Institut für Softwaretechnologie

Universität Stuttgart
Universitätsstraße 38
D–70569 Stuttgart

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

Die Sicherheitsanalyse moderner Systeme wird immer anspruchsvoller; Vor allem auch wegen der immer größer werdenden Rolle des *Human Factor* werden Sicherheits- und vor allem Gefahrenanalysen schon in frühen Phasen des Systems notwendig. Mit STPA (Systems-Theoretic Process Analysis) wurde 2011 eine Methode zur systematischen Gefahrenanalyse unter Zuhilfenahme der System Theorie vorgestellt, die genau diese Anforderungen erfüllt. Mit STPA wurde nicht nur eine Gefahrenanalyse zur Entwicklung sicherheitsgetriebener Systemdesigns, mittels abstrakter Modellierung des gesamten Regelkreises vorgestellt, sondern auch die Sicherheit eines Systems als Regelungsproblem definiert. 2017 wurde mit „Engineering for Humans: A New Extension to STPA“eine Erweiterung von STPA um Methoden zur Modellierung menschlichen Verhaltens und zur Anpassung der STPA an die Anforderungen einer *Human Factor* Analyse vorgestellt. Im Gegensatz zu traditionellen Verfahren zur Analyse des *Human Factor* handelt es sich bei der STPA nicht um eine Expertenanalyse, wodurch die Frage nach dem Mehrwert der Analyse entsteht. Hierzu wurden im Verlauf dieser Arbeit eine STPA und eine traditionelle Analyse anhand eines zukünftigen Systems zum automatisierten Fahren durchgeführt und anhand der Ergebnisse der Mehrwert durch den Einsatz von STPA gegenüber einem traditionellen Verfahren evaluiert.

Danksagung

Ich möchte mich an dieser Stelle bei Wolfgang Fechner und Pierre Blüher für ihre Unterstützung und Anleitung durch den Entstehungsprozess dieser Arbeit bedanken.
Desweiteren gilt mein Dank der Continental Teves AG & Co. oHG und insbesondere Pierre Blüher und Alexander Rudolph für die Ermöglichung dieser Arbeit und der Unterstützung bei der Durchführung und Evaluation der Analysen.
Zuletzt möchte ich mich noch bei meiner Familie und allen Beteiligten, die mir mit wertvollem Feedback geholfen haben die Arbeit fertig zu stellen, bedanken.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

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

Die untenstehenden Definitionen sind der *SEA J3016* [Int16] sowie dem *STPA Handbook* von Leveson [LT18], dem *Engineering for Humans: A new extension for STPA* von France [Fra17] sowie dem *Extending the Human Controller methodology in systems-Theoretic Process Analysis (STPA)* von Thornberry et al. [LT14] entnommen, für die vollständigen Definitionen der Bergriffe wird auf die jeweilige Quelle verwiesen.

Begriff	Definition
Accident/Loss (in dieser Arbeit immer als *Accident* bezeichnet)	Ein Loss beinhaltet etwas, das für die Stakeholder von Wert ist. Ein Loss könnte den Verlust von menschlichem Leben oder menschliche Verletzung, Sachschäden, Umweltverschmutzung, Scheitern der Mission, Verlust von Ruf oder sensiblen Informationen oder andere Verluste enthalten, die für die Stakeholder von Relevanz sind.
Control Action	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]
Control Action Selection	Der Entscheidungsprozess des Menschen für eine bestimmte *Control Action* basierend auf den Informationen aus den *Mental Models*.[Fra17]
Control Algorithm	Der Algorithmus eines automatisierten *Controllers* zur Selektion einer *Control Action* basierend auf den *Process Models* des *Controllers*.[LT18]
Control Strategy	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.
Control Structure	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]
Controlled Process	Der vom *Controller* regulierte Prozess, bspw. ein Fahrzeug welches von einem *Human Controller* gesteuert wird.

Begriff	Definition
Controller	Eine Komponente die mittels *Control Actions* und *Feedback* einen *Controlled Process* reguliert. Man kann generell zwischen zwei Arten von *Controllern* unterscheiden: *Human Controller* Ein Mensch der mit vier Komponenten modelliert wird; der *Control Action Selection*, der *Mental Models*, dem *Mental Model Update* und einer *Sensory Perception*. *Automated Controller* Ein automatisierter *Controller* besteht aus einem *Process Model* sowie einem *Control Algorithm*.
Dynamic Driving Task(DDT)	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]
DDT-Fallback	Die Antwort des Benutzers oder 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]
Feedbackschleife	Das System aus *Control Action*, welche von einem *Actuator* ausgeführt wird, und Feedback über eventuelle Änderungen des Systemzustandes. Die gesamte *Feedback Schleife* wird in einer *Control Structure* modelliert.
Hazard	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]
Mental Models	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: • Das *Mental Model* des Prozesszustandes • Das *Mental Model* des Prozessverhaltens • Das *Mental Model* der Umwelt (des Prozesses) [Fra17]
Mental Model Update	Der Prozess durch den Feedback oder Informationen über äußere Faktoren in die *Mental Models* integriert werden.[Fra17]

Begriff	Definition
Minimal Risk Condition (MRC)	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]
Operational Design Domain(ODD)	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]
Safety Coinstraint	Formulierung einer zu treffenden Sicherheitsmaßnahme im Systemdesign zur Verhinderung eines *Hazards*. Die Ergebnissmenge STPA (Systems Theoretic and Process Analysis) besteht aus mehreren *Safety Constraints*.
Sensory Perception	Das unverarbeitete Feedback welches der Mensch durch visuelle, tiefensensible oder vestibuläre Wahrnehmung empfängt und welches nicht Teil des Systemdesigns ist.[LT14]
Sicherheit (Safety)	Die Freiheit von Accidents. [LT18]
System	Ein System besteht aus einer Reihe von Komponenten, die als Ganzes zusammenwirken, um definierte Systemziele umzusetzen. Ein System kann Subsysteme enthalten und kann auch Teil von einem größeren System sein.[LT18]
Unsafe Control Action	Eine *Control Action*, die in einem bestimmten Kontext und unter Worst-Case-Bedingungen zu einem *Hazard* führt.[LT18]
Process Model	Die Informationen, die ein *Controller* über den von ihm regulierten Prozess besitzt, ein *Process Model* ist hierbei eine Ansammlung an Prozessvariablen mit denen der *Control Algorithm* eines automatisierten *Controllers* eine passende *Control Action* auswählt. Ein *Controller* kann auch mehrere *Process Models* besitzen, die Informationen über Prozesse (intern sowie extern) aber auch das Gesamtsystem oder dessen Umwelt beinhalten.[LT18]

1. Einleitung

Durch die immer komplexer werdenden Systeme, und die immer stärker in den Fokus rückende Rolle des Menschen als sicherheitskritischen Faktor in diesen, sind weitgehende Gefahrenanalysen schon in der Designphase unumgänglich. Hierbei sind neue Denkansätze notwendig, um traditionelle Analyseverfahren dahingehend anzupassen, dass sie die gestiegenen Anforderungen durch die steigende Digitalisierung von Systemen und die dadurch entstehende höhere Komplexität[Lev11] in Betracht ziehen. In rein mechanischen Systemen ist die *Feedbackschleife* eines Systems durch direktes Feedback des mechanischen Prozesses wie z.B. Abwärme eines Motors, Vibrationen durch den Betrieb oder druckgesteuerte Displays in einer Lokomotive noch klarer geregelt. Moderne Systeme bringen mit dem Einsatz von digitalen Bedieneinheiten und Displays ganz neue Herausforderungen in Sachen Sicherheitsanalyse und Mensch-Maschinen Interaktion mit sich.
Leveson hat 2011 mit *Systems-Theoretic Process Analysis* (STPA) eine neue Analyse ins Spiel gebracht, die mithilfe der System Theorie versucht die Problematik zu lösen und damit traditionelle Verfahren zu ersetzen oder zu ergänzen. Zusätzlich ist in Mensch-Maschinen Systemen, wie sie beim automatisierten Fahren eingesetzt werden, eine intensive Analyse des *Human Factors* notwendig. Der Mensch ist ein unüberschaubar komplexes System, dessen genaue Abbildung nahezu unmöglich ist; weswegen sich zu diesem Thema eine schier unüberschaubare Menge an Literatur findet, die die menschliche Psyche erklärt und anhand dieser Verhaltensmodelle aufstellt [Ras83]. Durch diese Vielfalt an Wissen sind traditionelle Methoden als Expertenanalysen ausgelegt, die anhand von historischem Wissen und Experteneinschätzungen Komponenten Interaktionen analysieren. Thornberry[LT14] und France [Fra17] beschreiben Methoden zur anwendungsbezogenen Abstrahierung der menschlichen Wahrnehmung, um versierte Aussagen über menschliches Verhalten auf Basis einer einfach zu verstehenden Modellierung treffen zu können.

1.1. Problemstellung

Das Problem der Gefahrenanalyse beschränkt sich schon lange nicht nur auf die Sicherstellung einer genügenden Zuverlässigkeit der einzelnen Komponenten, sondern beinhaltet die Sicherstellung der notwendigen Regulierungsmaßnahmen um Sicherheitslücken zu vermeiden. Traditionell werden hierzu Sicherheitsanalysen nach dem „Chain-of-Events Modell“ durchgeführt, die auf das gestiegene Anforderungsprofil durch digitale Komponenten und menschliche Einflüsse erweitert werden [Mod11][Rudgu]. Hierbei werden Expertenanalysen durchgeführt, in denen *Hazards* im System durch Expertenwissen und anhand von Erfahrungswerten bewertet werden. Solche Verfahren und vor allem deren Betrachtung des *Human Factor* setzen vor allem auf vorhandenes Wissen über das System und mögliche Einflüsse des Menschen auf dieses. Im Gegensatz dazu bietet STPA einen schrittweisen Aufbau des Systemdesigns und stellt mit den Erweiterungen von Thornberry[LT14] und France[Fra17] Modelle für eine abstrakte Modellierung des *Human Factor* auf, ohne ein tiefes Expertenwissen zu fordern.

1.2. Ziel der Arbeit

Ziel dieser Arbeit ist eine Aufstellung von Vor- und Nachteilen des Einsatzes und eine Bewertung des Mehrwertes von STPA in der Gefahrenanalyse von komplexen Systemen zum automatisierten Fahren unter Berücksichtigung des *Human Factors*. Durch eine solche Aufstellung könnte ein Entscheidungsprozess, ob sich ein Umstieg auf die STPA Methode lohnt, mittels konkreter Argumente vorangetrieben werden. Eine weitere Frage, die diese Arbeit versucht zu beantworten, ist ob die Durchführung einer STPA und der damit verbundene Einsatz der System Theorie in der Gefahrenanalyse von komplexen Systemen tatsächlich einen Mehrwert für die Sicherheit eines Systems liefert. Dies resultiert nicht nur in der Prüfung ob eine solche Analyse eine größere Ergebnismenge liefert, sondern auch ob die Ergebnismenge tatsächlich eine höhere thematische Überdeckung sicherheitskritischer Komponenten bringt. Das Ziel der Arbeit ist eine Empfehlung zu einem Einsatz von STPA zu geben, welche auf der Analyse der Vor- und Nachteile sowie der thematischen Überdeckung der im Verlauf der Arbeit gesammelten Erkenntnisse basiert.

1.3. Struktur der Arbeit

Diese Arbeit ist in fünf Kapitel unterteilt, die erst in das Thema einführen und anschließend die Herangehensweise an die Problemstellung, sowie eine Diskussion der Ergebnisse vorstellen.
Das erste Kapitel hat eine Einführung in die Thematik und die Ziele dieser Arbeit gegeben. In Kapitel 2 wird eine Übersicht über vorhandene Literatur gegeben. Kapitel 3 enthält konkrete Beschreibungen der *Human Error Analysis* (HEA) und der STPA, wobei letztere in Form einer Guideline zur Nachvollziehbarkeit der Analyse des *Human Factor* bereitgestellt wird. Zur Untermauerung der in Abschnitt 1.2 vorgestellten Ziele werden in Kapitel 4 eine STPA und eine HEA eines Beispielsystems vorgestellt und deren Ergebnisse verglichen. Den Abschluss dieser Arbeit bildet Kapitel 5 mit einer Zusammenfassung und einem Ausblick auf weitere Forschungsmöglichkeiten aufbauend auf den Resultaten dieser 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

Angefangen mit Heinrichs Domino Modell von 1931 haben traditionelle Kausalitätsmodelle gemeinsam, dass sie den Menschen als eines von mehreren Gliedern in einer Ereigniskette betrachten, an deren Ende ein Unfall bzw. eine Konsequenz steht [BL76][Lev11]. Die Annahme ist hier immer, dass ein Fehler in einer Komponente, der Fall eines Dominosteins oder die Überwindung einer Verteidigungslinie im Swiss Cheese Modell von Reason [Rea00] das Potenzial hat, eine solche Ereigniskette auszulösen. Reason [Rea90] unterscheidet dabei zwischen aktivem und latentem Versagen, welches in unterschiedlichen Stufen eines Systems entstehen kann wie in Abbildung 2.1 dargestellt ist. Mit dieser prinzipiellen Differenzierung wird zwischen tatsächlichem Versagen, Ausfällen oder Fehlaktionen und deren Symptomen, die durch Aktionen in einer früheren Stufe des Systems stattgefunden haben, unterschieden. Unfälle sind häufig das Resultat des Zusammenwirkens mehrerer Fehler im System und werden eher selten durch eine alleinstehende Aktion oder einen alleinstehenden Fehler ausgelöst.

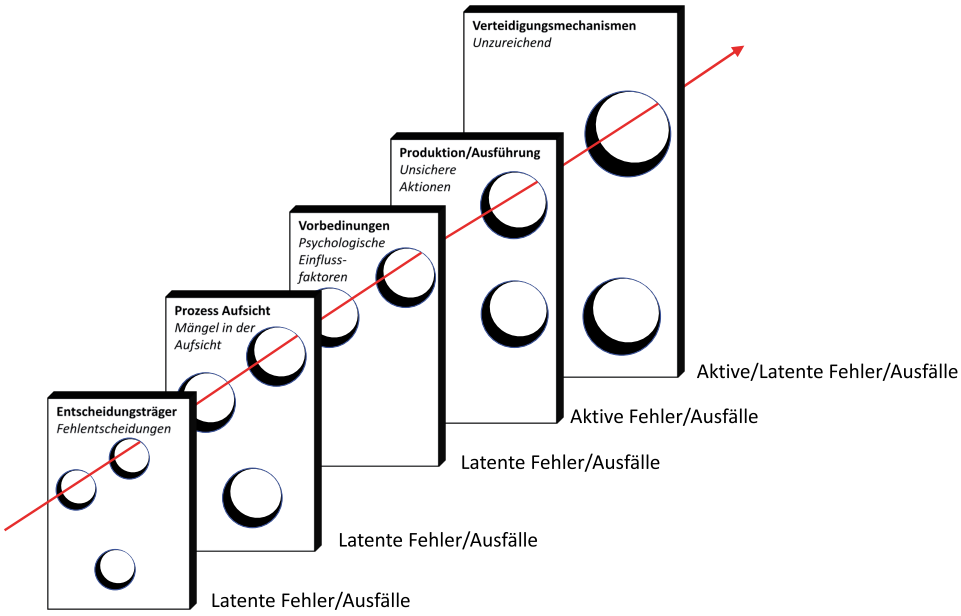


Abbildung 2.1.: Das 1990 vorgestellte Modell eines Produktiv-Systems von James Reason[Rea90], welches in jeder Stufe des Systems Beispiele für menschliches Versagen (*kursiv dargestellt*) definiert (angelehnt an die Darstellung des ICAO (International Civil Aviation Organisation) Circular 240-AN/144[Shea])

Hierdurch entsteht die Annahme, dass ein System durch Beseitigung dieser Ursachen, oder zumindest der Reduzierung der Auftretenswahrscheinlichkeit, sicher gemacht werden kann. Dekker [DM07] beschreibt den *Human Factor* in einem System als einen Akteur, der anhand von Regeln handelt und ähnlich wie eine automatisierte Komponente so eine Fehlerquelle darstellt, die durch klare Maßnahmen wie Auswechslung der Komponente, Redundanz oder besseres Training behoben werden kann. Die von Dekker beschriebene „Bad Apple Theory“ geht davon aus, dass ein System durch gezieltes Entfernen von Schwachstellen (hier. „Bad Apples“) sicher gemacht werden kann und überträgt diese Anschauung auch auf den Menschen. Der *Human Factor* spielt eine entscheidende Rolle in der Sicherheit und dem Design von komplexen Systemen wie sie in der Luftfahrt oder in der Automobilindustrie vorkommen. In dem 1972 von Elwyn Edwards beschriebenen und später von der *International Civil Aviation Organisation* (ICAO) übernommenen *Software, Hardware, Environment, Liveware, Liveware Model* (Shell-Modell)[Sheb] wird erstmals ein Modell für die Analyse des *Human Factor* in komplexen Mensch-Maschinen Systemen beschrieben. Das Model wurde von Edwards im Kontext der Luftfahrt entworfen, wird aber auch aufgrund seiner allgemeinen Forderungen für die Betrachtung des *Human Factor* in anderen Bereichen eingesetzt [Rudgu].

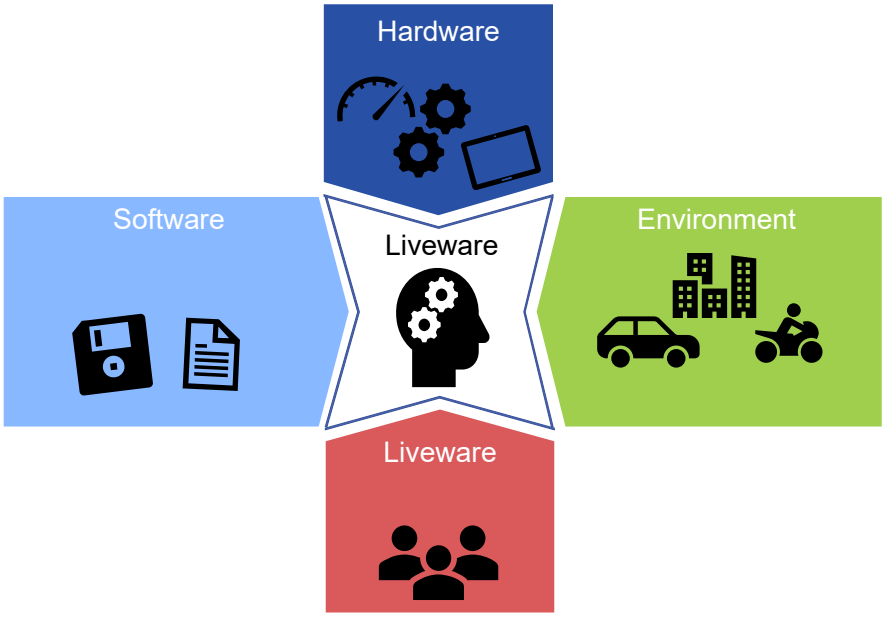


Abbildung 2.2.: Das in ICAO(International Civil Aviation Organisation) Circular 216-AN31[Sheb] vorgestellte Shell Modell (Software, Hardware, Environment and Liveware) welches die Beziehung zwischen dem Menschen mit Software, Hardware, seiner Umwelt und Mitmenschen darstellt

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

Die Schnittstelle zwischen Mensch und Software kann vorhandenes Wissen oder Annahmen über die Fahrzeuglogik sein, aber auch Hilfsmittel wie Anleitungen oder Handbücher darstellen. Probleme in diesem Interface gehen vor allem vom Nutzer des Systems aus und sind abhängig dessen Fähigkeiten und Kenntnissen. Dadurch sind Probleme hier nur schwer zu finden, können aber fatale Folgen haben wie z.B. fehlende sicherheitskritische Eingaben aufgrund einer Fehlannahme über den Systemzustand.

Liveware-Hardware

Bei der Liveware-Hardware Schnittstelle handelt es sich um physische Kontaktpunkte zwischen Nutzer und System also Anzeigen, Displays, Knöpfe aber auch Elemente wie das Design von Sitzen oder mechanische Feedback-Systeme wie Vibratoren in den Sitzen und haptisches Feedback.

Liveware-Liveware

Eine weitere wichtige Erweiterung der *Human Factor* Analyse stellt die Betrachtung der Schnittstelle zu anderen Menschen z.B. zu Beifahrern oder anderen Autofahrern. Andere Menschen oder soziale Gruppen können die Leistung eines Menschen sowohl positiv als auch negativ beeinflussen und sowohl unterstützend als auch repressierend wirken. Auch die Abwesenheit anderer Menschen kann hier, abhängig vom Charakter des zentralen Operators, unterschiedliche Einflüsse haben. Beispielsweise kann ein Autofahrer durch die Abwesenheit eines Beifahrers fokussierter sein; er kann aber auch Einsamkeit verspüren oder schneller ermüden.

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 Fahrfunktionen 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 komplette 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[Gol+16].
Je höher der Anteil wird, zu dem das *Automated Driving System* (ADS) die Rolle des Fahrers übernimmt, desto wichtiger wird die Betrachtung der Übernahmefähigkeit des Fahrers. Diese wird in einer Studie von Körber et al. [Kör+15] in Zusammenhang mit der individuellen Multitasking-Fähigkeit gebracht. Dabei bezieht sich die Studie auf den *out-of-the-loop* Zustand, d.h. den passiven Zustand, in dem der Fahrer die Fahraufgaben an das ADS abgegeben hat und sich mit fahrfremden Tätigkeiten beschäftigt. Außerdem zeigt die Studie, dass die Übernahmefähigkeit zwar proportional zur Erfahrung sinkt, es jedoch eine stabile Abweichung zwischen Individuen gibt.
Ein weiterer Faktor in der Betrachtung des *Human Factor* kann das Alter des Fahrers darstellen. Hierzu wurde 2016 in einer Studie von Körber et. al [Kör+16] widerlegt, dass das Alter sich auf die Lernfähigkeit oder die Übernahmezeit positiv oder negativ auswirkt. So wird unabhängig vom Alter einer Personen eine höhere Übernahmezeit bei höherem Verkehrsaufkommen bei ebenfalls altersunabhängigem Umgang mit kritischen Situationen festgestellt [Gol+16][Kör+15][Kör+16]. Dieser Anstieg in der Übernahmezeit wird hauptsächlich durch den höheren Stress ausgelöst, begründet durch die komplexeren Situationen. Interessant ist jedoch, dass entgegen der Übernahmezeit, die Zeit die der Fahrer braucht, um das Steuer wieder zu übernehmen nicht mit dem Verkehr steigt

[Gol+13][Gol+16]. Hierzu betrachten Radlmayr et al.[Rad+16] neben der Übernahmezeit auch die Übernahmequalität, die Aufschluss über die Kollisionswahrscheinlichkeit oder die Quer-/Längs Beschleunigung des Fahrzeugs gibt. Um die zu erwartende Übernahmequalität zu beurteilen muss der Zustand des Fahrers oder besser gesagt seine Aktiviertheit (schläfrig, energiegeladen, etc.) und die Aufmerksamkeit [Rau+09] messbar gemacht werden. Hierbei ist vor allem die aktive und passive Erschöpfung für die Betrachtung des *Human Factor* von Bedeutung. Erschöpfung wird dabei in aktive und passive Erschöpfung unterteilt, je nachdem ob die Ursache Vigilanz oder Daueraufmerksamkeit ist. Als mögliche Instrumente für die Überwachung des Fahrerzustandes und damit der Vorhersage der Übernahmequalität empfehlen Radlmayr et al.[Rad+16] den Einsatz von Instrumenten wie Eye-Tracking und Sensoren.

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*

Die Analyse des *Human Factor* basiert traditionell auf anwendungsspezifischen Listen von als *Performance Inducing Factor* (PIF) oder *Performance Shaping Factor* (PSF) bezeichneten Kontext Faktoren, die die Wahrscheinlichkeit eines Human Error beeinflussen [KJ03][Sta04][Dou93]. Kirwan et al.[Kir] stellt eine Reihe von Methoden zur Analyse des *Human Factor* in Kontext einer *Human Risk Assessment* (HRA) vor, die versucht, die Wahrscheinlichkeit für menschliches Versagen zu analysieren. Die traditionelle Herangehensweise an die Analyse des *Human Factor* nach dem HRA Framework, welches in Abbildung 2.3 dargestellt ist, kann in drei Bereiche unterteilt werden. Der Fehler Kontext (1) bedarf der Aufstellung einer Liste an domänespezifischen PSF basierend auf Expertenwissen und/oder Erfahrungswerten[WS01] die von Methode zu Methode variieren[KJ03]. Eine weitere Charakteristik die Cooper et al. [Coo+96] nennen, ist dass diese Listen in einem zusätzlichen Prozess befüllt werden, wodurch relevante Fehlerdaten oft erst nach dem Auftreten der Fehler einer solchen Fehlerdatenbanken hinzugefügt werden können[WS01]. Hierbei beeinflusst ein PSF die Leistung, die ein Mensch bei einer bestimmten Aufgabe im System erbringen kann. Beispielsweise wären Stress oder Müdigkeit ein PSF beim Autofahren; aber auch soziale oder organisatorische Faktoren wie Arbeitsdruck oder Verantwortung können die Ausführung einer Aufgabe beeinflussen.
Ein Beispiel einer Analyse die *Performance Inducing Factors* nutzt, ist *Predictive Human Error Analysis* (PHEA) 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.

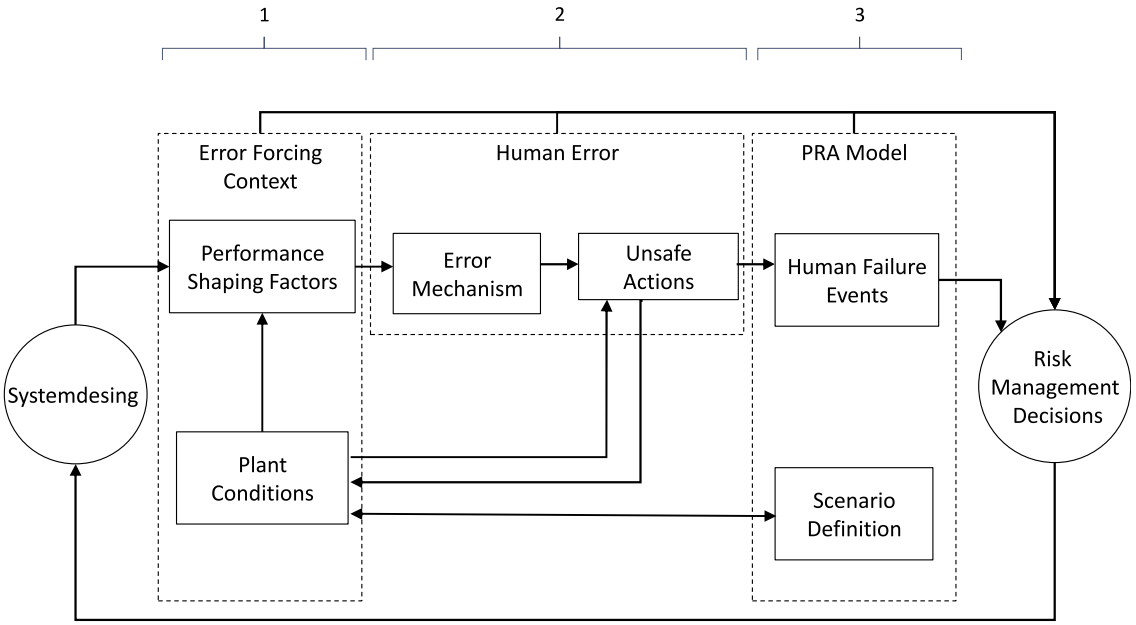


Abbildung 2.3.: Multidisziplinares Model des HRA (Human Risk Assesment) Frameworks[Coo+96]

Der Human Error (2) ist im HRA Framework als Kombination einer Unsafe Action [WS01] und einem Error Mechanism definiert. Eine Unsafe Action (oder Unsafe Act) kann ein Interaktionsfehler des Anwenders mit dem System sein, es kann sich aber auch um einen Verstoß gegen ein Regularium handeln. Auf der anderen Seite handelt es sich bei einem *Error Mechanism* (auch *Error Mode* in der PHEA[Emb+94] und *Systematic Human Error Reduction and Prediction Approach* (SHERPA)[Emb86]) um einen Faktor, der durch einen PSF oder durch Anlagenbedingungen ausgelöst wird. Ein Error Mechanism löst, in Kombination mit einer Interaktion oder Ausführung einer Bedienaufgabe, eine Unsafe Action aus, die wiederum zu einem *Human Failure Event* führen kann. Ein Beispiel für einen Error Mechanism wäre, dass zu späte, zu frühe oder unvollständige Ausführen einer Aufgabe, aber auch die Anwendung einer falschen Methode wie z.B. das versehentliche Drücken des Gaspedals anstatt des Bremspedals um zu bremsen.

Die finale Komponente einer HRA ist das *Probabilistic Risk Assessment* (PRA) Model (3), welches das resultierende *Human Failure Event* und dessen Wahrscheinlichkeit basierend auf Experteneinschätzungen beinhaltet. Abhängig von der Kombination des PSF und des Human Error kann dann für jedes Szenario eine Strategie zu dessen Verhinderung entwickelt werden.
Ähnlich wie die PHEA setzt auch die 2004 von Embrey[Emb86] vorgestellte SHERPA auf die Analyse von Bedienaufgaben zum Finden möglicher Ursachen für Fehler. Anders als in PHEA schlägt Embrey für SHERPA eine Dokumentation der *Performance Shaping Factors* und somit einen nachvollziehbaren Bezug zwischen PSF und Verhinderungsstrategie vor.

Action Errors	
A1	Action too long/short
A2	Action mistimed
A3	Action in wrong direction
A4	Action too little/too much
A5	Misalign
A6	Right action on wrong object
A7	Wrong action on right objec
A8	Action omitte
A9	Action incomplete
A10	Wrong action on wrong object
Checking Errors	
Cl	Checking omitted
C2	Check incomplete
C3	Right check on wrong object
C4	Wrong check on right object
C5	Check mistimed
C6	Wrong check on wrong object
Retrieval Errors	
R1	Information not obtained
R2	Wrong information obtained
R3	Information retrieval incomplete
Transmission Errors	
T1	Information not transmitted
T2	Wrong information transmitted
T3	Information transmission incomplete
Selection Errors	
51	Selection omitted
52	Wrong selection made
Plan Errors	
P1	Plan preconditions ignored
P2	Incorrect plan executed

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

Der Schwachpunkt aller traditionellen Verfahren zur Gefahren- oder Unfallanalyse ist, dass aufgrund des „chain-of-event" Modells der Fokus immer auf Fehlern in einzelnen Komponenten liegt. Leveson führt in [Lev11] aus, dass durch diese Beschränkung der Analyse Fehler im Design der Schnittstellen oder im Aufbau der Regelschleife vernachlässigt werden können[Fra17]. Klassische mechanische Systeme werden immer häufiger abgelöst von Systemen, in denen mechanische Prozesse nur noch über digitale Schnittstellen bedient und kontrolliert werden. Durch diese Änderung wird der Bedarf, für die Analyse der Schnittstellen und der Fehlerquellen, in der Digitalisierung des erforderlichen Feedbacks des Systems, erhöht. In mechanischen Systemen, in denen der Mensch noch direkten Bezug zum kontrollierten Prozess hat, besteht ein direkter Feedback Kanal zwischen Mensch und Maschine bspw. ein Auto in dem der Fahrer direktes Feedback über den Zustand des Motors, über dessen Geräusche, Vibrationen oder Abwärme bekommt. In elektromechanischen oder gar digitalen Systemen ist dies nicht mehr oder nur beschränkt der Fall, da *Controls* räumlich unabhängig von den mechanischen Elementen des Systems platziert sein können und das Feedback dadurch nicht mehr direkt wahrgenommen, sondern über entsprechende Feedback Kanäle an den Nutzer weitergeleitet werden muss [Lev11].

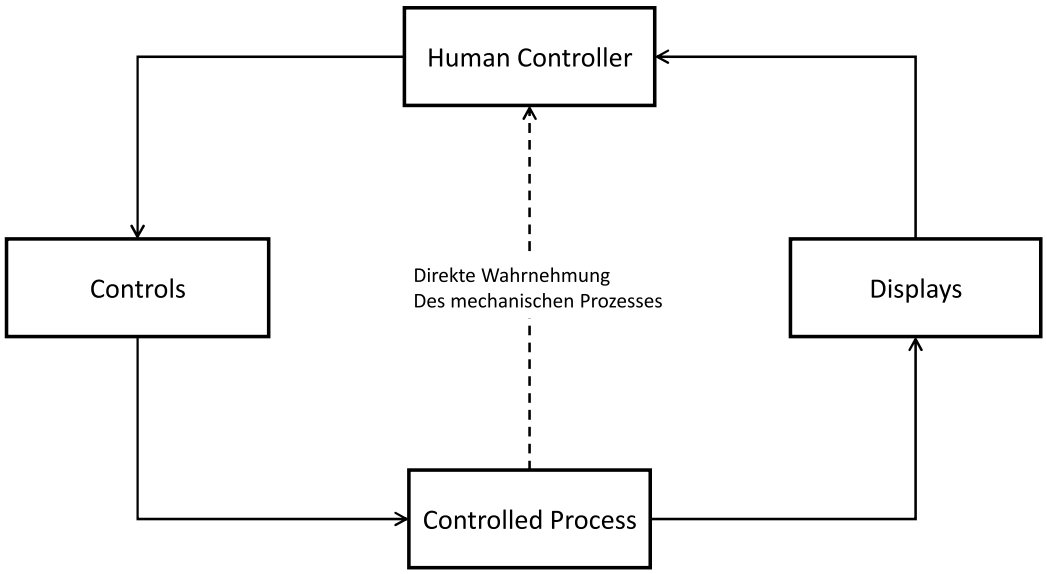


Abbildung 2.4.: Control Stucture eines mechanischen Systems, in dem der *Human Controller* durch die notwendige räumliche Nähe, um den Prozess steuern zu können z.B. ein konventionelles Fahrzeug welches durch unmittelbar verbundene mechanische Instrumente betrieben wird [Lev11]

In [LT18] beschreibt Leveson als Hauptmerkmale des systemtheoretischen Ansatzes an Systemsicherheit die ganzheitliche Betrachtung eines Systems sowie die daraus resultierende Betrachtung von Sicherheit als emergente Eigenschaft. Mit STAMP und STPA stellt Leveson dem traditionellen Ansatz ein neues Kausalitätsmodell und eine darauf aufbauende Gefahrenanalyse gegenüber, welche Systemsicherheit als emergente Eigenschaft des Systems definieren. Dabei wird ein System als sicher (engl. safe) betrachtet, wenn jeder mögliche *Hazard* durch entsprechende Kontrollmechanismen verhindert wird. Hierzu basiert Leveson STAMP auf drei Grundkonzepten:

Safety Constraints	Das Konzept der *Safety Constraints* ist, Reglementierungen zu formulieren, die jegliche *Hazards* im System durch Forderungen an Design und Zustand des Systems verhindern.
Control Structure	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].
Process Models	Eine wichtige Komponente von menschlichen sowie automatisierten Controllern ist das Modell eines Prozesses, welcher entweder direkt oder indirekt durch das Senden von Control Actions reguliert wird. Ein *Process Model* enthält die momentan angenommenen Werte der, für die Aufgabe(n) des *Controllers* wichtigen, Prozessvariablen.

In Werken von France[Fra17] und Thornberry et. al [LT14] wurden die vorgestellten Grundkonzepte zusätzlich um Komponenten zur genaueren Beschreibung des Menschen und dessen Einflusses auf das System erweitert.

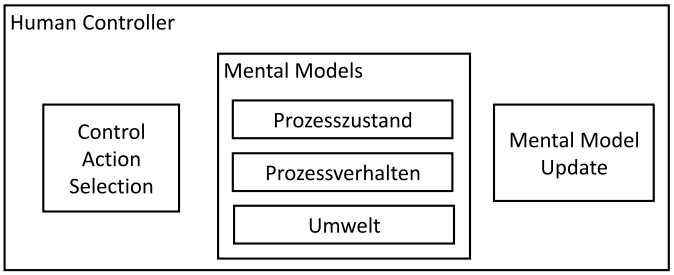


Abbildung 2.5.: Das *Engineering for Humans* Modell zur Beschreibung der mentalen Prozesse des Menschen (Quelle: France[Fra17])

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

erforderlichen Methoden als auch auf psychologische Faktoren wie Stress oder Zeitdruck setzt. Aufgrund ihrer Komplexität werden zusätzlich noch die *Mental Model Updates* miteinbezogen. Anders als bei automatisierten Controllern, die ihre *Process Models* einfach aufgrund des Feedbacks aktualisieren, handelt es sich beim *Mental Model Update* um einen komplexen Prozess, der Interpretation und Extrapolation von vielfältigen Einflüssen durch Umwelt, System und eigene Wahrnehmung beschreibt.
Die *Control Action Selection* wählt anhand der *Mental Models* eine *Control Action* zur Anpassung des Prozesszustandes Eine Analyse dieser Komponente versucht, die Frage zu beantworten, warum eine bestimmte *Control Action* ausgewählt wurde, unter expliziter Miteinbeziehung des Kontextes in dem gehandelt wurde. Hier können Faktoren wie unterschiedliche Ziele des Operators und des System Designers eine Rolle spielen, z.B. Fokus auf Sicherheit vs. Fokus auf Erreichen des Ziels. Ein weiterer Punkt sind die unterschiedlichen Entscheidungsmöglichkeiten: Der Fahrer könnte beispielsweise einem Hindernis ausweichen, er könnte aber auch davor stehen bleiben und warten. Hier unterscheidet Rasmussen in [Ras82] zwischen Regel-, Fähigkeits- oder Wissens-basierten Entscheidungen. Diese Kategorisierung unterteilt die Annahmen, die zu einer Entscheidung führen in drei Kategorien:

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.

Unabhängig von der Art der Entscheidungsfindung ist die Selektion der *Control Action* für ein bestimmtes Szenario; allerdings immer abhängig vom Zeitdruck, dem der Mensch ausgesetzt ist. Auch Faktoren wie Müdigkeit oder Stress, welche eng mit Zeitdruck zusammenhängen, können Auswirkungen darauf haben ob und wie tatsächlich alle Informationen der *Mental Models* genutzt werden können oder ob die Wahl anhand von spontanen Ideen oder Erfahrungswerten getroffen wird [DM07][Lev11].
Zur Modellierung der Wahrnehmung definiert Thornberry in [LT14] die *Sensory Perception* die die Wahrnehmung von Feedback über die natürlichen Sensoren (bzw. Sinne) des Menschen beschreibt. Beispielhaft für die *Sensory Perception* wäre die veränderte visuelle Wahrnehmung bei dichtem Verkehr, wodurch die Aufmerksamkeit mehr auf den Verkehr gerichtet ist und visuelles Feedback über einen Display eventuell übersehen wird. Thornberry formuliert dies als: „*Sensory Perception* includes that raw visual, proprioceptive, and vestibular feedback the human receives

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.

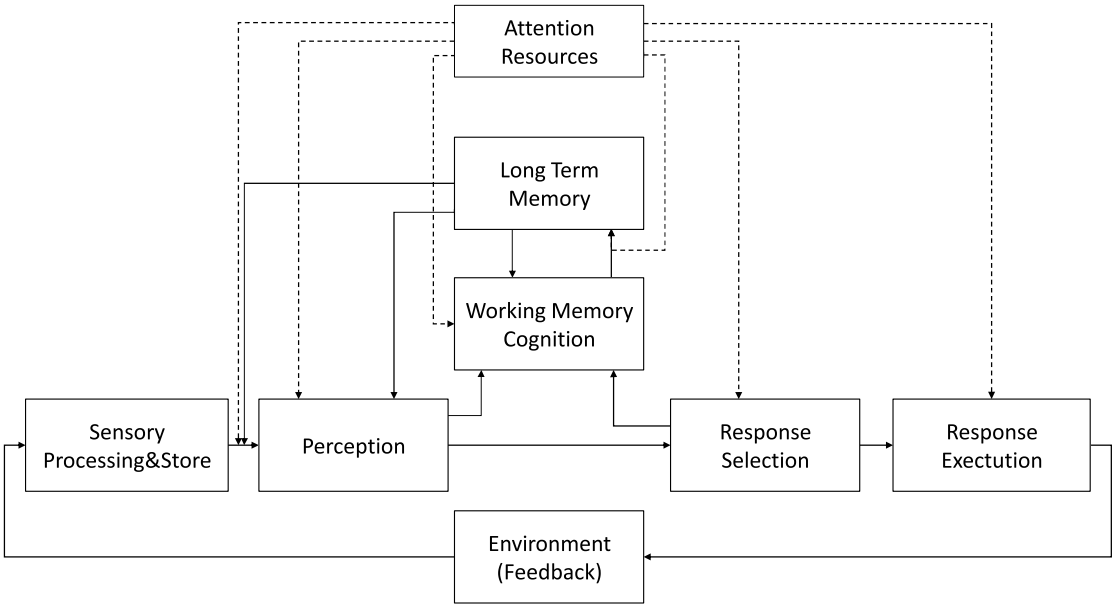


Abbildung 2.6.: *Wickens' Human Information-Processing Model*[Wic02][Wic+15]

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)

Zur Repräsentation einer traditionellen Gefahrenanalyse, die in der Industrie Anwendung findet, wurde für diese Arbeit eine HEA durchgeführt wie sie in Abschnitt 2.3 beschrieben wurde. Das Verfahren und die angewendeten Begrifflichkeiten wurden von der Continental Teves AG & Co. oHG (in der restlichen Arbeit als Continental bezeichnet) in [Rudgu][1] festgelegt.
Die Analyse bezieht sich auf konkrete Aufgaben des Operators und untersucht diese auf mögliche *Human Error Mode*s (HEMs), die bei bestimmten PSF auftreten können. Hierzu geht das Verfahren zuerst auf die Definition der Aufgabe ein und fordert eine Aufstellung aller zur Durchführung benötigten Schritte und der (gedanklichen) Planung dieser. Das in Tabelle 3.1 dargestellte Schema definiert außerdem noch die Wahrscheinlichkeit für das Auftreten des jeweiligen Error Modes welche die von der Ford Motor Company in [Mod11] auf Seite 135 vorgestellt wird. Die

Operator Task	Discription	Goal	Actions	Plans	Performance shaping factors	Human error mode	Occurance Propability	Human error effect	*Control Strategy*

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

Very High	$\geqq$ 1 in 10
High	1 in 20
Moderate	1 in 500 bis 1 in 2000
Low	1 in 10.000 bis 1.000.000
Very Low	Auftreten des Fehlers wird durch andere Maßnahmen verhindert

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.

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

3.2. STPA Guideline zur Durchführung einer *Human Factor* Analyse

In diesem Abschnitt wird die Vorgehensweise bei der, im Rahmen dieser Arbeit durchgeführten, STPA mit Fokus auf dem *Human Factor* (im Folgenden als Beispielanalyse bezeichnet) in Form einer Guideline dargestellt. Diese Guideline soll sowohl zur Nachvollziehbarkeit der Beispielanalyse als auch zur Hilfestellung in der Anfertigung ähnlicher Analysen dienen und erhebt keinen Anspruch auf eine vollständige Abdeckung des von Leveson definierten STPA Prozesses[Lev11]. Für eine vollständige Abbildung des Ablaufes einer STPA wird auf das STPA Handbook von Leveson [LT18] verwiesen, welches auch Grundlage für diese Guideline ist. STPA ist eine schrittbasierte iterative Gefahrenanalyse, sowohl zur Gefahrenerkennung in existierenden Software-intensiven Systemen als auch zur Erstellung von sicherheitsgetriebenem System-Designs. Hierbei definiert STPA einen vierstufigen Prozess:

Schritt 1: Definition des Systems und des Analyseumfangs

Schritt 2: Modellierung der *Control Structure*

Schritt 3: Analyse der *Unsafe Control Action*s (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 gemütlich 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*

2. Aufstellung einer initialen Liste aller *Accidents* und *Hazards* die beim Erfüllen der Ziele auftreten können. Auch diese Liste sollte nicht den Anspruch haben, final zu sein, da eine Verfeinerung und Ergänzung der Einträge zu einem späteren Zeitpunkt in der Analyse zu einer Verfeinerung der *Safety Constraints* auf Systemebene führt.
   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*

Dabei dienen *Actuators* und *Sensors* zur Signalübertragung zwischen *Controller* und *Controlled Process* und müssen erst bei der Analyse der *Causal Factors* in Schritt 4 berücksichtigt werden, um Fehler in der Kommunikation genauer zu analysieren. Zur Übersichtlichkeit können sie in diesem Schritt, je nach Komplexität des Systems, vernachlässigt werden. Bei den erwähnten Signalen wird zwischen drei Arten unterschieden:

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

Control Actions beschreiben explizite Kommandos, die von einem *Controller* an seinen *Controlled Process* oder einen weiteren *Controller* gestellt werden. Eine *Control Action* wird dabei durch einen *Actuator* ausgeführt, wodurch der Zustand des *Controlled Process* oder des angesprochenen *Controllers* verändert wird[Ant13]. Eine so ausgelöste Zustandsänderung kann dann durch einen entsprechenden *Sensor* in Form von Feedback an den *Controller* zurückgegeben werden. Es müssen allerdings auch noch andere Aus- und Eingaben berücksichtigt werden, die auf das Verhalten des Systems wirken. Hier ist zu unterscheiden zwischen äußeren Faktoren wie Temperatur oder Luftfeuchtigkeit, die physischen Einfluss auf das System nehmen und prinzipiell bei einer Analyse der *Causal Factors* berücksichtigt werden müssen, und Input der die Wahl einer passenden *Control Action* beeinflusst. Der zu berücksichtigende Input unterscheidet sich danach, ob ein automatisierter oder ein menschlicher *Controller* betrachtet wird.
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.

Operative Kultur Kulturelle Unterschiede in der Handhabung von Situationen wie Konfliktlösung, Zusammenarbeit oder Durchführung bestimmter Systemfunktionen (z.B. Miteinbeziehung von Feedback des Beifahrers).

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.

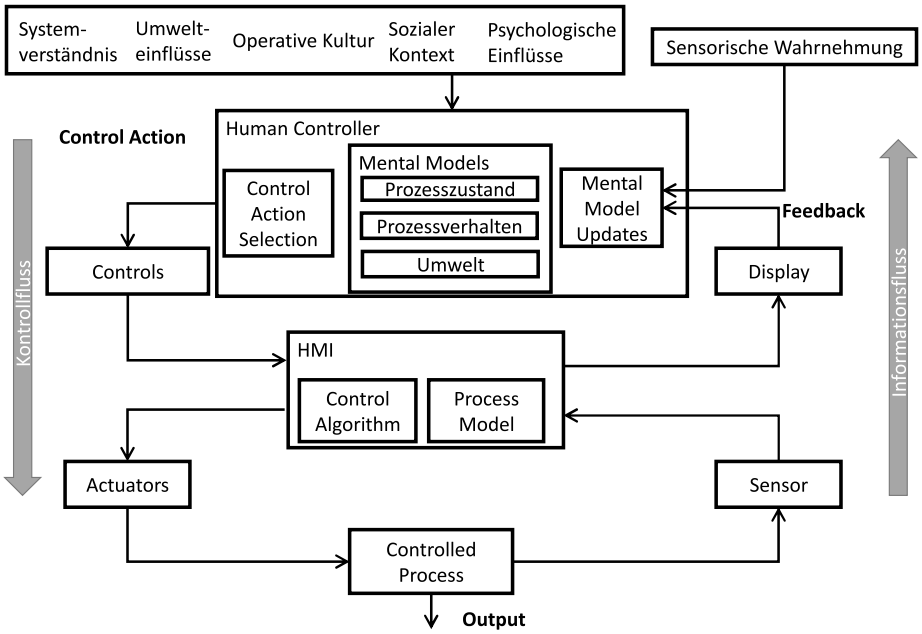


Abbildung 3.1.: Der Aufbau einer hierarchischen *Control Structure*, wie von Leveson in [Lev11] beschrieben, unter Berücksichtigung der Erweiterungen von France[Fra17] und Thornberry[LT14]. Die *Control Structure* stellt ein System dar, in dem die Mensch-Maschinen Interaktionen über ein HMI (Human Maschine Interface) geregelt werden.

In Abbildung Abbildung 3.1 ist eine *Control Structure* mit den oben beschriebenen Input Feldern abgebildet. In der Abbildung wird ein System beschrieben, in dem ein menschlicher Operator über eine Schnittstelle mit den mechanischen Prozessen des Systems kommuniziert. Hierbei beinhaltet das System nicht nur die *Actuators* und *Sensors*, die für die direkte Interaktion mit dem Prozess verantwortlich sind, sondern auch eine Zwischenschicht für elektromechanische oder digitale *Controls*, mit denen ein Operator über ein *Human Maschine Interface* (HMI) in das System eingreifen kann.

Beim Erstellen der *Control Stucture* kann eine iterative Vorgehensweise, wie schon im letzten Schritt angewendet, von Vorteil sein; insbesondere wenn die finale Architektur des Zielsystems noch nicht feststeht. Durch die fortlaufende Ergänzung der hier initial erstellten *Control Structure* im Verlauf der Analyse durch weitere Regelschleifen und Komponenten können die benötigten *Safety Constraints* direkt umgesetzt werden. Abbildung 3.2 und 3.3 stellen jeweils einen Ausschnitt der *Control Structure* aus der Beispielanalyse dar, in dem die Interaktion der zwei Komponenten *Driver* und *HMI* zusammen mit den zu analysierenden *Control Actions* dargestellt sind.

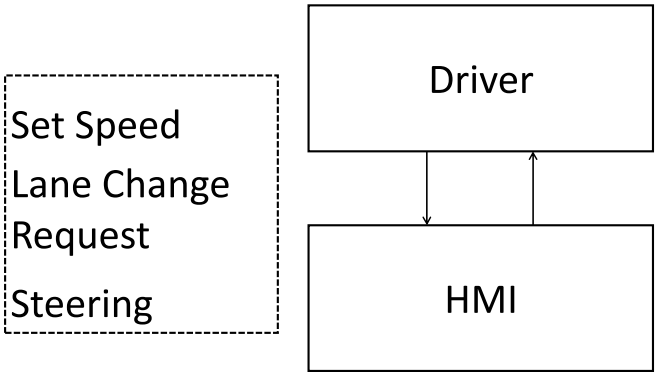


Abbildung 3.2.: Die Regelschleife zwischen HMI (Human Maschine Interface) und Driver im betrachteten Beispielsystems

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.

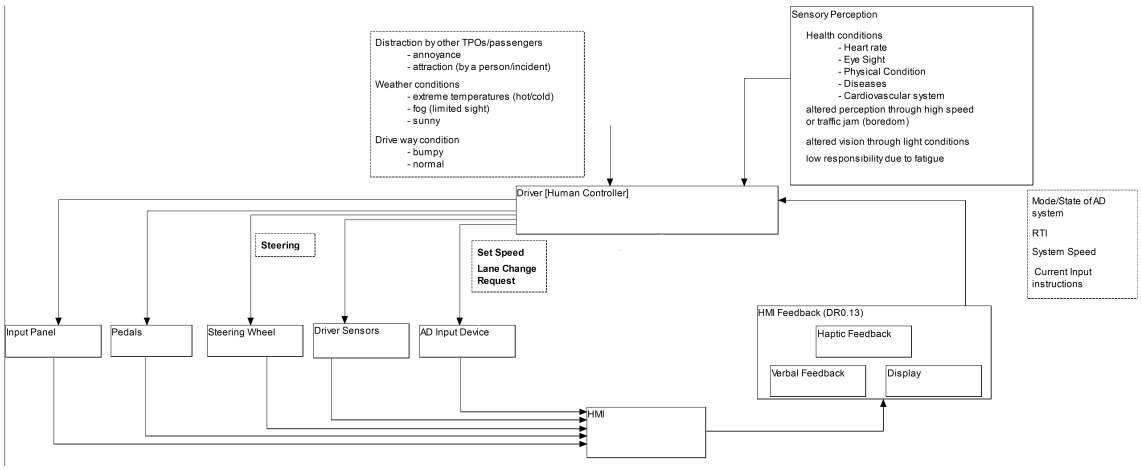


Abbildung 3.3.: Die verfeinerte Regelschleife zwischen HMI (Human Maschine Interface) und Driver im betrachteten Beispielsystem

Schritt 3: Analyse der UCAs

Der dritte Schritt dient der Analyse der in Schritt 2 hinzugefügten Control Actions auf potenzielle *Unsafe Control Actions*, die in einem entsprechenden Kontext auftreten können. Hierzu werden die aufgestellten Aktionen systematisch auf vier von Leveson in [LT18] definierte Gefährdungskategorien untersucht.
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

Control Action	Nicht ausführen der CA führt zur *Hazard*	Ausführung der CA führt zur *Hazard*	Falsches Timing der CA führt zur *Hazard*	Zu lange oder kurze Ausführung führt zur *Hazard*
CA-1				
...				

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.

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 komplette 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

Wie in den Beispielen (UCA-1 - 4) aus Schritt 3 zu sehen ist, muss bei der Analyse von Systemen nach dem Shell-Modell auf die besondere Rolle des Menschen in der Selektion und Ausführung von Control Actions, wie bereits in 2.2 beschrieben, geachtet werden. Besonders Einflüsse wie Stress, mangelnde Erfahrung in der Bedienung von *Controls* oder eine veränderte *Sensory Perception* können *Unsafe Control Actions* auslösen und müssen in Form von *Causal Factors* dokumentiert werden. Weitere Ursachen für *Unsafe Control Actions* können Fehlfunktionen in dem *Controller*, der die *Control Action* ausgibt, sein sowie ein fehlender oder kaputter *Sensor* oder *Actuator*, durch den eine *Control Action* ungewollt ausgelöst oder verhindert werden kann. Deshalb müssen alle Komponenten, die in die *Feedbackschleife* der *Control Action* mit eingebunden sind, betrachtet werden um mögliche Ursachen von *Unsafe Control Actions* zu verhindern.

In Abbildung 3.4 sind die *Causal Factors*, die bei der Analyse eines komplexen Systems mit besonderem Fokus auf den *Human Factor* berücksichtigt werden müssen [LT18][LT14], dargestellt. Bei der Analyse ist zwischen vier Arten von möglichen Ursachen zu unterscheiden, die von verschiedenen Teilen des Systems ausgehen. Die ersten beiden Kategorien, die im Folgenden mit Fokus auf den *Human Factor* genauer erläutert werden, beziehen sich auf den menschlichen oder automatisierten *Controller* und auf den Feedback- und Informationsfluss durch Sensoren oder Displays. Die Kategorien drei und vier unterscheiden sich nicht von der Vorgehensweise einer STPA ohne Einbeziehung des *Human Factor* und werden deshalb nur grob skizziert, wobei für eine detailierte Beschreibung auf das STPA Handbook von Leveson verwiesen wird[LT18].

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 Akkuratheit 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 vorausfahrende Fahrzeug Gas geben wird, und gibt Gas, ohne auf die Situation zu achten.

- *Fehler in der Ausführung einer Control Action durch den Human Controller*
  Wenn eine *Control Action* ausgewählt wurde, bildet die Ausführung dieser den letzten zu analysierenden Schritt im *Human Controller*[LT14]. Hierbei werden Faktoren wie versehentliche Ausführung einer *Control Action* oder falsches Timing einbezogen. Diese Stufe des Verhaltens des *Human Controller* ist unabhängig von der Selektion der *Control Action* und betrifft nur noch die physische Umsetzung dieser. So kann z.B. die richtige *Control Action* gewählt werden, aber bei der Umsetzung dieser (bspw. dem Betätigen des Gaspedals) entsteht eine UCA (bspw. durch Verwechslung mit dem Bremspedal).

Unzureichendes Feedback oder Informationen als Ursache für Unsafe Control Actions

Bei der Betrachtung des Feedbacks und dessen Verarbeitung durch einen *Human Controller* kommen die, in STPA Schritt 2 modellierten, Komponenten der *Sensory Perception* und das *Mental Model Update* ins Spiel. Hier müssen nun zusätzlich zur Erwägung der, in Abbildung 3.4 unter Feedback aufgeführten, Punkte die Einflüsse durch die menschliche Wahrnehmung[Wic02][Wic+15] und die Verwertung dieser berücksichtigt werden.

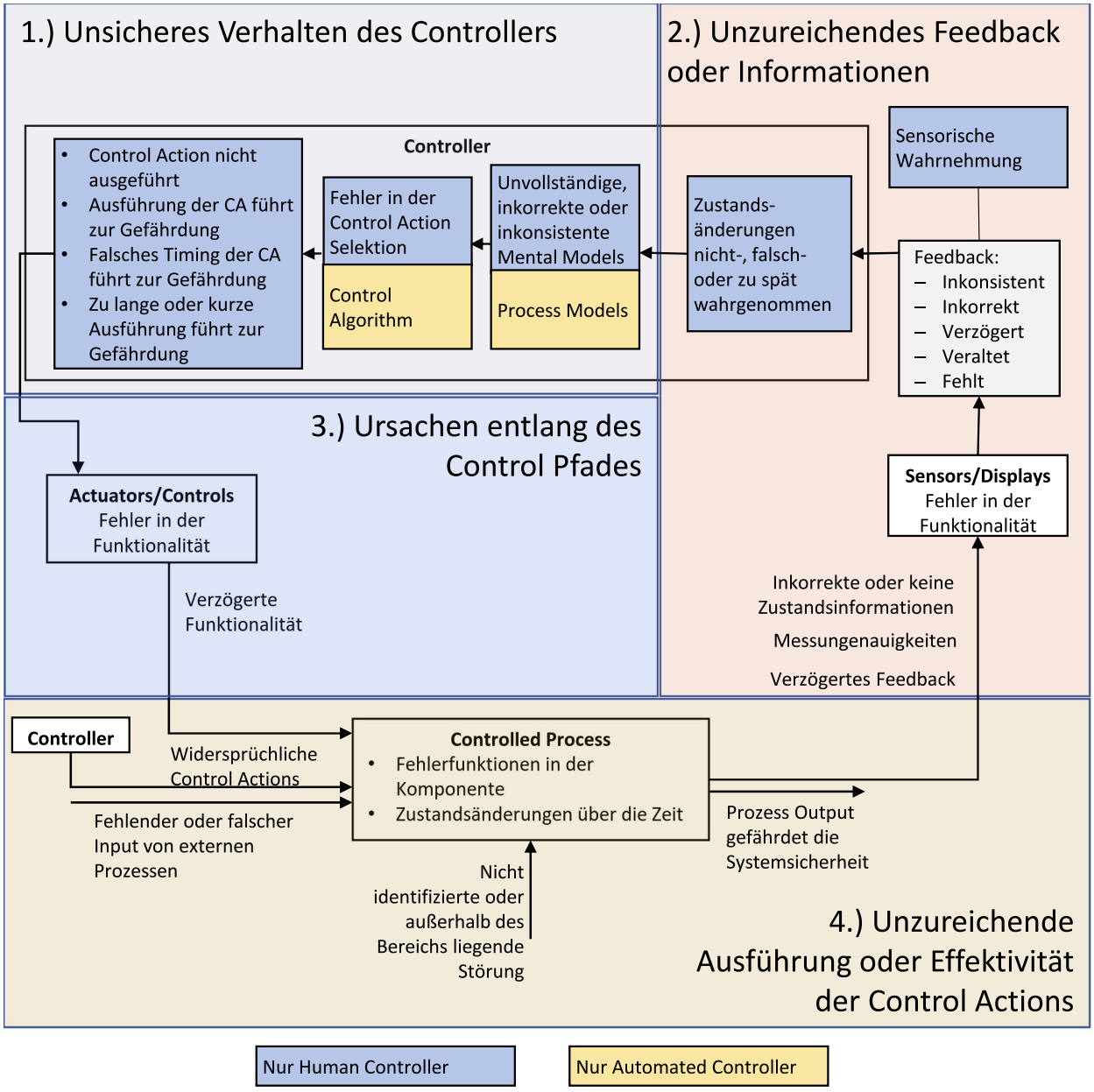


Abbildung 3.4.: Die unterschiedlichen *Causal Factors* die zu UCAs (Unsafe Control Actions) führen können [Lev11][Fra17][LT14]

4. Evaluation des Mehrwerts von STPA ggü. traditionellen Verfahren

Für die Evaluation des Mehrwerts durch die Verwendung von STPA verglichen mit der traditionellen HEA Methode wurden die Ergebnisse der, in den Kapiteln 4.3 und 4.4 beschriebenen, Analysen verwendet. Hierdurch wurden die Unterschiede anhand der Analyse eines begrenzten Funktionsbereiches des Beispielsystems, welches in Abschnitt 4.2 beschrieben wird, deutlich gemacht. Abschnitt 4.1 beschreibt das Design der in diesem Kapitel durchgeführten Fallstudie und vermittelt einen genaueren Überblick über die Methodik. In Abschnitt 4.5 werden in einem ersten Schritt die gesammelten Ergebnisse in einer Überdeckungsmatrix auf Abdeckung der Sicherheitsanforderungen der STPA *Safety Contstraints* durch entsprechende *Control Strategies* aus der HEA analysiert. Um ein genaueres Bild der regulierten Bereiche des Systems durch beide Analysen zu bekommen, wurde danach eine Liste an sicherheitsrelevanten Kategorien aufgestellt und die Abdeckung jeder Kategorie durch einen entsprechenden *Safety Constraint*/*Control Strategy* geprüft.
Die Evaluation wird durch eine Auflistung der herausgearbeiteten Vor- und Nachteile in Abschnitt 4.6 und eine Einschätzung der Validität der jeweiligen Ergebnisse in Abschnitt 4.7 abgeschossen.

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

Die Fallstudie beschäftigt sich mit der Effizienz verschiedener Gefahrenanalysen bei der Analyse des *Human Factor*. Dabei setzt sich der behandelte Fall aus der Gefahrenanalyse und einem System zusammen, welches mit Fokus auf den *Human Factor* hin analysiert wird. Die Einheiten, die in dieser Arbeit zur Beantwortung der Forschungsfrage betrachtet wurden sind einmal die Gefahrenanalysen STPA und HEA, wobei letztere ein traditionelles Verfahren darstellt, und zum anderen ein konzeptionelles System zum automatisierten Fahren.

4.1.4. Forschungs Methodik

Im Rahmen dieser Arbeit wurden eine HEA und eine STPA des, in Abschnitt 4.2 vorgestellten Systems zum automatisierten Fahren (im Folgenden als Beispielsystem bezeichnet), durchgeführt. Beide Analysen wurden in Absprache mit Continental durchgeführt, wobei die HEA auf einer von Rudolph im Auftrag von Continental verfassten Guideline[Rudgu], wie in Abschnitt 3.1 beschrieben, basiert. Die Analysen wurden jeweils, wie in Abbildung 4.1 beschrieben, auf demselben System und mit denselben Systemfunktionen, teilweise parallel durchgeführt. Beide Analysen wie auch die Evaluation der Ergebnisse wurden hierbei vom Autor dieser Arbeit erstellt und die Ergebnisse in Abschnitt 4.3 bzw. 4.4 erläutert.

Spurwechselanforderung(an das ADS) (engl. Lane Change Request)	Während das ADS aktiv ist kann der Nutzer des Fahrzeuges einen Spurwechsel, zu einer verfügbaren Fahrspur, über das HMI beantragen.
Manuelle Steuerung (engl. Manual Steering)	Der Fahrer des Fahrzeuges kann jederzeit die Kontrolle über das Fahrzeug durch einen Lenkeingriff übernehmen. Eine alternative Funktion dieser *Control Action* wäre eine Beeinflussung des ADS während dieses aktiv ist und bleibt.
Geschwindigkeitseingabe (engl. Set Speed)	Während das ADS aktiv ist, kann der Nutzer des Fahrzeuges eine Änderung der Geschwindigkeit auf einen definierten Wert über das HMI beantragen.

Tabelle 4.1.: Beschreibung der Systemfunktionen des ADS, die in der Beispielanalyse 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:**
  Z.B. kann *Manuelle Steuerung* sowohl während des automatisierten Fahrens als Eingriff in das Fahrgeschehen ausgeführt werden, als auch während des manuellen Fahrbetriebs. Dadurch ergeben sich für die Betrachtung des *Human Factors* kritische Situationen, wie z.B. die Annahmen des Fahrers über die Reaktion des Lenkrades im aktuellen Modus des Systems oder die Reaktion des Systems auf plötzliche, möglicherweise gefährdende Eingriffe des Fahrers.

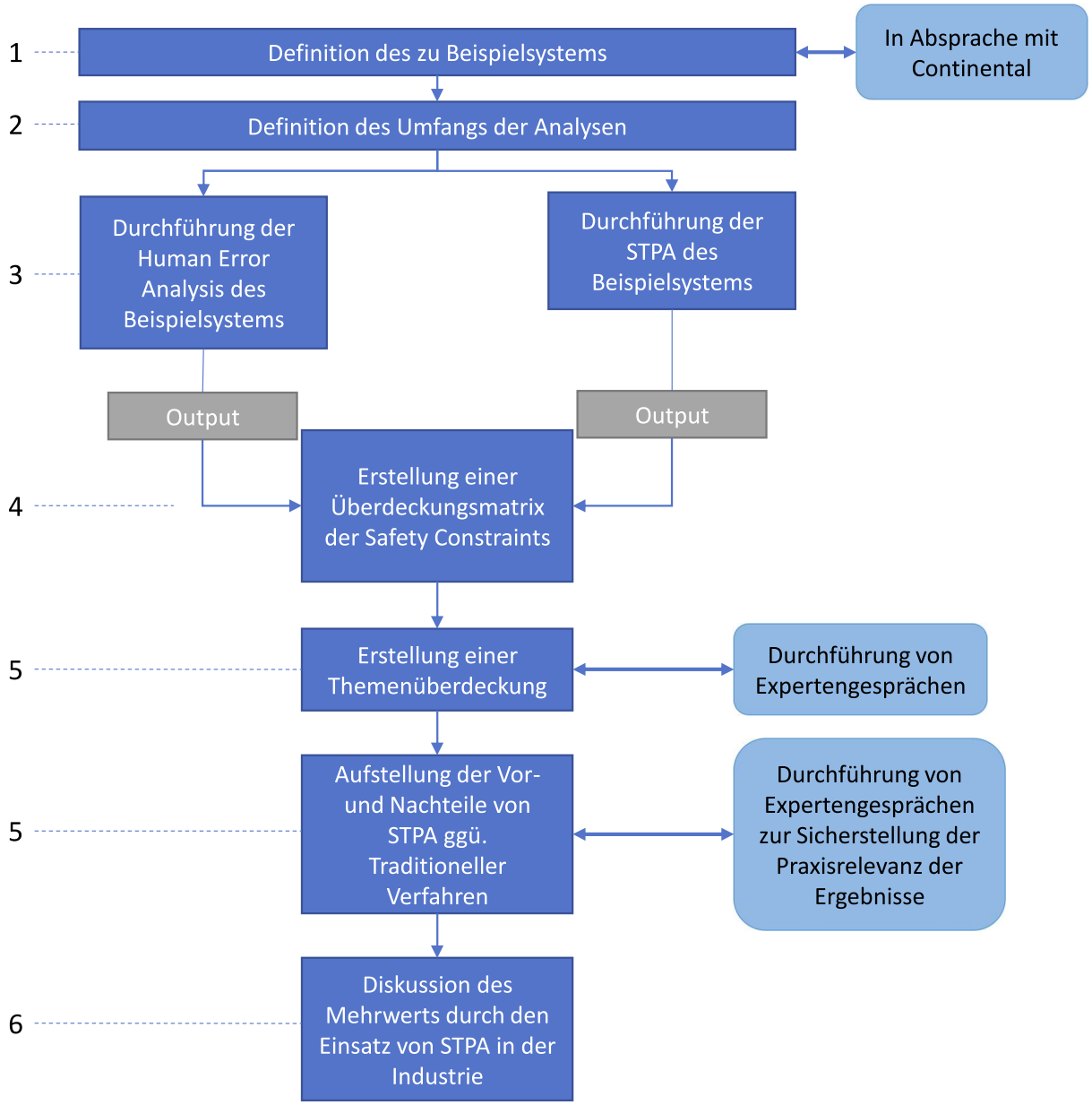


Abbildung 4.1.: Die einzelnen Schritte der Evaluation

Die Ergebnisse der beiden Analysen wurden nach deren Abschluss einer Überdeckungsanalyse unterzogen, wobei die Frage beantwortet wurde, inwiefern die *Safety Constraints* der STPA durch *Control Strategies* der HEA überdeckt werden. Hierzu wurde sowohl eine Analyse der Übereinstimmung der jeweiligen Ergebnisse vorgenommen, als auch die Abdeckung sicherheitsrelevanter Kategorien, die unter Abstimmung mit Experten erstellt wurden, bestimmt. Aus den Daten der Analysen selbst und der Abdeckungsanalyse wurden dann in Schritt fünf die Vor- und Nachteile der STPA ggü. traditionellen Verfahren aufgestellt und in Expertengesprächen eine Praxisrelevanz der

Ergebnisse sichergestellt. Als letzter Schritt wurde der Mehrwert durch den Einsatz von STPA zur *Human Factor* Analyse herausgearbeitet und in einer Schlussfolgerung die wichtigsten Punkte aus der Arbeit zusammengefasst.

4.1.5. Sammlung der Daten

Die Informationen über das analysierte System zum automatisierten Fahren wurden aus existierenden Analysen und aus, von Continental zur Verfügung gestellten, Dokumenten gesammelt. Zur Durchführung und Dokumentation der Analysen wurden im Fall der HEA die von Rudolph[Rudgu] und im Fall von STPA die von Leveson[LT18][Lev11], France[Fra17] und Thornberry [LT14] beschriebenen Methoden verwendet. Zur Analyse der Ergebnisse wurden die in den Analysen gesammelten Daten sowie Informationen aus Expertengesprächen genutzt. Die vollständige Dokumentation der Analysen ist dieser Arbeit als Anlage A und B angehängt.

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.

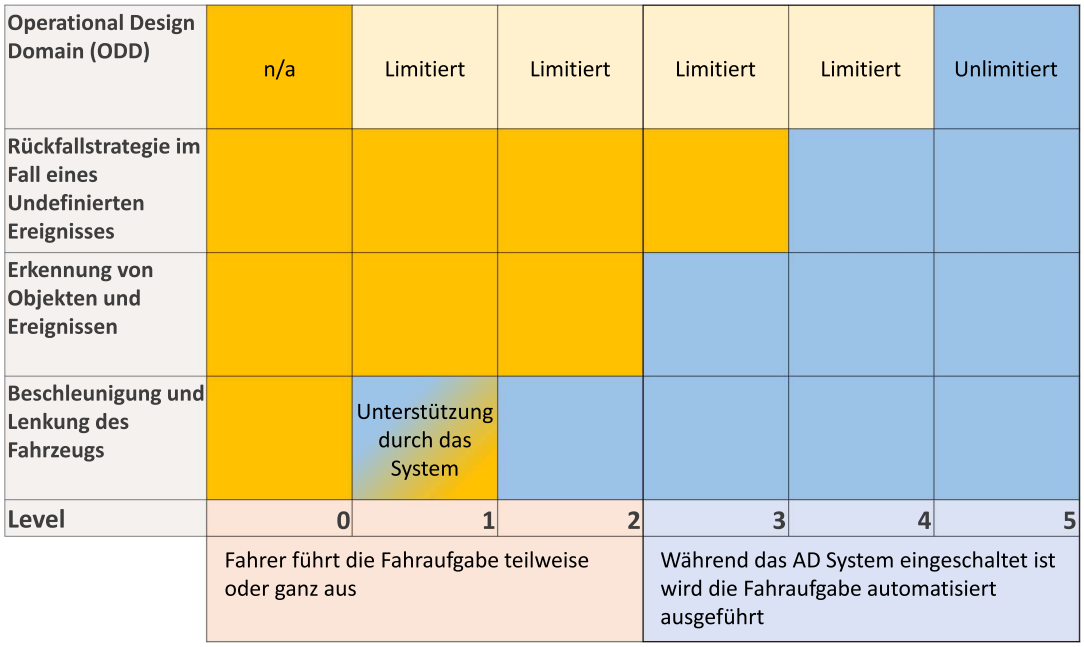


Abbildung 4.2.: Die fünf Level autonomen Fahrens der SAE (Society of Automotive Engineers) J3016[Int16]

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 Fahrassistenzsystem, 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 fahrfremden 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

Die STPA Analyse des in Abschnitt 4.2 vorgestellten Beispielsystems wurde mittels des A-STPA Plugins der XSTAMPP Plattform durchgeführt[1] [AW16] und ist in diesem Dokument in Anhang A zu finden. Die Analyse ist nicht als vollständige STPA des Systems zu betrachten, da dies den Rahmen der Arbeit überschreiten würde und für das in Abschnitt 1.2 definierte Ziel nicht notwendig ist. Anstatt dessen beschränkt sich die Analyse auf drei, für diese Arbeit notwendige, Systemfunktionen (siehe Tabelle 4.1). Die Priorisierung der Ergebnisse der STPA wurde durch eine Einschätzung der Severity nach der ISO26262 [Sch11], die in Tabelle 4.2 abgebildet ist, durchgeführt. Hierzu wurde, wie im STPA Handbook [LT18] vorgeschlagen, bei der Analyse der *Accidents* in Schritt 1 der Analyse eine initiale Priorisierung vorgenommen. Diese wurde dann als Grundlage für die weitere Bewertung der Hazards und *Unsafe Control Actions* verwendet, um eine möglichst granulare Priorisierung der *Safety Constraints* zu erreichen.

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

Severity	SO	S1	S2	S3
Beschreibung	Keine Verletzungen	Leichte/ moderate Verletzungen	Schwere/ lebensbedrohliche Verletzungen (Überleben wahrscheinlich)	Lebensbedrohliche Verletzungen (Überleben ungewiss) oder tödliche Verletzungen

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

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.

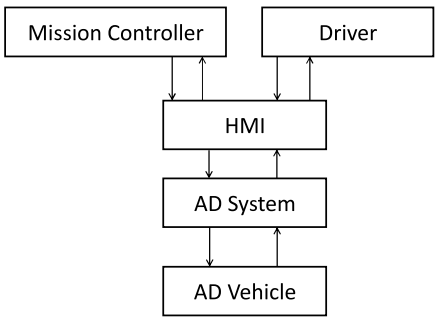


Abbildung 4.3.: Die initiale *Control Structure* des Beispielsystems

Nach einer initialen Beschreibung des Systems wurde der Umfang der Analyse durch eine Auflistung der funktionalen Ziele (*System Goals*) bzw. *Accidents* und *Hazards* auf Systemebene definiert. Die *System Goals* wurden hierbei so ausgewählt, dass die zu betrachtenden Funktionen in Form von Zielen definiert wurden, wie beispielsweise *SG-1 - Perform Lane Change* welches den Spurwechsel als klare Funktion definiert. Des Weiteren beinhaltet die Liste allgemeine funktionale Anforderungen, die zur Ausführung dieser Funktionen erfüllt sein müssen wie beispielhaft zu sehen in *SG-11 - Fail Operational*. Als direkte Antwort auf die initialen Definitionen wurden für die Hazards entsprechende *Safety Constraints* aufgestellt. Abschließend wurden die Anforderungen an das System Design, die durch die *Safety Constraints* und *System Goals* in Form von Design Requirements an die *Control Structure* aufgestellt wurden, festgehalten.

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

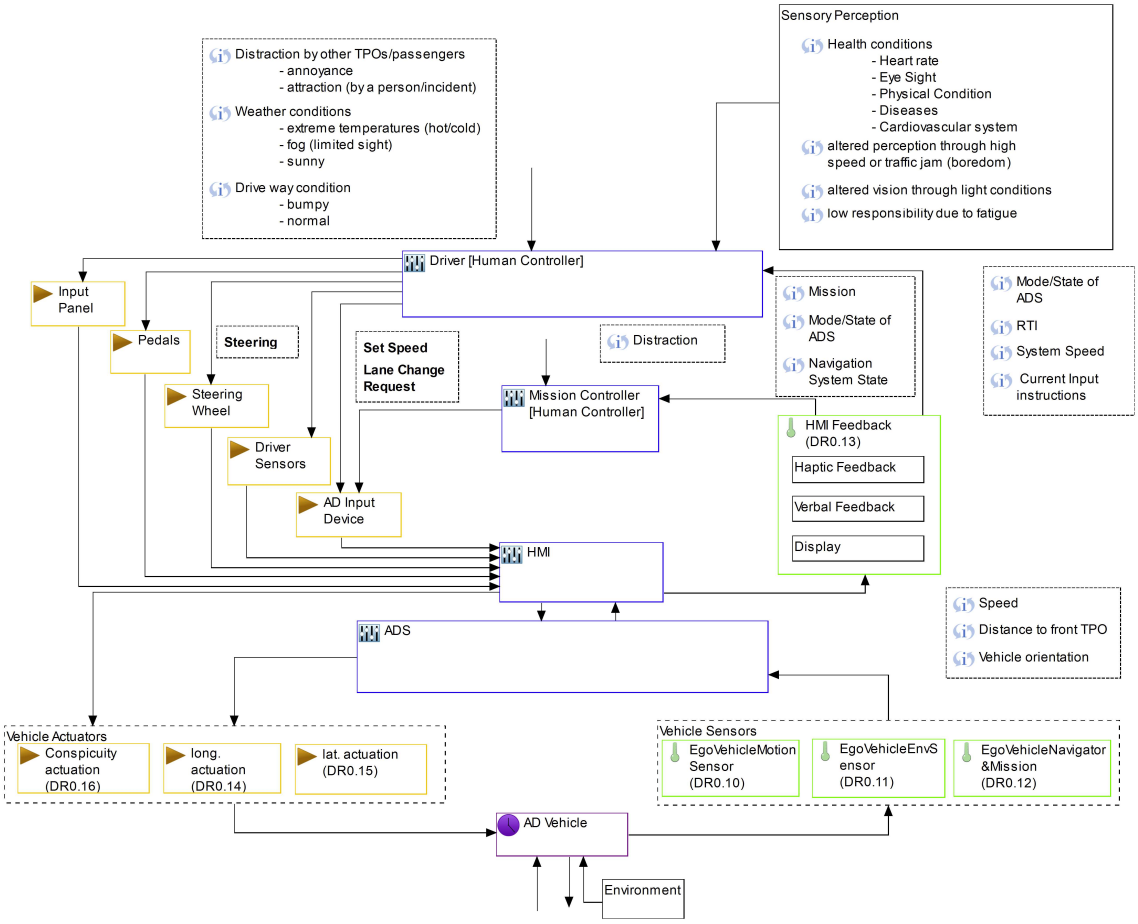


Abbildung 4.4.: Die finale *Control Structure* der in Anhang A zu findenden STPA eines ADS (Automated Driving System)

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*

Der erste Teil der Umsetzung von Schritt 4 in XSTAMPP beinhaltet die Definition aller Process bzw. *Mental Models*, wie in der Guideline in Abschnitt 3.2 beschrieben. In Abbildung 4.5 sind die *Mental Model* des Fahrers abgebildet, die das relevante Wissen des Fahrers über das Fahrzeug und das ADS darstellen. Die Erstellung der *Process Models* wurde unter Zuhilfenahme existierender Dokumentation vorgenommen, um möglichst viele Prozessvariablen bei der Analyse der *Causal Factors* berücksichtigen zu können.

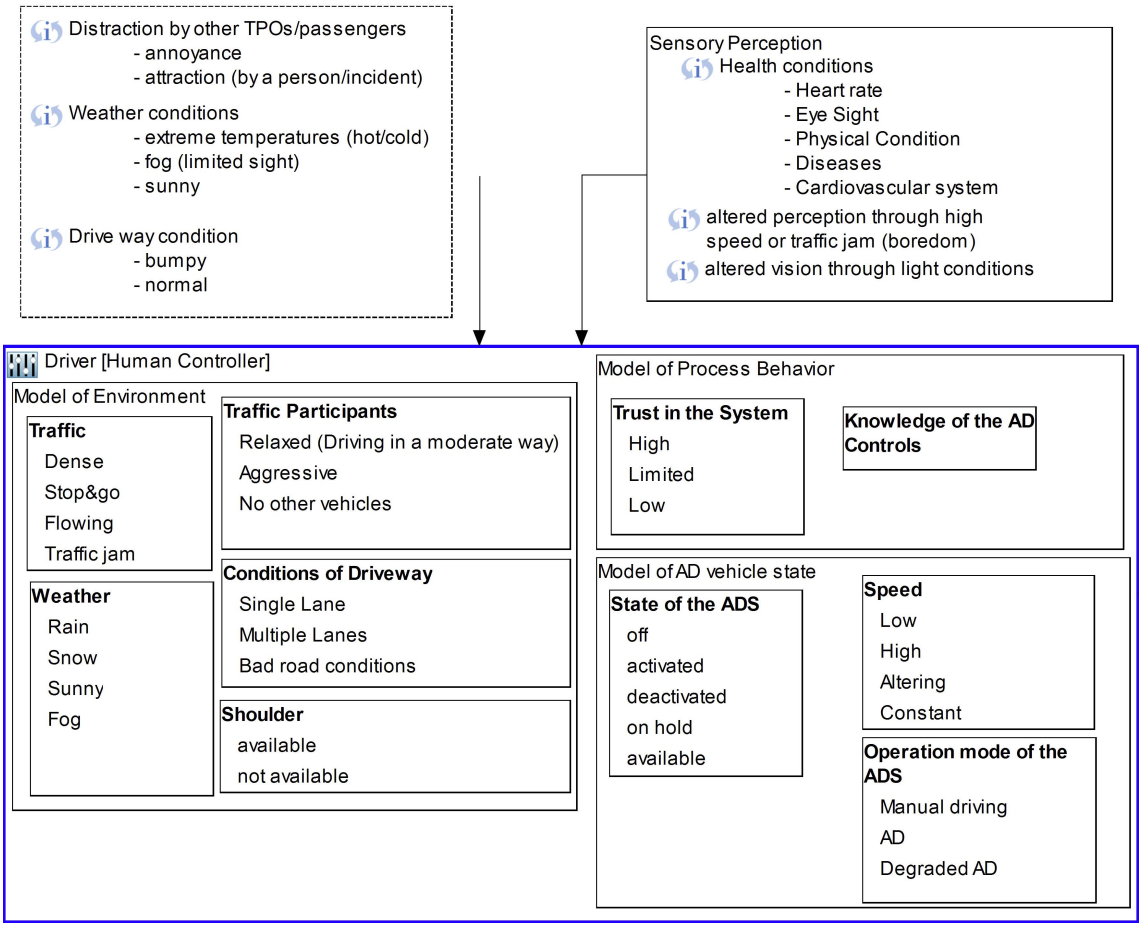


Abbildung 4.5.: *Process Model* des Drivers in der STPA des Breispielsystems mit den *Mental Models*, dem Input und der *Sensory Perception*

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

Die HEA des Beispielsystems wurde nach der, in Abschnitt 3.1 beschriebenen Vorgehensweise, durchgeführt und analysiert. Die, in Tabelle 4.1 beschriebenen, Systemfunktionen werden im Folgenden als Operator Tasks bezeichnet. Zusätzlich wurde aufgrund der steuerungsbasierten Vorgehensweise der HEA noch ein weiterer Operator Task hinzugefügt, der die Beobachtung und Reaktionsfähigkeit auf Feedback durch den Operator beschreibt. Die PSF wurden anhand

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

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 erstrebten Ziels
  - Erstrebung eines inkorrekten 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/kurz angewendet
  - In die falsche Richtung ausgeführt
  - Richtige Aktion auf falschem Objekt
  - Falsche Aktion auf richtigem Objekt
  - Flasche 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[Rudgu]

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.

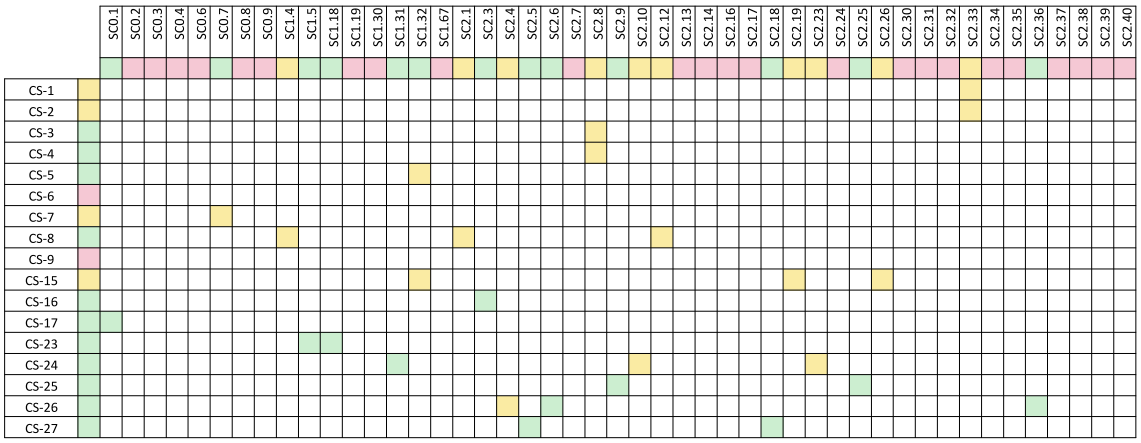


Abbildung 4.6.: Überdeckungsmatrix der *Safety Constraints*(SC) aus der STPA und der *Control Strategies*(CS) aus der HEA

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:

Weiß	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

Anhand der Überdeckungsmatrix kann die Abdeckung der *Safety Constraints*, die bei der Analyse des Systems in der STPA gefunden wurden, durch die in der HEA gefundenen *Control Strategies* überprüft werden. Hierbei kommt man auf eine Abdeckung von lediglich 49%, oder 23, der insgesamt 47 STPA *Safety Constraints* durch entsprechende *Control Strategies*, die in der HEA aufgestellt wurden. Andersherum wurden 88%, oder 15, von insgesamt 17 aller *Control Strategies* der HEA in der STPA gefunden.
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*

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

Auch wenn beide Constraints hier letztendlich dieselbe Anforderung an die Geschwindigkeit des Fahrzeugs stellen, ist CS-8 wesentlich allgemeiner formuliert, wodurch nicht nur SC1.4 sondern auch SC1.67 und SC2.12 abgedeckt werden. Auf der einen Seite hat man damit weniger und allgemeinere Constraints, auf der anderen Seite sind präzisere Formulierungen, wie in Abschnitt 4.6.1 vertieft wird, für eine Umsetzung des Constraints wichtig. Abbildung 4.7 verdeutlicht zusätzlich noch die Verteilung der STPA *Safety Contraints* und deren Überdeckung durch die HEA auf den drei Analyseebenen, die in STPA Schritt eins, drei und vier betrachtet werden (siehe Tabelle 4.5).

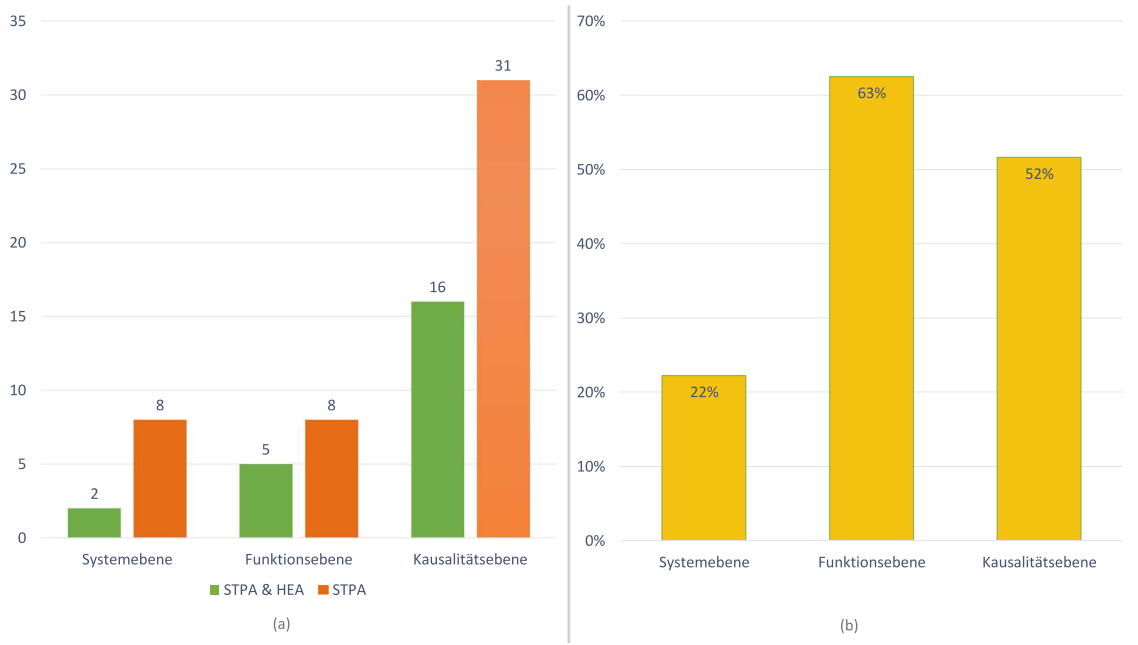


Abbildung 4.7.: Absolute (a) und prozentuale(b) Verteilung der STPA *Safety Constraints* (in Orange) auf die drei Ebenen der STPA und die Abdeckung der jeweiligen *Safety Constraints* durch entsprechende *Control Strategies* der HEA (in Grün)

In Abbildung 4.7 und 4.8 sind die Ergebnisse aus den beiden Analysen dargestellt. Zur Differenzierung sind die Ergebnisse aufgeteilt auf die drei, in Tabelle 4.5 aufgelisteten Ebenen. Hierbei vergleicht Abbildung 4.8 die absoluten Zahlen der Constraints beider Analysen, wohingegen sich Abbildung 4.7 auf die Abdeckung der STPA *Safety Constraints* beschränkt und diese sowohl anhand der Anzahl an *Safety Constraints* als auch mittels der prozentualen Überdeckung dieser darstellt.

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

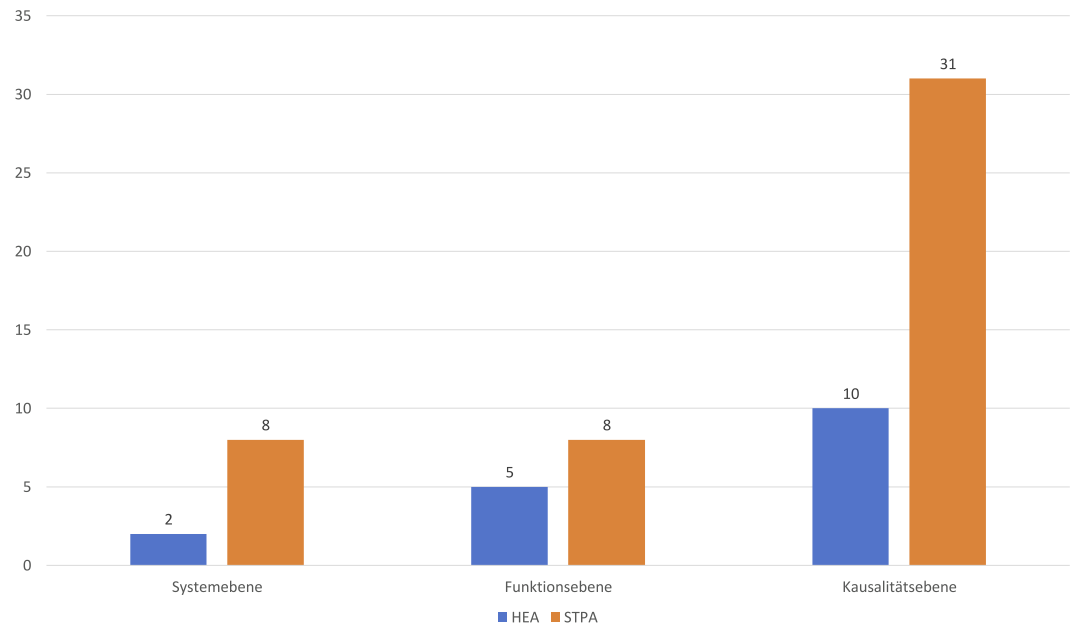


Abbildung 4.8.: Absolute Verteilung der STPA *Safety Constraints* (in Orange) und der *Control Strategies* der HEA (in Blau) auf die drei Ebenen der STPA

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**
   Sicherstellung der korrekten Funktion der Automatisierung und Instandhaltung der mechanischen Komponenten des Systems. Eine regelmäßige Wartung des Systems ist Grundvoraussetzung der sicheren Umsetzung von Anforderungen, der, in den nächsten Punkten definierten, Kategorien.

Systemebene	Hier werden *Safety Constraints*, zur Vermeidung oder Mitigation von *Hazards* auf Systemebene, abgeleitet. In STPA geschieht dies in Schritt 1 der Analyse.
Funktionsebene	Umfasst die *Safety Constraints* aus STPA Schritt 3 die zur Beherschung der *Unsafe Control Actions* erstellt werden. Ein Beispiel wären hier plötzliche Lenkbewegungen in dichtem Verkehr, wodurch die Gefahr eines Unfalls entsteht. Für das obige Beispiel wäre ein beispielhafter Constraint auf dieser Ebene: Das Fahrzeug soll h plötzlichen Lenkbewegungen durch den Fahrer in dichtem Verkehr entgegenwirken.
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**
   Die Kategorien in diesem Bereich kontrollieren die effektive Umsetzung des Feedbacksystems. Hierbei wird eine korrekte Kommunikation des Systemzustandes zum Fahrer reguliert, wodurch *Safety Constraints* in diesem Bereich eine Schlüsselrolle in der Erstellung sicherer Systeme einnehmen.

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.

Nr.	Thema	HEA	STPA	
1	Sicherstellung der Einhaltung von Gesetzen	0	2	Einbeziehung äußerer Regularien und Bedingungen
2	Sicherstellung der Kontrollierbarkeit (durch ADS oder Fahrer) des Fahrzeugs	0	1	
3	Sicherheitsabstand zu Verkehrsteilnehmern/Hindernissen	1	3	
4	Regelmäßige Instandhaltung des Systems	0	4	Wartung und Instandhaltung
5	Sicherstellung von Sicherheitskritischen Funktionen	0	1	
6	Automatisierte Funktionskontrolle des Systems	0	1	
7	Sicherstellung eines "fail operational"	0	2	Sicherstellung der Rahmenbedingungen und Definitionen
8	Verhinderung von Verlassen des Fahrbereiches	0	1	
9	Verhinderung von undefinierten Zustandsänderungen	0	1	
10	Verhinderung von illegalen/gefährdenden Interaktionen durch den Nutzer	0	1	
11	Dynamische Anpassung des Displays	1	2	Kommunikation mit dem Fahrer
12	Feedback durch das AD System	10	10	
13	Benachrichtigung des Fahrers über RTI by the System	1	1	
14	Steuereingriffe über das HMI während des Autonomen Fahrens	1	2	Übernahme und Steuerung des Fahrzeug durch den Nutzer
15	Dokumentation der Fahrfunktionen	2	1	
16	Aufmerksamkeits Überprüfung	1	2	
17	Mechanismus um versehentliche interaktion mit dem "AD Input Device" zu verhindern	1	1	
18	Manuelles Eingreifen durch den Fahrer während AD	3	4	
19	Kontrollübergabe von AD zum Fahrer	1	2	
20	Design des "AD Input Device"	1	0	

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 duch 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.

Allerdings ist auf der rechten Seite des Diagramms ebenfalls eine einzelne Kategorie, die sowohl von HEA als auch STPA abgedeckt wird, durch eine einzelne eins dargestellt. Dieser Ausreißer aus den Hauptkategorien der HEA ist mit der STPA zu erklären, bei der eine intensive Analyse des Systems noch vor Durchführung der HEA, ausgeführt wurde. Dadurch wurde ein Expertenwissen über das System gesammelt, welches zu einer zusätzlichen Analyse von Szenarien, in dem Bereich der äußeren Faktoren, führt. Dies lässt den Schluss zu, dass die HEA ein breites Expertenwissen über das System benötigt, um die gleiche Abdeckung der Kategorien wie die STPA zu erreichen.

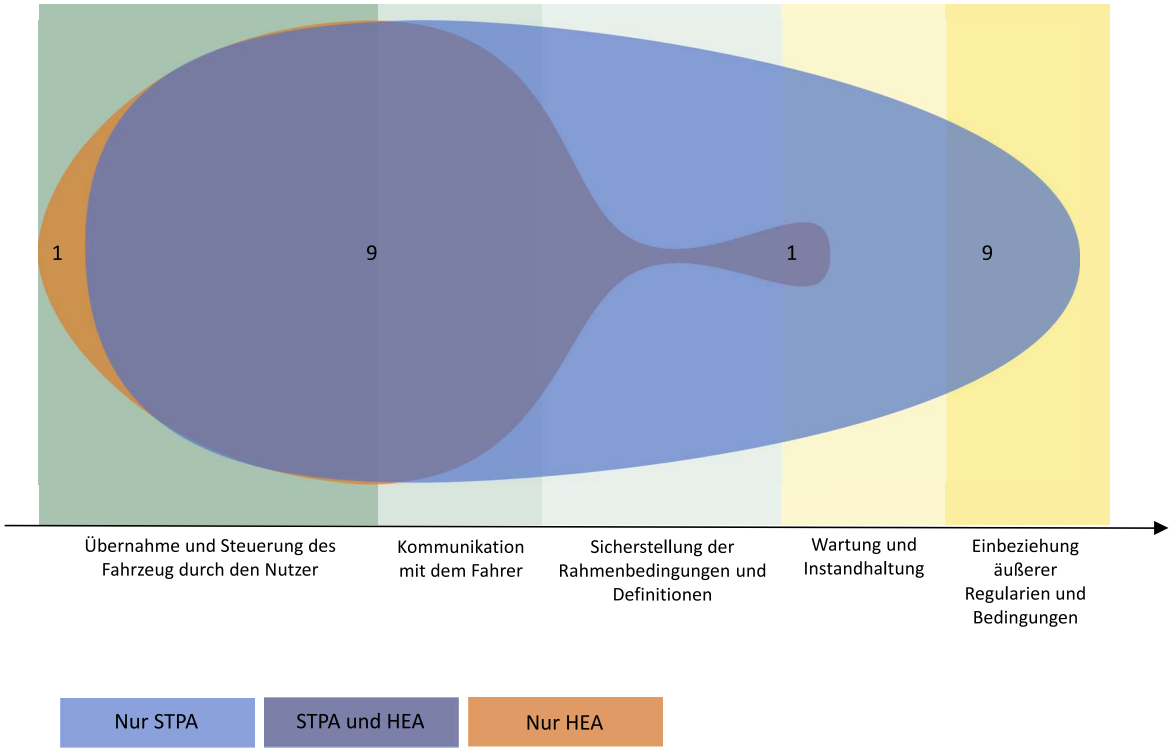


Abbildung 4.10.: Visuaisierung der Themenüberdeckung der HEA im Vergleich zur STPA des Beispielsystems

4.6. Vor- und Nachteile der STPA ggü. traditionellen Methoden

4.6.1. Vorteile derSTPA ggü. der HEA

STPA unterstützt eine gesamtheitliche Betrachtung des Systems

Als Expertenanalysen neigen traditionelle Analysen dazu sich, durch denBedarf an Expertenwissen, zu sehr auf bestimmte Bereiche eines Systems zu fokussieren. Dadurch werden mögliche Fehlerzustände vernachlässigt, die nur durch eine erweiterte Sicht auf die gesamte Feedbackschleife des Systems erkannt werden können. Beispielhaft sind die „Operator Tasks“in der HEA oder Prozesse/(Sub-)Systeme in einer normalen *Failure Mode and Effect Analysis* (FMEA), die die Analyse auf eine Interaktion beschränken ohne den Bezug zum Gesamtsystem herzustellen. Dieser Ansatz, eine isolierte Einheit eines Systems getrennt zu analysieren und Systemfehler anhand von selbst definierten Variablen aufzustellen, ist sehr viel ineffizienter als die Aufstellung der Gesamtstruktur und die strukturierte Ableitung der möglichen Einflussvariablen des Gesamtsystems. Durch den Schrittbasierten Aufbau der STPA wird der Analyst von einer abstrakten Sichtweise auf das System, die eine Analyse von *Hazards* auf Systemebene erlaubt, hin zu einer detaillierten Betrachtung der für die individuelle Analyse interessanten Regelschleife, geführt. Aufgrund dessen betrachten traditionelle Analysen wie die HEA jede Steuerungsaktion für sich allein wobei der

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 Steuerungsaktionen 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 in 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

Durch die klare Definition der erforderlichen Schritte zur Durchführung einer STPA wird der Analyst hier, im Gegensatz zu traditionellen Analysen, von Anfang an an die Hand genommen. Die meisten traditionellen Analysen, wie eine FMEA oder HAZOP, gehen nach dem *bottom up* Prinzip vor, wodurch eingrößeres Wissen über das System schon zu Beginn der Analyse benötigt wird. Hierzu wird meist ein Schema vorgegeben welches wasserfallartig von Experten abgearbeitet und in entsprechender Form dokumentiert. Im Gegensatz dazu gibt STPA iterative Schritte vor und unterstützt den Anwender durch die drei *Safety Constraint* Ebenen (Systemebene, Funktionsebene, Kausalitätsebene) in der Top-Down Manier. Dadurch wird erreicht das man, vor allem in sehr komplexen Systemen, durch die Ein-/Ausblendung von Details Zusammenhänge und Informationsflüsse im System einfacher nachvollziehen kann.

STPA erlaubt die Entwicklung eines sicherheitsgetrieben Designs

Anders als traditionelle Verfahren erlaubt STPA schon einen Einsatz während der Entwurfsphase des Systems. Erreicht wird dies durch den System theoretischen Top-Down Ansatz mit dem STPA einzelne angestrebte Systemfunktionen durch *Safety Constraints* verfeinert und so im Design benötigte Komponenten quasi als Nebenprodukt definiert[Lev11]. Dadurch ist STPA nicht nur ein Werkzeug zur Gefährdungsanalyse, sondern auch zur Erstellung eines sicherheitsgetrieben Designs durch Schritt für Schritt Verfeinerung eines Systemkonzeptes. Somit kann STPA den meisten Mehrwert bringen, wenn es bereits in einer frühen Phase des Entwicklungsprozesses eingesetzt wird[Lev11].

Systematische Betrachtung des *Human Factors* durch die *Mental Models*

Durch die Erweiterungen des STPA Prozesses in [Fra17] und [LT14] wird dem Analysten ein Werkzeug in die Hand gegeben mit dem er den hoch komplexen Informationsfluss in einem Menschen auf nachvollziehbare Art und Weise repräsentieren kann. Durch die Integration der Analyse in STPA wird eine Betrachtung des *Human Factor* nach dem Shell-Modell in eine Gefahrenanalyse mit einbezogen und kann schon zu Design-Zeit berücksichtigt werden. Die Einbindung der *Mental Models* in den iterativen Prozess erlaubt außerdem auch Fehler in der Informationsverarbeitung des Menschen aufzudecken und in die Ableitung von *Safety Constraints* einfließen zu lassen. Dadurch kann das HMI sicherheitsgetrieben entwickelt und gleichzeitig erforderliche Maßnahmen zur Bereitstellung der erforderlichen Informationen an die *Mental Models* getroffen werden.

Berücksichtigung des *Human Factor* in allen Phasen der System Entwicklung

Resultierend aus den zwei vorangegangenen Punkten kann man schließen dass STPA mit der erweiterten Betrachtung des *Human Factor* erlaubt, eine detaillierte Analyse der, im Shell-Modell[Shea] beschriebenen Interaktionen, schon in der Designphase des Systems durchzuführen und so auch den *Human Factor* in frühe Design Entscheidungen einzubeziehen. Als Resultat wird der zusätzliche Schritt einer *Human Factor* Analyse, wie sie in dieser Arbeit durchgeführt wurde hinfällig.

Übersichtlichere Dokumentation und angeleitete Analyse durch größeren Tool Support

Durch den Schritt-basierten, klar gegliederten Ablauf können Analysten durch User Software wie XSTAMPP [AW15][AW16] bei der Durchführung einer STPA unterstützt werden.

Formulierung von präziseren *Safety Constraints* durch genauere Kontextinformationen

Durch die Modellierung der Systemzustände durch *Process Models*, *Mental Models* und Abbildung der *Feedbackschleife* bietet STPA wichtige Kontextinformationen über gefährdende Zustände, wodurch die Formulierung von präziseren *Safety Constraints* ermöglicht wird. Zu beobachten ist dies bei der Betrachtung der Überdeckungsmatrix in Abbildung 4.6; hier kann man sehen, dass viele Felder gelb hinterlegt sind, wodurch eine nur teilweise Überdeckung des *Safety Constraints* durch die *Control Strategy* der HEA gegeben ist. Beispielhaft dafür ist das Feld [CS-8, SC1.4], welches die teilweise Überdeckung des *Safety Constraints* 1.4 mit der *Control Strategy* 8 aufzeigt.

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

4.3 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 Zeitersparniss, 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 Analyserrgebnisse ist. Dabei bedeutet vollständig und minimal, dass das Modell genau die für die Aufgabe des *Controllers* nötigen Informationen beinhaltet.

Fehlende Prioritätskennzahlen in STPA

Während in der durchgeführten STPA Kennzahlen für die Schwere (engl. Severity) der jeweiligen *Hazard* als Prioritätskennzahl für die *Safety Constraints* verwendet wurden, wird in der STPA von Leveson [LT18] keine explizite Priorisierung der *Safety Constraints* vorgenommen. Leveson schlägt hier lediglich eine Priorisierung der *Accidents*, welche als Grundlage für die Analyse dienen, vor. Dadurch ist zwar eine indirekte Priorisierung der *Safety Constraints*, durch die referenzierten *Accidents*, möglich allerdings werden dadurch sämtliche *Safety Constraints* mit Referenz zu einem *Accident* mit (mindestens) dessen Priorität bedacht.
Bspw. wurden in der durchgeführten STPA 27 *Safety Constraints* zur Verhinderung von *Hazard-7* aufgestellt, die wiederum auf *Accident-4* referenziert. Durch diese Referenz wurden alle 27 *Safety Constraints* mindestens mit der, von *Accident-4* definierten, Priorität belegt, ohne die Wahrscheinlichkeiten mancher Ursachenszenarios zu berücksichtigen. Hierdurch läuft man Gefahr dass, gerade bei komplexeren Systemen, falsche Prioritäten in der Abarbeitung der *Safety Constraints* gesetzt werden, die sich nicht an dem reglementierten Ursachenszenarien an sich, sondern an Gesichtspunkten wie Anordnung auf dem Ergebnisblatt, orientieren. Die traditionelle Priorisierung anhand der Auftretenswahrscheinlichkeit eines *Human Failure Event* (HFE) ist hier wesentlich feiner durch eine priorisierung anhand der reglementierten Ursache.

Redundante *Safety Constraints* durch den iterativen Ansatz der STPA

Der letzte Punkt ist ein weit verbreitetes Problem und hängt auch mit der generellen Usability listenbasierter 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 unnötiger Constraints, 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

Diese beschäftigt sich mit dem Zusammenhang zwischen den Forschungsfragen und der angewendeten Methodik, also mit der Frage: *„Wurde die Fallstudie zielgerichtet durchgeführt?“*
Die zwei Forschungsfragen, die in Abschnitt 4.1.2 gestellt wurden, fragen nach dem Mehrwert bzw. den Vor- und Nachteilen der STPA ggü. traditionellen Verfahren. Diese wurden durch Durchführung und Gegenüberstellung einer STPA und einer HEA beantwortet. Um die Validität des Konstruktes sicherzustellen, wurden regelmäßige Meetings abgehalten in denen das Vorgehen und die Gestaltung der Methoden von akademischer sowie von Expertenseite besprochen wurden. Des Weiteren wurde auch die Evaluation und Aufstellung der, in Abschnitt 4.5 vorgestellten Kategorien, durch den Autor dieser Arbeit durchgeführt, wodurch die Gefahr der Voreingenommenheit der Ergebnisse besteht. Um dem zu begegnen, wurden sowohl die Ergebnisse als auch die Erstellung der Kategorisierung sowie der Vor- und Nachteile in Expertengesprächen validiert und auf Praxisrelevanz geprüft.

Interne Validität

Die interne Validität diskutiert den Einfluss verschiedener interner Störfaktoren auf die Studie. Was sich hier auf die Interne Validität auswirken kann ist, dass beide Analysen vom gleichen Autor verfasst wurden, wodurch das Wissen um das System unweigerlich durch die zeitliche Überschneidung der Durchführung beeinflusst wurde. Hier ist allerdings zu argumentieren, dass die STPA als Grundlage für das Verständnis des Systems in Kooperation mit Systemexperten bei Continental erstellt wurde. Dadurch wurde ein, für eine praxisnahe Durchführung einer Expertenanalyse wie der HEA, notwendiges Systemwissen etabliert.
Eine weitere Gefährdung der Validität stellen ein unterschiedlicher Wissensstand oder falsche Annahmen über die Methoden dar. Für diesen Zweck wurde vor Beginn der Analysen jeweils eine ein-monatige Einarbeitungsphase eingeplant und die Analysen selbst unter regelmäßigem Review durchgeführt.

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.
Für die Erstellung der Guideline wurde die, von Leveson im STPA Handbook [LT18] beschriebene STPA Methode mit den Erweiterungen von France[Fra17] und Thornberry[LT14] ergänzt und zu der vorliegenden STPA Guideline für die *Human Factor* Analyse zusammengefasst. Die in dieser Arbeit vorgestellte STPA wurde auf Grundlage der erstellten STPA Guideline durchgeführt, um die Nachvollziehbarkeit der erzielten Ergebnisse zu dokumentieren.
Der Mehrwert, den die Einführung der STPA zur Analyse des *Human Factor* leisten kann, wurde anhand der beiden Analysen eines Beispielsystems hergeleitet. Die erzielten Ergebnisse beider Analysen wurden dabei gegenübergestellt und einer Überdeckungsanalyse, nicht nur untereinander sondern auch gegenüber einer, von den Analyseergebnissen unabhängigen Liste von sicherheitskritischen Kategorien, unterzogen.
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

Aus den aufgestellten Vor- und Nachteilen kombiniert mit der Analyse der Ergebnisse aus der HEA und STPA kann geschlussfolgert werden, dass die STPA Methode, durch die Erweiterungen auf die verschiedenen Modelle menschlichen Verhaltens, ein effektives Werkzeug zur gefahrenorientierten Designentwicklung für die Ursachenvermeidung darstellt. STPA bietet dabei trotz der hohen Komplexität, die durch die Einführung der System Theorie und des geführten Prozesses entsteht, eine vereinfachte Modellierung des menschlichen Verhaltens, wodurch Anwender bei der Erkennung von Ursachen Szenarien unterstützt werden. Durch die Definition von *Process*- und *Mental Models* bietet STPA zudem eine systematische und geführte Analyse basierend auf Verhaltensmodellen. Im Gegensatz dazu stehen traditionelle Verfahren, die auf Expertenwissen bzw. Erfahrungswerten basieren. Durch den Einsatz der Modellierungswerkzeuge bei Verwendung einer STPA kann bereits die Designphase des Systems durch einen frühzeitigen Einsatz der Methode unterstützt werden, indem hier schon Szenarien anhand der Modelle vorhergesagt werden können. Außerdem bietet STPA durch seine Einsatzfähigkeit zur sicherheitsgetriebenen Designentwicklung eine Berücksichtigung des *Human Factor* in allen Phasen der Systementwicklung.
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.

5.2. Ausblick

Anhand der Erkenntnisse aus dieser Arbeit können weiterführende Arbeiten auf Basis der vorgestellten STPA Guideline unter Berücksichtigung des *Human Factor* durchgeführt werden. So wurde die vorliegende Fallstudie lediglich von einem Autor durchgeführt. Anhand der gegebenen Methodenbeschreibung könnte die Studie jedoch auch von mehreren Autoren oder Expertenteams durchgeführt werden, um so Schlüsse über Einflussfaktoren wie Methoden- oder Fachwissen ziehen zu können. Ebenfalls könnten die, in der durchgeführten STPA aufgestellten *Mental Models* zu allgemeingültigen Modellen für den Bereich des automatisierten Fahrens erweitert werden, um eine Grundlage für zukünftige Gefahrenanalysen auf dem Gebiet zu bieten. Durch eine Kombination traditioneller Verfahren mit STPA könnte die Hürde reduziert werden, die durch die hohe Komplexität der STPA entsteht und die durch Erweiterungen dieser noch verstärkt wird. Eine Möglichkeit wäre, STPA als eine initiale Methode für den Design Prozess und die Aufstellung der *Control Structure* zu nutzen und in späteren Analysen auf einfachere Verfahren zurückzugreifen, die die Informationen der STPA z.B. zur Generierung von PSFs verwenden. Bspw. eine Kombination aus einer STPA Iteration zur Definition der *Control Structure* und einer anschließenden HEA zur vereinfachten Analyse der definierten *Control Actions*.
In Abschnitt 4.6.2 wird das Problem der redundanten *Safety Constraints* angesprochen, welches ein generelles Problem großer Analysen oder Listen ist, die manuell ausgefüllt werden müssen. Hier kann wiederum die Tool Landschaft Abhilfe schaffen: Durch entsprechende Mechanismen wie Coding oder Natural Language Processing[Teu89], die den Analysten beim Finden verwandter *Safety Constraints* unterstützen können. So könnte der Mehrwert eines Analyseergebnisses durch Gruppierung der *Safety Constraints* nach deren Kontext verbessert werden. Dadurch ließe sich die zu betrachtende Menge an *Safety Constraints* auf eine kleinere Menge an Kategorien reduzieren, die dann zur kontextbasierten Priorisierung genutzt werden können. Des Weiteren könnte dieses Problem auch durch eine effiziente Verlinkung und/oder eine Kontexthilfe für die existierenden *Safety Constraints* gelöst werden.
In dieser Arbeit wurde keine tiefergehende STPA durchgeführt. Durch eine solche detailliertere Analyse des *Human Factor* des Systems könnten weitere *Safety Constraints* auf Basis verfeinerter *Mental Models* gefunden werden.

A. STPA eines zukünftigen Systems zum automatisierten Fahren

A-STPA-Report

Human Factor Analysis of an ADS

Title	Human Factor Analysis of an ADS
Date and Time	13.10.2018, 10:21:26
Description	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 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-maschine interaktions. 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

ID	Title	Description	SEV*	Links
A-1	Loss of or serious damage to human live	People die/are harmed by a collision of ego vehicle with other (non over-drivable) objects	S3	H-1, H-11
A-2	Damage to ego or other vehicle/ the environment	Damage to Ego or other vehicle/ the environment	S2	H-3, H-1, H-9, H-10, H-11
A-3	mission loss	The AD vehicle fails in executing the mission (correctly) and drives to an undefined/-desired location	S1	H-3, H-1, H-8
A-4	impairment of traffic participants/other AD vehicles	impairment of traffic participants/other AD vehicles	S2	H-1, H-3, H-10, H-7, H-11

*Severity

Hazards

ID	Title	Description	SEV*	Links
H-1	The AD vehicle cannot be controlled	The AD Vehicle is operated uncontrolled by the ADS or the Driver which means that state changes can't be anticipated. This hazard differes 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.	S3	A-1, A-2, A-4, A-3, SC0.1
H-3	Driver has hands off controls when AD is not active	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 inconsistancy between the Drivers assumption over the current state of the ADS and the actual state.	S2	A-3, A-2, A-4, SC0.3
H-7	Violation of Traffic laws	The ego vehicle applies one of the following: - unexpected braking - unexpected acceleration - unexpected steering	S2	A-4, SC0.4
H-8	The AD vehicle doesn't follow the mission goal	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.	S1	A-3, SC0.5
H-9	The AD vehicle violates the safe distance to TPOs	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.	S2	A-2, SC0.6
H-10	The AD vehicle is in AD mode while in an unpredicted/ undefined Situation	The AD mode of a SEA Level 4 automatition 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.	S3	A-2, A-4, SC0.7, SC0.2
H-11	The AD vehicle violates the driving scope	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.	S2	A-2, A-1, A-4, SC0.8
H-12	The AD vehicle looses traction or is physically uncontrollable	If the vehicle looses traction due to longitudinal/lateral forces. E.g. when the driver over steers and the wheels loose traction, or when the vehicle is too fast for the driving scenario.	S3	SC0.9

*Severity

Safety Constraints

ID	Safety Constraint	Description	Links
SC0.1	The ADS must always be controllable through manual intervention	The ADS must always yield before manual intervention through the Driver	H-1, DR0.6
SC0.2	The ADS must implement a fail operational when the driver does not take over	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.	H-10, DR0.5
SC0.3	The Driver must never take hands off controls when AD is not available	The ADS must always ensure that the Driver has his hands and feet on the controls when the ADS is not available	H-3, DR0.3, DR0.8
SC0.4	The ADS must always heed the current traffic laws		H-7, DR0.2, DR0.9
SC0.5	The ADS must always act based on the driving mission defined by the Mission Controller when in AD mode	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.	H-8, DR0.7, DR0.8
SC0.6	The ADS must always keep the safe distance to TPOs		H-9, DR0.1
SC0.7	The ADS must always notify the driver in time before a shut down	The Driver must always be notified timely in order to enable a manual intervention before a shut down is executed (	H-10, DR0.4
SC0.8	The ADS mustn't violate the driving scope	The ADS must always ensure that the vehicle stays on the road and does not violate any road markings like solid lines, arrows etc.	H-11, DR0.2
SC0.9	The ADS must minimize the risk of loosing the control over the vehicle		H-12

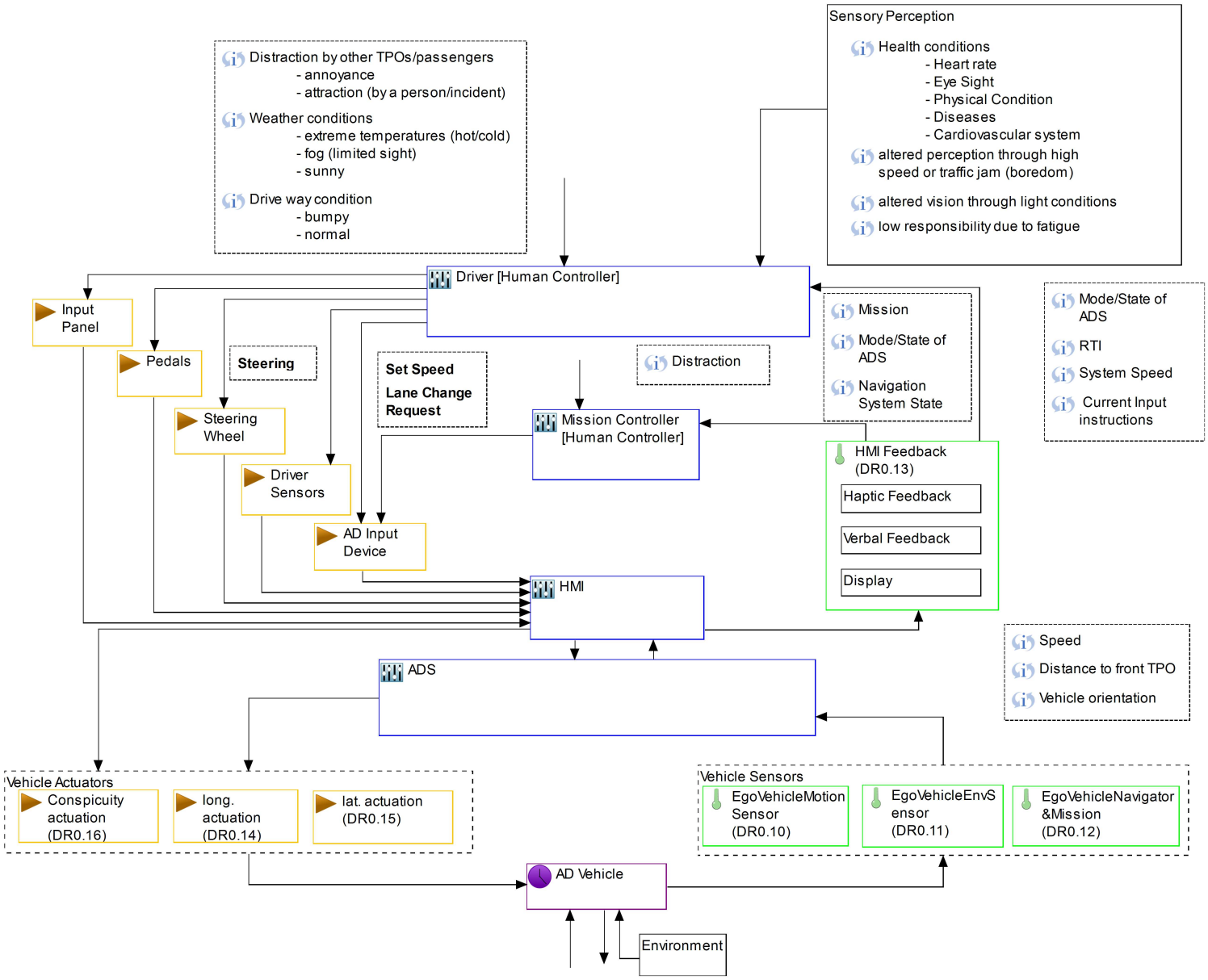
System Goals

No.	System Goal	Description
SG-1	Perform Lane Change	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 a 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.
SG-2	Perform Lane Keeping	When engaged the ADS should always be able to keep the lane it is currenty driving on by itselfe when in a defined driving situation.
SG-10	Switch between automated- and manual driving mode	The Driver should be able to switch between manual driving and automated driving
SG-11	Cancel Lane Change	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 initiaded by the ADS.
SG-13	Set Speed	The driver can request a speed change while in automated driving mode between 0 - 120 km/h(ACC limit)
SG-14	Fail Operational	The ADS should always ensure reaching an MRC before shutting down.

Design Requirements

No.	Design Requirement	Description	Links
DR0.1	Collision avoidance	Safety critical feature of Cruising Chauffeur through which an imminent collision is avoided.	SC0.6
DR0.2	System- & Geo-fencing	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	SC0.4, SC0.8
DR0.3	User Monitoring	The system should always ensure that the user is capable of taking over control before handing it over	SC0.3
DR0.4	Request-to-intervene	A notification send by the ADS prior to a situation in which the AD functions become unavailable	SC0.7
DR0.5	Minimal Risk Maneuver	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.	SC0.2
DR0.6	Driver override	The driver is able to intervene in the AD at any time during a normal driving situation	SC0.1
DR0.7	Mission check before activation		SC0.5
DR0.8	The ADS must always provide information about it's state		SC0.3, SC0.5
DR0.9	The ADS shall always be aware of the traffic laws		SC0.4
DR0.10	EgoVehicleMotionSensor	The current state of vehicle's motion is monitored by the EgoVehicleMotionSensor. This Sensor is responsible for acquirering the current Speed and Orientation of the vehicle.	
DR0.11	EgoVehicleEnvSensor	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.	
DR0.12	EgoVehicleNavigator&Mission	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.	
DR0.13	HMI Feedback Component for providing sufficient Feedback over the DDT	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.	
DR0.14	Longitudinal actuation	Acceleration in Longitudinal direction is the main acceleration of the vehicle responsible for actuating the DDT	
DR0.15	Lateral actuation	Responsible for maintaining stability of the vehicle and counter lateral forces like g-forces, wind etc.	
DR0.16	Conspicuity actuation		
DR0.17	Driver Sensors	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 senors 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.	
DR0.18	Input Panel	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	
DR0.19	AD Input Device	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	

Control Structure Diagram



Control Actions

Id	Control Action	Description
CA-4	Set Speed	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_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.
CA-5	Lane Change Request	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
CA-9	Steering	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.

Unsafe Control Actions

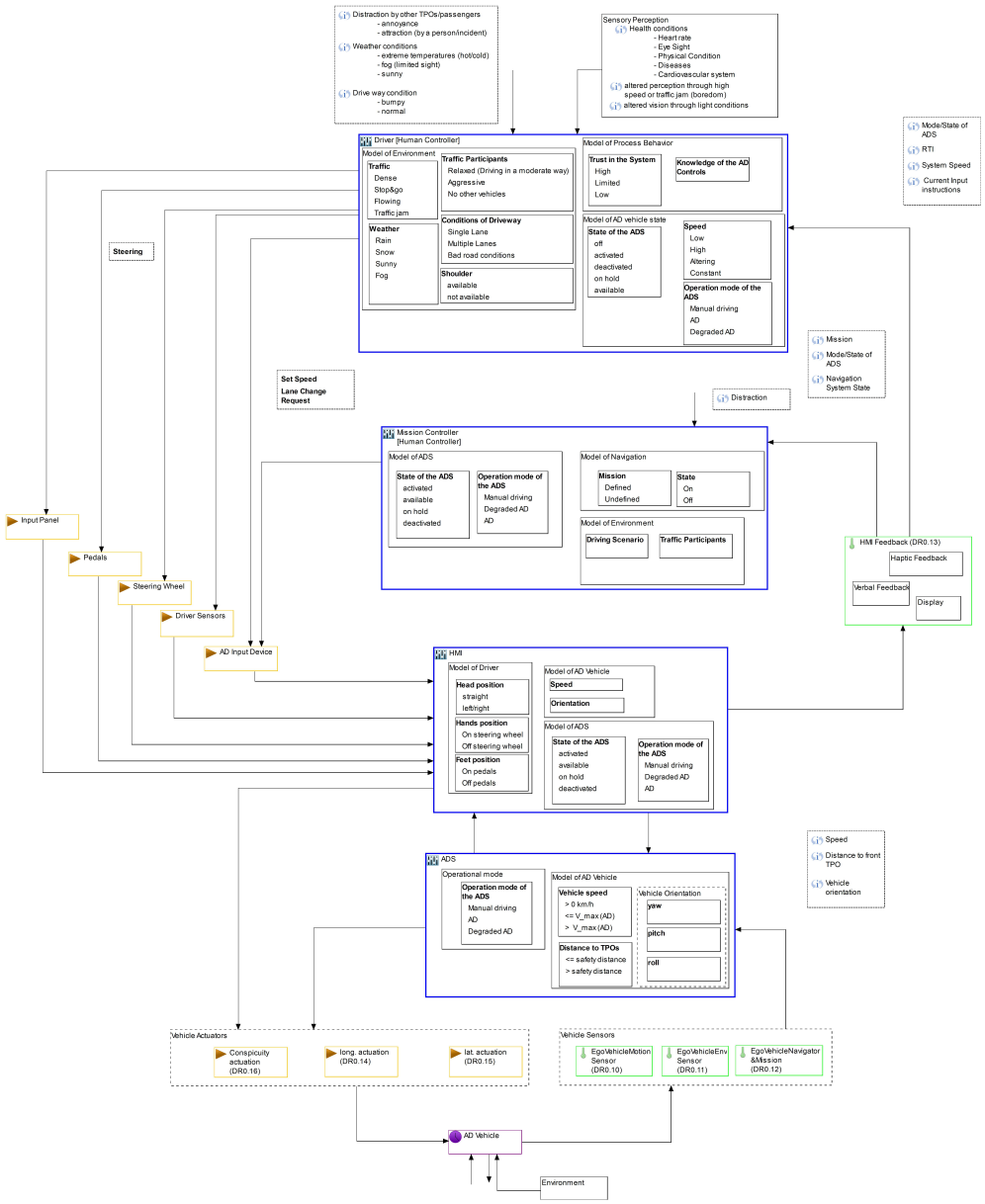
Control Action	Not providing causes hazard	SEV*	Providing causes hazard	SEV*	Wrong timing or order causes hazard	SEV*	Stopped too soon or applied too long	SEV*
Set Speed	UCA1.4 The Driver does not provide the Set Speed command while driving too fast when it's raining [H-7]	S2	UCA1.5 The Driver provides the Set Speed command with a value above the speed limit while in normal traffic [H-7, H-11, H-12]	S3	UCA1.6 The Driver provides the Set Speed command to reduce speed when driving in a steep curve only when already in the curve [H-11]	S2	UCA1.8 N/A [Not Hazardous]	S2
			UCA1.67 The Driver provides the Set Speed command during a lane change [H-11, H-12]	S3				
Lane Change Request	UCA1.13 The default lane change behavior of the ADS is assumed not be hazardous in the STPA [Not Hazardous]	S0	UCA1.18 The Driver performs a Lane Change Request to an undesired lane [H-8]	S1	UCA1.21 The Driver performs a Lane Change Request when not longer possible due to lane restrictions, traffic etc. [H-7]	S2	UCA1.20 N/A [Not Hazardous]	S0
			UCA1.19 The Driver performs a Lane Change Request that is not allowed [H-7]	S2				
Steering	UCA1.30 The Driver doesn't provide Steering when AD mode is being deactivated and steering is required [H-7, H-11]	S3	UCA1.31 The Driver provides Steering in an illegal direction (Scope violating) while in AD mode [H-7, H-11]	S2	UCA1.32 The Driver provides Steering while in AD mode and next to an exit just too short before or after missing the exit [H-7, H-11]	S2	UCA1.65 The Driver provides Steering too long (over steers) while in AD mode [H-7, H-9]	S2

*Severity

Corresponding Safety Constraints

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

Control Structure Diagram with Process Model



Causal Factors Table

Component	Causal Factor	Unsafe Control Action	Hazard Links	Safety Constraint	Design hints	Links	Notes
Driver [Human Controller]	Driver issues a set speed command based on experience without considering dynamic factors like wet road or sudden traffic changes	UCA1.5 The Driver provides the Set Speed command with a value above the speed limit while in normal traffic	H-7, H-11, H-12	The ADS must always check requested speed changes are potentially hazardous in the current driving situation and prevent them if necessary	The ADS must monitor it*s environment through utilization of the vehicles environment sensors (traction, TPOs etc.) and could simulate possible driving speeds before adapting them		
	The Driver increases the speed over a safe limit due to a false estimation of for the current driving situation	UCA1.6 The Driver provides the Set Speed command to reduce speed when driving in a steep curve only when already in the curve	H-11	The ADS must always check requested speed changes are potentially hazardous in the current driving situation and prevent them if necessary	The AD vehicle should define a dynamic speed limit for the current driving situation based on the environmental conditions		
			—	—	—	—	—
	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	UCA1.4 The Driver does not provide the Set Speed command while driving too fast when it's raining	H-7	The ADS mustn't rely on the driver to execute any safety critical functions while in AD mode	The ADS should implement all safety critical functions and always ensure a MRC when no driver input is given after an RTI		
	The Driver issues a set speed request with a too high value due too lack of experience with the system	UCA1.5 The Driver provides the Set Speed command with a value above the speed limit while in normal traffic	H-7, H-11, H-12	The ADS must provide a documentation or tutorial to allow the Driver to familiarize learn the AD vehicle controls in a safe environment	The ADS could implement a tutorial or walk through of the AD functions		
	The Driver requests a very low speed due to a lack of trust in the system	UCA1.5 The Driver provides the Set Speed command with a value above the speed limit while in normal traffic	H-7, H-11, H-12	The ADS must always provide Feedback about its state, the driving mode and the actions planned by the system			
	The Driver requests a speed change due to high traffic on the target lane instead of canceling the lane change	UCA1.67 The Driver provides the Set Speed command during a lane change	H-12, H-11	When a speed change is requested during a lane change the ADS should ask the Driver to cancel a lane			

Component	Causal Factor	Unsafe Control Action	Hazard Links	Safety Constraint	Design hints	Links	Notes
				change instead of changing the speed			
	The Driver requests a speed change due to a confusion about the initialization of a lane change	UCA1.67 The Driver provides the Set Speed command during a lane change	H-12, H-11	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			
	The Driver accidentally issues a lane change request while not paying attention to the driving situation	UCA1.18 The Driver performs a Lane Change Request to an undesired lane	H-8	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	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		
	The Driver issues an incorrect lane change due to a wrong handling of the AD input device	UCA1.18 The Driver performs a Lane Change Request to an undesired lane	H-8	The ADS must provide a documentation or tutorial to allow the Driver to familiarize learn the AD vehicle controls in a safe environment			
	The Driver issues a lane change to an undesired lane in an attempt to cancel a previous lane change	UCA1.18 The Driver performs a Lane Change Request to an undesired lane	H-8				
	The Driver doesn't see that the lanes are separated by a solid line	UCA1.19 The Driver performs a Lane Change Request that is not allowed	H-7	The ADS must check the legality of lane changes before executing them and notify the Driver about any traffic violations			
	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)	UCA1.30 The Driver doesn't provide Steering when AD mode is being deactivated and steering is required	H-7, H-11	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	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		

Component	Causal Factor	Unsafe Control Action	Hazard Links	Safety Constraint	Design hints	Links	Notes
	The Driver doesn't provide steering due to wrong expectations from the ADS(expectation to support the manual controls)	UCA1.30 The Driver doesn't provide Steering when AD mode is being deactivated and steering is required	H-7, H-11	The ADS must always provide clear and minimal feedback about the current state and instructions to the Driver to prevent redundant information			
	The Driver provides steering in an illegal direction to counter a lane change to an undesired lane	UCA1.31 The Driver provides Steering in an illegal direction (Scope violating) while in AD mode	H-7, H-11	The ADS must always prevent hazardous manual interventions that could potentially lead to a severe accident			
	The Driver provides steering too late due to a wrong perception of the driving speed	UCA1.32 The Driver provides Steering while in AD mode and next to an exit just too short before or after missing the exit	H-7, H-11	The ADS must always prevent hazardous manual interventions that could potentially lead to a severe accident			
	The Driver provides steering too long due to a wrong expectation of the steering effect	UCA1.65 The Driver provides Steering too long (over steers) while in AD mode	H-7, H-9	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			
	The Driver performs a Lane Change Request when not possible due to low attention to the driving situation	UCA1.21 The Driver performs a Lane Change Request when not longer possible due to lane restrictions, traffic etc.	H-7	The ADS must always check the legality of the Driver requests issued over the AD Input Device and give detailed Feedback about illegal requests.			
	The Driver doesn't recognize that an obstacle or a solid line due to distraction by his environment	UCA1.31 The Driver provides Steering in an illegal direction (Scope violating) while in AD mode	H-7, H-11	The ADS must always prevent hazardous manual interventions that could potentially lead to a severe accident			

Component	Causal Factor	Unsafe Control Action	Hazard Links	Safety Constraint	Design hints	Links		Notes
	The Driver doesn't react correctly due to time pressure created by a dense traffic situation in which he needs to react quick		—	—	—	—	—	
	The Driver doesn't react as required by the whether conditions like heavy snow or slippery drive way due to rain		—	—	—	—	—	
			—	—	—	—	—	
HMI Feedback (DR0.13)	The Driver receives incorrect feedback of the state of the ADS from the Display		—	—	—	—	—	
	The Driver is not able to receive the feedback due to bad readability of the display caused by direct sunlight		—	—	—	—	—	
	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)		—	—	—	—	—	
	The Driver provides the set speed command with an incorrect value due to a wrong feedback provided on the Display	UCA1.5 The Driver provides the Set Speed command with a value above the speed limit while in normal traffic	H-7, H-11, H-12	The HMI should always double-check its internal Model of the ADS with the actual state of the ADS and correct wrong entries				
	The Driver provides the Set Speed command too late due to a delayed feedback on the display	UCA1.6 The Driver provides the Set Speed command to reduce speed when driving in a steep curve only when already in the curve	H-11	The Display must be regularly maintained and checked for the required functional requirements				
	The Driver provides the Set Speed command too late due to bad readability of the Display	UCA1.6 The Driver provides the Set Speed command to reduce speed when driving in a steep curve only when already in the curve	H-11	The visual parameters (brightness, color, contrast) of the Display must be adjustable to fit the driving	The Display should automatically adapt to changing lighting			

Component	Causal Factor	Unsafe Control Action	Hazard Links	Safety Constraint	Design hints	Links	Notes
				scenario and the Drivers preferences			
	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	UCA1.18 The Driver performs a Lane Change Request to an undesired lane	H-8	The ADS should always provide Feedback over redundant channels to prevent information loss			
	The Driver doesn't receive the feedback about the legality of his request due to an occupied display	UCA1.19 The Driver performs a Lane Change Request that is not allowed	H-7	The display of the HMI must always show the most recent and important information and should never omit feedback due to pending information			
	The Driver doesn't provide steering because of wrong feedback on the Display about the AD mode	UCA1.30 The Driver doesn't provide Steering when AD mode is being deactivated and steering is required	H-7, H-11	The HMI should always double-check its internal Model of the ADS with the actual state of the ADS and correct wrong entries			
	The Driver doesn't provide Steering because of missing feedback due to an error in the HMI Feedback	UCA1.30 The Driver doesn't provide Steering when AD mode is being deactivated and steering is required	H-7, H-11	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.			
HMI	The HMI doesn't send the ADS state to the Display		—	—	—	—	—
AD Input Device	The Driver rests his hand on the AD input device and accidentally provides Input	UCA1.5 The Driver provides the Set Speed command with a value above the speed limit while in normal traffic	H-7, H-11, H-12	The AD input Device must not react to inputs (pulls/pushes) below a (user-)defined threshold to prevent accidental interactions			

Component	Causal Factor	Unsafe Control Action	Hazard Links	Safety Constraint	Design hints	Links	Notes
	The AD input device misinterprets the input due to wrong software/ calibration	UCA1.5 The Driver provides the Set Speed command with a value above the speed limit while in normal traffic	H-7, H-11, H-12	The AD input Device must be maintained regularly to prevent malfunction	The ADS could implement a self-check that regularly checks the controls hard- and software		
	The AD input device delays the execution of the Set Speed command due to an internal error	UCA1.6 The Driver provides the Set Speed command to reduce speed when driving in a steep curve only when already in the curve	H-11	The ADS must monitor the vehicle controls and send an RTI or perform an automatic MRM if the controls do not function as expected			
	The AD input device issues a speed change as a result of a misinterpretation of an other command	UCA1.67 The Driver provides the Set Speed command during a lane change	H-12, H-11	The AD input Device must be maintained regularly to prevent malfunction			
	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	UCA1.18 The Driver performs a Lane Change Request to an undesired lane	H-8	The ADS should always provide Feedback over redundant channels to prevent information loss			
	The Set Speed CA is not executed due to a malfunction of the AD Input Device	UCA1.4 The Driver does not provide the Set Speed command while driving too fast when it's raining	H-7	The AD input Device must be maintained regularly to prevent malfunction			
	The Driver doesn't execute the Set Speed CA due to a false perception of the road conditions	UCA1.4 The Driver does not provide the Set Speed command while driving too fast when it's raining	H-7	The AD Vehicle should always warn the Driver about hazardous road conditions like wet or snowy			
	The AD Input Device issues a speed change due to a false input signal when the Driver is not giving any input	UCA1.67 The Driver provides the Set Speed command during a lane change	H-12, H-11	The attention of the Driver must be checked by the Driver Sensors before accepting any CAs from over the AD Input Device			
	The Driver issues the Lane Change accidentally by pushing the AD Input Device while not paying attention to the driving task	UCA1.18 The Driver performs a Lane Change Request to an undesired lane	H-8	Before accepting requests issued by the Driver in AD mode over the AD input device the ADS must check			

Component	Causal Factor	Unsafe Control Action	Hazard Links	Safety Constraint	Design hints	Links	Notes
				the drivers attention to the driving situation			
	The ADS falsely assumes that the driver is paying attention to the DDT and executes a accidentally provided Lane Change Request	UCA1.18 The Driver performs a Lane Change Request to an undesired lane	H-8	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			
EgoVehicleMotionSensor (DR0.10)	The Driver assumes a wrong value for the vehicle speed due to wrong data from the EgoVehicleMotionSensor	UCA1.5 The Driver provides the Set Speed command with a value above the speed limit while in normal traffic	H-7, H-11, H-12	The ADS must always use the information of the Navigation and the EgoVehicleMotionSensor to determine the correct speed of the vehicle and request immediate maintainance of the vehicle in case of an inconsistency.			
	The Driver assumes a wrong value for the vehicle speed due to missing data from the EgoVehicleMotionSensor	UCA1.5 The Driver provides the Set Speed command with a value above the speed limit while in normal traffic	H-7, H-11, H-12	The ADS must always check for regular data from the Vehicle Sensors and request immediate maintanance if a sensor does not report data withing a normal timewindow.			
Steering Wheel	The Steering command isn't executed due to an error in the actuator of the steering wheel	UCA1.30 The Driver doesn't provide Steering when AD mode is being deactivated and steering is required	H-7, H-11	The manual controls of the vehicle must be maintained regularly to prevent malfunction	The correct function of the steering wheel could be checked by monitoring the movement of the wheel and the resulting orientation of the vehicle		
	The steering wheel gets stuck in a turned state	UCA1.65 The Driver provides Steering too long (over steers) while in AD mode	H-7, H-9	The manual controls of the vehicle must be maintained regularly to prevent malfunction			

Safety Constraints Step 4

ID	Safety Constraint	Description	Links
	The ADS must always check requested speed changes are potentially hazardous in the current driving situation and prevent them if necessary		
	The ADS must notify the Driver vigorously before changing the driving mode		
	The ADS must always provide feedback about the current state over more than one channel to prevent incorrect feedback		
	The ADS must always ensure good readability of the Display when in bright sunlight		
	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		
	The ADS mustn't rely on the driver to execute any safety critical functions while in AD mode		
	The ADS must provide a documentation or tutorial to allow the Driver to familiarize learn the AD vehicle controls in a safe environment		
	The ADS must always provide Feedback about its state, the driving mode and the actions planned by the system		
	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		
	The AD input Device must not react to inputs (pulls/pushes) below a (user-)defined threshold to prevent accidental interactions		
	The AD input Device must be maintained regularly to prevent malfunction		
	The ADS must monitor the vehicle controls and send an RTI or perform an automatic MRM if the controls do not function as expected		
	The HMI should always double-check its internal Model of the ADS with the actual state of the ADS and correct wrong entries		
	The Display must be regularly maintained and checked for the required functional requirements		

ID	Safety Constraint	Description	Links
	The visual parameters (brightness, color, contrast) of the Display must be adjustable to fit the driving scenario and the Drivers preferences		
	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		
	The ADS must check the legality of lane changes before executing them and notify the Driver about any traffic violations		
	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		
	The ADS must always provide clear and minimal feedback about the current state and instructions to the Driver to prevent redundant information		
	The ADS must always prevent hazardous manual interventions that could potentially lead to a severe accident		
	The ADS must always check the legality of the Driver requests issued over the AD Input Device and give detailed Feedback about illegal requests.		
	The manual controls of the vehicle must be maintained regularly to prevent malfunction		
	Feedback about the (un-)successful execution of a Driver requested AD task has to be provided on redundant channels to prevent information loss		
	The display of the HMI must always show the most recent and important information and should never omit feedback due to pending information		
	The AD Vehicle should always warn the Driver about hazardous road conditions like wet or snowy		
	The attention of the Driver must be checked by the Driver Sensors before accepting any CAs from over the AD Input Device		
	The ADS should always provide Feedback over redundant channels to prevent information loss		
	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		
	The ADS must always use the information of the Navigation and the EgoVehicleMotionSensor to determine the correct speed of		

ID	Safety Constraint	Description	Links
	the vehicle and request immediate maintainance of the vehicle in case of an inconsistency.		
	The ADS must always check for regular data from the Vehicle Sensors and request immediate maintanance if a sensor does not report data withing a normal timewindow.	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 than predict a sensor malfunction in case of a decreasing data rate.	
	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.		

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

	Title	Description	Operator	Goals	Actions	Plans	Performance Shaping Factors	Human error mode	occurrence probability	human error effects	detection, correction and compensation, Control Strategie (CS)	
Task 1	Lane Change	The Driver requests the AD controller to perform a Lane change if possible.	Driver	AD vehicle performes 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 manuver highlighted on the display	Interruptions through environment	confirmation omitted	Moderate	Lane change confirmation dialog is not closed	CS-1	The AD system must notify the driver when the confirmation dialog is not answered
								confirmation of the right manuver too late	Moderate	Lane change request is omitted/canceled	CS-2	The AD system must set a reasonable timeout for the lane change confirmation dialog
							Wrong coordination/perception between direction of lane change and pulling direction	wrong procedure selected/lane change in wrong direction	Low	Lane change omitted or in wrong direction	CS-3	The AD system must give clear guidance on the handling of the AD input device
							confusion about option to cancel lane change	inappropriate goal selected	Low	Lane change executed unwanted/accidentally	CS-4	The Driver must be informed about the option to cancel the lane change request
							need to carry out multiple tasks in same time window	inappropriate goal selected	Moderate	Lane change executed unwanted/accidentally	CS-23	The AD system must always request a confirmation of Driver inputs over the AD Input Device
							Wrong Training in AD functions	lane change executed with manual controls instead of the AD Input Device	Low	The AD system performs an RTI and deactivates	CS-5	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 omitted	Moderate	The lane change is omitted	CS-1	The AD system must notify the driver when the confirmation dialog is not answered
							confirmation dialog shown too short/long	selection of lane change omitted	Moderate	The AD system performs an MRM	CS-6	The AD System must define a reasonable timeout for HMI dialogs to prevent showing dialogs too short/long
									Moderate		CS-7	The AD System must inform the Driver in time before an MRM about the action and the interaktion possibilities during the action.
Task 2	Speed Change	The Driver can request a change of the maximum speed which can be aquired 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	Effects of traffic jam, long ride (tiered, exhausted)	inappropriate speed selected	Moderate	The speed is increased/decreased too an undesired level	CS-8	The AD vehicle must prevent undesired high/low speed changes
							Poor design of the Input device	Lane change/cancel instead of set Speed command selected	High	The current lane change is canceled/ executed	CS-9	The AD Input Device's design must ensure a clear distinction between set speed and the lane change/cancel command
							insufficient detailed description of the Mechanics	inappropriate speed selected	High	The speed is increased/decreased too an undesired level	CS-8	The AD vehicle must prevent undesired high/low speed changes

	Title	Description	Operator	Goals	Actions	Plans	Performance Shaping Factors	Human error mode	occurrence probability	human error effects	detection, correction and compensation, Control Strategie (CS)	
Task 3	React to Display and the Haptic/ Visual or Verbal Feedback	The Driver gets feedback over the current jurney and possible RTI's over multiple feedback Channals	Driver	Get notified when the attention of the Driver is required	Listen to vehicle feedback	1. Observe the given Feedback 2. Decide upon a response to the Feedback	Distranction by environment (passengers, TPOs)	Feedback omitted	Moderate	Driver doesn't react to feedback	CS-10	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.
							Poorly designed display layout showing too much information	Driver can't react appropreatly	Low	Driver reacts too late/incorrect to feedback	CS-25	The layout of the Display must at all times display only the minimal amount of required information too prevent overcroweding the layout
							Extreme wheather conditions (darkness, brightness) make it difficult to see the display	Feedback omitted	Moderate	Driver doesn't react to feedback	CS-26	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).
									Moderate		CS-27	The AD system must always adapt the brightness of the display according to the driving situation.
							Fatigue due to long ride, hot temperature	incorrect identification of situation	Moderate	Driver reacts to feedback in an incorrect way	CS-11	The AD vehicle must implement a confirmation dialog for all interactions with the AD system
										Driver overreacts to Feedback	CS-8	The AD vehicle must prevent undesired high/low speed changes
Task 5	Manual Steering	The Driver can intervene in any normal driving situation, by giving manual control input (steering, pedals) the AD system will than ask the driver to take over control and disable itself when the request is followed.	Driver	Override the driving activities planed by the AD system	apply steering wheel/pedals React to RTI from AD system	1. Decide upon an action to perform 1.1 React to environmental happening (police car, rescue alley, etc.) 1.2 Flash indicators 2. Interprete RTI	distraction by passengers, TPOs	Accidental intervention	High	The Driver provides unwanted manual control input	CS-15	The AD system must prevent any manual interventions when the driver has not taken over completely(hands and feet on controls, head straight)
							Sleepyness/drowsiness due too long ride, bordom etc.	steering in wrong direction or steering too sharp	Moderate	Impairment of TPOs, violation of driving scope	CS-24	The AD system must always warn the driver through multiple Feedback channels about dangerous interventions
							inadequate experience with the AD system	incorrect identification of system state,	Moderate	the Driver does not steer when AD mode is off	CS-16	The AD system must provide feedback over multiple channels when the driving mode changes.
							AD system treats intervention as illeagal and blocks it	Unwanted prevention of a necessary Driver intervention	Moderate	Attempted prevention of accidental intervention by AD system on necessary intervention	CS-17	The Driver must always be able to take over control emidiately by putting hands and feet on the controls and turning the head straight

Literaturverzeichnis

[AW15] A. Abdulkhaleq, S. Wagner. „XSTAMPP: an eXtensible STAMP platform as tool support for safety engineering“. In: (2015) (zitiert auf S. 61).

[AW16] A. Abdulkhaleq, S. Wagner. „XSTAMPP 2.0: new improvements to XSTAMPP including CAST accident analysis and an extended approach to STPA“. In: (2016) (zitiert auf S. 48, 61).

[Ant13] B. Antoine. „Systems Theoretic Hazard Analysis (STPA) applied to the risk review of complex systems: an example from the medical device industry“. Diss. Massachusetts Institute of Technology, 2013 (zitiert auf S. 36).

[BL76] F. E. Bird, R. G. Loftus. *Loss control management*. Institute Press, 1976 (zitiert auf S. 21).

[Coo+96] S. E. Cooper, A. Ramey-Smith, J Wreathall, G. Parry. *A technique for human error analysis (ATHEANA)*. Techn. Ber. Nuclear Regulatory Commission, 1996 (zitiert auf S. 25, 26).

[DM07] S Dekker, C. Manning. „The Field Guide to Understanding Human Error.“ In: *Aviation, Space, and Environmental Medicine* 78.2 (2007), S. 148–148 (zitiert auf S. 22, 30).

[Dam+12] D. Damböck, M. Farid, L. Tönert, K. Bengler. „Übernahmezeiten beim hochautomatisierten Fahren“. In: *Tagung Fahrerassistenz. München* 15 (2012), S. 16 (zitiert auf S. 25).

[Dou93] E. Dougherty. „Context and human reliability analysis“. In: *Reliability Engineering & System Safety* 41.1 (1993), S. 25–47 (zitiert auf S. 25).

[Emb+94] D. Embrey, T. Kontogiannis, M. Green. „Guidelines for preventing human error in process safety“. In: *Center for Chemical Process Safety* 1.1 (1994) (zitiert auf S. 25–27).

[Emb86] D. Embrey. „SHERPA: A systematic human error reduction and prediction approach“. In: *Proceedings of the international topical meeting on advances in human factors in nuclear power systems*. 1986 (zitiert auf S. 26).

[Fra17] M. E. France. „Engineering for Humans: A new Extension to STPA“. Diss. Massachusetts Institute of Technology, 2017 (zitiert auf S. 15, 16, 19, 28, 29, 37, 40, 42, 47, 61, 65).

[Gol+13] C. Gold, D. Damböck, L. Lorenz, K. Bengler. „“Take over!” How long does it take to get the driver back into the loop?“ In: *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. Bd. 57. 1. SAGE Publications Sage CA: Los Angeles, CA. 2013, S. 1938–1942 (zitiert auf S. 25).

[Gol+16] C. Gold, M. Körber, D. Lechner, K. Bengler. „Taking over control from highly automated vehicles in complex traffic situations: the role of traffic density“. In: *Human factors* 58.4 (2016), S. 642–652 (zitiert auf S. 24, 25).

[Int16] S. International. *Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles*. 2016 (zitiert auf S. 15–17, 47).

[KJ03] J. W. Kim, W. Jung. „A taxonomy of performance influencing factors for human reliability analysis of emergency tasks“. In: *Journal of loss prevention in the process industries* 16.6 (2003), S. 479–495 (zitiert auf S. 25).

[Kir] B. Kirwan. „Human Error Identification Techniques for Risk Assessment and Ergonomics Evaluations of High Risk Systems-Part 2: Evaluation of techniques and specification of criteria for a new system“. In: () (zitiert auf S. 25).

[Kör+15] M. Körber, T. Weißgerber, L. Kalb, C. Blaschke, M. Farid. „Prediction of take-over time in highly automated driving by two psychometric tests“. In: *Dyna* 82.193 (2015), S. 195–201 (zitiert auf S. 24).

[Kör+16] M. Körber, C. Gold, D. Lechner, K. Bengler. „The influence of age on the take-over of vehicle control in highly automated driving“. In: *Transportation research part F: traffic psychology and behaviour* 39 (2016), S. 19–32 (zitiert auf S. 24).

[LT14] N. G. Leveson, C. L. Thornberry. „Extending the human controller methodology in systems-Theoretic Process Analysis (STPA)“. Diss. Massachusetts Institute of Technology, 2014 (zitiert auf S. 15, 17, 19, 29–31, 36, 37, 40–42, 47, 61, 65).

[LT18] N. Leveson, J. Thomas. *STPA Handbook*. WordPress, 2018 (zitiert auf S. 15–17, 29, 34, 38–40, 47, 48, 61, 62, 65).

[Lev11] N. Leveson. *Engineering a safer world: Systems thinking applied to safety*. MIT press, 2011 (zitiert auf S. 19, 21, 28, 30, 34, 37, 42, 47, 60).

[MJ09] N. Merat, A. H. Jamson. „How do drivers behave in a highly automated car?“ In: (2009) (zitiert auf S. 25).

[Mod11] F. Mode. „Effects Analysis FMEA Handbook (with Robustness Linkages) v4. 2“. In: *Ford Motor Company* (2011) (zitiert auf S. 19, 33).

[Rad+14] J. Radlmayr, C. Gold, L. Lorenz, M. Farid, K. Bengler. „How traffic situations and non-driving related tasks affect the take-over quality in highly automated driving“. In: *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. Bd. 58. 1. Sage Publications Sage CA: Los Angeles, CA. 2014, S. 2063–2067 (zitiert auf S. 25).

[Rad+16] J. Radlmayr, M. Körber, A. Feldhütter, K. Bengler. „Methoden und Fahrermodelle für Hochautomatisiertes Fahren“. In: (2016) (zitiert auf S. 24, 25).

[Ras82] J. Rasmussen. „Human errors. A taxonomy for describing human malfunction in industrial installations“. In: *Journal of occupational accidents* 4.2-4 (1982), S. 311–333 (zitiert auf S. 30, 41).

[Ras83] J. Rasmussen. „Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models“. In: *IEEE transactions on systems, man, and cybernetics* 3 (1983), S. 257–266 (zitiert auf S. 19, 52).

[Rau+09] N. Rauch, A. Kaussner, H.-P. Krüger, S. Boverie, F. Flemisch. „The importance of driver state assessment within highly automated vehicles“. In: *16th ITS World Congress, Stockholm, Sweden*. Bd. 21. 2009, S. 25 (zitiert auf S. 25).

[Rea00] J. Reason. „Human error: models and management“. In: *Bmj* 320.7237 (2000), S. 768–770 (zitiert auf S. 21).

[Rea90] J. Reason. *Human error*. Cambridge university press, 1990 (zitiert auf S. 21, 22).

[Rudgu] A. Rudolph. *Guideline for Human Error Analysis*. Continental Teves AG & Co. oHG. August 2016 (zitiert auf S. 19, 22, 33, 44, 47, 52, 53).

[Run+12] P. Runeson, M. Host, A. Rainer, B. Regnell. *Case study research in software engineering: Guidelines and examples*. John Wiley & Sons, 2012 (zitiert auf S. 63).

[Sch11] J. Schaffner. „Gefahrenanalyse und Sicherheitskonzept nach ISO 26262 für Fahrerassistenzsysteme“. In: *ATZelektronik* 6.1 (2011), S. 34–39 (zitiert auf S. 48, 49).

[Shea] *CIRCULAR 240-AN/144 - HUMAN FACTORS DIGEST No. 7*. ICAO, 1989 (zitiert auf S. 22, 61).

[Sheb] *ICAO Circular 216-AN31 - HUMAN FACTORS DIGEST No. 1*. ICAO, 1989 (zitiert auf S. 22, 23).

[Sta04] N. A. Stanton. „Systematic human error reduction and prediction approach (SHERPA)“. In: *Handbook of human factors and ergonomics methods*. CRC Press, 2004, S. 394–403 (zitiert auf S. 25).

[Teu89] B. Teufel. „Informationsspuren zum numerischen und graphischen Vergleich von reduzierten natürlichsprachlichen Texten“. Diss. ETH Zurich, 1989 (zitiert auf S. 66).

[WS01] D. A. Wiegmann, S. A. Shappell. „Human error analysis of commercial aviation accidents: Application of the Human Factors Analysis and Classification System (HFACS)“. In: *Aviation, space, and environmental medicine* 72.11 (2001), S. 1006–1016 (zitiert auf S. 25, 26).

[Wic+15] C. D. Wickens, J. G. Hollands, S. Banbury, R. Parasuraman. *Engineering psychology & human performance*. Psychology Press, 2015 (zitiert auf S. 31, 41).

[Wic02] C. D. Wickens. „Multiple resources and performance prediction“. In: *Theoretical issues in ergonomics science* 3.2 (2002), S. 159–177 (zitiert auf S. 31, 41).

[YS07] M. S. Young, N. A. Stanton. „Back to the future: Brake reaction times for manual and automated vehicles“. In: *Ergonomics* 50.1 (2007), S. 46–58 (zitiert auf S. 25).

[Yin03] R. K. Yin. „Case study research design and methods third edition“. In: *Applied social research methods series* 5 (2003) (zitiert auf S. 63).

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

Erklärung

Ich versichere, diese Arbeit selbstständig verfasst zu haben. Ich habe keine anderen als die angegebenen Quellen benutzt und alle wörtlich oder sinngemäß aus anderen Werken übernommene Aussagen als solche gekennzeichnet. Weder diese Arbeit noch wesentliche Teile daraus waren bisher Gegenstand eines anderen Prüfungsverfahrens. Ich habe diese Arbeit bisher weder teilweise noch vollständig veröffentlicht. Das elektronische Exemplar stimmt mit allen eingereichten Exemplaren überein.

Ort, Datum, Unterschrift

Gelesen und freigegeben von der Continental Teves AG & Co. oHG

25.10.2018 P. Blüher

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