilen, ist die Gefahr viele Safety Constraints auf verschiedenen Ebenen aufzustellen, die den gleichen Kontext behandeln und somit unnötigen Mehraufwand, durch Ermitteln und Eliminieren unnützer Constrains, bedeuten. Dieses Problem kann mehrere Ursachen haben wie z.B. mangelnde Übersicht über das bisherige Arbeitsprodukt durch den Analysten oder Copy & Paste Fehler (ein
Einmal erstellter Constraint wird mehrfach kopiert), und wird durch den iterativen Ablauf der STPA lediglich verstärkt. Ein Beispiel wäre eine UCA in der STPA, die in der Kausalen Analyse durch mehrere verschiedene Faktoren ausgelöst werden kann, wodurch mehrere ähnliche Szenarien aufgestellt werden, die zu mehreren ähnlichen Safety Constraints führen.

4.7. Validität der Fallstudie

In diesem Abschnitt wird die Glaubwürdigkeit der Arbeit, die Unvoreingenommenheit der Ergebnisse und der Zusammenhang zwischen Forschungsziel und Methode diskutiert. Im Zuge dessen wird im Folgenden auf die interne und externe Validität sowie auf die Validität des Konstruktes und die Zuverlässigkeit eingegangen[Run+12][Yin03].

Validität des Konstruktes


Interne Validität


Externe Validität

Hier wird der Grad, zu welchem die in dieser Arbeit erzielten Ergebnisse, insbesondere ob die Vor und Nachteile verallgemeinerbar sind, diskutiert. Die Allgemeingültigkeit der Ergebnisse wurde sowohl durch Abgleich mit relevanter Literatur, als auch durch Expertengespräche und dem damit
verbundenen Abgleich mit Erfahrungswerten aus der Praxis, sichergestellt. Wie bei der internen Validität schon angesprochen, wurden auch die Analysen so in den Ablauf integriert, dass der Wissensstand den jeweiligen Bedürfnissen für die Analysen entsprach. So wurde die STPA erst zur Etablierung eines Expertenwissens durchgeführt, welches notwendig ist um eine praxisrelevante HEA durchführen zu können.

Zuverlässigkeit

Die Zuverlässigkeit der Studie beschäftigt sich mit der Frage, ob die Fallstudie in dieser Form wiederholt werden kann oder ob die Durchführung vom Autor und Vorwissen abhängig ist. Die einzelnen Schritte sind dafür im Abschnitt 4.1 beschrieben und beide Analysemethoden und deren Durchführung in Kapitel 3 dokumentiert. Dadurch und durch die Auflistung und Erläuterung des, für die Evaluation verwendeten, Kategorienkataloges wurde die Nachvollziehbarkeit der Fallstudie durch die zu Verfügung gestellten Informationen sichergestellt.
5. Zusammenfassung und Schlussfolgerung

In dieser Arbeit wurde eine STPA Guideline für die Human Factor Analyse, eine Aufstellung der Vor- und Nachteile durch den Einsatz von STPA und eine Einschätzung über den Mehrwert der STPA erstellt. Im Zuge der Arbeit wurden hierfür eine STPA und eine HEA eines Beispielsystems durchgeführt. Auf die Validität der Analysen wird in Abschnitt 4.7 zur Validität des Arbeitsproduktes, eingegangen.


Als dritten Beitrag dieser Arbeit, der gleichzeitig als weitere Bewertungsmethode des Mehrwerts dient, wurde eine Liste von Vor- und Nachteilen durch den Einsatz von STPA aufgestellt.

5.1. Schlussfolgerung


Abschließend ist die Komplexität und Zeitintensität einer vollständigen STPA noch abzuwägen gegen die notwendigen Anpassungen traditioneller Methoden und deren Aufbau als Expertenanalyse, die auf Erfahrung mit dem zu analysierenden System setzt.
5. Zusammenfassung und Schlussfolgerung

5.2. Ausblick


A. STPA eines zukünftigen Systems zum automatisierten Fahren
# Human Factor Analysis of an ADS

<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>Human Factor Analysis of an ADS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Date and Time</strong></td>
<td>13.10.2018, 10:21:26</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>The scope of this project is the development of the automated driving feature aiming to cover SAEJ3016 level 4 - high automation. V_max = maximum speed defined for automated driving. DDT - Dynamic Driving Task. TPO - Traffic Participant Object. MRM - Minimum Risk Maneuver. MRE - Minimal Risk Environment. MRC - Minimal Risk Condition. RTI - Request to intervene. ADS - Automated Driving System.</td>
</tr>
</tbody>
</table>

### Description of the System Components

- **Driver**: The Human performing the driving task and is responsible for interacting with the ADS in AD mode as well as with the vehicle’s actuators when in manual mode.
- **Mission**: The mission goal defines the current navigation target and how to accomplish it. The ADS should always try to find a route to and reach the mission goal.
- **Mission Controller**: The Mission Controller is a Human Controller responsible for defining and handling the Mission.
- **HMI**: The interface between the Human Controller and the ADS, this can be a part of the ADS but is here modeled as Independent part to highlight the role of the hmi in the system as an individual component for Design considerations and functional requirements towards the human-machine interactions.
- **ADS**: The automated Controller that is responsible for translating the requests issued by a human Controller over the HMI to the actuators of the vehicle.
- **AD Vehicle**: The physical vehicle which is the target process of the HMI inputs.
## Accidents

<table>
<thead>
<tr>
<th>ID</th>
<th>Title</th>
<th>Description</th>
<th>SEV*</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>A-1</td>
<td>Loss of or serious damage to human live</td>
<td>People die/are harmed by a collision of ego vehicle with other (non over-drivable) objects</td>
<td>S3</td>
<td>H-1, H-11</td>
</tr>
<tr>
<td>A-2</td>
<td>Damage to ego or other vehicle/ the environment</td>
<td>Damage to Ego or other vehicle/ the environment</td>
<td>S2</td>
<td>H-3, H-1, H-9, H-10, H-11</td>
</tr>
<tr>
<td>A-3</td>
<td>mission loss</td>
<td>The AD vehicle fails in executing the mission (correctly) and drives to an undefined/-desired location</td>
<td>S1</td>
<td>H-3, H-1, H-8</td>
</tr>
<tr>
<td>A-4</td>
<td>impairment of traffic participants/other AD vehicles</td>
<td>impairment of traffic participants/other AD vehicles</td>
<td>S2</td>
<td>H-1, H-3, H-10, H-7, H-11</td>
</tr>
<tr>
<td>ID</td>
<td>Title</td>
<td>Description</td>
<td>SEV*</td>
<td>Links</td>
</tr>
<tr>
<td>----</td>
<td>----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>H-1</td>
<td>The AD vehicle cannot be controlled</td>
<td>The AD Vehicle is operated uncontrolled by the ADS or the Driver which means that state changes can’t be anticipated. This hazard differs to H-12 by the fact that this refers to a malfunction of the vehicle controls where no manual interventions are possible while H-12 refers to a situation where the vehicle is physically uncontrollable.</td>
<td>S3</td>
<td>A-1, A-2, A-4, A-3, SC0.1</td>
</tr>
<tr>
<td>H-3</td>
<td>Driver has hands off controls when AD is not active</td>
<td>The Driver does not take control over the driving task while the AD Vehicle is driving and the ADS is not active, this hazard can refer to an inconsistency between the Drivers assumption over the current state of the ADS and the actual state.</td>
<td>S2</td>
<td>A-3, A-2, A-4, SC0.3</td>
</tr>
<tr>
<td>H-7</td>
<td>Violation of Traffic laws</td>
<td>The ego vehicle applies one of the following: - unexpected braking - unexpected acceleration - unexpected steering</td>
<td>S2</td>
<td>A-4, SC0.4</td>
</tr>
<tr>
<td>H-8</td>
<td>The AD vehicle doesn’t follow the mission goal</td>
<td>If the ADS is in AD mode but for some reason doesn’t follow the intendent mission goal of the driver because of either internal or external factors.</td>
<td>S1</td>
<td>A-3, SC0.5</td>
</tr>
<tr>
<td>H-9</td>
<td>The AD vehicle violates the safe distance to TPOs</td>
<td>The AD Vehicle violates the safe distance by driving to close to a TPO in the path of the vehicle, this can the case for TPOs in front or behind the vehicle. The safe distance is regulated in the traffic laws and depends on the speed of the vehicle and on environmental factors like fog or snow.</td>
<td>S2</td>
<td>A-2, SC0.6</td>
</tr>
<tr>
<td>H-10</td>
<td>The AD vehicle is in AD mode while in an unpredicted/undefined Situation</td>
<td>The AD mode of a SEA Level 4 automation is defined for a range of different driving situations in which the AD functions are available and safety critical functions can be fulfilled by the System. However if in any other situation the AD mode must be deactivated with a respective RTI to the driver.</td>
<td>S3</td>
<td>A-2, A-4, SC0.7, SC0.2</td>
</tr>
<tr>
<td>H-11</td>
<td>The AD vehicle violates the driving scope</td>
<td>This refers to the situation where the defined driving scope, meaning the drive way, the route defined by the mission goal or the legal scope for AD is left.</td>
<td>S2</td>
<td>A-2, A-1, A-4, SC0.8</td>
</tr>
<tr>
<td>H-12</td>
<td>The AD vehicle looses traction or is physically uncontrollable</td>
<td>If the vehicle looses traction due to longitudinal/lateral forces. E.g. when the driver over steers and the wheels lose traction, or when the vehicle is too fast for the driving scenario.</td>
<td>S3</td>
<td>SC0.9</td>
</tr>
<tr>
<td>ID</td>
<td>Safety Constraint</td>
<td>Description</td>
<td>Links</td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td></td>
</tr>
<tr>
<td>SC0.1</td>
<td>The ADS must always be controllable through manual intervention</td>
<td>The ADS must always yield before manual intervention through the Driver</td>
<td>H-1, DR0.6</td>
<td></td>
</tr>
<tr>
<td>SC0.2</td>
<td>The ADS must implement a fail operational when the driver does not take over</td>
<td>The AD vehicle should according to the requirements of a level 4 automated driving system implement a automatism to cope with a situation where a RTI (Request to intervene) was send but not followed by the driver.</td>
<td>H-10, DR0.5</td>
<td></td>
</tr>
<tr>
<td>SC0.3</td>
<td>The Driver must never take hands off controls when AD is not available</td>
<td>The ADS must always ensure that the Driver has his hands and feet on the controls when the ADS is not available</td>
<td>H-3, DR0.3, DR0.8</td>
<td></td>
</tr>
<tr>
<td>SC0.4</td>
<td>The ADS must always heed the current traffic laws</td>
<td></td>
<td>H-7, DR0.2, DR0.9</td>
<td></td>
</tr>
<tr>
<td>SC0.5</td>
<td>The ADS must always act based on the driving mission defined by the Mission Controller when in AD mode</td>
<td>When the ADS is in a safe scenario than every decision made by the ADS (Lane Change, Speed, Highway Exit etc.) must be based on the navigation mission in order to be able to ultimately fulfill it.</td>
<td>H-8, DR0.7, DR0.8</td>
<td></td>
</tr>
<tr>
<td>SC0.6</td>
<td>The ADS must always keep the safe distance to TPOs</td>
<td></td>
<td>H-9, DR0.1</td>
<td></td>
</tr>
<tr>
<td>SC0.7</td>
<td>The ADS must always notify the driver in time before a shut down</td>
<td>The Driver must always be notified timely in order to enable a manual intervention before a shut down is executed.</td>
<td>H-10, DR0.4</td>
<td></td>
</tr>
<tr>
<td>SC0.8</td>
<td>The ADS mustn't violate the driving scope</td>
<td>The ADS must always ensure that the vehicle stays on the road and does not violate any road markings like solid lines, arrows etc.</td>
<td>H-11, DR0.2</td>
<td></td>
</tr>
<tr>
<td>SC0.9</td>
<td>The ADS must minimize the risk of loosing the control over the vehicle</td>
<td></td>
<td>H-12</td>
<td></td>
</tr>
</tbody>
</table>
## System Goals

<table>
<thead>
<tr>
<th>No.</th>
<th>System Goal</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SG-1</td>
<td>Perform Lane Change</td>
<td>The System should provide means to perform an automated Lane Change, while considering all safety critical variables (distance to TPOs, traffic, speed, lateral-/longitudinal forces on the vehicle). Moreover this requirement is directly related to SG-11 Cancel Lane Change due to the requirement that the driver should be able to cancel a lane change if possible by means of safety.</td>
</tr>
<tr>
<td>SG-2</td>
<td>Perform Lane Keeping</td>
<td>When engaged the ADS should always be able to keep the lane it is currently driving on by itself when in a defined driving situation.</td>
</tr>
<tr>
<td>SG-10</td>
<td>Switch between automated- and manual driving mode</td>
<td>The Driver should be able to switch between manual driving and automated driving</td>
</tr>
<tr>
<td>SG-11</td>
<td>Cancel Lane Change</td>
<td>The driver should be able to cancel a lane change if possible by means of safety. This goal is not limited to lane changes that have been requested by the driver but extends also to lane changes initiated by the ADS.</td>
</tr>
<tr>
<td>SG-13</td>
<td>Set Speed</td>
<td>The driver can request a speed change while in automated driving mode between 0 - 120 km/h (ACC limit)</td>
</tr>
<tr>
<td>SG-14</td>
<td>Fail Operational</td>
<td>The ADS should always ensure reaching an MRC before shutting down.</td>
</tr>
</tbody>
</table>
# Design Requirements

<table>
<thead>
<tr>
<th>No.</th>
<th>Design Requirement</th>
<th>Description</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>DR0.1</td>
<td>Collision avoidance</td>
<td>Safety critical feature of Cruising Chauffeur through which an imminent collision is avoided.</td>
<td>SC0.6</td>
</tr>
<tr>
<td>DR0.2</td>
<td>System- &amp; Geo-fencing</td>
<td>The system shall implement a mechanism to ensure that the vehicle stays in the defined geographical limits as well as the one's dictated for the ADS itself</td>
<td>SC0.4, SC0.8</td>
</tr>
<tr>
<td>DR0.3</td>
<td>User Monitoring</td>
<td>The system should always ensure that the user is capable of taking over control before handing it over</td>
<td>SC0.3</td>
</tr>
<tr>
<td>DR0.4</td>
<td>Request-to-intervene</td>
<td>A notification send by the ADS prior to a situation in which the AD functions become unavailable</td>
<td>SC0.7</td>
</tr>
<tr>
<td>DR0.5</td>
<td>Minimal Risk Maneuver</td>
<td>Safety critical feature of Cruising Chauffeur that brings the ego vehicle in a Minimum Risk Condition in presence of system malfunctions, system limitations or unavailability of user/driver.</td>
<td>SC0.2</td>
</tr>
<tr>
<td>DR0.6</td>
<td>Driver override</td>
<td>The driver is able to intervene in the AD at any time during a normal driving situation</td>
<td>SC0.1</td>
</tr>
<tr>
<td>DR0.7</td>
<td>Mission check before activation</td>
<td></td>
<td>SC0.5</td>
</tr>
<tr>
<td>DR0.8</td>
<td>The ADS must always provide information about its state</td>
<td>The driver is able to intervene in the AD at any time during a normal driving situation</td>
<td>SC0.3, SC0.5</td>
</tr>
<tr>
<td>DR0.9</td>
<td>The ADS shall always be aware of the traffic laws</td>
<td></td>
<td>SC0.4</td>
</tr>
<tr>
<td>DR0.10</td>
<td>EgoVehicleMotionSensor</td>
<td>The current state of vehicle's motion is monitored by the EgoVehicleMotionSensor. This Sensor is responsible for acquiring the current Speed and Orientation of the vehicle.</td>
<td>SC0.5</td>
</tr>
<tr>
<td>DR0.11</td>
<td>EgoVehicleEnvSensor</td>
<td>This sensor collects information about the environment of the vehicle acquired data include: - Distance to TPOs - weather data (temperature, precipitation, etc.) - Road conditions (wet, ice, etc.) - etc.</td>
<td>SC0.4</td>
</tr>
<tr>
<td>DR0.12</td>
<td>EgoVehicleNavigator&amp;Mission</td>
<td>The sensor for navigation and Mission keeps track of the GPS data of the vehicle, and data about the traffic situation transmitted over satellite/RDS and allows the ADS to keep track of the current state of the mission.</td>
<td>SC0.5</td>
</tr>
<tr>
<td>DR0.13</td>
<td>HMI Feedback Component for providing sufficient Feedback over the DDT</td>
<td>The HMI Feedback Component is a composite component of all components of the vehicle that are utilized by the HMI to provide the Feedback of the current System state gathered from the Vehicle Sensors to the Human Controllers. By design this component provides feedback over multiple channels and is composed of a Display, a unit for providing haptic feedback (vibrating seat) and a verbal feedback system.</td>
<td>SC0.5</td>
</tr>
<tr>
<td>DR0.14</td>
<td>Longitudinal actuation</td>
<td>Acceleration in Longitudinal direction is the main acceleration of the vehicle responsible for actuating the DDT</td>
<td>SC0.5</td>
</tr>
<tr>
<td>DR0.15</td>
<td>Lateral actuation</td>
<td>Responsible for maintaining stability of the vehicle and counter lateral forces like g-forces, wind etc.</td>
<td>SC0.5</td>
</tr>
<tr>
<td>DR0.16</td>
<td>Conspicuity actuation</td>
<td></td>
<td>SC0.5</td>
</tr>
<tr>
<td>DR0.17</td>
<td>Driver Sensors</td>
<td>The Sensors responsible for monitoring the Driver this includes a Sensor for the Pedals (Brake-, Gas-Pedal), for the steering wheel and for monitoring the Driver's head position these sensors are responsible for transmitting the Driver's ability to take-over the vehicle controls when switching from AD mode to manual and for monitoring the Driver's attention. In the control structure of this system the driver sensors act as an actuator since they are responsible for transmitting the ability to take-over to the HMI and thus actuate the switch to manual control.</td>
<td>SC0.5</td>
</tr>
<tr>
<td>DR0.18</td>
<td>Input Panel</td>
<td>The Panel where buttons for various vehicle functions are located including the button for turning on/off the ADS and a button for (de-)activating the AD mode</td>
<td>SC0.5</td>
</tr>
<tr>
<td>DR0.19</td>
<td>AD Input Device</td>
<td>The AD input device is designed as a joystick that can be moved on 3 axis (x,y,z) to issue set speed and lane change requests as well as navigate the GUI of the system</td>
<td>SC0.5</td>
</tr>
</tbody>
</table>
## Control Actions

<table>
<thead>
<tr>
<th>Id</th>
<th>Control Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA-4</td>
<td>Set Speed</td>
<td>To request a speed change while in AD mode the driver has to push the AD input device forward or backward to request an increase or decrease in speed. The Set Speed which is limited to $V_{\text{max}}$ (see system description) is stored in the AD Controller and than applied when possible. The difference between this CA and CA-10: Accelerate is that the set speed command is that the request is issued over the AD input device and than processed directly by the HMI and applied only if suitable. The Set Speed CA is the preferred method to change speed while in AD mode.</td>
</tr>
<tr>
<td>CA-5</td>
<td>Lane Change Request</td>
<td>Lane Change can be requested by pulling the AD Input device to the left (change to left lane) or the right (change to right lane), this action can be canceled by pulling/pushing the input device or pulling it in the other direction. The request is either executed immediately if possible or canceled by the system.</td>
</tr>
<tr>
<td>CA-9</td>
<td>Steering</td>
<td>This CA describes a normal rotation of the steering wheel to steer the vehicle to the left/right. When executed in manual mode this CA will perform as expected. In AD mode this is treated as an intervention by the driver which will lead to an RTI issued by the ADS except when the the steering input is smaller than a defined threshold and the indicators are not ignited.</td>
</tr>
</tbody>
</table>
## Unsafe Control Actions

<table>
<thead>
<tr>
<th>Control Action</th>
<th>Not providing causes hazard</th>
<th>Providing causes hazard</th>
<th>Wrong timing or order causes hazard</th>
<th>Stopped too soon or applied too long</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Set Speed</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UCA1.4</td>
<td>S2</td>
<td>UCA1.5</td>
<td>S3</td>
<td>S2</td>
</tr>
<tr>
<td>The Driver does not provide the Set Speed command while driving too fast when it's raining</td>
<td>[H-7]</td>
<td>The Driver provides the Set Speed command with a value above the speed limit while in normal traffic</td>
<td>[H-7, H-11, H-12]</td>
<td>The Driver provides the Set Speed command to reduce speed when driving in a steep curve only when already in the curve</td>
</tr>
<tr>
<td>UCA1.6</td>
<td></td>
<td>UCA1.67</td>
<td>S3</td>
<td></td>
</tr>
<tr>
<td>The Driver provides the Set Speed command during a lane change</td>
<td>[H-11, H-12]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Lane Change Request</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UCA1.13</td>
<td>S0</td>
<td>UCA1.18</td>
<td>S1</td>
<td>S2</td>
</tr>
<tr>
<td>The default lane change behavior of the ADS is assumed not be hazardous in the STPA</td>
<td>[Not Hazardous]</td>
<td>The Driver performs a Lane Change Request to an undesired lane</td>
<td>[H-8]</td>
<td>The Driver performs a Lane Change Request when not longer possible due to lane restrictions, traffic etc.</td>
</tr>
<tr>
<td>UCA1.19</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Driver performs a Lane Change Request that is not allowed</td>
<td>[H-7]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Steering</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UCA1.30</td>
<td>S3</td>
<td>UCA1.31</td>
<td>S2</td>
<td>S2</td>
</tr>
<tr>
<td>The Driver doesn't provide Steering when AD mode is being deactivated and steering is required</td>
<td>[H-7, H-11]</td>
<td>The Driver provides Steering in an illegal direction (Scope violating) while in AD mode</td>
<td>[H-7, H-11]</td>
<td>The Driver provides Steering while in AD mode and next to an exit just too short before or after missing the exit</td>
</tr>
<tr>
<td>UCA1.65</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Driver provides Steering too long (over steers) while in AD mode</td>
<td>[H-7, H-9]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Severity*
## Corresponding Safety Constraints

<table>
<thead>
<tr>
<th>ID</th>
<th>Unsafe Control Actions</th>
<th>ID</th>
<th>Corresponding Safety Constraints</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCA1.4</td>
<td>The Driver does not provide the Set Speed command while driving too fast when it's raining</td>
<td>SC1.4</td>
<td>The ADS must always assume a correct speed according to the traffic regulations and situation</td>
<td></td>
</tr>
<tr>
<td>UCA1.5</td>
<td>The Driver provides the Set Speed command with a value above the speed limit while in normal traffic</td>
<td>SC1.5</td>
<td>The ADS must always ask for confirmation of inputs from the AD Input Device</td>
<td></td>
</tr>
<tr>
<td>UCA1.6</td>
<td>The Driver provides the Set Speed command to reduce speed when driving in a steep curve only when already in the curve</td>
<td>SC1.6</td>
<td></td>
<td>SC1.4</td>
</tr>
<tr>
<td>UCA1.67</td>
<td>The Driver provides the Set Speed command during a lane change</td>
<td>SC1.67</td>
<td>The ADS must prevent speed changes through the Driver during lane changes</td>
<td></td>
</tr>
<tr>
<td>UCA1.18</td>
<td>The Driver performs a Lane Change Request to an undesired lane</td>
<td>SC1.18</td>
<td>In case the Driver issued a lane change the ADS must always ask for a confirmation by the Driver before initializing a lane change.</td>
<td></td>
</tr>
<tr>
<td>UCA1.19</td>
<td>The Driver performs a Lane Change Request that is not allowed</td>
<td>SC1.19</td>
<td>The ADS must always check the legality of the Driver requests issued over the AD Input Device and give detailed feedback about illegal requests.</td>
<td></td>
</tr>
<tr>
<td>UCA1.21</td>
<td>The Driver performs a Lane Change Request when not longer possible due to lane restrictions, traffic etc.</td>
<td>SC1.21</td>
<td></td>
<td>SC1.19</td>
</tr>
<tr>
<td>UCA1.30</td>
<td>The Driver doesn’t provide Steering when AD mode is being deactivated and steering is required</td>
<td>SC1.30</td>
<td>The ADS must always ensure that the Driver has completely taken over the controls before shut down.</td>
<td></td>
</tr>
<tr>
<td>UCA1.31</td>
<td>The Driver provides Steering in an illegal direction (Scope violating ) while in AD mode</td>
<td>SC1.31</td>
<td>The ADS must warn the Driver vigorously about all violations of the driving scope</td>
<td></td>
</tr>
<tr>
<td>UCA1.32</td>
<td>The Driver provides Steering while in AD mode and next to an exit just too short before or after missing the exit</td>
<td>SC1.32</td>
<td>While in AD mode the ADS must prevent any manual input leading to any of the defined Hazards and give strong feedback on multiple channels</td>
<td></td>
</tr>
<tr>
<td>UCA1.65</td>
<td>The Driver provides Steering too long (over steers) while in AD mode</td>
<td>SC1.65</td>
<td></td>
<td>SC1.32</td>
</tr>
</tbody>
</table>
## Causal Factors Table

<table>
<thead>
<tr>
<th>Component</th>
<th>Causal Factor</th>
<th>Unsafe Control Action</th>
<th>Hazard Links</th>
<th>Safety Constraint</th>
<th>Design hints</th>
<th>Links</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Driver [Human Controller]</td>
<td>Driver issues a set speed command based on experience without considering dynamic factors like wet road or sudden traffic changes</td>
<td>UCA1.5 The Driver provides the Set Speed command with a value above the speed limit while in normal traffic</td>
<td>H-7, H-11, H-12</td>
<td>The ADS must always check requested speed changes are potentially hazardous in the current driving situation and prevent them if necessary</td>
<td>The ADS must monitor its environment through utilization of the vehicles environment sensors (traction, TPOs etc.) and could simulate possible driving speeds before adapting them</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Driver increases the speed over a safe limit due to a false estimation of for the current driving situation</td>
<td>UCA1.6 The Driver provides the Set Speed command to reduce speed when driving in a steep curve only when already in the curve</td>
<td>H-11</td>
<td>The ADS must always check requested speed changes are potentially hazardous in the current driving situation and prevent them if necessary</td>
<td>The AD vehicle should define a dynamic speed limit for the current driving situation based on the environmental conditions</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Driver doesn't recognize the current need for an adaptation of the speed due to lack of oversight over the situation or low attention</td>
<td>UCA1.4 The Driver does not provide the Set Speed command while driving too fast when it's raining</td>
<td>H-7</td>
<td>The ADS mustn't rely on the driver to execute any safety critical functions while in AD mode</td>
<td>The AD should implement all safety critical functions and always ensure a MRC when no driver input is given after an RTI</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Driver issues a set speed request with a too high value due too lack of experience with the system</td>
<td>UCA1.5 The Driver provides the Set Speed command with a value above the speed limit while in normal traffic</td>
<td>H-7, H-11, H-12</td>
<td>The ADS must provide a documentation or tutorial to allow the Driver to familiarize learn the AD vehicle controls in a safe environment</td>
<td>The ADS could implement a tutorial or walk through of the AD functions</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Driver requests a very low speed due to a lack of trust in the system</td>
<td>UCA1.5 The Driver provides the Set Speed command with a value above the speed limit while in normal traffic</td>
<td>H-7, H-11, H-12</td>
<td>The ADS must always provide Feedback about its state, the driving mode and the actions planned by the system</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Driver requests a speed change due to high traffic on the target lane instead of canceling the lane change</td>
<td>UCA1.67 The Driver provides the Set Speed command during a lane change</td>
<td>H-12, H-11</td>
<td>When a speed change is requested during a lane change the ADS should ask the Driver to cancel a lane</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Causal Factor</td>
<td>Unsafe Control Action</td>
<td>Hazard Links</td>
<td>Safety Constraint</td>
<td>Design hints</td>
<td>Links</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td></td>
<td>The Driver requests a speed change due to a confusion about the initialization of a lane change</td>
<td>UCA1.67 The Driver provides the Set Speed command during a lane change</td>
<td>H-12, H-11</td>
<td>When a speed change is requested during a lane change the ADS should ask the Driver to cancel a lane change instead of changing the speed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Driver accidentally issues a lane change request while not paying attention to the driving situation</td>
<td>UCA1.18 The Driver performs a Lane Change Request to an undesired lane</td>
<td>H-8</td>
<td>Before accepting requests issued by the Driver in AD mode over the AD input device the ADS must check the drivers attention to the driving situation</td>
<td>The ADS could use the Driver Sensor to check the head position of the Driver and reject any requests when the head is not facing the road</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Driver issues an incorrect lane change due to a wrong handling of the AD input device</td>
<td>UCA1.18 The Driver performs a Lane Change Request to an undesired lane</td>
<td>H-8</td>
<td>The ADS must provide a documentation or tutorial to allow the Driver to familiarize learn the AD vehicle controls in a safe environment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Driver issues a lane change to an undesired lane in an attempt to cancel a previous lane change</td>
<td>UCA1.18 The Driver performs a Lane Change Request to an undesired lane</td>
<td>H-8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Driver doesn't see that the lanes are separated by a solid line</td>
<td>UCA1.19 The Driver performs a Lane Change Request that is not allowed</td>
<td>H-7</td>
<td>The ADS must check the legality of lane changes before executing them and notify the Driver about any traffic violations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Driver doesn't provide Steering when the AD mode is deactivated due to misjudgment of the road conditions (the car is stabilizing the car in AD mode, and it suddenly breaks out when the AD mode is deactivated)</td>
<td>UCA1.30 The Driver doesn't provide Steering when AD mode is being deactivated and steering is required</td>
<td>H-7, H-11</td>
<td>The ADS must always ensure that the Driver is aware of the driving situation before a hand-over to ensure a smooth take-over without breaking out or sudden peaks/drops in speed</td>
<td>The ADS could implement a hand-over phase in which the manual controls must be supported by the AD controller to ensure a smooth take-over</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Causal Factor</td>
<td>Unsafe Control Action</td>
<td>Hazard Links</td>
<td>Safety Constraint</td>
<td>Design hints</td>
<td>Links</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>--------------</td>
<td>------------------</td>
<td>-------------</td>
<td>-------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>The Driver doesn't provide steering due to wrong expectations from the ADS (expectation to support the manual controls)</td>
<td>UCA1.30 The Driver doesn't provide steering when AD mode is being deactivated and steering is required</td>
<td>H-7, H-11</td>
<td>The ADS must always provide clear and minimal feedback about the current state and instructions to the Driver to prevent redundant information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Driver provides steering in an illegal direction to counter a lane change to an undesired lane</td>
<td>UCA1.31 The Driver provides Steering in an illegal direction (Scope violating ) while in AD mode</td>
<td>H-7, H-11</td>
<td>The ADS must always prevent hazardous manual interventions that could potentially lead to a severe accident</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Driver provides steering too late due to a wrong perception of the driving speed</td>
<td>UCA1.32 The Driver provides Steering while in AD mode and next to an exit just too short before or after missing the exit</td>
<td>H-7, H-11</td>
<td>The ADS must always prevent hazardous manual interventions that could potentially lead to a severe accident</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Driver provides steering too long due to a wrong expectation of the steering effect</td>
<td>UCA1.65 The Driver provides Steering too long (over steers) while in AD mode</td>
<td>H-7, H-9</td>
<td>The ADS must always ensure that the Driver is aware of the driving situation before a hand-over to ensure a smooth take-over without breaking out or sudden peaks/drops in speed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Driver performs a Lane Change Request when not possible due to low attention to the driving situation</td>
<td>UCA1.21 The Driver performs a Lane Change Request when not longer possible due to lane restrictions, traffic etc.</td>
<td>H-7</td>
<td>The ADS must always check the legality of the Driver requests issued over the AD Input Device and give detailed Feedback about illegal requests.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Driver doesn't recognize that an obstacle or a solid line due to distraction by his environment</td>
<td>UCA1.31 The Driver provides Steering in an illegal direction (Scope violating ) while in AD mode</td>
<td>H-7, H-11</td>
<td>The ADS must always prevent hazardous manual interventions that could potentially lead to a severe accident</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Causal Factor</td>
<td>Unsafe Control Action</td>
<td>Hazard</td>
<td>Safety Constraint</td>
<td>Design hints</td>
<td>Links</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------</td>
<td>-----------------------</td>
<td>--------</td>
<td>------------------</td>
<td>--------------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td></td>
<td>The Driver doesn't react correctly due to time pressure created by a dense traffic situation in which he needs to react quick</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>The Driver doesn't react as required by the whether conditions like heavy snow or slippery drive way due to rain</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

**HMI Feedback (DR0.13)**

<table>
<thead>
<tr>
<th>Component</th>
<th>Causal Factor</th>
<th>Unsafe Control Action</th>
<th>Hazard</th>
<th>Safety Constraint</th>
<th>Design hints</th>
<th>Links</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The Driver receives incorrect feedback of the state of the ADS from the Display</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>The Driver is not able to receive the feedback due to bad readability of the display caused by direct sunlight</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>The Driver is not able to receive the feedback due to bad readability of the display caused by bad road conditions (Display is shaking on bumpy road)</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>The Driver provides the set speed command with an incorrect value due to a wrong feedback provided on the Display</td>
<td>UCA1.5 The Driver provides the Set Speed command with a value above the speed limit while in normal traffic</td>
<td>H-7, H-11, H-12</td>
<td>The HMI should always double-check its internal Model of the ADS with the actual state of the ADS and correct wrong entries</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>The Driver provides the Set Speed command too late due to a delayed feedback on the display</td>
<td>UCA1.6 The Driver provides the Set Speed command to reduce speed when driving in a steep curve only when already in the curve</td>
<td>H-11</td>
<td>The Display must be regularly maintained and checked for the required functional requirements</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>The Driver provides the Set Speed command too late due to bad readability of the Display</td>
<td>UCA1.6 The Driver provides the Set Speed command to reduce speed when driving in a steep curve only when already in the curve</td>
<td>H-11</td>
<td>The visual parameters (brightness, color, contrast) of the Display must be adjustable to fit the driving</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Component</td>
<td>Causal Factor</td>
<td>Unsafe Control Action</td>
<td>Hazard Links</td>
<td>Safety Constraint</td>
<td>Design hints</td>
<td>Links</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
<td>--------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td></td>
<td>The Driver tries to cancel a Lane Change but accidentally executes an other Lane Change due to a Missing Feedback that the Lane Change has already been canceled</td>
<td>UCA1.18 The Driver performs a Lane Change Request to an undesired lane</td>
<td>H-8</td>
<td>The ADS should always provide Feedback over redundant channels to prevent information loss</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Driver doesn’t receive the feedback about the legality of his request due to an occupied display</td>
<td>UCA1.19 The Driver performs a Lane Change Request that is not allowed</td>
<td>H-7</td>
<td>The display of the HMI must always show the most recent and important information and should never omit feedback due to pending information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Driver doesn’t provide steering because of wrong feedback on the Display about the AD mode</td>
<td>UCA1.30 The Driver doesn’t provide steering when AD mode is being deactivated and steering is required</td>
<td>H-7, H-11</td>
<td>The HMI should always double-check its internal Model of the ADS with the actual state of the ADS and correct wrong entries</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Driver doesn’t provide Steering because of missing feedback due to an error in the HMI Feedback</td>
<td>UCA1.30 The Driver doesn’t provide Steering when AD mode is being deactivated and steering is required</td>
<td>H-7, H-11</td>
<td>The HMI must always ensure that incase of a malfunction in the Feedback system (no Display, Haptic Feedback) the other Feedback channels can compensate the loss or if an immediate MRM is required.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HMI</td>
<td>The HMI doesn’t send the ADS state to the Display</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AD Input Device</td>
<td>The Driver rests his hand on the AD input device and accidentally provides Input</td>
<td>UCA1.5 The Driver provides the Set Speed command with a value above the speed limit while in normal traffic</td>
<td>H-7, H-11, H-12</td>
<td>The AD input Device must not react to inputs (pulls/pushes) below a (user-)defined threshold to prevent accidental interactions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Component</td>
<td>Causal Factor</td>
<td>Unsafe Control Action</td>
<td>Hazard Links</td>
<td>Safety Constraint</td>
<td>Design hints</td>
<td>Notes</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The AD input device misinterprets the input due to wrong software/</td>
<td>UCA1.5 The Driver provides the Set Speed command with a value above the speed limit</td>
<td>H-7, H-11,</td>
<td>The AD input Device must be maintained regularly to prevent malfunction</td>
<td>The ADS could implement a self-check that regularly checks the controls hard-</td>
<td>The ADS should always provide Feedback over redundant channels to prevent information loss</td>
<td></td>
</tr>
<tr>
<td></td>
<td>calibration</td>
<td>while in normal traffic</td>
<td>H-12</td>
<td></td>
<td>and software</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The AD input device delays the execution of the Set Speed command due to an</td>
<td>UCA1.6 The Driver provides the Set Speed command to reduce speed when driving in a</td>
<td>H-11</td>
<td>The ADS must monitor the vehicle controls and send an RTI or perform an automatic</td>
<td>The ADS should always warn the Driver about hazardous road conditions like wet</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>internal error</td>
<td>steep curve only when already in the curve</td>
<td></td>
<td>MRM if the controls do not function as expected</td>
<td>or snowy</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The AD input device issues a speed change as a result of a misinterpretation</td>
<td>UCA1.67 The Driver provides the Set Speed command during a lane change</td>
<td>H-12, H-11</td>
<td>The AD input Device must be maintained regularly to prevent malfunction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>of another command</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Driver tries to cancel a Lane Change but accidentally executes another</td>
<td>UCA1.18 The Driver performs a Lane Change Request to an undesired lane</td>
<td>H-8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lane Change due to a Missing Feedback that the Lane Change has already been</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>canceled</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Set Speed CA is not executed due to a malfunction of the AD Input Device</td>
<td>UCA1.4 The Driver does not provide the Set Speed command while driving too fast when</td>
<td>H-7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>it’s raining</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Driver doesn’t execute the Set Speed CA due to a false perception of the</td>
<td>UCA1.4 The Driver does not provide the Set Speed command while driving too fast when</td>
<td>H-7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>road conditions</td>
<td>it’s raining</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The AD Input Device issues a speed change due to a false input signal when</td>
<td>UCA1.67 The Driver provides the Set Speed command during a lane change</td>
<td>H-12, H-11</td>
<td></td>
<td></td>
<td>The attention of the Driver must be checked by the Driver Sensors before accepting any CAs from over the AD Input Device</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the Driver is not giving any input</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Driver issues the Lane Change accidentally by pushing the AD Input Device</td>
<td>UCA1.18 The Driver performs a Lane Change Request to an undesired lane</td>
<td>H-8</td>
<td></td>
<td>Before accepting requests issued by the Driver in AD mode over the AD input</td>
<td>The ADS should always warn the Driver about hazardous road conditions like wet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>while not paying attention to the driving task</td>
<td></td>
<td></td>
<td></td>
<td>device the ADS must check</td>
<td>or snowy</td>
<td></td>
</tr>
</tbody>
</table>

Created with A-STPA 3.1.0
<table>
<thead>
<tr>
<th>Component</th>
<th>Causal Factor</th>
<th>Unsafe Control Action</th>
<th>Hazard Links</th>
<th>Safety Constraint</th>
<th>Design hints</th>
<th>Links</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The ADS falsely assumes that the driver is paying attention to the DDT and</td>
<td>the ADS performs a Lane Change Request to an undesired lane</td>
<td>H-8</td>
<td>The ADS must check the attention of the Driver with multiple/redundant Sensors and terminate the AD mode immediately if the Sensors become unavailable or provide inconsistent information</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>executes a accidentally provided Lane Change Request</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EgoVehicleMotionSensor</td>
<td>The Driver assumes a wrong value for the vehicle speed due to wrong data from</td>
<td>UCA1.5 The Driver provides the Set Speed command with a value above the speed limit while in normal traffic</td>
<td>H-7, H-11, H-12</td>
<td>The ADS must always use the information of the Navigation and the EgoVehicleMotionSensor to determine the correct speed of the vehicle and request immediate maintenance of the vehicle in case of an inconsistency</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(DR0.10)</td>
<td>the EgoVehicleMotionSensor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Driver assumes a wrong value for the vehicle speed due to missing data from</td>
<td>UCA1.5 The Driver provides the Set Speed command with a value above the speed limit while in normal traffic</td>
<td>H-7, H-11, H-12</td>
<td>The ADS must always check for regular data from the Vehicle Sensors and request immediate maintenance if a sensor does not report data withing a normal timewindow.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>the EgoVehicleMotionSensor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Steering Wheel</td>
<td>The Steering command isn't executed due to an error in the actuator of the</td>
<td>UCA1.30 The Driver doesn't provide Steering when AD mode is being deactivated and steering is required</td>
<td>H-7, H-11</td>
<td>The manual controls of the vehicle must be maintained regularly to prevent malfunction</td>
<td>The correct function of the steering wheel could be checked by monitoring the movement of the wheel and the resulting orientation of the vehicle</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>steering wheel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The steering wheel gets stuck in a turned state</td>
<td>UCA1.65 The Driver provides Steering too long (over steers) while in AD mode</td>
<td>H-7, H-9</td>
<td>The manual controls of the vehicle must be maintained regularly to prevent malfunction</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Safety Constraints Step 4

<table>
<thead>
<tr>
<th>ID</th>
<th>Safety Constraint</th>
<th>Description</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The ADS must always check requested speed changes are potential hazardous in the current driving situation and prevent them if necessary</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The ADS must notify the Driver vigorously before changing the driving mode</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The ADS must always provide feedback about the current state over more than one channel to prevent incorrect feedback</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The ADS must ensure good readability of the Display when in bright sunlight</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The ADS must ensure that when the Display is not readable due to an internal error or external conditions important informations about the system state are transmitted through other channels</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The ADS mustn’t rely on the driver to execute any safety critical functions while in AD mode</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The ADS must provide a documentation or tutorial to allow the Driver to familiarize learn the AD vehicle controls in a safe environment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The ADS must always provide feedback about its state, the driving mode and the actions planned by the system</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>When a speed change is requested during a lane change the ADS should ask the Driver to cancel a lane change instead of changing the speed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The AD input Device must not react to inputs (pulls/pushes) below a (user-)defined threshold to prevent accidental interactions</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The AD input Device must be maintained regularly to prevent malfunction</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The ADS must monitor the vehicle controls and send an RTI or perform an automatic MRM if the controls do not function as expected</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The HMI should always double-check its internal Model of the ADS with the actual state of the ADS and correct wrong entries</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Display must be regularly maintained and checked for the required functional requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Safety Constraint</td>
<td>Description</td>
<td>Links</td>
</tr>
<tr>
<td>----</td>
<td>-------------------</td>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td></td>
<td>The visual parameters (brightness, color, contrast) of the Display must be adjustable to fit the driving scenario and the Drivers preferences.</td>
<td>Before accepting requests issued by the Driver in AD mode over the AD input device the ADS must check the drivers attention to the driving situation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The ADS must check the legality of lane changes before executing them and notify the Driver about any traffic violations.</td>
<td>The ADS must always ensure that the Driver is aware of the driving situation before a hand-over to ensure a smooth take-over without breaking out or sudden peaks/drops in speed.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The ADS must always provide clear and minimal feedback about the current state and instructions to the Driver to prevent redundant information.</td>
<td>The ADS must always check the legality of lane changes before executing them and notify the Driver about any traffic violations.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The ADS must always prevent hazardous manual interventions that could potentially lead to a severe accident.</td>
<td>The ADS must always check the legality of lane changes before executing them and notify the Driver about any traffic violations.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The manual controls of the vehicle must be maintained regularly to prevent malfunction.</td>
<td>Feedback about the (un-)successful execution of a Driver requested AD task has to be provided on redundant channels to prevent information loss.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The display of the HMI must always show the most recent and important information and should never omit feedback due to pending information.</td>
<td>The ADS should always provide feedback over redundant channels to prevent information loss.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The AD Vehicle should always warn the Driver about hazardous road conditions like wet or snowy.</td>
<td>The ADS should always provide feedback over redundant channels to prevent information loss.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The attention of the Driver must be checked by the Driver Sensors before accepting any CAs from over the AD Input Device.</td>
<td>The ADS must check the attention of the Driver with multiple/redundant Sensors and terminate the AD mode immediately if the Sensors become unavailable or provide inconsistent information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The ADS must always use the information of the Navigation and the EgoVehicleMotionSensor to determine the correct speed of the vehicle.</td>
<td>The ADS must always use the information of the Navigation and the EgoVehicleMotionSensor to determine the correct speed of the vehicle.</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Safety Constraint</td>
<td>Description</td>
<td>Links</td>
</tr>
<tr>
<td>----</td>
<td>-------------------</td>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td></td>
<td>the vehicle and request immediate maintainance of the vehicle in case of an inconsistency.</td>
<td>The ADS must always check for regular data from the Vehicle Sensors and request immediate maintenance if a sensor does not report data within a normal timewindow.</td>
<td>The ADS should calculate a time window in which it expects new data from a sensor (e.g. based on old/historical response data) so it can then predict a sensor malfunction in case of a decreasing data rate.</td>
</tr>
<tr>
<td></td>
<td>The HMI must always ensure that in case of a malfunction in the Feedback system (no Display, Haptic Feedback) the other Feedback channels can compensate the loss or if an immediate MRM is required.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Glossary

ACCIDENT
undesired or unplanned event that results in a loss, including loss or injury to human life, property damage, environmental pollution, mission loss etc.

ACTUATOR
a human operator or mechanical device tasked with directly acting upon a process and changing its physical state. Valve systems (valve + the motor associated to it), doors, magnets (their electronic controller and power source included) or a nurse are actuators that respectively implement control on the following processes: "fluid flow", "egress availability", "beam position", "patient position". Actuators, like sensors, can be smart in that they can be programmable; they may therefore need to be studied with the same concepts as the controllers are.

CAUSAL FACTOR
cause of a (hazardous) scenario (STPA Step 2).

COMMAND
a signal providing a set of instructions (goals, set points, order) issued by a controller with the intent of acting upon a process by activation of a device or implementation of a procedure. Communication and Control, along with Hierarchy and Emergence, are fundamental systems theory concepts at the foundation of STAMP. Commands are issued by Controllers, with the intent that they be implemented by Actuators to act on the Controlled Process.

CONTROL ACTION
the bringing about of an alteration in the system's state through activation of a device or implementation of a procedure with the intent of regulating or guiding the operation of a human being, machine, apparatus, or system. They are the result of an Actuator implementing a control Command issued by a Controller, and aim at controlling the state of the Controlled Process.

CONTROL STRUCTURE
hierarchy of process loops created to steer a system's operations and control its states. In the context of a hazard analysis, we are most concerned with the control of hazardous states aimed at eliminating, reducing or mitigating them.

CONTROLLED PROCESS
although at times reducible to the state of a physical element (e.g. framing a "door" as a controlled process whose values can be "open" or "shut"), it appears fruitful to rather consider the controlled process identified in STAMP process loops to be the system's attribute or state variable that the controller aims to control (e.g. thinking of the door not as the controlled process but, together with its motor, as an actuator that implements control on the possibility of egress).

CONTROLLER
a human or automated system that is responsible for controlling the system's processes by issuing commands to be implemented by system actuators.

FEEDBACK evaluative or corrective information about an action, event, or process that is transmitted to the original or controlling source.
HAZARD
system state of set or conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident.

LOSS
decrease in amount, magnitude or degree including destruction or ruin.

SAFETY
freedom from loss.

SAFETY CONSTRAINT
bound set on system design options and operations to restrict, compel to avoid or forbid the performance of actions that would lead to a hazard.

SAFETY/DESIGN REQUIREMENT
design requirement formulated to include the enforcement of safety constraints as a design objective.

(HAZARDOUS) SCENARIO
an account or synopsis of a possible course of action or events resulting in a hazard. See Causal Factor.

SENSOR
human or mechanical device tasked with measuring a process variable by responding to a physical stimulus (as heat, light, sound, pressure, magnetism, or a particular motion) and transmit a resulting impulse (as for measurement or operating a control).

UNSAFE CONTROL ACTION
control action that leads to a hazard (STPA Step 1).

Definitions from:
Antoine, B. (2013). Systems Theoretic Hazard Analysis (STPA) applied to the risk review of complex systems: an example from the medical device industry (Doctoral dissertation, Massachusetts Institute of Technology).
B. Human Error Analysis eines zukünftigen Systems zum automatisierten Fahren
<table>
<thead>
<tr>
<th>Task 1</th>
<th>Title</th>
<th>Description</th>
<th>Operator</th>
<th>Goals</th>
<th>Actions</th>
<th>Plans</th>
<th>Performance Shaping Factors</th>
<th>Human error mode</th>
<th>occurrence probability</th>
<th>Human error effects</th>
<th>detection, correction and compensation, Control Strategies (CS)</th>
</tr>
</thead>
</table>
| Lane Change | The Driver requests the AD controller to perform a lane change if possible. | Driver | AD vehicle performs a lane change | Push the AD input device in the direction of the lane change | 1. Deciding on the Lane to change to.  
2. Moving the Input Device in the decided on direction  
3. Confirmation of the correct maneuver highlighted on the display | Interruptions through environment  
Wrong coordination/perception between direction of lane change and pulling direction | confirmation omitted  
Wrong procedure selected/lane change in wrong direction | Moderate  
Low | Lane change confirmation dialog is not closed  
Lane change request is omitted/cancelled | CS-1  
CS-2 | The AD system must notify the driver when the confirmation dialog is not answered  
The AD system must set a reasonable timeout for the lane change confirmation dialog  
The AD system must give clear guidance on the handling of the AD input device |
| | | | | | | confusion about option to cancel lane change  
need to carry out multiple tasks in same time window  
Wrong Training in AD functions | inappropriate goal selected  
inappropriate goal selected  
lane change executed with manual controls instead of the AD input Device | Inappropriate goal selected  
Inappropriate goal selected  
Lan e change executed unwanted/accidentally | Low  
Moderate  
Low | The Driver must be informed about the option to cancel the lane change request  
The AD system must always request a confirmation of Driver inputs over the AD Input Device  
The AD System must strongly notify the Driver as soon as he touches the manual controls if he really wants to intervene |
| | | | | | | Confusion about the confirmation due to poorly designed Confirmation Dialog  
confirmation dialog shown too short/long | Confirmation omitted  
Selection of lane change omitted | Confirmation omitted  
Selection of lane change omitted | Moderate  
Moderate | The lane change is omitted  
The AD system performs an MRM  
The AD System must define a reasonable timeout for HMI dialogs to prevent showing dialogs too short/long  
The AD System must inform the Driver in time before an MRM about the action and the interaction possibilities during the action |
| Task 2 | Speed Change | The Driver can request a change of the maximum speed which can be acquired by the AD vehicle, the speed will be adapted within the defined speed limits known to the AD vehicle | Driver | change the max speed to which the AD vehicle should accelerate | Push the AD input for or backwards to request a increase or decrease of speed | 1. Decide upon a decrease/increase of the driving speed  
2. Moving the Input Device in the decided on direction  
3. Insufficient detailed description of the Mechanics | Effects of traffic jam, long ride (tired, exhausted)  
Poor design of the Input device  
Insufficient detailed description of the Mechanics | Inappropriate speed selected  
Lan e change/cancel instead of set Speed command selected  
Inappropriate speed selected | Moderate  
High  
High | The speed is increased/decreased too an undesired level  
The current lane change is cancelled/ executed  
The speed is increased/decreased too an undesired level | CS-8  
CS-9  
CS-8 | The AD vehicle must prevent undesired high/low speed changes  
The AD Input Device’s design must ensure a clear distinction between set speed and the lane change/cancel command  
The AD vehicle must prevent undesired high/low speed changes |
<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Operator</th>
<th>Goals</th>
<th>Actions</th>
<th>Plans</th>
<th>Performance Shaping Factors</th>
<th>Human error mode</th>
<th>occurrence probability</th>
<th>human error effects</th>
<th>detection, correction and compensation, Control Strategie (CS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>React to Display and the Haptic/ Visual or Verbal Feedback</td>
<td>The Driver gets feedback over the current journey and possible RTI's over multiple feedback channels</td>
<td>Driver</td>
<td>Get notified when the attention of the Driver is required</td>
<td>Listen to vehicle feedback 1. Observe the given Feedback 2. Decide upon a response to the Feedback</td>
<td>Distraction by environment (passengers, TPOs) Feedback omitted</td>
<td>Driver doesn’t react to feedback</td>
<td>Moderate</td>
<td></td>
<td>CS-10</td>
<td>The AD vehicle must always provide feedback on multiple channels (optical, physical, verbal, etc.) depending on the urgency of the feedback to ensure the drivers attention.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Poorly designed display layout showing too much information</td>
<td>Driver can’t react appropriately</td>
<td>Low</td>
<td></td>
<td>CS-25</td>
<td>The layout of the Display must at all times display only the minimal amount of required information too prevent overcrowding the layout.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Extreme weather conditions (darkness, brightness) make it difficult to see the display</td>
<td>Feedback omitted</td>
<td>Moderate</td>
<td></td>
<td>CS-26</td>
<td>The AD system must always provide feedback about safety critical state changes and informations on redundant channels (e.g. display and sound or haptic feedback).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Fatigue due to long ride, hot temperature</td>
<td>Incorrect identification of situation</td>
<td>Moderate</td>
<td></td>
<td>CS-11</td>
<td>The AD vehicle must implement a confirmation dialog for all interactions with the AD system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Sleepiness/drowsiness due to long ride, boredom etc.</td>
<td>Steering in wrong direction or steering too sharp</td>
<td>Moderate</td>
<td></td>
<td>CS-15</td>
<td>The AD system must prevent any manual interventions when the driver has not taken over completely (hands and feet on controls, head straight).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Inadequate experience with the AD system</td>
<td>Incorrect identification of system state</td>
<td>Moderate</td>
<td></td>
<td>CS-24</td>
<td>The AD system must warn the driver through multiple feedback channels about dangerous interventions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AD system treats intervention as illegal and blocs it</td>
<td>Unwanted prevention of a necessary Driver intervention</td>
<td>Moderate</td>
<td></td>
<td>CS-16</td>
<td>The AD system must provide feedback over multiple channels when the driving mode changes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CS-17</td>
<td>The Driver must always be able to take over control eminately by putting hands and feet on the controls and turning the head straight.</td>
</tr>
</tbody>
</table>
Literaturverzeichnis


Literaturverzeichnis


Alle URLs wurden zuletzt am 25. 10. 2018 geprüft.
Erklärung


Ort, Datum, Unterschrift
25.10.2018

Pierre Blüher
Senior Expert Safety Engineering for Automated Driving
Systems & Technology - Advanced Technology - Safety

30.10.2018

Dr. Alexander Rudolph
Head of Safety, Safety-in-Use & Cybersecurity
Systems & Technology - Division Chassis & Safety