Hochschule Ruhr West

Fachbereich 4, Institut Naturwissenschaften

Studiengang Sicherheitstechnik

Andreas Braasch (Prof. Dr.-Ing.)

EPS: Die elektrisch betriebene Lenkung unter Berücksichtigung der ISO 26262 und ISO 21448 (SOTIF) – Anforderungen und Sicherheitsanalysen

Bachelorarbeit

Berke Ertugrul

M.-Nr. 10009314

Erstprüfer Andreas Braasch (Prof. Dr.-Ing.)

Zweitprüfer David Schepers (Prof. Dr.-Ing.)

Ausgabe des Themas 2022-02-15

Abgabe der Arbeit 2022-04-29

Version

Bachelorarbeit Berke Ertugrul im Ausdruck vom 2022-04-29

Inhaltsverzeichnis

1 Einleitung

Ziel dieser Arbeit ist es, ein grundlegendes Verständnis eines elektrisch betriebenen Lenksystems zu schaffen und dessen zugehörige Anforderungen und Analysen seitens der funktionalen Sicherheit darzustellen. Beginnend mit der theoretischen Darstellung des Lenksystems und den Normen wird im praktischen Teil der Arbeit diese Theorie angewandt. Zudem werden Autonomiestufen und deren rechtliche Grundlage in Deutschland aufgeführt und diskutiert.

Hierbei wird auf die Norm für die funktionale Sicherheit, die ISO 26262 und auf die Norm für die Sicherheit der Funktion, die ISO 21448 eingegangen. Es wird erläutert, welchen Zweck die Anwendung der ISO 26262 hat und wie sie aufgrund der zunehmenden Komplexität in der Automobilbranche durch die ISO 21448 (SOTIF) ergänzt wird. Dazu wird herausgearbeitet, wann die ISO 26262 an ihre Grenzen stößt und wie unabdingbar die Anwendung von SOTIF wird.

Einhergehend mit der technologischen Entwicklung und der zunehmenden Komplexität treten nämlich vermehrt Aspekte auf, die mit der ISO 26262 allein nicht abgedeckt werden können. Sicherheitsaspekte nehmen zu und verändern sich mit neuen Komfort- und Assistenzsystemen kontinuierlich. Daher ist es aufgrund der sich ändernden Technologien und derer Komplexität unabdingbar, bestehende Ansätze zu verbessern und zusätzliche neue Methoden für die Sicherheit des Endproduktes zu entwickeln und neben den etablierten Methoden anzuwenden.

Welchen Einfluss dies auf ein modernes Lenksystem hat und wie in diesem Zusammenhang das Zusammenspiel der ISO 26262 und ISO 21448 mit klassischen Methoden wie der Fehlermöglichkeits- und Einflussanalyse (FMEA) betrachtet werden muss, wird in dieser Arbeit dargestellt. Automobilhersteller sind heute bereits in der Lage Fahrzeuge automatisiert in bestimmten Betriebsgrenzen und Bereichen fahren zu lassen. Doch was muss getan werden, um sämtliche Betriebsgrenzen aufzuheben und ein Fahrzeug „autonom“ zu gestalten? Regulatorien, Standards und Richtlinien sind bereits heute auf dem besten Weg dorthin, doch ist es in der Praxis tatsächlich realisierbar?

1.1 Glossar

Ausfall	Verlust der Fähigkeit, wie gefordert zu funktionieren.
fail-operational	Der fail-operational ist ein Konstruktionsprinzip in der Sicherheitstechnik. Das jeweilige System wird automatisch in einen reduziert-operativen Zustand überführt sofern ein unvorhergesehener Fehler, Defekt oder Ausfall eintrifft. Dieses Prinzip wird bei sicherheitskritischen Anwendungen eingesetzt, um im Fehlerfall eine Grundfunktionalität zu gewährleiten.
fail-safe	Der fail-safe ist ein Konstruktionsprinzip in der Sicherheitstechnik. Das jeweilige System wird automatisch in einen passiven sicheren Zustand überführt sofern ein unvorhergesehener Fehler, Defekt oder Ausfall eintrifft.
Funktionale Sicherheit	Teil der Gesamtsicherheit, der von der korrekten Funktion eines Systems und anderer Maßnahmen abhängt.
Gefährdung	Potenzielle Schadensquelle.
Komponente	Eine Komponente ist ein Element bzw. Bestandteil eines Moduls, wie z.B. ein Schalter. Somit ist es die kleinste Stufe eines zerlegten Systems.
Redundanz	Vorhandensein von mehr als nur einer funktional gleichen oder vergleichbaren Ressource eines technischen Systems.
µ-Split	Mü (µ) ist eine physikalische Einheit, welche den Reibwert einer Oberfläche bezeichnet. Eine µ-Split Strecke besteht aus unterschiedlichen Oberflächen mit unterschiedlichen Reibwerten [1].

1.2 Abkürzungen

ACC	Adaptive Cruise Control
ADAS	Advanced Driver Assistance System
ADS	Autonomous driving system
ASIL	Automotive Safety Integrity Level
EPS	Electric power steering
ESP	Elektronisches Stabilitätsprogramm
FTTI	Fault Tolerant Time Interval
LKAS	Lane Keeping Assist System
ODD	Operational Design Domain
SAE	Society of Automotive Engineers

SOTIF	Safety of The Intended Functionality
STAMP	Systems-theoretic accident model and processes
STPA	Systems-theoretic process Analysis

1.3 Symbole

MTTF	Mean operating time to failure, mittlere Betriebszeit bis zum Ausfall [2].
MTTR	Mean time to restoration, mittlere Dauer bis zur Wiederherstellung [3].

2 Die elektrisch betriebene Lenkung

Lenksysteme haben in den letzten Jahren durch die stetige Weiterentwicklung und zunehmende Automatisierung einen massiven Wandel erlebt. Die bisher eingesetzten hydraulisch unterstützten Lenkungen werden zunehmend von rein elektrisch unterstützten Lenksystemen abgelöst. Elektrisch unterstützte Lenksysteme (engl. Electric power steering, EPS) bieten dabei in den verschiedensten Bereichen Vorteile im Vergleich zu hydraulischen Lenksystemen.

Unterstützte Lenksysteme, auch Servolenkungen genannt, haben einen mechanischen Aufbau, welcher den Fahrer bei der Lenkung unterstützt. Dafür wird die vom Fahrer am Lenkrad aufgebrachte Lenkkraft verstärkt und somit die zum Lenken benötigte Kraft reduziert. [4]

Klassisch konstruierte hydraulische Servolenkungen verstärken die Lenkkraft über einen Hydraulikzylinder, welcher Teil eines Servomechanismus ist. Dabei existiert eine direkte mechanische Verbindung zwischen dem Lenkrad und dem Lenkgestänge, welches die Räder lenkt. Diese mechanische Verbindung enthält auf der Lenkradseite eine Torsionsfeder (in der Regel in Form eines Torsionsstabs), die eine geringe Relativbewegung zwischen Lenkrad und Lenkgestänge zulässt. Zur Erzeugung der Unterstützungskraft wird die vom Fahrer erzeugte Relativbewegung über ein Hydraulikventil erfasst, wodurch ein Druck im Hydraulikzylinder aufgebaut wird. Dadurch ist die Unterstützungskraft direkt von der vom Fahrer aufgebrachten Lenkkraft abhängig. [5, S. 183–184]

Bei einem Ausfall der Servolenkung ist der Fahrer immer noch in der Lage das Fahrzeug, ohne diese Unterstützung zu lenken. Die Manöver werden deutlich erschwert sein, die mechanische Verbindung stellt jedoch eine Rückfallebene dar, um das Fahrzeug sicher an den Fahrbahnrand manövrieren zu können.

Eine elektrische Servolenkung ist in der Basisfunktionalität der hydraulischen Servolenkung ähnlich, dabei wird jedoch die Torsionsfeder und das Hydraulikventil durch einen Momentensensor und der Hydraulikzylinder durch einen Elektromotor ersetzt. Dabei bieten bestimmte Positionierungen der Komponenten unterschiedliche Vor- und Nachteile und können je nach Einsatzzweck unterschiedlich angeordnet werden. In der Abbildung 1 ist die Servoeinheit zum Beispiel an der Lenksäule untergebracht. [6]

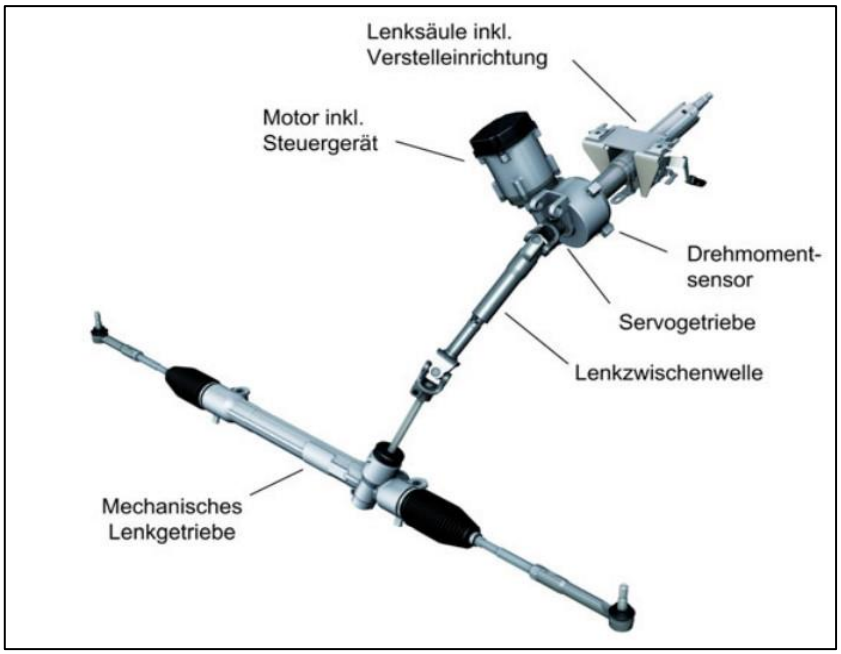


Abbildung 1: Ein elektrisch betriebenes Lenksystem mit der Servoeinheit an der Lenksäule

Diese Positionierung ist bei Kleinwagen sehr gängig, da sie aufgrund ihrer Größe und des Gewichts keine hohe Lenkkraft benötigen. Dies ist wichtig, da die Übertragung der Lenkkräfte bei solch einem Aufbau über die Lenksäule, Lenkzwischenwelle und dem Lenkritzel läuft und somit durch diese Komponenten in Bezug auf die maximal zu erreichende Lenkkraft begrenzt ist. Die Servoeinheit ist dabei im Innenraum des Fahrzeugs und hat keine erschwerten umwelttechnischen Anforderungen zu erfüllen. So muss sie zum Beispiel nicht wasserdicht sein. Zudem tritt im Fahrzeuginneren ebenso ein geringerer Temperaturbereich auf, wobei gerade hohe Temperaturen für die elektronischen Komponenten in dem Steuergerät (engl. Electronic Control Unit, ECU) oftmals ein Problem darstellen [8]. Nachteil ist, dass Störgeräusche seitens der Servoeinheit den Fahrer stören oder in der Konzentration beeinträchtigen könnten. Des Weiteren ist die Crash-Sicherheit bei dieser Art von Positionierung oft eine Herausforderung.

In der Abbildung 2 wurde die Servoeinheit mit direkter Verbindung zum Lenkgetriebe bzw. dem Lenkritzel positioniert. Dadurch kann das System deutlich höhere Lenkleistungen erreichen, da die Kraft nicht mehr über die Lenksäule und der Lenkzwischenwelle übertragen werden muss [7]. Daraus folgt, dass die Lenkunterstützung ausreichend ist, um ein komfortables und gefahrfreies Lenken von Kompaktfahrzuge bis SUVs zu ermöglichen. Die Servoeinheit befindet sich bei dieser Positionierung nicht mehr im Fahrzeuginneren und muss somit Umwelteinflüssen wie Wasser, Dreck, Temperatur und Vibrationen standhalten.

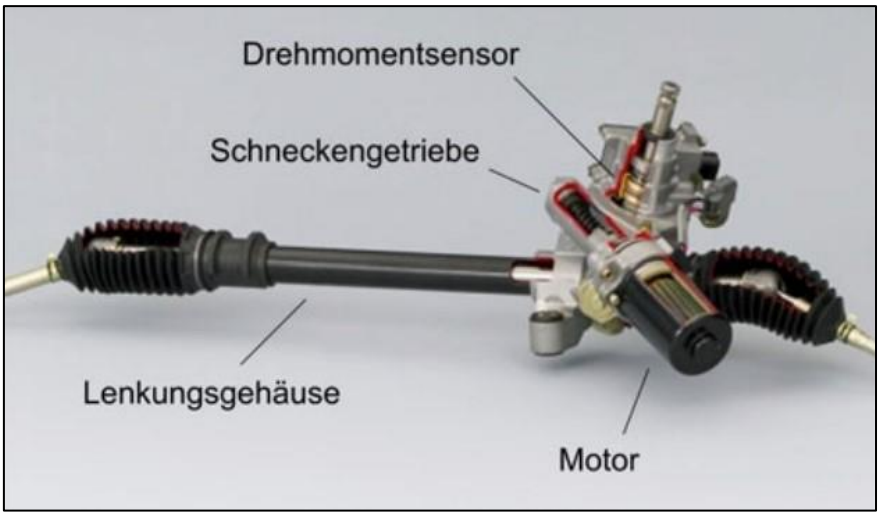


Abbildung 2: Ein elektrisch betriebenes Lenksystem mit der Servoeinheit am Lenkgetriebe

Das auf die Lenksäule ausgeübte Drehmoment sowie die Position des Lenkrads werden von Sensoren erfasst. Mittels eines Steuergerätes (ECU), welches meistens an dem Lenkgetriebe oder der Lenksäule angebracht ist und eines Motors, wird in Abhängigkeit von der Fahrsituation ein unterstützendes Drehmoment aufgeprägt. Diese Unterstützung ist je nach Fahrsituation unterschiedlich stark und wird während der Entwicklung auf das jeweilige Fahrzeug angepasst. Dadurch kann das Ansprechverhalten der Lenkung individuell auf den Kundenwunsch sowie Besonderheiten des Fahrzeugs wie Federungssysteme mit variabler Rate und variabler Dämpfung abgestimmt werden, um somit die Handhabung sowie das Fahrverhalten optimal anzupassen.

Abgesehen von technischen Vorteilen bietet die EPS unter anderem einen Vorteil für die Umwelt. Bei einer hydraulischen Lenkung ist die Hydraulikpumpe kontinuierlich im Betrieb, da diese mittels eines Riementriebs an den Verbrennungsmotor angebunden ist. Sie läuft dadurch mit der Motordrehzahl, wodurch der Volumenstrom unabhängig davon, ob die Lenkung aktiv genutzt wird, stets durch das Lenksystem gefördert wird [9]. Da die Pumpe für die Leerlaufdrehzahl des Motors ausgelegt sein muss, wird bei höheren Drehzahlen ein unnötig hoher Volumenstrom erzeugt.

Bei der EPS wird die Unterstützung mittels eines Elektromotors bereitgestellt. Die Lenkunterstützung wird lediglich nach Bedarf eingesetzt, man spricht bei so einem Verhalten von einem Power-On-Demand-System. Dies führt zu einer Kraftstoffersparnis von bis zu 0,8 l/ 100km im Vergleich zu konventionellen hydraulischen Lenksystemen [5, S. 347].

Zusätzlich zum Riementrieb entfallen ebenfalls einige Hochdruck-Hydraulikschläuche, welche die Hydraulikpumpe mit dem Lenkgetriebe verbinden. Dieser Wegfall vereinfacht die Wartung und Herstellung. Zudem kann die EPS für unterschiedliche Motoren eingesetzt werden, ohne sie anpassen zu müssen. Eine konventionelle Hydraulische Lenkung ist in der Regel aufgrund des Riementriebs für einen quer eingebauten 4-Zylinder anders zu platzieren als für einen V-8 Motor.

Die EPS hat in der Entwicklung unter anderem neue Möglichkeiten mit sich gebracht, um verbesserte Funktionalitäten hinzuzufügen. Einer der wesentlichen Vorteile ist, dass die Lenkung adaptiv ausgelegt ist und somit durch Assistenzsysteme überlagert werden kann. Zusätzlich kann das Lenkradmoment

unabhängig von der Fahrzeuggeschwindigkeit und dem Unterstützungsmoment eingestellt werden. Somit werden Auslegungskonflikte wie hohe Unterstützungsmomente bei niedrigen Lenkradmomenten aufgrund hoher Reifenreibung beim Einparken und geringe Unterstützung bei höheren Lenkradmomenten bei schnellem Fahren aufgelöst.
Weit verbreitete zusätzliche Funktionen sind der Fahrspurassistent, die Windkraftkorrektur oder ebenso das automatische Einparken in Verbindung mit anderen Systemen. Zudem können Assistenzfunktionen dem Fahrer eine passende Lenkempfehlung geben, damit er in besonders kritischen Fahrsituationen korrekt reagieren kann. Bei einer Übersteuerung oder bei einem Bremsmanöver auf μ-Split (links und rechts unterschiedliche Straßen-Reibwerte) kann das Elektronische Stabilitätsprogramm (ESP) zusätzliches Drehmoment um die Hochachse des Fahrzeugs von der Lenkung anfordern, um den Fahrer zu unterstützen [1].

2.1 Sicherheitstechnische Anforderungen für ein elektrisch betriebenes Lenksystem

In der Entwicklung einer elektrisch betriebenen Lenkung gehören sicherheitstechnische Anforderungen ebenso dazu wie technische Herausforderungen. Die Sicherheit der einzelnen Funktionen selbst muss gewährleitet sein, sie muss ein grundlegender Bestandteil des Produktes sein.
Um eine Lenkung funktional sicher zu entwickeln, muss der gesamte Sicherheitslebenszyklus betrachtet werden. Dieser umfasst die Konzepterstellung des jeweiligen Produktes, die Planung, Entwicklung, Umsetzung, Inbetriebnahme sowie die Instandhaltung. Detaillierte Arbeitsschritte zum Beispiel in der ISO 26262 aufgeführt (siehe Kapitel 4.1, Die grundlegende Struktur der ISO 26262).
Die Aufgabe eines Sicherheitskonzeptes besteht darin, eintretende Fehler sicher beherrschbar zu gestalten. Es beginnt bei der Hardware, bei der gewisse Fehler bereits durch ein an dem Stand der Technik orientiertes mechanisches Design ausgeschlossen werden können. Im Weiteren können Fehler durch ein passend entwickeltes Sicherheitskonzept schnell erkannt und das System daraufhin in einen sicheren Zustand überführt werden. Die Voraussetzung hierfür ist selbstverständlich das Vorhandensein eines solchen sicheren Systemzustands.
Der sichere Zustand, im Englischen „Safe State“, kann bei den meisten EPS Anwendungen durch das Abschalten der Lenkunterstützung erreicht werden. Das bedeutet, dass die EPS keine Lenkunterstützung mehr generieren darf. Um den sicheren Zustand wieder verlassen zu können, muss das System in der Regel aus- und eingeschaltet und das Steuergerät erfolgreich initialisiert werden. Dieser sichere Zustand setzt voraus, dass die mechanische Lenkfähigkeit gemäß der ECE R79 Regelung gewährleistet ist [10].
In der Abbildung 3 ist eine beispielhafte Darstellung zu sehen, wie die einzelnen Systemzustände einer EPS miteinander verknüpft sind. Es ist zu sehen, dass der Systemzustand „EPS Aktiv“ ausschließlich nach erfolgreicher Initialisierung eingenommen werden kann. Lediglich in diesem Zustand kann die Lenkunterstützung bereitgestellt werden. Der sichere Zustand kann, wie in Abbildung 3 zu sehen ist, nach einem fehlerhaftem Selbsttest und nach einem Fehler im aktiven Zustand eingenommen werden. Ein sicherheitskritischer Fehler muss innerhalb der Fehlertoleranzzeit, im Englischen „Fault Tolerant Time Intervall“

(FTTI), mithilfe von Abschaltpfaden, die das System in den sicheren Zustand überführen, behandelt werden. Die FTTI ist die maximal akzeptierbare Zeit eines kritischen Fehlers, nach Auftreten bis zum Wirksamwerden der Gegenmaßnahme. Sie muss so kurz bemessen sein, dass der Fehler in dieser Zeit keine inakzeptablen Risiken verursacht. Die Fehlererkennung und die anschließenden Fehlerreaktionen müssen daher innerhalb dieser Zeit stattfinden. [11]

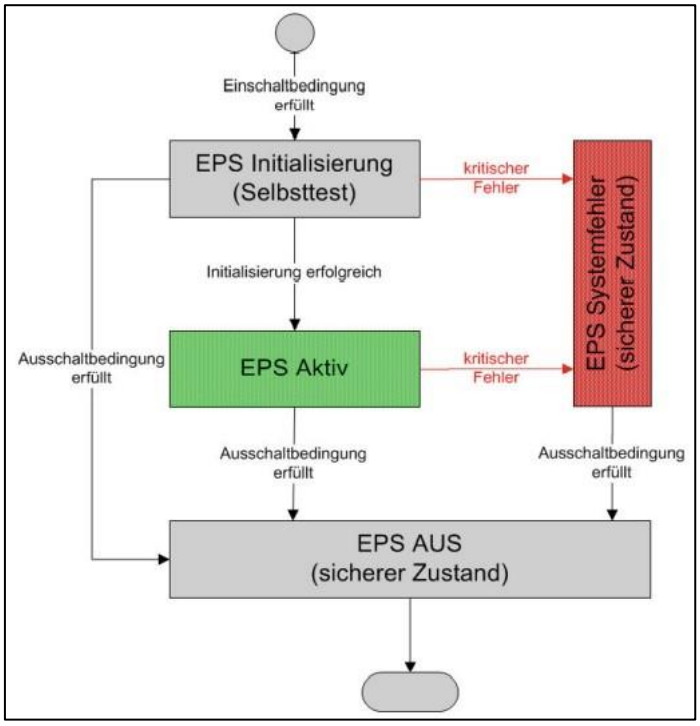


Abbildung 3: Systemzustände eines elektrisch betriebenen Lenksystems

Um zu bestimmen, ob ein Risiko akzeptabel ist, wird durch eine Gefahren- und Risikoanalyse zunächst ohne die Berücksichtigung von Sicherheitsmaßnahmen gemäß ISO 26262 eine Sicherheitsanforderungsstufe, im Englischen „Automotive Safety Integrity Level“ (ASIL), für sämtliche Fehlfunktionen ermittelt. Eine beispielhafte ASIL Einstufung für eine gewöhnliche EPS könnte folgendermaßen sein:

- Ausfall der Lenkunterstützung →QM
- Schwergängigkeit bzw. Blockade des Lenksystems →ASIL D
- Übermäßiges Einsetzen der Lenkunterstützung →ASIL D
- Zu geringe Bereitstellung der Lenkunterstützung →QM
- Ungewollte Bereitstellung der Lenkunterstützung →ASIL D

Für diese Fehlfunktionen werden dann im Sicherheitskonzept Schutzziele definiert. Durch die Implementierung von Funktionen, die diese Schutzziele garantieren, wird das Risiko auf eine akzeptable Restgröße reduziert.

Beispielhafte Schutzziele oder im Englischen „Safety Goals“ könnten folgendermaßen aufgebaut sein:

1. Das System muss Fehler, die zu einer Schwergängigkeit bzw. Blockade des Lenksystems führen, gemäß ASIL D Anforderungen erkennen und in den sicheren Zustand wechseln.

2. Das System muss Fehler, die zu übermäßigem Einsetzen der Lenkunterstützung führen, gemäß ASIL D Anforderungen erkennen und in den sicheren Zustand wechseln.

Für mechanische Komponenten sieht die ISO 26262 keine besonderen Anforderungen vor, trotzdem müssen Fehler im mechanischen Design ausgeschlossen werden. Dies wird während der Entwicklung der Mechanik durch Verwendung geeigneter Methoden wie zum Beispiel einer FMEA sichergestellt. Ein verheerendes Versagen wäre zum Beispiel der Verlust des mechanischen Durchgriffs zwischen den Rädern und dem Lenkrad. Durch geeignete Dimensionierung der Komponenten kann dies jedoch ausgeschlossen werden.

2.2 Steer by Wire und Funktionale Sicherheit

Eine „Steer by Wire“ Lenkung ist ein System in einem Fahrzeug, bei dem keine mechanische Verbindung zwischen dem Lenkrad und den Rädern besteht. Eine vom Fahrer ausgeführte Lenkbewegung am Lenkrad wird von einem Sensor erfasst und in einem elektronischen Lenksteuergerät zu einem Lenkbefehl verarbeitet. Dieser wird elektrisch an einen Aktor weitergeleitet, welcher den Lenkbefehl an den gelenkten Rädern ausführt. Aufgrund der fehlenden mechanischen Verbindung erfolgt keine Rückkopplung von der Straße, daher wird mittels eines Feedback-Aktuators die Rückführung der Lenkkräfte so wie die Einflüsse des Fahrbahnuntergrundes am Lenkrad simuliert. [5, S. 447–452, 12]

Diese Art von „by Wire“ Technologie hat in der Automobilbranche erstmals mit dem elektronischen Gaspedal Einzug gefunden. Die herkömmliche mechanische Verbindung mittels eines Gaszugs wurde durch ein elektronisches Gaspedal ersetzt.

Aufgrund der rein elektrischen Übertragung des Lenkwinkels werden Steer by Wire Systeme nicht als gleichermaßen technologisch beherrschbar wie mechanische oder hydraulische Systeme empfunden. Elektronische Komponenten wird aufgrund des zufälligen Ausfallverhaltens ein deutlich geringeres Vertrauen entgegengebracht.

Eine klassische EPS hat bei einem Ausfall der Servounterstützung stets die mechanische Rückfallebene und stellt somit auch weiterhin die Lenkfunktion und damit die Verfügbarkeit der Lenkung sicher. Um eine ständige Verfügbarkeit eines Steer by Wire Systems zu gewährleisten, muss das System fähig sein, Fehler in einzelnen Baugruppen zu tolerieren und fallweise auf redundante Komponenten umzuschalten. Die Zuverlässigkeit des Systems ist ebenfalls in direkter Relation mit der Aufrechterhaltung der Funktionsfähigkeit, dem Gefährdungspotential und der Sicherheit zu sehen. Dabei hat ein Steer by Wire System die gleichen Anforderungen an die Zuverlässigkeit und funktionale Sicherheit wie ein SAE Stufe 5 System (siehe Kapitel 3.1) und muss dementsprechend entwickelt werden. Bei einem Stufe 5 System existiert auf Grund des Verzichts auf einen Fahrer ebenfalls keine Rückfallebene, daher muss das System dementsprechend ausgelegt werden.

Die Systeme müssen die höchsten Anforderungen an die Eigensicherheit erfüllen, da der Fahrer im Systemfehlerfall keine Möglichkeit hat einzugreifen. Der Hersteller eines Steer by Wire Systems muss somit

nachweisen, dass ein Funktionsfehler des Systems zu keinem Verlust der Lenkfunktion führen kann. Alle wichtigen Funktionen müssen mindestens zweikanalig aufgebaut sein, um ein redundantes System zu haben. [13]

Die grundlegenden Sicherheitseigenschaften eines elektrischen oder elektronischen Systems sind die Zuverlässigkeit, die Verfügbarkeit und die Sicherheit. Unter dem Begriff Zuverlässigkeit versteht man in der Funktionalen Sicherheit die Wahrscheinlichkeit, in der das System eine beabsichtigte Funktion in einem definierten Zeitintervall ausführt bzw. erfüllt. Die Verfügbarkeit hingegen, ist die Wahrscheinlichkeit, mit der ein System zu einem bestimmten Zeitpunkt über die gesamte Lebensdauer betrachtet betriebsbereit ist. Die Verfügbarkeit wird durch die mittlere Betriebsdauer bis zum Ausfall (Mean time to failure, „MTTF“) und der mittleren Reparaturzeit nach einem Ausfall berechnet (Mean time to repair, „MTTR“).

Die Berechnung ist folgendermaßen: Verfügbarkeit = MTTF / (MTTF + MTTR). Die Berechnung basiert auf rein statistischen Größen, menschliche Faktoren bleiben unberücksichtigt. Eine hohe Systemverfügbarkeit wird erreicht, wenn der MTTF Wert groß und der MTTR Wert klein ist. Ein hoher MTTF Wert wird erreicht, wenn die Einheit selten ausfällt, welches somit dann unter anderem einer kleinen Ausfallrate entspricht. [14]

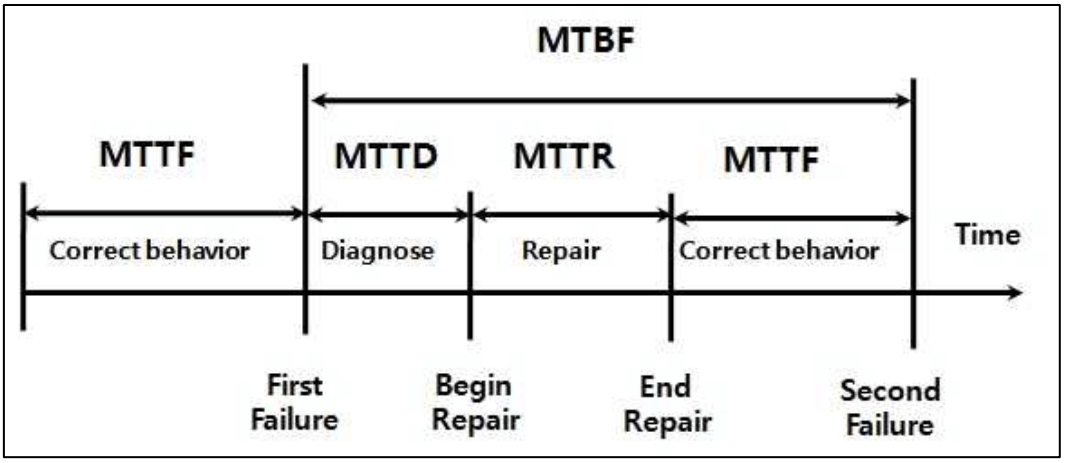


Abbildung 4: Schematische Darstellung der einzelnen Fehlerraten

Ein mögliches Beispiel für die Zuverlässigkeit, übertragen auf ein Fahrzeug, wäre zum Beispiel die Wahrscheinlichkeit, dass das Fahrzeug ein bestimmtes Ziel erreicht, ohne dass ein Ausfall auftritt. Bei der Verfügbarkeit handelt es sich zum Beispiel um die Wahrscheinlichkeit, dass das Fahrzeug gerade betriebsbereit ist und nicht aufgrund eines Defektes instandgesetzt werden muss. Die Sicherheit als letzte Eigenschaft bedeutet, dass das Fahrzeug keine Gefahr für den Menschen darstellt oder verursacht.

2.3 Fail Safe und Fail Operational

Aufgrund der zunehmenden Automatisierung werden immer mehr elektrische oder elektronische Systeme aktiv an der Fahrzeugführung beteiligt. Somit ist das Abschalten des Systems im Fehlerfall nicht möglich,

da dies eine aktive Gefährdung für den Menschen darstellen würde. Daher muss das System so ausgelegt werden, dass es im Fehlerfall weiterhin die Grundfunktionalität ausführen kann.

Der „Fail Safe“ ist ein Systemzustand, bei dem das System in einem Fehlerfall einer Komponente in einen sicheren passiven Zustand übergeht. Bei einer klassischen EPS wird er durch Abschalten der Unterstützung erreicht. Dies ist grundlegend ausreichend, da bei einem Ausfall der Lenkunterstützung der Fahrer durch die mechanische Rückfallebene stets die Möglichkeit besitzt das Fahrzeug ausreichend sicher zu bewegen. Eine Fehlfunktion, wie eine zu hohe Lenkunterstützung, kann bei hohen Geschwindigkeiten schwerwiegende Folgen haben. Das Sicherheitskonzept würde diese Fehlfunktion erkennen und als Gegenmaßnahme als „Fail Safe“ die Lenkunterstützung abschalten. Ein System, welches aufgrund eines transienten Fehlers eine Fehlfunktion ausgelöst hat, wird in der Regel nach einem Reset und einem Selbsttestzyklus wieder zur Verfügung stehen.

In der Abbildung 5 ist diese Strategie dargestellt. Im Fehlerfall geht das System unverzüglich in den sicheren Zustand. Nach erfolgter „Reparatur“ des Systems ist dieses wieder betriebsbereit und wird wieder den operativen Zustand einnehmen. Wurde die Fehlfunktion jedoch nicht aufgrund einer Transiente oder Ähnlichem ausgelöst, wird das System bei häufigem Auftreten von Fehlern ein Zuverlässigkeits- und Verfügbarkeitsproblem haben. [15, S. 23–53]

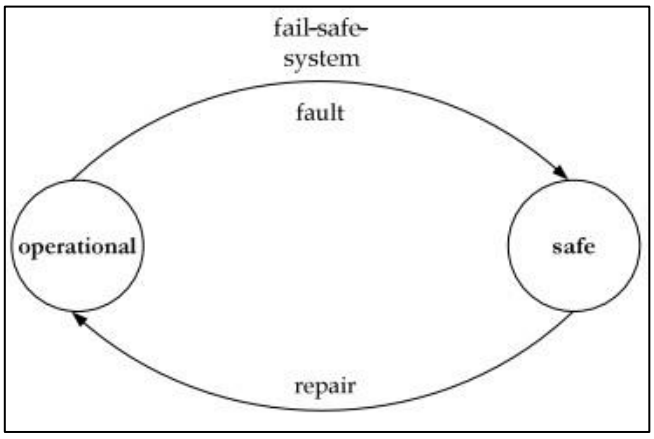


Abbildung 5: Fail-Safe System

Die Fail Operational-Strategie ist eine Fehlerbehandlung, bei der das System im Fehlerfall nicht komplett abgeschaltet wird. In einigen Anwendungen oder Betriebsphasen eines Systems ist das Abschalten sicherheitskritisch und kann den Menschen gefährden. In diesen Anwendungen oder Betriebsphasen müssen aus Sicherheitsgründen Fehlertoleranzmaßnahmen vorgesehen werden, welche im Fehlerfall den (Not)-Betrieb einleiten können. Das System muss somit im Fehlerfall die grundlegende Funktionalität weiter ausführen können. Bei einem Fail Operational System sind Redundanzen notwendig, um die Funktion des Systems zu gewährleisten, dafür werden strukturelle-, funktionelle-, Informations- und Zeitredundanzen als Fehlertoleranzmaßnahmen eingesetzt.

In der Abbildung 6 ist die Fail Operational Strategie dargestellt. In einem ersten Fehlerfall geht das System nicht wie im Fail Safe unverzüglich in einen passiven sicheren Zustand über. Im konkreten Fall würde das

Lenksystem einen reduzierten, jedoch operativen Zustand einnehmen. Die grundlegende Funktionalität wäre weiterhin gegeben und das Fahrzeug wäre lenkbar. Tritt nun jedoch ein weiterer Fehler auf, könnte dies zu einem unsicheren Zustand führen. Die Konsequenz dafür ist die Herabsetzung bei einem zweiten Fehler zu einem Fail Safe Prinzip. Damit dies möglich wird, werden in der Regel Betriebseinschränkungen während des Fail Operational-Betriebs wie zum Beispiel eine verringerte Geschwindigkeit notwendig. [16, S. 25–27]

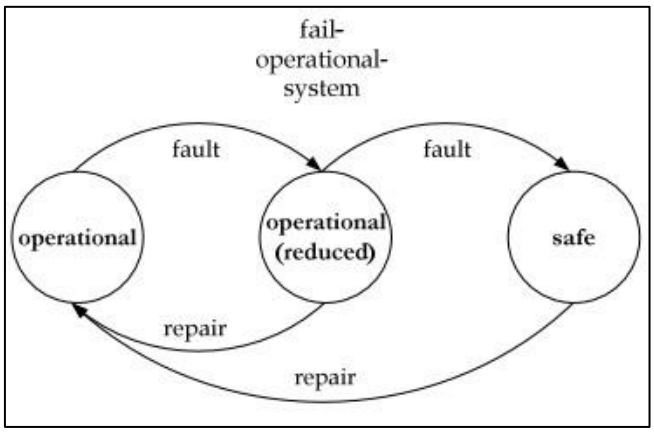


Abbildung 6: Fail-Operational System

Die Fail Operational Strategie wurde bei Lenksystemen eingesetzt, da Fahrzeuge mittlerweile über die ersten Automatisierungsstufen hinweg entwickelt werden. Konkret sind damit die SAE Stufen 3, 4 und 5 gemeint. In den Stufen 4 und 5 wird der Fahrzeugführer nicht mehr als Rückfallebene betrachtet. Aus diesem Grund muss das System ausfallsicher sein und dies erfordert eine entsprechende Systemarchitektur. Durch eine ausfallsichere Systemarchitektur wird die volle oder eingeschränkte Funktionalität des Systems ebenso im Fall eines ersten Fehlers weiterhin gewährleistet. Diese Systeme erfordern ein hohes Maß an Zuverlässigkeit, Verfügbarkeit und Sicherheit.

Je nach SAE Level kann es reichen, wenn OEMs eine Backup Funktion lediglich für einige Sekunden bis Minuten bereitstellen. In der Stufe 3 wird der Fahrer vom System informiert, dass eine Störung vorliegt und wird aufgefordert die Kontrolle zu übernehmen. In der Stufe 4 wird der Fahrer auch in einem solchen Fall informiert, mit dem Unterschied, dass das System selbständig in der Lage sein muss, das Fahrzeug bei einer Nichtübernahme in einen sicheren Bereich abzustellen.

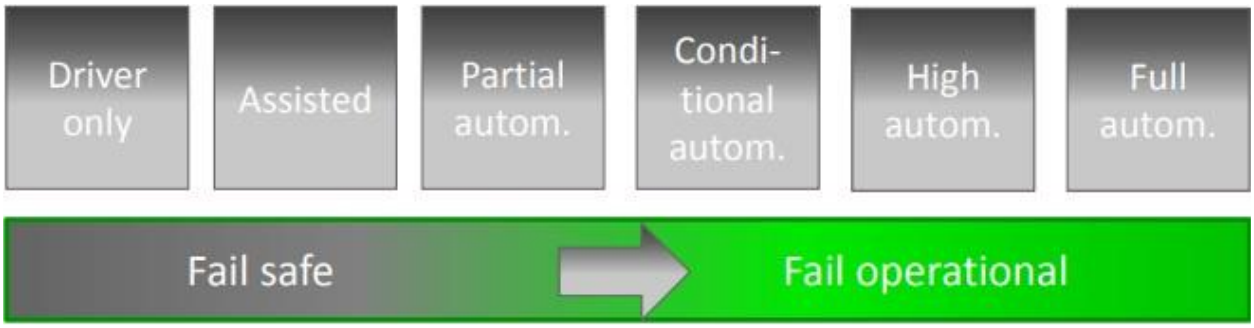


Abbildung 7: Autonomiestufen und der Übergang von Fail-Safe zu Fail-Operational

Grundsätzlich lassen sich die Elemente eines Fail-Safe-Steuerungskanals von den Sensoren bis zu den Aktoren für ein Fail-Operational-System wiederverwenden. Im einfachsten Fall wird der Steuerungskanal verdoppelt und mit eigenen Sensoren, Aktuatoren, einer eigenen Recheneinheit, deren Verkabelung und insbesondere auch einem völlig unabhängigem Stromversorgungs-, Takt- und Resetsystem aufgebaut [14, 17]. Eine Logik entscheidet dann, ob ein Kanal fehlerhaft arbeitet und schaltet diesen Kanal dann ab. Diese Logik kann entweder Bestandteil des jeweiligen Kanals sein (als Eigendiagnose) oder getrennt von diesen arbeiten. Im zweiten Fall stellt die Logik einen dritten Kanal dar, so dass eine 2 aus 3-Auswahl getroffen wird. Wird eine noch höhere Verfügbarkeit benötigt können weitere Kanäle hinzugefügt werden. Die korrekt arbeitenden Kanäle würden dann durch einen Mehrheitsentscheid bestimmt werden. [18]
In sämtlichen Fällen spielt die Vermeidung von gemeinsamen Ausfallursachen, im Englischen als „Common Cause Failures“ bezeichnet, eine große Rolle. So würde zum Beispiel der Verlust einer gemeinsamen Stromversorgung der Kanäle direkt dazu führen, dass ein Fail Operational-Betrieb nicht mehr möglich ist.

3 Die grundlegende Funktionsweise des autonomen Fahrens

Autonome Fahrzeuge stützen sich auf Sensoren, Aktoren, komplexe Algorithmen, maschinelle Lernsysteme und leistungsstarke Prozessoren. Die Fahrzeuge erstellen und pflegen in Echtzeit ein virtuelles Abbild ihrer Umgebung mittels zahlreicher Sensoren, die sich an den verschiedensten Stellen des Fahrzeugs befinden. So ist ein Radarsensor in Kombination mit einer Kamera in der Lage die exakte Position anderer Fahrzeuge in der Umgebung zu bestimmen. Kameras können Ampeln, Verkehrsschilder und andere Verkehrsteilnehmer wie Fußgänger erkennen.

Lidar-Sensoren (engl. Light Detection and Ranging) senden Lichtimpulse in die Umgebung des Fahrzeugs und bestimmen mit der Reflektionszeit die Entfernungen zu Fahrzeugen und anderen Objekten. Das Fahrzeug kann zudem Signale von Satelliten über das GPS-System empfangen und so seine genaue Position bestimmen. Automatisierte Fahrzeuge können sich über Mobilfunk und WLAN mit anderen Fahrzeugen und Datenquellen austauschen, sodass mögliche Hindernisse frühzeitig anderen Verkehrsteilnehmern mitgeteilt werden können.

Eine komplexe Software verarbeitet all diese sensorischen Informationen, berechnet einen Sollweg und sendet Anweisungen an die Aktuatoren des Fahrzeugs, welche die Beschleunigung, das Bremsen und das Lenken steuern. Fest kodierte Regeln, Algorithmen zur Hindernisvermeidung, vorausschauende Modellierung und Objekterkennung helfen der Software, Verkehrsregeln zu befolgen und Hindernisse zu umfahren. Wenn das Fahrzeug zum Beispiel einen Fußgänger und dessen Geschwindigkeit und Bewegungsrichtung erkennt, kann es durch das Berechnen von Wahrscheinlichkeiten die weiteren Bewegungen prognostizieren und vorausschauend agieren.

Autonom fahrende Fahrzeuge können im Vergleich zu von Menschen gesteuerten Fahrzeugen bestimmte Vorteile bieten. Ein solcher potenzieller Vorteil besteht darin, dass sie für mehr Sicherheit im Straßenverkehr sorgen könnten. Fahrzeugunfälle durch menschliches Versagen fordern jedes Jahr viele Todesopfer. Automatisierte Fahrzeuge könnten die Zahl der Unfallopfer verringern, da die in ihnen verwendete Software im Vergleich zu Menschen nicht abgelenkt wird, schneller reagiert, sich immer an die Verkehrsregeln hält und sich stets der Situation anpasst. Durch die Kommunikation zwischen den Fahrzeugen kann ebenso eine übergeordnete Koordination des Verkehrs stattfinden, wodurch es zu einer Verringerung der Verkehrsstaus kommen kann.

Um diese Vorteile nutzen zu können müssen allerdings die einzelnen Fahrzeugsysteme auf den Betrieb in einem autonomen Fahrzeug vorbereitet sein.

3.1 Anforderungen an ein System der Kategorie SAE 1-5

Der Begriff autonomes Fahren ist ein in der Gesellschaft viel diskutierter Begriff, welcher nicht bei jeder Person auf das gleiche Verständnis trifft. Getrennt gesehen, ist autonom ein in der künstlichen Intelligenz gängiger Begriff. In der KI und Robotik ist autonom ein Begriff, welcher ein System bezeichnet, welches in der Lage ist und die Autorität besitzt, Entscheidungen eigenständig und unabhängig zu treffen. Der Begriff wurde im Laufe der Zeit nicht mehr ausschließlich für die Entscheidung als solches, sondern für die

gesamte Systemfunktionalität verwendet und wurde so zu einem Synonym für „automatisiert“. Somit verdeckt der Ausdruck autonomes Fahrzeug Thematiken bzw. Fragen wie oder ob das Fahrzeug auf Kommunikationen mit externen Einheiten für die Datenerfassung und -sammlung angewiesen ist.

Einige Systeme für das automatisierte Fahren können sicherlich autonom sein, wenn es eine unabhängige und autarke Entscheidungsmacht besitzt. Eine Abhängigkeit von Kommunikation und oder Zusammenarbeit mit einem externen System, stellt den Begriff kooperativ statt autonom in den Vordergrund. Des Weiteren bezieht sich der Begriff Autonomie in der Rechtsprechung auf die Fähigkeit zur Selbstverwaltung. Ebenfalls in diesem Sinne ist "autonom" eine problematische Bezeichnung, wenn es um automatisiertes Fahren geht, denn selbst die fortschrittlichsten „Autonomous driving systems“ (ADS) sind nicht „selbststeuernd“. Vielmehr arbeiten ADS auf der Grundlage von Algorithmen und gehorchen den Befehlen der Nutzer.

Um ein einheitliches Verständnis der verschiedenen Autonomie- beziehungsweise Automatisierungsgrade zu erzielen, wurde die Norm J3016 von der SAE geschaffen. Die „Society of Automotive Engineers“ (SAE) ist ein Berufs- und Fachverband, der 1905 in den USA gegründet wurde. Sie ist eine weltweite Vereinigung von mehr als 128 000 Ingenieuren bestehend aus Experten aus der Luft- und Raumfahrt und der Automobil- und Nutzfahrzeugindustrie. Die SAE International ist einer der führenden Verbände für Mobilitätstechnologien, welche Standards entwickelt, Materialspezifikationen erstellet und regelmäßig technische Berichte veröffentlicht.

Die Norm SAE J3016 klassifiziert den Automatisierungsgrad in 6 Automatisierungsstufen. In den SAE Stufen 0 bis 2 überwacht der Fahrer den Fahrbereich, in den SAE Stufen 3-5 überwacht das System den Fahrbereich.

In der SAE Stufe 0 ist der Fahrer vollständig für die Steuerung des Fahrzeugs verantwortlich und führt sämtliche relevanten Aufgaben wie Beschleunigen, Bremsen und Lenken selbst durch. Bezüglich Assistenzsysteme können Fahrzeuge mit gewissen Extras wie eine Rückfahrkamera oder einem Toter-Winkel-Warner ausgestattet sein. Diese Systeme werden als Stufe 0 eingestuft, da sie keine relevanten Aufgaben übernehmen.

In der SAE Stufe 1 beherrscht der Fahrer weiterhin das Fahrzeug. Jedoch greifen hier die ersten automatisierten Systeme aktiv ein, die in gewissen Situationen die Kontrolle des Fahrzeugs teilweise übernehmen. Dabei wird nicht die komplette Fahrzeugführung übernommen. Zum Beispiel steuert ein Abstandstempomat (engl. Adaptive Cruise control, ACC) nach Aktivierung lediglich die Beschleunigung und das Bremsen des Fahrzeugs. In der Regel wird diese Funktion bei einer Autobahnfahrt genutzt. Der Fahrer kann die Füße von den Pedalen nehmen, muss jedoch stets die Lenkbewegungen ausführen und als Rückfallebene in der Lage sein, bei Fehlern die Kontrolle zu übernehmen.

In der SAE Stufe 2, kann das Fahrzeug einige Aufgaben zeitweilig vollständig selbst ausführen. Zum Beispiel wäre ein solches Fahrzeug in der Lage, gleichzeitig die Spur und die Geschwindigkeit zu halten. Dazu werden zwei Einzelsysteme miteinander kombiniert: das sogenannte „Lane Keeping Assistant System“ (LKAS) und das ACC. Selbst das automatische Einparken, ohne dass der Fahrer in das Lenkrad greifen

muss, ist eine SAE Stufe 2 Funktion. Wenn das Fahrzeug die erwähnte Fahrsituation ausführt, darf der Fahrer ebenfalls für einen kurzen Zeitraum die Hände vom Lenkrad nehmen. Der Fahrer muss die Assistenzsysteme jedoch stets überwachen und muss in der Lage sein im Fehlerfall einzugreifen.
In der SAE Stufe 3 kann das Fahrzeug bestimmte Fahrfunktionen für einen begrenzten Zeitraum ohne Überwachung des Fahrers selbst übernehmen. Beispielsweise kann das Fahrzeug im Zusammenspiel von ACC und LKAS zusätzlich andere Fahrzeuge überholen, wenn die Fahrsituation dies erfordert. Das System übernimmt nun erstmalig die Aufgabe der vollständigen Umgebungsbeobachtung. Obwohl dem Fahrer theoretisch ermöglicht wird während der eingeschalteten Automatisierungsstufe eine Zeitung zu lesen, ist er stets in der Verantwortung bei Problemen das Steuer übernehmen zu können. Diese Übernahme kann von dem Fahrzeug mit einer Vorwarnzeit mittels einer akustischen und visuellen Meldung angefordert werden. Diese Stufe wird daher ebenso als „Einstieg“ in das autonome Fahren bezeichnet.
In der SAE Stufe 4 ist das autonome Fahrsystem des Fahrzeugs vollständig in der Lage sämtliche Fahrfunktionen, die innerhalb seines Betriebsbereiches (engl. „Operational Design Domain“, ODD) definiert sind, zu übernehmen. Einige Beispiele für ODD Parameter sind:

- Geschwindigkeit
- Umgebung (Stadtverkehr, Landstraße, Autobahn)
- Umweltbedingungen wie Wetter oder Tageszeit
- Verkehr

Somit existieren gewissen Betriebsbereiche, welche die menschliche Kontrolle erfordern. Das Fahrzeug erkennt, ob es in einer bestimmten Situation an seine Betriebsgrenzen stößt und warnt rechtzeitig den aktuell inaktiven Fahrer. Falls der Fahrer nicht die Kontrolle über das Fahrzeug übernimmt, wird das Fahrzeug vom System in den sicheren Zustand gebracht. Die notwendige Vorwarnzeit ist aktuell noch in keiner Norm oder Standard festgelegt und wird daher unterschiedlich ausgelegt. Angaben von einer halben Minute bis zu einigen Minuten sind aktuelle Diskussionen in der Fachwelt.
In der SAE Stufe 5 (Vollautomatisierung / Autonomes Fahren), werden schließlich sämtliche Funktionen durch das Fahrzeug/ System übernommen, sodass kein Fahrer notwendig ist. Das Fahrzeug fährt und meistert sämtliche Situationen autark. In dieser Stufe gibt es keinen Fahrer mehr, sondern lediglich noch „Passagiere“. Die SAE J3016 definiert einen unbegrenzten Betriebsbereich, sodass selbst Fahrten ganz ohne Insassen möglich sind. [19]

3.2 Rechtliche Anforderungen

Am 21. Juni 2017 sind in Deutschland zum ersten Mal Regeln zum automatisierten Fahren in Kraft getreten. Es ging hierbei um veränderte Rechte und Pflichten des Fahrzeugführers während der automatisierten Fahrphase. Seitdem darf ein Fahrzeug unter bestimmten Voraussetzungen in einem SAE Level 3 Modus unterwegs sein. Der nächste Schritt erfolgte 2021, als der Bundestag am 20.05.2021 ein neues Gesetz beschlossen hat, welches am 28. Juli 2021 in Kraft getreten ist [20]. Dieses Gesetz erlaubt nun Kraftfahrzeuge, welche auf bestimmten, festgelegten Strecken in einem SAE Level 4 unterwegs sind. Abgesehen von

privaten Zwecken, bietet dies nun unter anderem einige andere mögliche Einsatzszenarien. Es können zum Beispiel Shuttle-Verkehre noch weiter automatisiert werden oder auch Busse, die auf festgelegten Routen unterwegs sind.

Im Koalitionsvertrag von 2021 wurde als Ziel festgesetzt, dass bis zum Ende der Legislaturperiode die rechtlichen Voraussetzungen für vollautonome Fahrzeuge auf geeigneten Infrastrukturen geschaffen werden. Im Februar 2022 hat das Bundeskabinett einen weiteren großen Schritt zum autonomen Fahren beschlossen. Wie das Verkehrsministerium in Berlin mitteilte, ist ein Kern der Rechtsverordnung eine Regelung, wie genau die Zulassung von Kraftfahrzeugen mit autonomer Fahrfunktion zum Straßenverkehr durch das Kraftfahrt-Bundesamt aussieht. Der Bundesrat muss der Verordnung noch zustimmen.

Konkret geht es bei der Verordnung um die SAE Stufe 4, bei der das Fahrzeug vollautomatisiert in seinen festgelegten Betriebsgrenzen fahren kann [21]. Die Bundesregierung hat das Gesetz zum autonomen Fahren um eine weitere Verordnung ergänzt, die eine Art Gesamtprüfung für das Fahrzeug regelt. Der Hersteller muss laut der „Verordnung zur Regelung des Betriebs von Kraftfahrzeugen mit automatisierter und autonomer Fahrfunktion und zur Änderung straßenverkehrsrechtlicher Vorschriften“, ein Sicherheitskonzept vorlegen, welche die verwendete Informationstechnik einschließt.

Zudem müssen Funktionen des Fahrzeugs beschrieben werden und ein Katalog mit Testszenarien erstellt werden. Des Weiteren enthält die Verordnung eine Liste von Daten, die nichtflüchtig gespeichert werden müssen wie die Fahrzeugidentifizierungsnummer, Positionsdaten, Systemüberwachungsdaten, Geschwindigkeit und mit externen Stellen ausgetauschten Daten. Daten- und Informationssicherheit spielen dabei eine große Rolle.

Daher müssen die Anforderungen der EU-Verordnung 2016/679 zum Schutz personenbezogener Daten und zum freien Datenverkehr (DSGVO) eingehalten werden [23]. Die Original Equipment Manufacturer (OEM) müssen zudem mit einer Gefährdungsanalyse darstellen und aufzeigen, wie die technische Ausrüstung in möglichen Betriebssituationen im Fehlerfall reagiert und welchen Einfluss diese Reaktionen auf die Sicherheit und Kontrollierbarkeit des Fahrzeugs haben. Zusätzlich kommen weitgehende Prüfpflichten auf den Halter zu. So muss vor jeder Fahrt eine Abfahrkontrolle durchgeführt werden, bei der unter anderem die Brems-, Lenk- und Lichtanlagen sowie das Fahrwerk und elektronisch geregelte Fahrzeugsysteme überprüft werden.

Zusätzlich muss der Halter nach dem Gesetz alle 90 Tage von „geeigneten Betrieben/ Personen“ eine Prüfung nach den Vorgaben des Betriebshandbuchs vornehmen lassen [22]. Zudem müssen die Halter nachweisen können, dass die autonome Fahrfunktion zu jedem Zeitpunkt deaktiviert werden kann.

Diese Entwicklung verdeutlicht, dass in Zukunft noch deutlich höhere Anforderungen an die Sicherheit der Fahrzeugsysteme sowie an die Zuverlässigkeit der Fahrfunktionen gestellt werden. Um diese Anforderungen zu erfüllen, wurden zwei Normen geschaffen, die die notwendige Qualität der Entwicklung und der Systeme sicherstellen sollen: Die ISO 26262, die sich um die funktionale Sicherheit der Fahrzeugsysteme kümmert und die ISO 21448, die die Zuverlässigkeit und Sicherheit der implementierten Funktionalität garantieren soll.

4 Normative Vorgaben

4.1 Die grundlegende Struktur der ISO 26262

Die ISO 26262 ist eine ISO-Norm für elektrische/ elektronische / programmierbar-elektronische Systeme in Kraftfahrzeugen. Sie soll die Sicherheit der Funktion von elektrischen/ elektronischen Komponenten im Kraftfahrzeug gewährleisten. Nicht im Fokus der ISO 26262 sind mögliche Gefährdungen durch mechanische Komponenten sowie nicht-funktionale Gefährdungen wie zum Beispiel Feuer, Rauch, Hitze und Strahlung, sofern diese nicht unmittelbar durch Fehlfunktionen des E/ E-Systems ausgelöst werden. Die ISO 26262 ist eine Anpassung der IEC 61508 an die spezifischen Gegebenheiten im Automobilbereich. Die IEC 61508 ist die domänenübergreifende Grundnorm für die funktionale Sicherheit. Sie wurde im Jahre 1998 eingeführt und im Jahr 2010 erfolgte die Einführung einer neuen Version, die zum jetzigen Zeitpunkt die aktuelle Version repräsentiert.

Allerdings zeigten sich Schwächen bei der Anwendung der IEC 61508 in der Automobilbranche: Zum einen geht die IEC 61508 von einem geschulten Bediener und nicht ausschließlich von einem Anwender wie dem Fahrer eines PKWs aus. Zum anderen gibt es im Gegensatz zu zum Beispiel chemischen Anlagen keine katastrophalen Ereignisse, die durch Fahrzeugsysteme ausgelöst werden können und ganze Landstriche verwüsten. Dafür macht es Sinn, feinere Abgrenzungen zwischen den einzelnen Risikostufen vornehmen zu können.

Um diese Schwächen zu beseitigen, wurde die ISO 26262 im April 2011 als 9-teilige Norm veröffentlicht, wobei ein zehnter Teil nachträglich im November 2011 in Kraft gesetzt wurde. Seit Dezember 2018 ist die „2nd Edition“ verfügbar, welche zwei zusätzliche Teile beinhaltet. Die zunehmende Komplexität in der Automobilindustrie bringt die verstärkte Bemühung mit sich, sicherheitskonforme Systeme zu entwickeln und bereitzustellen. Die Implementierung der ISO 26262 hat somit die Nutzung eines gemeinsamen Standards zur Gewährleistung der Sicherheit eines Systems ermöglicht.

Dazu hat die ISO 26262 eine Risikobewertung in Form eines ASIL (Automotive Safety Integrity Level) in den Stufen QM, A, B, C und D eingeführt, wobei der ASIL QM dem niedrigsten und der ASIL D dem höchsten Risiko entspricht. Die Risikobewertung basiert dabei auf der Schwere der Fehlerfolge (Severity „S“), der Häufigkeit oder Dauer der Fahrsituation in der die Fehlfunktion zu einer Gefährdung führt (Exposure „E“), sowie der Kontrollierbarkeit der Fehlfunktion durch den Fahrer oder andere Verkehrsteilnehmer (Controllability „C“).

Des Weiteren wurde Wert auf einen sehr prozessorientierten Sicherheitsstandard gelegt, da die Automobilindustrie sehr prozessorientiert getrieben ist. In der Abbildung 8 wird das sogenannte „V-Modell“ dargestellt, welches ein Vorgehensmodell ist und ursprünglich für die Softwareentwicklung konzipiert wurde. Wenn man mit dem Stand der Technik gleich auf sein möchte, empfiehlt es sich sehr nach dem V-Modell zu arbeiten. Das V-Modell definiert jede Entwicklungsphase in einem Entwicklungsprojekt und gibt ebenso an, worauf es in den einzelnen Phasen ankommt.

Die linke Seite beginnt mit einer funktionalen fachlichen Spezifikation, welche dann in der Tiefe immer detaillierter zu einer technischen Spezifikation und Implementierungsgrundlage ausgebaut wird. Unten an der Spitze des V-Modells erfolgt die Implementierung, welche dann auf der rechten Seite gegen die einzelnen Spezifikationen der linken Seite getestet wird.

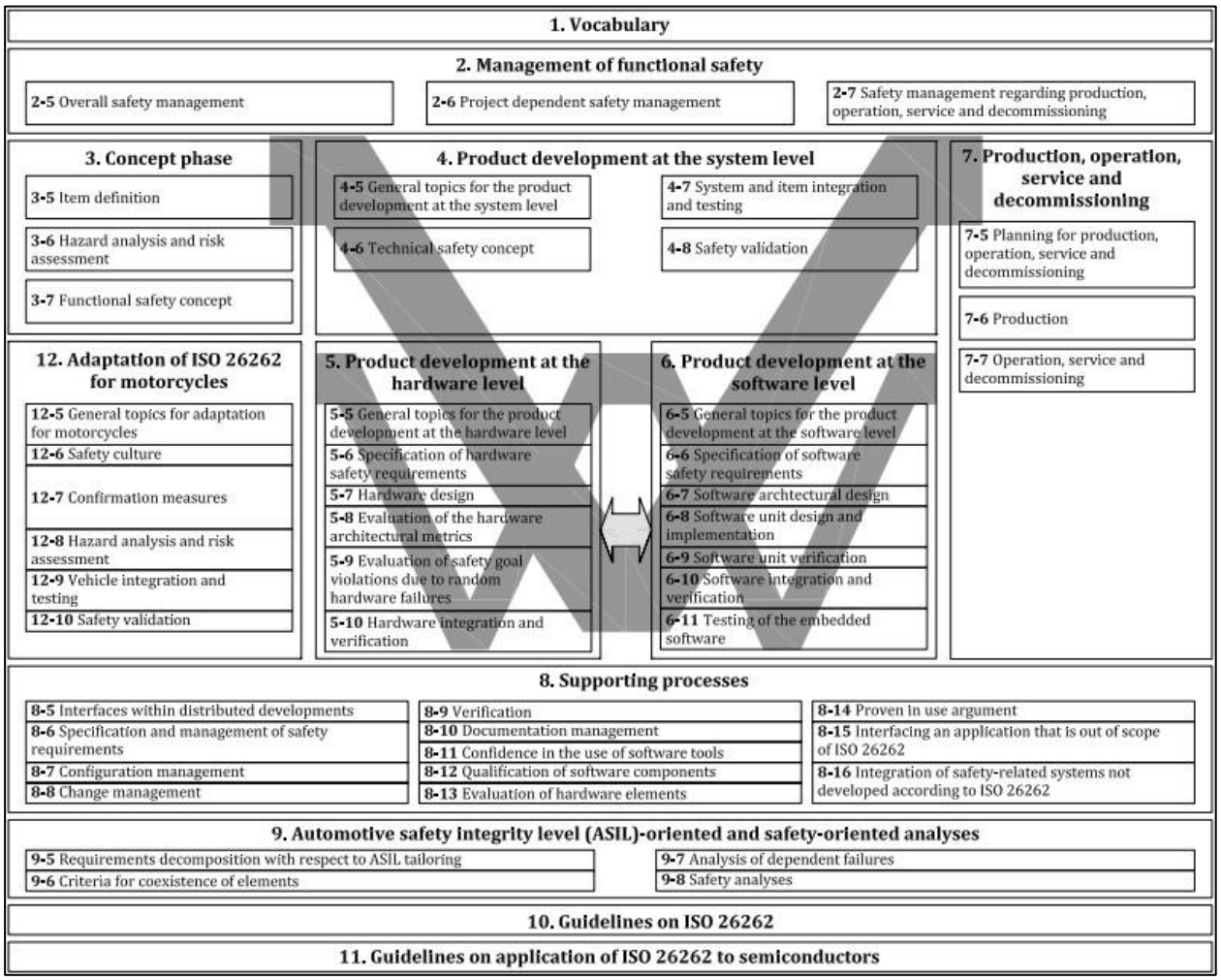


Abbildung 8: V-Modell nach ISO 26262 [25]

Die einzelnen Teile der ISO orientieren sich dabei an den Phasen des V-Modells. Der Teil 1 umfasst das Vokabular für sicherheitsrelevante Systeme, die in serienmäßigen Straßenfahrzeugen mit E/ E-Architekturen eingebaut werden. Durch die Definition der Begriffe und des Vokabulars, die bei der Entwicklung sicherheitsrelevanter E/ E-Systeme verwendet werden, stellt dieser Abschnitt den Rahmen für die erfolgreiche Umsetzung der funktionalen Sicherheit.

Der Teil 2 beschreibt die Methodik und die Anforderung an das Management der funktionalen Sicherheit. Zudem werden projektspezifische Informationen zu den Managementaktivitäten in den verschiedenen Phasen des Produktlebenszyklus beschrieben. Ebenso werden die Absicherungsmaßnahmen zum Nachweis der Normkonformität thematisiert.

Der dritte Teil der ISO 26262 beschreibt die frühen Phasen der Entwicklung und definiert diverse Prozesse, die notwendig sind, um die funktionale Sicherheit bereits in der Konzeptphase einer Entwicklung zu

gewährleisten. Dazu gehört die Durchführung einer Gefährdungsanalyse und Risikoabschätzung, in der die Gefährdungen mit dem Sicherheitsintegritätslevel klassifiziert werden.

Der Teil 4 behandelt eine Reihe von Themen zur Produktentwicklung auf Systemebene. Arbeitsergebnisse sind sämtliche Dokumente bezüglich der Produktentwicklung auf Systemebene, die Spezifikationen für die technische Sicherheit, das technische Sicherheitskonzept, den Entwurf der Systemarchitektur, die Integration und Prüfung von Elementen sowie die Sicherheitsvalidierung.

Der Teil 5 der ISO 26262 befasst sich mit der Produktentwicklung auf Hardware-Ebene. Themen wie die Hardwarespezifikation, Hardwaresicherheit, Hardwaredesign und die Bewertung der zufälligen Hardwareausfälle stehen im Vordergrund. Dazu gehört ebenfalls die Bewertung der Metriken zum Thema zufällige Fehler, Latente Fehler und dem diagnostischen Deckungsgrad.

Der Teil 6 definiert die funktionale Sicherheit auf Softwareebene während der Produktentwicklung und behandelt allgemeine Themen wie die Spezifikationen für die Softwaresicherheit, das Softwarearchitekturdesign, Softwarekomponentendesign und -implementierung, Softwarekomponentenverifizierung, Softwareintegration und -verifizierung sowie das Testen eingebetteter Software.

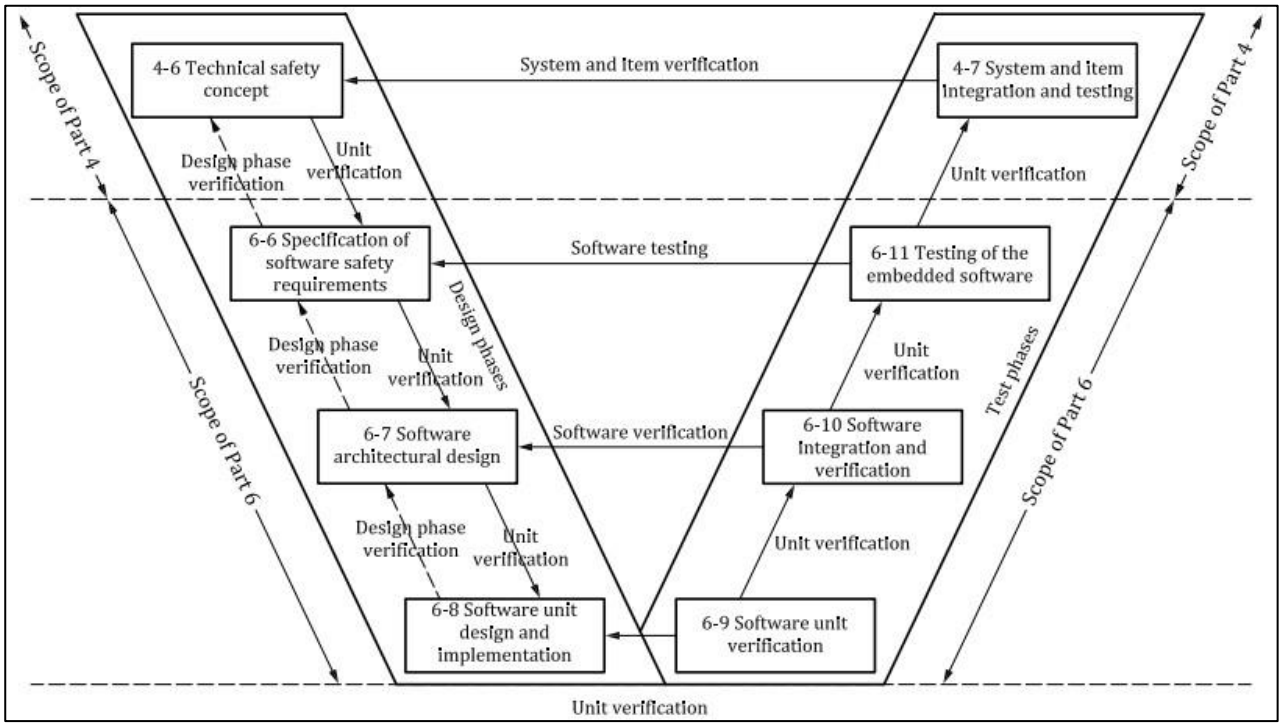


Abbildung 9: V-Modell der Softwareentwicklung nach ISO 26262 [25]

Die Abbildung 9 beschreibt die Softwareentwicklung gemäß der ISO 26262. In dem Automobilsektor gibt es häufig zusätzlich Applikationsphasen, die in diesem Modell nicht mit aufgeführt sind. Im normativen Anhang der ISO 26262 befinden sich Anforderungen an die Applikation, welche den Umgang mit konfigurierbarer Software beschreiben.

Der Teil 7 enthält grundlegende Verfahren zur Erstellung von Produktions- und Installationsplänen für sicherheitsrelevante Systeme, um die Anforderungen an die funktionale Sicherheit beim Produktions- und

Installationsprozess sicherzustellen, sowie die Anforderungen, die den Betrieb, die Wartung, die Reparatur und die Stilllegung unter der Einhaltung sämtlicher Sicherheitsaspekte gewährleisten sollen.
Der Teil 8 der Norm spezifiziert verschiedene unterstützende Prozesse für die funktionale Sicherheit bei der Entwicklung von sicherheitsrelevanten E/ E-Systemen. Diese Prozesse umfassen:

- Schnittstellen innerhalb verteilter Entwicklungen
- Sicherheitsmanagement
- Konfigurationsmanagement
- Änderungsmanagement/ Verifikation
- Verwaltung der Dokumentation
- Vertrauensniveau bei der Verwendung von Software-Tools
- Qualifizierung von Softwarekomponenten
- Bewertung von Hardware-Elementen
- Nachweis der Betriebsbewährtheit (Proven in use)
- Einbindung einer Anwendung, die nicht in den Geltungsbereich der ISO 26262 fällt
- Integration von sicherheitsrelevanten Systemen, die nicht nach der ISO 26262 entwickelt wurden

Der Teil 9 beschreibt spezielle sicherheitsorientierte Methoden. Zum einen die ASIL-Dekomposition oder Kriterien zur Koexistenz von Elementen unterschiedlicher ASIL-Einstufungen in einem System sowie Anforderungen an Sicherheitsanalysen.
Der Teil 10 bietet einen Überblick über die ISO 26262. Es soll somit das Verständnis der anderen Teile erleichtert werden. Unter anderem wird das Konzept des „Safety Element out of Context (SEooC)“ ausführlich beschrieben.
Der Teil 11 charakterisiert einen informativen und nicht normativen Teil der ISO 26262 und enthält detaillierte Informationen zur Unterstützung von Halbleiterherstellern. Darüber hinaus werden die Stärken und Schwächen der verschiedenen Zuverlässigkeitsstandards (SN 29500, IEC TR 62380 und FIDES) in Bezug auf die Ausfallraten von Bauteilen bewertet. Ferner werden ebenfalls Überlegungen zum Gehäuse und der Pinbelegung behandelt. Zudem sind detailliertere Definitionen von transienten Fehlern als in der ursprünglichen Version der ISO 26262 enthalten. Damit existiert nun ein großer Umfang an dokumentierten Überlegungen zu transienten Fehlern verursacht durch α-, β-, Neutronen- oder γ-Strahlungsquellen.
Während die ISO 26262 ursprünglich für Personenkraftwagen bis 3.5 Tonnen Gesamtgewicht gedacht war, wurde der Anwendungsbereich mit der zweiten Edition ebenso auf Nutzkraftfahrzeuge und Motorräder erweitert Dazu thematisiert Teil 12 speziell die notwendigen Anpassungen an Motorräder. Zu diesem Zweck werden allgemeine Themen zur Anpassung von Motorrädern, Sicherheitskultur, Bestätigungsmaßnahmen, Gefahrenanalyse und Risikobewertung, Fahrzeugintegration und -prüfung sowie die Sicherheitsvalidierung behandelt.

Obwohl die ISO 26262 mit der Veröffentlichung und späteren Überarbeitung mit der 2nd Edition einen bis dato erstmals für die Automobilbranche angepassten Standard herausgebracht hat, gibt es Kritik. Die ISO 26262 hat bedeutende Fortschritte bei der Bewältigung des sich rasch verändernden E/ E-Umfelds und der Auswirkungen auf die funktionale Sicherheit erzielt. Jedoch sind die Regulierungsbehörden der Ansicht, dass mehrere neu aufkommende Technologien in der Überarbeitung noch nicht angemessen berücksichtigt wurden. Während die ISO 26262 den Standard für die Funktionale Sicherheit setzt, indem sie versucht, Fehlfunktionen elektrischer/ elektronischer Systeme zu eliminieren, hängt die Sicherheit von automatisiert fahrenden Systemen nicht ausschließlich mit E/ E-Fehlern zusammen. Ebenso Faktoren wie die denkbaren Missbräuche der Funktionen durch den Fahrer, den Leistungsgrenzen von Sensoren und Systemen oder auch unvorhergesehene Veränderungen in der Fahrzeugumgebung müssen berücksichtigt werden. Daher haben Regulierungsbehörden, Sicherheitslobbyisten und ganz besonders die Industrie im Allgemeinen Überlegungen durchgeführt, um diese Lücken mit einem neuen Standard zu füllen. Dieser Standard ist nun als ISO 21448 veröffentlicht und wird im nachfolgenden untersucht. [24, 25]

4.2 Die grundlegende Struktur der ISO 21448 (SOTIF)

Die ISO 21448 - ursprünglich als Erweiterung der ISO 26262:18 vorgesehen, wurde aufgrund ihrer komplexen Struktur nicht zusammen mit der 2nd Edition der ISO 26262 veröffentlich. Der Veröffentlichungsdatum hätte sich stark verschoben, daher wurde SOTIF als eigenständiger Standard veröffentlicht. Der SOTIF Standard zielt darauf ab, folgende Sicherheitsrisiken zu reduzieren:

- Das Restrisiko der beabsichtigten Sollfunktion
- Das unbeabsichtigte Verhalten bei bekannten Situationen
- Unbekannte Situationen, die zu unbeabsichtigtem Verhalten führen können

Während die ISO 26262 Konzepte, Maßnahmen und Verfahren für Fehler vorgibt, die zum Ausfall des technischen Systems führen, definiert SOTIF Vorgehensweisen für Fehler, welche sich aus der Limitierung der definierten Funktionalität ergeben. Im Kern steht die Frage, wie eine Sollfunktion zu spezifizieren, zu entwickeln, zu verifizieren und zu validieren ist. Gerade im Hinblick auf das autonome Fahren, kommen neue komplexe Funktionen wie „Advanced Driver Assistance Systems“ (ADAS) ins Spiel. Hier soll die ISO 21448 helfen Risiken zu vermeiden, die sich zum Beispiel aus technologischen Grenzen eines verwendeten Aktors oder Sensors ergeben oder die auf Grund von Umweltbedingungen entstehen.
Die Entwicklung nach der ISO 26262 steht nach wie vor für bestehende Systeme wie ein Airbag zur Verfügung. Die Wahrscheinlichkeit einer Aktivierung des Airbags während der Fahrt oder ein kompletter Ausfall kann durch die funktionale Sicherheit mittels Verringerung des Risikos durch gewisse Maßnahmen abgesichert werden. Jedoch besteht ein Risiko nicht ausschließlich durch einen Systemausfall. Moderne ADAS Systeme können ebenfalls Sicherheitsrisiken darstellen, trotz voller Systemfunktionalität.
Verglichen mit der ISO 26262 werden in dem SOTIF Standard keine grundlegenden neuen Methoden angewandt. Der wesentliche Unterschied liegt darin, dass in der ISO 21448 die eigentlich beabsichtigte

Funktionalität im Mittelpunkt steht. In der ISO 26262 hingegen stehen die zufälligen und systematischen Fehler, demnach Abweichungen von der definierten Funktion im Mittelpunkt.
In der Abbildung 11 ist die grundlegende Struktur des SOTIF-Prozesses zu sehen. Im Vergleich zu der ISO 26262 definiert die ISO 21448 keinen besonderen Entwicklungs- oder Engineering Prozess. Nach erfolgter SOTIF Analyse werden die Anforderungen jedoch an die Konzeptphase der ISO 26262 übergeben.
Trotz Anwendung der ISO 26262 und die Sicherstellung der Vermeidung von Funktionsausfällen, kann es im Straßenverkehr vier mögliche Ereignisräume von Systemzuständen geben. Diese wären:

- Bereich bekannter und sicherer Systemzustände
- Bereich bekannter und unsicherer Systemzustände
- Bereich unbekannter und unsicherer Systemzustände
- Bereich unbekannter und sicherer Systemzustände

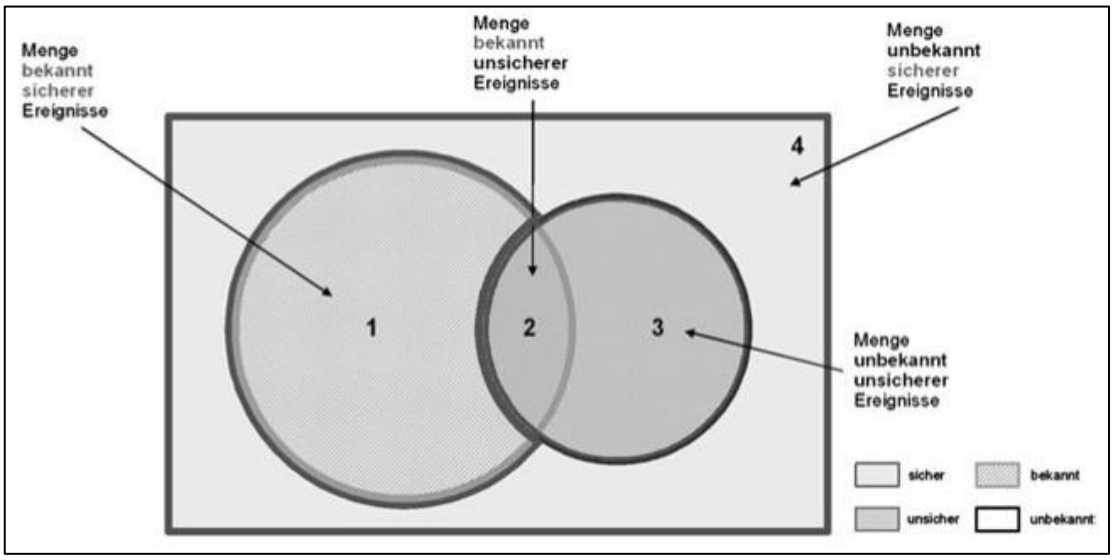


Abbildung 10: Mengendarstellung von sicheren und unsicheren Ereignissen [26]

Die ISO 21448 hat das Ziel, einen möglichst strukturierten Entwurfsprozess für die Vermeidung von Sicherheitsverletzungen durch eine fehlerbehaftete Sollfunktion zu definieren. Daher liegt der Fokus auf dem Bereich 3 (unbekannte und unsichere Ereignisse) der Abbildung 10. Nach Anwendung der Methoden, welche die Menge unbekannter und unsicherer Ereignisse reduzieren, können Maßnahmen zur Gefährdungsbeherrschung ergriffen werden. Diese Maßnahmen reduzieren die Menge an bekannten unsicheren Ereignissen und tragen somit dazu bei, das System sicherer zu gestalten.
Das Ziel von SOTIF ist eine verbesserte Erkenntnis über das mögliche Systemverhalten ebenso bei bislang unbekannten Anwendungsszenarien zu erlangen. Die ISO 21448 hat keinen eigenständigen Entwicklungsprozess definiert, der Schwerpunkt von SOTIF liegt daher auf der Konzeptphase. [26, S. 9–10]

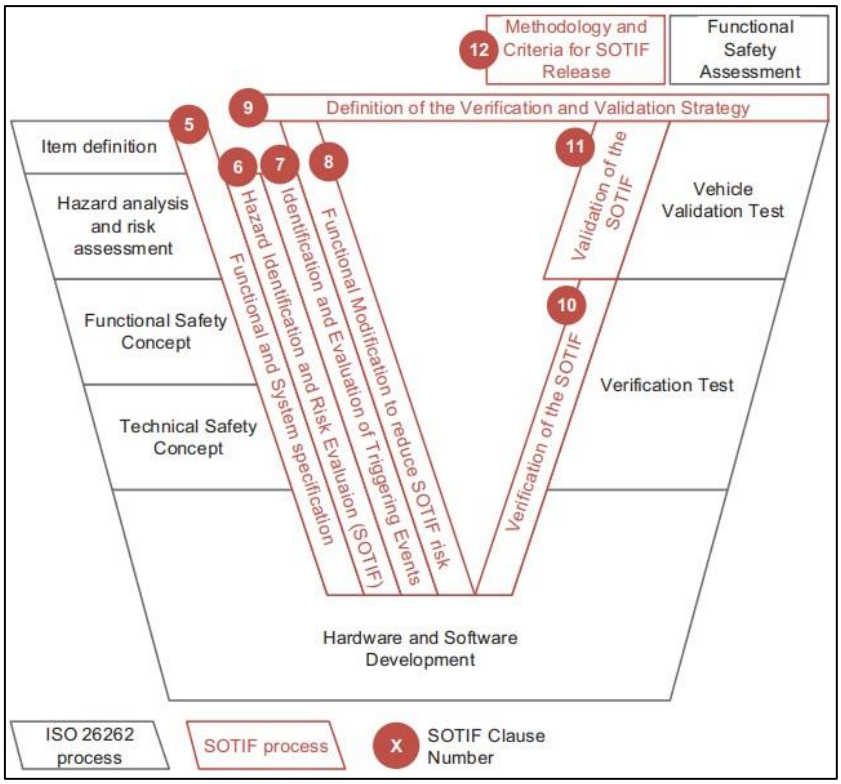


Abbildung 11: SOTIF Vorgehensweise während der ISO 26262 [26]

Die SOTIF-Konzeptphase beginnt mit der Erstellung der Funktions- und Systemspezifikation. Bei jeder Entwicklung von Automatisierungsfunktionen für Kraftfahrzeuge ist die Erstellung der Funktions- und Systemspezifikation der Ausgangspunkt. Die Beschreibung der Ziele der beabsichtigten Funktionen sowie die Abhängigkeiten der Funktionen zu anderen Fahrzeugfunktionen und -systemen und relevante Umweltbedingungen sind Kern dieses Dokuments.

Der nächste Punkt (Clause 6) behandelt die Identifikation von SOTIF Risiken. Daran schließt sich eine systematische Identifikation der aus dem Fehlverhalten der betrachteten Funktion resultierenden Gefährdungen an. Hier wird in dem Standard eine ähnliche Herangehensweise wie bei der HARA und HAZOP Analyse vorgesehen. Risiken oder potenzielle Gefährdungen werden mittels Leitworte für bestimmte Aktionen ermittelt. Wie bei der ISO 26262 kann hier ebenso eine Bewertung der erkannten Gefährdungen nach Exposure (E), Severity (S) und Controllability (C) vorgenommen werden. Der wesentliche Unterschied ist jedoch, dass für die Klassifizierung gefährlicher Ereignisse ebenso eine verzögerte oder ausbleibende Reaktion des Fahrers zur Kontrolle des kritischen Fahrmanövers in Betracht gezogen wird.

Bei dem Paragraf 7 handelt es sich um die Identifikation und Bewertung gefährlicher Anwendungsfälle. Die Identifikation möglicher Systemschwächen steht hier im Mittelpunkt. Durch diese Systemschwächen, die durch bestimmte Ereignisse ausgelöst werden, kann ein nicht beabsichtigtes Systemverhalten zu Stande kommen. Auslösende Ereignisse können zum Beispiel nicht passende Sensoren oder Aktoren sein. In der ISO 21448 wird ebenfalls der Mensch als auslösendes Ereignis betrachtet. Systemschwächen könnten zum Beispiel durch einen Fehlgebrauch der Systeme ausgelöst werden. Daher ist ebenso die Mensch-Maschine-Interaktion ein wichtiger Bestandteil der ISO 21448.

In dem Paragraf 8 werden Maßnahmen zur Reduktion des SOTIF Risikos identifiziert. Diese umfassen zum Beispiel Systemverbesserungen der Sensoren und Aktoren.
In dem 9. Paragraf wird die Planung der Verifikation und Validation thematisiert. Die Verifikation adressiert den Test, der auf die Beherrschung bekannter und unsicherer Ereignisse abzielt. Die Validierung hingegen adressiert den Nachweis einer Robustheit des Systems gegen unbekannte und unsichere Ereignisse. Hierbei muss ebenso ein Validierungsziel bestimmt werden.
Paragraf 10 definiert daraufhin, dass das System mit seinen Komponenten verifiziert werden muss. Das Ziel ist es, zu zeigen, dass sich bei bekannten und unsicheren Szenarien erwartungsgemäße Verhaltungsweisen zeigen. Zudem müssen diese von den durchgeführten Tests ausreichend abgedeckt werden. Ein weiterer Punkt bei der Validierung ist die System- und Komponenten-Validierung. Es soll gezeigt werden, dass diese in realen Testfällen kein unangemessenes Risiko verursachen. Dabei dienen empirisch ermittelte Unfallzahlen aktueller Fahrzeugsysteme als Grundlage für geeignete kumulierte Testlängen. Es wird eine repräsentative und realistische Verteilung der kumulierten Testlängen auf verschiedene Testszenarien wie zum Beispiel Fahrten auf der Autobahn, Fahrten bei Dunkelheit oder Fahrten bei Regen bestimmt. [26]
Abschließend muss die SOTIF Freigabe erfolgen, für die zu zeigen ist, dass eine ausreichende Verifikation und Validation durchgeführt wurde und mögliche Restrisiken akzeptiert werden können. Nach der Freigabe werden Felddaten während des Betriebs der Systeme strukturiert erfasst. Auf deren Grundlage muss jede Abweichung vom vorgegebenen Sollverhalten identifiziert, offengelegt und bewertet werden. Falls notwendig, müssen kurzfristig Korrekturen an Fahrzeugen im Feld durchgeführt werden. [27]

5 Analysen

5.1 Gefährdungsanalyse nach ISO 26262 (HARA)

Die HARA, Hazard Analysis and Risk Assessment oder im Deutschen Gefahren- und Risikoanalyse ist einer der wichtigsten Analysen in einem Entwicklungsprojekt. Die HARA wird ganz am Anfang einer Entwicklung durchgeführt und liefert als Ergebnis die ASIL-Bewertungen sämtlicher Fehlfunktionen und die Sicherheitsziele für jedes gefährliche Ereignis mit einem ASIL. Auf diesen Sicherheitszielen mit dazu gehörendem ASIL stützt sich ein großer Teil der funktionalen Entwicklung. Das jeweilige System wird auf seine potenziell gefährlichen Ausfälle und Ereignisse untersucht und bewertet. Die Definition der konkreten Sicherheitsziele ist für jedes System unterschiedlich, sie ergeben sich aus dem Zusammenspiel der einzelnen Funktionen, Fehlfunktionen und Bewertungen. Die gesamte HARA basiert rein auf dem funktionalen Verhalten des Systems, dabei ist kein genauer bzw. detaillierter Entwurf des Systems notwendig. Sie ist daher Teil der Konzeptphase der Entwicklung.

In der HARA wird die Kritikalität von Fehlfunktionen mit Hilfe dreier Einstufungen (Schadensschwere, im Englischen „Severity“, Eintretenswahrscheinlichkeit, im Englischen „Exposure“ und Kontrollierbarkeit, im Englischen „Controllability“) bestimmt:

1. Severity (S): Wenn die Fehlfunktion in der angenommenen Situation auftritt und nicht beherrscht werden kann, wie groß ist dann die Schwere der Auswirkung.
2. Exposure (E): Wie häufig sind Situationen, in denen die Fehlfunktion relevant ist.
3. Controllability (C): Wenn die Fehlfunktion in der angenommenen Situation auftritt, wie gut kann sie dann beherrscht werden.

Aus diesen 3 Parametern ergibt sich der ASIL auf einer Skala A bis D (bzw. QM für Fehlfunktionen mit so geringer Kritikalität, dass die üblichen Qualitäts-Management Vorgaben zur Entwicklung ausreichen), wobei der ASIL A die niedrigste und der ASIL D die höchste Einstufung darstellt. Diese Einstufungen entscheiden darüber, welche Anforderungen an die Entwicklungen gestellt werden.

Die Abbildung 12, Abbildung 13 und Abbildung 14 zeigen die jeweiligen Beschreibungen der einzelnen Parameter, die für die Bestimmung der Severity, Exposure und Controllability verwendet werden. Die Abbildung 15 zeigt den Risikograph aus der ISO 26262 für die ASIL Bestimmung der jeweiligen Funktion.

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

Abbildung 12: Severity Bewertung nach ISO 26262

	Class				
	E0	**E1**	**E2**	**E3**	**E4**
Description	Incredible	Very low probability	Low probability	Medium probability	High probability

Abbildung 13: Exposure Bewertung nach ISO 26262

	Class			
	C0	**C1**	**C2**	**C3**
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

Abbildung 14: Controllability Bewertung nach ISO 26262

Severity class	Exposure class	Controllability class		
		C1	**C2**	**C3**
S1	**E1**	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	**E1**	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	**E1**	QM	QM	A[a]
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Abbildung 15: ASIL Risikograph nach ISO 26262

Die ASIL-Parameter sollten dabei von einem Team von Experten bestimmt werden, um ein möglichst umfangreiches Wissensgebiet einzuschließen. Jede Einstufung, die nicht dem Maximum entspricht, muss dabei auf einer dokumentierten Begründung beruhen.

Die nachfolgende HARA soll schematisch darstellen, welche potenziellen Risiken und Gefährdungen man bei der Entwicklung eines elektrischen Lenksystems zu erwarten hat. Im Folgenden wurde eine grundlegende Hauptfunktion einer Servolenkung, die „Lenkunterstützung“ im (engl. steering assist), untersucht. Die Hauptfunktionen eines Systems ergeben sich aus der Systembeschreibung, im Englischen „Item Definition“, welche auch in dem V-Modell der ISO 26262 unter der Konzeptphase als erstes aufgelistet ist und somit einen elementaren Baustein für die weiteren Schritte liefert. Da im Folgenden lediglich eine grundlegende und allgemeine Funktion des Lenksystem mit einer Begrenzung auf vier operative Zustände für die beispielhafte Darstellung einer HARA verwendet wird, wurde von einer Durchführung der Item Definition in dieser Arbeit abgesehen.

Eine Hauptfunktionsliste einer elektrisch betriebenen Lenkung könnte jedoch folgendermaßen aussehen:

1. Steering Assist: die Basis-Unterstützungsfunktion
2. Active Return: eine Unterstützung beim Zurücklenken in die Geradeaus-Stellung

3. Active End Stop Feedback: Begrenzung des maximalen Lenkwinkels
4. Hands on Detection: Erkennung, ob der Fahrer das Lenkrad berührt
5. Side Wind Compensation: Unterstützt den Geradeauslauf bei Seitenwind
6. Pull Drift Compensation: Unterstützt den Geradeauslauf bei geneigter Fahrbahn
7. Zero Position Learning: Ermittelt die Geradeaus-Stellung bei verschiedenen Achslasten
8. Universal Joint Variation Compensation: Kompensation für geometrische Nichtlinearitäten
9. Self-Diagnostic: Eigendiagnose des Systems
10. Friction Compensation: Kompensation von mechanischen Reibungen
11. External Haptic Feedback Request: Verschiedene Lenkrad-Vibrationsmuster zur Rückmeldung an den Fahrer
12. Steering Characteristic External Torque Offset Request: Aufprägen eines Lenkradmoments durch weitere Fahrzeugsysteme (z.B. automatisches Einparken)

Nach Ermittlung der Hauptfunktionen müssen diesen alle möglichen Fehlfunktionen zugeordnet werden. Um diese Fehlfunktionen strukturiert zu ermitteln, wurde die DIN EN 61882: 2017-02 verwendet. Die Norm beschreibt das sogenannte HAZOP Verfahren (Hazard and Operability), welches ein Gefährdungsanalyseverfahren ist. Mittels dieses Verfahrens können mögliche Fehlfunktionen basierend auf den Hauptfunktionen ermittelt werden [28]. Unter der Tabelle 4.2 in der Norm findet man gewisse Adjektive bzw. elementare Leitworte, mit derer es möglich ist, passende Fehlfunktionen zu ermitteln (siehe Anhang 2 - HAZOP). Mithilfe dieser Tabelle haben sich 7 mögliche Fehlfunktionen für die Hauptfunktion „Steering Assist“ ergeben.
Da die Schwere, Eintretenswahrscheinlichkeit und Kontrollierbarkeit von der jeweiligen Fahrsituation abhängen, in der ein Fehler auftritt, werden im Anschluss alle möglichen Betriebszustände und Fahrsituationen als Situationskatalog aufgeführt. Es folgt die Situationsanalyse, welche den operativen Modus eines Fahrzeugs und deren kritische Phase währenddessen darstellt, (siehe Anhang 3 – Situationskatalog und Situationsanalyse). Um das Ausmaß des Hazard and Risk Assesments zu beschränken werden in dieser Arbeit lediglich drei Fahrsituationen betrachtet, welche bei solch einem System am gängigsten sind.
Diese drei operativen/ kritischen Modi werden gemäß ihrer Relevanz für die EPS und ihrer Eintretenswahrscheinlichkeit basierend auf der prozentualen und Frequentativen Dauer während des operativen Zustands bewertet. Dabei sollten auch vorhersehbare missbräuchliche Einsätze des Systems berücksichtigt werden. In der eigentlichen Situationsanalyse werden diese drei Operativen Zustände zusammen mit einer ihrer kritischen Situationen mit den zuvor ermittelten Fehlfunktionen der Hauptfunktion gegenübergestellt. Aus dieser Situationsanalyse ergibt sich die Entscheidung, ob der jeweilige operative Zustand samt Fehlfunktion in der Einzelbewertung berücksichtigt wird, ob er bereits durch einen übergeordneten operativen Zustand abgedeckt wird oder ob diese Kombination nicht relevant ist.
Abschließend werden in der FHA die Einzelbewertungen für die relevanten Fehlfunktionen durchgeführt und ergeben somit einen ASIL nach dem Risikographen in Abbildung 15. Diesen ASIL relevanten

Fehlfunktionen werden zudem Sicherheitsziele zugeordnet. Diese Sicherheitsziele können unter Umständen unterschiedliche ASIL Bewertungen haben. Somit muss nach dem Max-ASIL-Prinzip die höchste ASIL Bewertung für das jeweilige Sicherheitsziel verwendet und zugeordnet werden (siehe Anhang 1 – FHA/ HARA & Safety Goals).
Die Spaltenbelegungen der durchgeführten Verfahren basieren alle auf dem Stand der Technik und spiegeln insbesondere eine sehr praxisorientierte Belegung dar. [29]

5.2 System-FMEA

Die Fehlermöglichkeits- und Einflussanalyse (engl. Failure Mode and Effect Analysis, FMEA) ist eine systematische Methode zur Analyse von Fehlern, deren Folgen und den einhergehenden Risiken. Die FMEA kann in vielen Bereichen eingesetzt werden. So können Fertigungsprozesse mit einer Prozess-FMEA analysiert werden, um besonders kritische Fertigungsschritte zu identifizieren. Eine Konstruktions-FMEA hingegen hilft, Schwachstellen in Konstruktionen, wie kritisch dimensionierte Bauteile zu finden. Eine System-FMEA hat den Zweck bzw. die Aufgabe Systementwürfe hinsichtlich des Ausfallrisikos einzelner Baugruppen qualitativ zu bewerten. Im Vordergrund steht dabei das Auffinden von Schwachstellen in einem System. Die System-FMEA unterstützt zudem dabei, Entwurfsverbesserungen bezüglich der Zuverlässigkeit, der Instandhaltung und der Sicherheit durchzuführen. Zudem werden nützliche Vorabinformationen über Ausfallwahrscheinlichkeiten und Ausfalleffekte für eine eventuell folgenden Fehlerbaumanalyse (engl. Falt Tree Analysis, FTA) geliefert. Die möglichen Fehler und ihre Folgen werden dabei hinsichtlich der folgenden drei Größen auf einer Skala von 1 bis 10 bewertet:

1. Auftrittswahrscheinlichkeit (A, im Englischen Occurence - O): Wie wahrscheinlich ist es, dass dieser Fehler vorkommt bzw. das Risiko eintritt. Wobei die Bewertung (1) ein Auftreten nahezu ausschließt und die Bewertung (10) vermittelt, dass der Fehler oder das Risiko regelmäßig auftritt.
2. Bedeutung (B, im Englischen Severity - S): Welche Wirkung durch das Auftreten des Fehlers entsteht. Hierbei steht die (1) für keine Auswirkung auf die Funktion, wodurch der Fehler vom Kunden nicht bemerkt wird. Mit einer (10) hingegen werden Folgen für Leib und Leben, schwere Verletzungen von Vorschriften oder hohe finanzielle Schäden bewertet.
3. Entdeckungswahrscheinlichkeit (E, im Englischen Detection - D): Wie wahrscheinlich ist es, dass der Fehler oder das Risiko nach Eintritt bemerkt wird. Wobei (1) eine zwangsläufige Entdeckung darstellt und die Bewertung (10) eine systematische Entdeckung ausschließt.

Die angehängte System FMEA wurde gemäß der noch weit verbreiteten „alten Herangehensweise“ durchgeführt. Hierbei wird, wie auch in der Spaltenbelegung zu sehen, eine Risikoprioritätszahl (RPZ) für die Beurteilung von Risikopotentialen genutzt. Die RPZ ergibt sich aus dem Produkt der drei Größen A, B und E. Dabei können verschiedene Kombinationen der Größen eine gleiche RPZ ergeben. Zum Beispiel kann eine RPZ von 120 durch A*B*E = 3*10*4 oder auch durch 4*5*6 entstehen. Hierbei kann der erste Fall

bei einer Bedeutung von 10 und eine Entdeckung von 4 im Vergleich zu einer Bedeutung von 5 und einer Entdeckung von 6 im zweiten Fall deutlich inakzeptabler sein, wenn die Bewertung der Bedeutung einer nichtlinearen Skala folgt, wie es bei der Möglichkeit von Personenschäden der Fall ist. Des Weiteren ist nicht sichergestellt, dass ähnlichen Risiken auch dieselbe RPZ zugeordnet wird. Diese Herangehensweise stand somit in der Kritik, da sie in vielen Fällen, bei denen Auswirkungen auf den Menschen möglich sind, nicht praktikabel bzw. optimal war.

Diese Schwächen wurden bereits 2006 in der DIN EN 60812 benannt und haben daraufhin grundlegende Arbeiten zur Erklärung und Behebung fortschreiten lassen, welche zum Beispiel in der DIN VDE V 0831-101 für die Eisenbahn-Signaltechnik bereits aufgenommen und eingeführt wurden. In der Automobilindustrie wurden diese Veränderungen in Relation zu anderen Branchen erst spät nach der Harmonisierung von der AIAG und dem VDA durch das FMEA Handbuch (2019) eingeführt [32].

Konkret geht es bei dieser Veränderung und neuen Herangehensweise darum, dass der alte RPZ- und Risikomatrixansatz durch eine Kennzahl für die Aufgaben-Priorisierung ersetz wurde. Die AP stellt die Notwendigkeit von zusätzlichen Verbesserungsmaßnahmen durch eine Bewertung in den Stufen „niedrig“, „mittel“ und „hoch“ dar und betrachtet dabei sämtliche Kombinationen der Größen A, B und E. Zudem sind weitere Spalten bei der Dokumentation im FMEA-Formblatt und ein weiterer Schritt (Betrachtungsumfang) bei der Herangehensweise hinzugekommen.

In der angehängten S-FMEA wurde exemplarisch die mögliche Fehlfunktion des übermäßigen Bereitstellens des Lenkunterstützungsmoments (engl. excessive provision of steering assist torque) auf ihre möglichen Fehlerursachen und Fehlerfolgen untersucht. Dabei wurden keine Defekte, die seitens der Konstruktion, Herstellung oder Montage entstehen können, berücksichtigt, da diese in der Konstruktions- beziehungsweise Prozess-FMEA behandelt werden.

Die FMEA ist ein lebendes Dokument, welches fortlaufend bearbeitet wird. Daher sind in der Dokumentation auch Spalten enthalten, die erst während der weiteren Entwicklung gefüllt werden. Eine dieser Spalten ist zum Beispiel die „getroffene Maßnahmen“, die dokumentiert, welche zusätzliche Maßnahmen nach dem Erstergebnis der FMEA getroffen wurden. Die System FMEA für die beispielhafte Darstellung im Rahmen dieser Arbeit stellt dabei den Erststand der FMEA dar. Daher sind die Spalten (K-P) im Allgemeinen nicht bearbeitet worden. Da zudem lediglich eine Fehlfunktion mit einer Fehlerfolge betrachtet wurde, ist die Bedeutung bei allen möglichen Fehlerursachen gleich, während die Kenngrößen A und E jeweils einzelnd bewertet wurden, um die weiteren Maßnahmen definieren und Aufgaben priorisieren zu können. [30 bis 32]

5.3 ISO 21448 (SOTIF) Analyse LKAS

Der Spurhalteassistent (engl. Lane Keeping Assist System) ist eines von vielen sicherheitstechnischen Assistenzsystemen in modernen Fahrzeugen. Die Hauptfunktion dieses Systems besteht darin, den Fahrer und andere Verkehrsteilnehmer von einem unbeabsichtigten Verlassen der Spur zu schützen. Die Funktion ist für Autobahnen und Schnellstraßen ausgelegt und wird in der Regel erst ab einer gewissen Geschwindigkeit

aktiviert. Das System bzw. das Fahrzeug warnt den Fahrer bei einem aktivierten Spurhalteassistenten visuell, akustisch und durch Vibration des Lenkrads vor einer bevorstehenden Gefahr durch Verlassen der Spur, was in den meisten Fällen durch Müdigkeit und Ablenkung verursacht wird. Zudem warnt das System ebenfalls aufgrund eines nicht getätigten Blinkers bei einem Spurwechsel. Zusätzlich zum Warnen gehört auch ein aktives Gegenlenken oder Korrigieren der Fahrtrichtung zu den Aufgaben des Systems, in vielen Fahrzeugen. [33]

Das LKAS fällt unter die SAE Stufe 2, da aufgrund des aktiven Gegenlenkens bzw. Eingreifens bereits die erste anfängliche Automatisierung erfolgt. Der Spurhalteassistent ist grundlegend bei jedem OEM ähnlich, kann jedoch, was die Positionierung der Kamera und Art und Stärke der Warnung und Korrektur angeht, unterschiedlich ausgelegt sein. Meistens ist eine intelligente Kamera hinter dem Rückspiegel des Fahrzeugs angebracht, welche die Linien und Markierungen auf der Straße erkennt [34]. Falls der Fahrer droht, unbeabsichtigt die Spur zu verlassen, wird das System entsprechend reagieren. Nach einer Warnung und der Missachtung des Warnsignals wird das System in den meisten Anwendungen aktiv korrigieren, um das Fahrzeug in der Spur zu halten.

Viele Systeme haben dabei zwei Unterstützungsstufen: Eine leichte Lenkradbewegung, welche den Fahrer daran erinnert in der Spur zu bleiben und einen Notfallmodus, der eine stärkere Korrektur vornimmt, wenn das System erkennt, dass eine größere Gefahr droht. Bei Fahrzeugen mit elektrischer Servolenkung (EPS) lenkt der Spurhalteassistent sanft, jedoch spürbar durch Verdrehen des Lenkrads gegen, um das Fahrzeug in der Spur zu halten. Bei Fahrzeugen ohne elektrische Servolenkung erfolgt das Gegenlenken durch das elektronische Stabilitätsprogramm (ESP) über das gezielte Abbremsen einzelner Räder, auch bekannt als selektives Bremsen [35].

Eines der wichtigsten sicherheitstechnischen Eigenschaften eines LKAS ist die Übersteuerbarkeit des Systems, denn in gewissen Situationen kann die Durchbrechung der Fahrbahnlinie notwendig sein, um ein katastrophales Ereignis zu vermeiden. Daher hat der Fahrzeugführer stets die Verpflichtung die Hände am Lenkrad zu halten, und die LKAS Funktion nicht als automatisches Fahrsystem zu missbrauchen. Um diesen Missbrauch zu vermeiden, nutzen Hersteller das Lenkmoment, um festzustellen, ob der Fahrer noch die Hände am Lenkrad hat. Dabei können auch sehr geringe und feine Lenkmomente festgestellt werden. Jedoch wurde in der Vergangenheit auch diese Überwachungsfunktion ausgehebelt (zum Beispiel durch in das Lenkrad geklemmte Gegenstände), wodurch die Hersteller dazu gedrängt wurden, neue Überwachungssysteme zu entwickeln.

Die Anwendung der ISO 26262 in der Entwicklung, kann das LKAS nahezu ausfallsicher gestalten und zudem das Risiko eines Fehlers oder einer Störung auf das akzeptable Maß verringern. Jedoch kann ein LKAS auch bei voller Verfügbarkeit im aktiven Zustand gefährliche Ereignisse auslösen. So können sich überschneide Fahrbahnmarkierungen zu einer falschen Erkennung der Markierungen führen, woraufhin das LKAS System eingreift um das Fahrzeug entsprechend zu steuern bzw. zu korrigieren. Diese Korrektur kann jedoch ein unsicheres Manöver sein, etwa wenn der falschen Markierung gefolgt wird.

Die ISO 26262 beschreibt keine speziellen Möglichkeiten, um derartige Gefahren auszuschließen. Auch die ISO 21448 kann durch die Umgebung entstehenden Gefahren oder Risiken nicht vollumfänglich ausschließen, bietet jedoch mit ihrer Herangehensweise eine sehr gute Möglichkeit einen Großteil dieser Risiken zu erkennen und sicher zu gestalten.

In der Konzeptphase werden dabei ausgehend von der Beschreibung der Funktionalität bzw. Funktion der Automation die Gefährdungen und Risiken methodisch abgeleitet. Bei einem Stufe 2 System wie einem LKAS liegt die Verantwortung stets bei dem Fahrzeugführer. Der Fahrer muss Informationen der Umgebung stets wahrnehmen und in der Lage sein unmittelbar auf potenziell gefährliche Situationen zu reagieren. Das LKA-System ist dabei ein weiterer Informationsgeber hinsichtlich der Umgebungswahrnehmung (durch die Warnfunktion), wodurch der Fahrer sein Verhalten hinsichtlich der Quer- und Längsführung besser anpassen kann.

Diese Interaktion zeigt bereits erste potenzielle Gefährdungen, die durch einen Ausfall der Sollfunktion (in diesem Fall die Warnung) entstehen können. Dabei können Sensoren, Aktoren, Regelalgorithmen, sowie ein Fehlverhalten des Fahrers Risiken und Gefährdungen erzeugen. In diesem konkreten Fall sind zwei wesentliche Gefährdungen, dass das LKAS System ein unsicheres Fahrmanöver ausführt oder dass der Fahrer dieses nicht korrigiert.

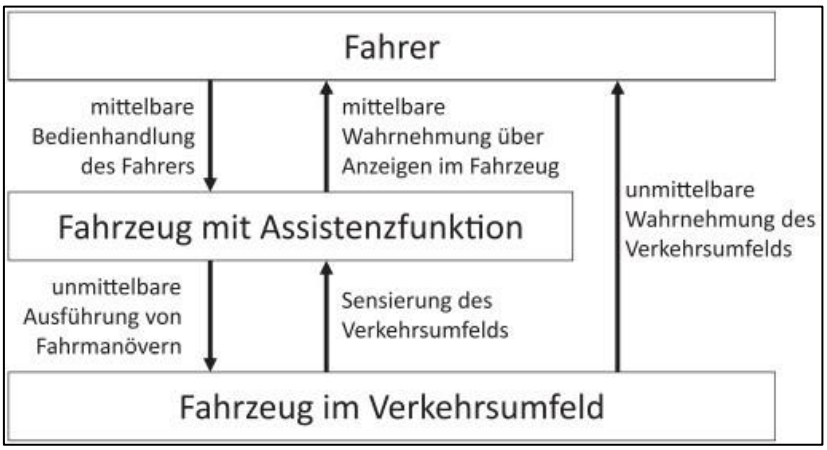


Abbildung 16: Wirkschema zwischen einem Fahrer und einer Stufe 2 Fahrzeugautomation

Bei der Konzeption einer Automatisierungsfunktion ist die Funktions- und Systembeschreibung der Ausgangspunkt für die Analysen nach der ISO 21448, gleichzeitig ist es jedoch auch ein lebendes und fortlaufendes Dokument und muss somit auch während der Entwicklung angepasst werden. Darin wird der Regelbetrieb sowie das Sollverhalten der Funktion beschrieben. Zudem werden die Grenzen der Funktionalität und ganz besonders die Betrachtung des Systemverhaltens bei entdeckten Einschränkungen und die damit verbundenen Warnhinweise und Übernahmeaufforderungen an den Fahrer thematisiert. Diese Beschreibung ist in der ISO 26262 als Item Definition bekannt, wobei die intensive Betrachtung der Warnhinweise und Übernahmeaufforderungen nicht in dem Ausmaß wie bei der ISO 21448 (SOTIF) erfolgt.

Die ISO 21448 nennt zahlreiche Gefährdungsanalysen, mit denen Gefährdungen im Sinne der Sollfunktionssicherheit systematisch identifiziert werden können. Allgemein betrachtet, können verschiedene

Methoden für das Identifizieren und Analysieren von unbekannten unsicheren Ereignissen auf Systemebene angewandt werden.

Aufgrund der zunehmenden neuen Technologien und derer Komplexität sind herkömmliche Ansätze bzw. Methoden zur Absicherung der Systemsicherheit nicht ausreichend. Einer der interessantesten und wichtigsten neuen Methoden ist die „system-theoretic accident model and processes“ (STAMP), welche 2012 in Nancy Levesons Buch „Engineering a Safer World“ vorgestellt wurde. Diese Gefährdungsanalysemethode untersucht strukturiert ein sicherheitsrelevantes System mittels einer semi-formalen Methode. Die Stärke von STAMP ist es, das System und die Fahrer- Fahrzeug- und Fahrumgebung als soziotechnisches System zu erfassen. Die „Systems-Theoretic-Process-Analysis“ (STPA) ist eine Gefährdungsanalyse auf Grundlage von STAMP. Diese neuen Ansätze und Methoden finden in den verschiedensten Branchen Einzug und zielen grundlegend auf die Sicherheit der Sollfunktion ab. [36]

Die STPA ist eine Top-Down Analyse, welche sukzessiv verfeinert wird und somit zu einem tieferen Systemverständnis führt. Verglichen mit einer induktiven Analysemethode wie die FMEA oder einer deduktiven Analysemethode wie der FTA kann die STPA wesentlich mehr Gefährdungen in einem System erkennen. Die „Causal Analysis Based on STAMP“ (CAST) ist eine weitere Methode, die von STAMP abgeleitet wurde, um aus Unfallanalysen ein vertieftes Verständnis von fehlerhaft realisierten Schutzfunktionen zu erlangen. Dies kann auch Anwendung bei der Validierung finden, da hier CAST bei einem unvorhersehbaren Systemverhalten Erklärungen für Testabweichung finden kann und somit auch geeignete SOTIF Maßnahmen identifiziert werden können. [36, 37]

Bei der Sicherheitsregelstruktur eines Systems mit LKAS wird der Fahrer als integraler Teil des Systems betrachtet, somit wird im Rahmen der STPA auch der potenzielle oder vorhersehbare Fehlgebrauch des LKAS frühzeitig betrachtet. Zusätzlich zum Fahrer wird die Umgebung auch in die Regelungsstruktur integriert, wodurch zum Beispiel Verkehrsmittel, Verkehrszeichen oder auch die allgemeine Umgebungsbedingung betrachtet wird.

Aus der bekannten Sicherheitsregelstruktur des Fahrers können unsichere Regelungsaktionen bestimmt werden. Um diese zu bestimmen, wird eine Leitwortmethode ähnlich wie bei der HAZOP angewandt, um Fehlerfälle der Regelungsaktionen festzulegen. Durch die Bewertung der einzelnen Kombinationen werden Fehlerfälle, die potenziell zu einem gefährlichen Zustand führen können, ermittelt. Es ergeben sich im gleichen Zug SOTIF Anforderungen für die Sicherheit der Sollfunktion.

Durch dieses gesamte Konstrukt vom Fahrer, dem System und der Umgebung können potenziell unsichere Regelungsaktionen oder fehlende Systemfunktionen identifiziert und behandelt werden, die sonst zu potenziell unsicherem Systemverhalten führen könnten.

Durch die im Anschluss folgende Implementierungsphase werden die Fehlfunktionalitäten beherrscht und stellen in Summe sicher, dass das SOTIF Risiko auf ein akzeptables Restrisiko gesenkt werden kann. Grundsätzlich werden dabei viele Maßnahmen in Kombination verwendet, um das bestmögliche Ergebnis zu erlangen. Darunter fallen Maßnahmen zur Systemverbesserung, die Einschränkung der Sollfunktion, die

Rückgabe der Verantwortung für die Fahraufgabe an den Fahrer, sowie die Beherrschung eines vorhersehbaren Fehlgebrauchs.

Abschließend wird durch die Verifikation und Validation der Nachweis erbracht, dass die beabsichtigte Sollfunktion mit ausreichender Sicherheit erfüllt wird. Ziel der Verifikation ist zudem, nachzuweisen, dass das jeweilige System sowohl bekannte als auch unbekannte Ereignisse beherrschen kann.

Um auf das Ausgangsbeispiel zurückzukommen muss abschließend bei der Validation das LKAS Systems und dessen Einsatzzweck untersucht werden. Hierbei werden bewusst variierende Parameter eingesetzt und beobachtet, ob es immer zu dem beabsichtigten Systemverhalten kommt. Um mögliche unbekannte und unsichere Ereignisse zu provozieren, gibt die ISO 21448 vor, auch Einsatz- und Umgebungsszenarien, die nicht vorgesehen sind, zu verwenden, um so durch das jeweilige Systemverhalten Rückschlüsse und Synergien zum eigentlichen Einsatzszenario zu ermitteln. Dies kann potenzielle unbekannte und unsichere Ereignisse entdecken, die möglicherweise auch im Solleinsatzszenario auftreten könnten.

Dies ist auch der wesentliche Unterschied zur Verifikation, die ausschließlich die Erfüllung von definierten Anforderungen nachweist. Durch die Kombination von Verifikation und Validation kann nachgewiesen werden, dass sowohl unbekannte als auch bekannte unsichere Ereignisse hinreichend selten auftreten. [26]

6 Ergebnisse der Methodiken diskutieren und vergleichen

Ein elektrisch betriebenes Lenksystem ist in der Entwicklung komplex und erfordert viel Erfahrung in zahlreichen Sicherheits- und Gefährdungsanalysen, da die Lenkung als System eine elementare Komponente mit hohem Gefährdungspotential im Fahrzeug ist. Um sicherheitskritischen Ausfälle zu vermeiden und das Ausfallrisiko zu minimieren, wird in der Entwicklung eine sehr umfangreiche HARA oder FMEA durchgeführt. Zum Beispiel würde eine vollständige HARA im realen Umfeld mehrere hundert bis tausend Zeilen umfassen.

Im Rahmen dieser Arbeit wurde eine HARA und eine System-FMEA für jeweils eine Hauptfunktion durchgeführt sowie eine SOTIF Analyse eines lenkbasierten Assistenzsystems erläutert. Dabei wurde in der HARA lediglich die Funktion „Lenkunterstützung“ (engl. steering assist“), in der System-FMEA die Fehlfunktionalität des übermäßigen bereitstellen eines Lenkunterstützungsmoments (engl. excessive provision of steering assist torque) und in der SOTIF Analyse das LKAS betrachtet, um den Rahmen der Arbeit nicht zu sprengen. Zusätzlich wurde für letztere lediglich der theoretische Rahmen dargelegt, um dem Leser die allgemeine Herangehensweise näher zu erläutern.

In der HARA konnte für die Funktion „Lenkunterstützung“ in einer HAZOP-Analyse sieben mögliche Fehlfunktionen mittels der Leitworte nach der DIN EN 61882 identifiziert werden. Ursprünglich wurden bei der Durchführung noch weitere Fehlfunktionen ermittelt, welche jedoch durch bereits vorhandene Fehlfunktionen abgedeckt wurden und somit auch nicht weiter berücksichtigt werden mussten.

Diese Reduktion auf das Notwendige in jedem Schritt ist entscheidend, um den Aufwand auf ein durchführbares Maß zu begrenzen.

Im Folgenden wurde ein Situationskatalog erstellt, welche vier operative Hauptzustände eines Lenksystems darstellt. Diese wurden gemäß ihrer Relevanz und Auftretenswahrscheinlichkeit aufgelistet. Anschließend wurden diese Situationen den vorab ermittelten Fehlfunktionen in einer Situationsanalyse gegenübergestellt. Bei diesem Abgleich lässt sich darstellen, ob die jeweilige Fehlfunktion relevant für den operativen Zustand ist und somit auch weiter in der FHA berücksichtigt werden muss. Hier hat sich zum Beispiel gezeigt, dass „city traffic in general“ sämtliche weiter folgenden „city traffic“ Situationen abdeckt. Das Ergebnis der Situationsanalyse zeigt uns, dass nicht alle ermittelten Situationen auch eine Relevanz für die weitere Betrachtung haben.

Im Rahmen der im Anschluss durchgeführten Einzelanalyse wurden daher ausschließlich die relevanten Fehlfunktions-Fahrsituations-Kombinationen bewertet. Als Ergebnis der Analyse wurden 10 Kombinationen mit ASIL D, 4 mit ASIL C, 3 mit ASIL B und 1 mit ASIL QM bewertet. Vier Kombinationen wurden auf Grund der gegebenen Kontrollierbarkeit (mit C0 bewertet) aus der weiteren Betrachtung herausgenommen (ohne ASIL).

Das keine Fehlfunktion mit ASIL A bewertet wurde liegt an der Bedeutung der Lenkung für den Fahrbetrieb. Es gibt keine Fehlfunktionen, die ausschließlich in Fahrsituationen mit mittlerer Auftretenswahrscheinlichkeit kritisch sind. Entweder ist die Fehlfunktion immer kritisch oder lediglich in sehr seltenen Fahrsituationen. Im ersten Fall führt bereits eine sehr gute Kontrollierbarkeit (C1) zu einem ASIL B,

während im zweiten Fall die Kontrollierbarkeit so gut ist, dass die Kombination mit einem ASIL QM bewertet werden kann. Aus den bewerteten Fehlfunktionen wurden dann auch Sicherheitsziele abgeleitet. Es wurde zwar lediglich eine Funktion betrachtet, jedoch wurde deutlich, dass bereits diese eine Funktion mit mehreren verschiedenen Sicherheitszielen abgesichert werden muss.

Bei einer vollständigen durchgeführten HARA würden noch weitere Sicherheitsziele identifiziert werden. Dabei sollte darauf geachtet werden, die Sicherheitsziele so allgemein wie möglich zu definieren, um mit einem Sicherheitsziel möglichst viele Fehlfunktionen abdecken zu können. Aus der Erkenntnis, dass die Fehlfunktion „No steering assist functions available“ auf Grund der guten Kontrollierbarkeit aus der weiteren Betrachtung herausgenommen werden konnte, lässt sich der sichere Zustand „EPS shall be deactivated (No steering assist functions active)“ ableiten.

Dieser Zustand wird bei sämtlichen kritischen Fehlern eingenommen, um potenziell weitere oder größere Gefährdungen auszuschließen. Zusammenfassend wird deutlich, dass die Funktion bzw. das Lenksystem auf einem hohen ASIL entwickelt werden muss, da das Lenksystem bei falscher Entwicklung eine Gefahr für den Menschen darstellt. Ebenso kann sicher abgeschätzt werden, dass auch andere Funktionen der EPS eine ähnliche Einstufung bei den ASIL-Bewertungen erhalten werden.

Aus der Fehlfunktion F02 hat sich das Sicherheitsziel „Too high (excessive) provision of steering assist torque shall be prevented“ ergeben. Dieses Sicherheitsziel wurde daraufhin für eine genauere Betrachtung in einer System-FMEA ausgewählt.

In der S-FMEA ergab sich als Fehlerfolge ein „loss of lateral vehicle stability“, demnach der Verlust der Längsstabilität. Diese Fehlerfolge ist für den Menschen ein potenziell gefährliches Ereignis, weswegen sie mit der Bedeutung 10 bewertet wurde.

Fehlerursachen, die das Unterstützungsmoment reduzieren, lassen sich leicht finden (zum Beispiel Reibung oder jeder mechanische Defekt, der die Kraftübertragung unterbricht). Die Fehlerursachen eines Fehlers, der „etwas“ hinzufügt oder vergrößert, sind hingegen nicht offensichtlich. Eine Bereitstellung eines zu hohen Lenkmoments kann nur durch die Mechanik, oder das E/ E System verursacht werden.

Seitens der Mechanik gibt es dabei lediglich drei verschiedene Fehlerursachen. Einer von diesen Ursachen ist ein zu großer Zylinder. Denn ein zu großer Zylinder kann dazu führen, dass bei einem definierten Druck zu viel Kraft bereitgestellt wird und somit auch ein zu hohes Lenkmoment generiert wird. Als Vermeidungsmaßnahme muss in den Anfangsphasen die Konstruktion mittels CAD und Berechnungen sicherstellen, dass der Zylinder für seinen Einsatz optimal ausgelegt ist. Diese Auslegung muss dann mit einem geeigneten Test überprüft werden.

Die Auftretenswahrscheinlichkeit sowie die Entdeckungswahrscheinlichkeit wurden für diese Fehlerursache beide mit einer 3 bewertet, da sowohl die Auslegung (Fläche=Kraft/Druck) als auch die Tests (Aufnahme einer Druck-Kraft-Kurve) gut bekannt und sehr zuverlässig sind. Eine weitere interessante mögliche Fehlerursache ist die Softwareberechnung, durch die bei falscher Berechnung der jeweiligen Eingangssignale ein zu hohes Lenkmoment erzeugen kann. Diese Art von Fehlerursache tritt in der Industrie tatsächlich häufig auf. Natürlich werden Methoden eingesetzt, die schon bei der Erstellung Fehler in der Software

verhindern sollen. Dazu gehören Programmierrichtlinien und die Wiederverwendung von bekannten Softwaremodulen (engl. Reuse of well known code). Erfahrungsgemäß decken diese jedoch nicht alle Fehlerquellen ab. Daher wurde diese Fehlerursache mit einer Auftretenswahrscheinlichkeit von 6 bewertet. Umso wichtiger ist es, dass die Software durch entsprechende Tests überprüft wird. Diese Tests zeigen eine hohe Entdeckungswahrscheinlichkeit von Fehlern, somit wurde diese mit einer 2 bewertet.

Insgesamt ist die S-FMEA der Fehlfunktion „Zu viel Unterstützungsmoment bereitgestellt“ vergleichsweise kurz und führt nur wenige Fehlerursachen auf. Dies hat den Grund, dass sich bei solch einem Fehler die Ursachen seitens der Mechanik sehr begrenzt halten. Auch die Ursachen seitens des E/ E Systems sind in Relation zu anderen möglichen Fehlern begrenzt. Daher war diese Funktion auch gut geeignet, um die Systematik der Erstellung einer S-FMEA in dieser Arbeit zu demonstrieren, ohne den Umfang der Arbeit zu sehr zu vergrößern.

Im Folgenden würde man die identifizierten Fehlerursachen den verschiedenen Subsystemen wie einem Sensor, der Mechanik oder dem Steuergerät zuordnen und diese dann in einer Design-FMEA noch weiter untersuchen. Dabei würden weitere Fehlerursachen identifiziert werden.

Allgemein kann man sehen, dass die Risikoprioritätszahl bei allen möglichen Fehlerursachen ein mittleres Risiko aufzeigt und somit weitere Maßnahmen in Erwägung gezogen werden sollten. Dabei kommen klassische Maßnahmen wie zusätzliche Tests oder Konstruktionsänderungen in Frage. Zusätzlich stehen aber für die Mechatronik Maßnahmen zur Verfügung, die in einer klassischen S-FMEA nicht berücksichtigt werden, wie zum Beispiel Online-Fehlererkennung und -behandlung durch das Steuergerät.

Interessant ist zudem der Vergleich verschiedener Bewertungen wie die Bewertung der Bedeutung allein, die RPZ oder das Produkt der Parameter A und B. Im Gegensatz zur RPZ, die bei allen Fehlerursachen einen Handlungsbedarf aufgezeigt hat, wird bei dieser Berechnung einem Großteil der Fehlerursachen ein minimales und akzeptables Risiko zugeschrieben, welches kein Handlungsbedarf mit sich bringt. Im Gegensatz dazu wird bei der Bewertung der Bedeutung allein nicht die Fehlerursache, sondern nur die Fehlerfolge bewertet, weswegen hier ebenfalls alle Fehlerursachen gleich betrachtet werden.

Diese Bewertungen sind schlussendlich nur ein Versuch, um möglichen Fehlerursachen eine Art Rangfolge zuzuordnen, wobei je nach Anwendungen, die eine oder andere Methode zu bevorzugen ist. Der Bewertung der Bedeutung allein kommt dabei eine Sonderposition zu, da diese verwendet wird, um sicherheitsrelevante Fehlerursachen als „Kritische Merkmale“ zu kennzeichnen.

Abschließend zeigt sich, dass der Ausgangsfehler „excessive provision of steering assist torque“ ein sicherheitskritischer Fehler ist. Die durchgeführte S-FMEA macht deutlich, dass jede einzelne Fehlerursache durch gewisse Maßnahmen sowohl auf Grund der Bedeutung als auch auf Grund der RPZ abgedeckt werden muss.

Die SOTIF Betrachtung des Assistenzsystems LKAS erfolgte lediglich in einem theoretischen Rahmen und bietet daher keine konkreten Ergebnisse. Daher wird in diesem Rahmen die Durchführung einer STPA Analyse besprochen. Der Startpunkt einer STPA Analyse ist die Kontrollstruktur, welche das System aus rein funktionaler Sicht darstellt und den exakten Kontroll- und Informationsfluss durch die Subsysteme

aufzeigt. Hierbei spielt es keine Rolle, ob das übergeordnete System ein Mensch oder ein E/E-basiertes Computersystem ist. Beide verteilen, agieren und bestimmen eine jeweilige Handlung.
Das LKAS hat nach Aktivierung die Aufgabe, seine grundlegende Funktionalität auszuführen. Der Mensch hat die Aufgabe, das System stets zu überwachen. Somit wäre ein potenzielles „Subsystem“ des Menschen die Hände am Lenkrad, mit denen der Fahrer die Querführung des Fahrzeugs steuert. Dabei kann auch ein Fehlgebrauch des Lenkrads seitens des Fahrers erfolgen, der mit in der Analyse betrachtet werden muss. Ein mögliches Subsystem des LKAS als solches, wäre die Kamera, welche Umgebungsinformationen aufnimmt und weitergibt.
Grundlegend ist der STPA Analyseprozess in zwei Schritte unterteilt. Im ersten Schritt werden potenziell gefährliche Kontrollaktionen (engl. unsafe control actions) identifiziert. Durch ein entsprechend angepasstes Systemdesign können bereits ermittelte gefährliche Kontrollaktionen ausgeschlossen werden. Ein Beispiel für gefährliche Kontrollaktionen des Systems, welche nicht einen Ausfall der Funktion, sondern eine fehlerhafte Funktionalität darstellen, ist das zu frühe Eingreifen der Sicherheitsaktion. So würde ein viel zu frühes eingreifen des LKAS dafür sorgen, dass das Fahrzeug in einen unbekannten und unsicheren Ereignisbereich gerät (zum Beispiel bei dem sich das Fahrzeug aufschaukelt). Um dies zu vermeiden, müssen zusätzlich zu der korrekten Auslegung des Systems im allgemeinen, auch kausale Faktoren mitberücksichtigt werden.
Im zweiten Schritt werden mögliche Ursachen und Szenarien, die zu einer gefährlichen Kontrollaktion führen können, ermittelt. Basierend darauf können zusätzliche Sicherheitsmaßnahmen für eine Risikominderung spezifiziert werden.
Das Ergebnis einer erfolgreichen Durchführung der SOTIF Betrachtung und der Durchführung einer STPA zeigt, ob das LKAS und dessen Subsysteme einen fehlerhaften Prozess, Algorithmus oder Austausch untereinander haben. Die Reduzierung all dieser Faktoren sorgt schlussendlich auch dafür, dass potenziell unbekannte und unsichere Ereignisse minimiert werden.

7 Zusammenfassung, Fazit und Ausblick

Das primäre Ziel der Bachelorarbeit ist es aufzuzeigen, wie ein elektrisch betriebenes Lenksystem aufgebaut ist und wie passende Gefährdungs- und Sicherheitsanalysen durchzuführen sind.
Die Arbeit setzt sich im Wesentlichen auch mit den Normen ISO 26262 und ISO 21448 (SOTIF) auseinander, um dem Leser ein theoretisches Wissen für die Herangehensweise der Funktionalen Sicherheit mitzugeben. Zudem werden ein potenzielles zukünftiges Lenksystem und die Automatisierung von Fahrzeugen erklärt.
Die Ergebnisse der Analysen zeigen, dass ein elektrisch betriebenes Lenksystem seitens der funktionalen Sicherheit durchaus kritisch und streng bewertet wird. Dieses Ergebnis überrascht nicht, da die Lenkung ein elementarer Bestandteil eines Fahrzeugs ist und bei Fehlern durchaus gefährliche Ereignisse auslösen kann. Lenksysteme entwickeln sich immer weiter und werden mit zahlreichen Assistenzsystemen ausgestattet. Diese Assistenzsysteme und derer Komplexität erfordern eine neue und angepasste Betrachtung, um auch deren potenziellen Fehlerquellen zu eliminieren. Die HARA sowie die FMEA können sehr gut aufzeigen, wie groß das Risiko von gewissen Fehlfunktionen oder Systemen ist. Doch die von der Funktionalität eines LKAS ausgehende potenzielle Gefahr, ist mit diesen Methoden allein definitiv nicht vollständig abzudecken. Durch eine Betrachtung der SOTIF-Methode wird klar, wie die Herangehensweise auszusehen hat und wie gewisse Erkenntnisse während der Durchführung bereits in das System eingepflegt werden können, um die vollständige Abdeckung zu erreichen.
Durch den weiteren Fokus auf die Automatisierung sowie deren rechtliche Grundlage in Deutschland, wird schnell deutlich, dass das Thema Automatisierung seitens Institutionen und Behörden schnell vorangetrieben wird. Doch diese schnelle Entwicklung kann von der Industrie nicht in diesem Maße begleitet werden. Die ISO 21448, die die SOTIF-Methode beschreibt, ist eine neue Norm, die bisher aber nur automatisierte Systeme bis SAE Level 2 abschließend behandelt. Daher wird sie in der Zukunft weitere Ergänzungen bekommen, um das schnell wachsende Bedürfnis nach einer Absicherung von Automatisierungen gerecht zu werden.
Im Vordergrund muss hier stets die Sicherheit der Menschen stehen, welche mit einer ordentlichen und bewussten Ausführung der Arbeiten zur funktionalen Sicherheit ein Stück mehr gewährleitet werden kann. Die Zukunft der Automatisierung wird noch viele weitere Herausforderungen und Neuerungen mit sich bringen.
Wichtig ist, diese stets kritisch zu hinterfragen und den Menschen sowie dessen Sicherheit immer an erster Stelle zu sehen.

Denn nur so kann gewährleitet werden, dass der Mensch das System anpasst und nicht das System den Menschen.

8 Referenzen

[1] Focus: Technik-Lexikon. Fahrdynamik und Fahrsicherheit: Mü-Split-Bremsung. FOCUS Online (2015)

[2] DKE: IEV-Woerterbuch, 2022. https://www2.dke.de/de/Online-Service/DKE-IEV/Seiten/IEV-Woerterbuch.aspx?search=192-05, abgerufen am: 27.04.2022

[3] ComputerWeekly.de: Was ist Mean Time To Repair (MTTR)? - Definition von WhatIs.com, 2021. https://www.computerweekly.com/de/definition/Mean-Time-To-Repair-MTTR, abgerufen am: 27.04.2022

[4] BMW: Das macht die typische BMW-Lenkung aus | BMW.com. BMW (2021)

[5] Pfeffer, P. u. Harrer, M. (Hrsg.): Lenkungshandbuch. Lenksysteme, Lenkgefühl, Fahrdynamik von Kraftfahrzeugen. ATZ / MTZ-Fachbuch. Wiesbaden, s.l.: Springer Fachmedien Wiesbaden 2013

[6] BOSCH: Elektrolenkung mit Servoeinheit an der Lenksäule, 2022. https://www.bosch-mobility-solutions.com/de/loesungen/lenkung/elektrolenkung-mit-servoeinheit-an-der-lenksaeule/, abgerufen am: 27.04.2022

[7] BOSCH: Elektrolenkung mit Servoeinheit an einem zweiten Ritzel, 2022. https://www.bosch-mobility-solutions.com/de/loesungen/lenkung/elektrolenkung-mit-servoeinheit-an-einem-zweiten-ritzel/, abgerufen am: 27.04.2022

[8] Mein-Autolexikon: Elektrisches Servo-Lenksystem | Mein Autolexikon, 2022. https://www.mein-autolexikon.de/lenkung/elektrisches-servo-lenksystem.html, abgerufen am: 27.04.2022

[9] Isgro, M.: Demnächst fahrerlos zum Ziel? Autonome Lenksysteme im Blick. EMAG GmbH & Co. KG (2018)

[10] United Nations Economic Commission for Europe: Regelung Nr. 79 der Wirtschaftskommission der Vereinten Nationen für Europa (UNECE) — Einheitliche Bedingungen für die Genehmigung der Fahrzeuge hinsichtlich der Lenkanlage. UNECE - R79. 2018

[11] Winkelman, J.: Preventing the Occurrence of a Hazard. FTTI at the Concept Level. kVA (2019)

[12] Revue, A.: Wenn ein Sensor das Ruder übernimmt, 2021. https://automobilrevue.ch/2021/08/25/technik-steer-by-wire/, abgerufen am: 27.04.2022

[13] Von Ralf Hickl, Product Sales Manager ABU bei Rutronik Elektronische Bauelemente: Steer-by-Wire. Drahtzieher auf dem Weg zum autonomen Fahren, 2019. https://www.elektroniknet.de/distribution/design-in/drahtzieher-auf-dem-weg-zum-autonomen-fahren.168236.html, abgerufen am: 27.04.2022

[14] Vilela, Von Christopher Temple und Antonio Dr.: Safety Automotive. Fehlertolerante Systeme im Fahrzeug – von "fail-safe" zu "fail-operational&quot, 2014. https://www.elektroniknet.de/automotive/assistenzsysteme/fehlertolerante-systeme-im-fahrzeug-von-fail-safe-zu-fail-operational.110612.html, abgerufen am: 27.04.2022

[15] Adam Schnellbach: Fail-operational automotive systems. Doctoral Thesis, . Graz, Wien (University of Technology)

[16] Dirk Wroblewski: Konzept einer fehlertoleranten, Konzept einer fehlertoleranten, elektrohydrauli schen steer-by-wire Lenkung für langsam fahrende Fahrzeuge, Universität Rostock. Rostock 2010

[17] Gerstl, S.: Anforderungen an Fail-Operational-Systeme in Fahrzeugen. Embedded Software Engineering (2019)

[18] Jean-Philippe Meunier: Automotive Functional Safety. The Evolution of Fail Safe to Fail Operational Architecture | NXP Semiconductors, 2022. https://www.nxp.com/company/blog/automotive-functional-safety-the-evolution-of-fail-safe-to-fail-operational-architecture:BL-AUTOMOTIVE-SAFETY-EVOLUTION, abgerufen am: 27.04.2022

[19] SAE J3016: 2021.04; 2021.04. *SAE J3016*

[20] Greis, F.: Verordnung beschlossen. Informatiker dürfen keine autonomen Autos überwachen - Golem.de. Golem.de (2022)

[21] Nachrichten, N.-t.: Bundesrat muss noch zustimmen. Kabinett lässt autonome Pkw auf die Straße. n-tv NACHRICHTEN (2022)

[22] Wilkens, A.: Verordnung für Autonomes Fahren. Alle 90 Tage Gesamtprüfung. heise online (2022)

[23] Bundesministerium für Digitales und Verkehr: erordnung zur Regelung des Betriebs von Kraftfahrzeugen mit automatisierter und autonomer Fahrfunktion und zur Änderung straßenverkehrsrechtlicher Vorschriften. BMVI. 2022

[24] NI: Was ist der funktionale Sicherheitsstandard ISO 26262?, 2021. https://www.ni.com/de-de/innovations/white-papers/11/what-is-the-iso-26262-functional-safety-standard-.html, abgerufen am: 27.04.2022

[25] ISO 26262: 2018-12; Second Edition 2018-12. *Road vehicles — Functional safety*

[26] Schnieder, L. u. Hosse, R. S.: Leitfaden Safety of the Intended Functionality. Verfeinerung der Sicherheit der Sollfunktion Auf Dem Weg Zum Autonomen Fahren. Essentials Ser. Wiesbaden: Springer Vieweg. in Springer Fachmedien Wiesbaden GmbH 2020

[27] ISO 21448: 2021. *Road vehicles — Safety of the intended functionality*

[28] Klessascheck, M.: HAZOP – Risikoanalyse konform IEC 61882. Johner Institut GmbH (2019)

[29] sasmita: How HARA Helps Functional Safety (ISO 26262) Consultants to Determine ASIL Values and Formulate Safety Goals. Embitel Technologies (2019)

[30] Dieckhöfer, L.: FMEA – Fehlermöglichkeits- und Einfluss Analyse. qmBase GmbH (2017)

[31] BMI: Organisationshandbuch - Fehlermöglichkeits- und Einflussanalyse, 2022. https://www.orghandbuch.de/OHB/DE/Organisationshandbuch/6_MethodenTechniken/63_Analysetechniken/633_FehlermoeglichkeitUndEinflussanalyse/fehlermoeglichkeitundeinflussanalyse-node.html, abgerufen am: 27.04.2022

[32] AIAG, V.D.A.: Failure Mode and Effects Analysis - FMEA Handbook. Design FMEA, process FMEA, supplemental FMEA for monitoring & system response. Southfild, Michigan, [Berlin]: Automotive Industry Action Group; [Verband der Automobilindustrie] 2019

[33] Francis, T.: What is lane-keeping assist? AutoExpress (2021)

[34] BOSCH: Multifunktionskamera, 2022. https://www.bosch-mobility-solutions.com/de/loesungen/kamera/multifunktionskamera/, abgerufen am: 27.04.2022

[35] Mobile: LDWS und LKAS. So funktionieren Spurhalteassistenten. undefined (2019)

[36] ZHAW Institut für Angewandte Mathematik und Physik IAMP: Gefährdungs- und Risikoanalytik | ZHAW Institut für Angewandte Mathematik und Physik IAMP, 2021. https://www.zhaw.ch/de/engineering/institute-zentren/iamp/sicherheitskritische-systeme/gefaehrdungs-und-risikoanalytik/, abgerufen am: 27.04.2022

[37] Dr. Qi Van Eikema Hommes: Applying STPA to Automotive Adaptive Cruise Control System. 2012

Abbildungsverzeichnis

Anhang 1 – FHA/ HARA & Safety Goals

ID	Function	Potential main Failure Mode	TOP Hazard	Operating Mode	Critical Operation Phase	Exposure	Indication to Driver	Driver's Action	Controllability	Failure Effect / Hazardous Situation	Severity	ASIL	Safety Goal	Safe State
S.0	Steering assist	F04 – Steering Assist Torque is applied without a request (e.g. from the driver or a superordinated system function)	Vehicle moves unintentionally in lateral direction	workshop	Maintanence by worker	E1	no driver while maintenance	no driver while maintenance	C1	Vehicle is in operating position/ Workers can be crushed due to moving wheels during repair	S3	QM	Unintended provision of steering assist torque shall be prevented	EPS shall be deactivated (No steering assist functions active)
C.1	Steering assist	F01 – Steering Assist Torque request is not fulfilled (no torque provided)	Steering ability of the vehicle is impaired	city traffic	city traffic in general	E4	Steering by the driver is impaired and more difficult	Controllable in general by the driver	C0	Vehicle could collide with other road users or obstacles	S3	-	Sudden loss of steering assist torque shall be prevented	EPS shall be deactivated (No steering assist functions active)
C.2	Steering assist	F02 – Provided Steering Assist Torque exceeds the requested value and limits	Vehicle steers more than requested	city traffic	city traffic in general	E4	Stronger steering of the vehicle than expected by the driver	Additional hand wheel torque by the driver to compensate for additional Steering Assist Torque	C2	The vehicle leaves the intended path which may lead to a collision with other road users or obstacles	S3	C	Too high (excessive) provision of steering assist torque shall be prevented	EPS shall be deactivated (No steering assist functions active)
C.3	Steering assist	F03 – Provided Steering Assist Torque is less than the requested value and limits	Vehicle steers less than requested	city traffic	city traffic in general	E4	Driver notices a too little steerings assist torque	Controllable in general by the driver	C0	Driving behavior does barely change due to easily compensatable missing steering assist torque	S1	-	Less provision of steering assist torque shall be prevented	EPS shall be deactivated (No steering assist functions active)
C.4	Steering assist	F04 – Steering Assist Torque is applied without a request (eg from the driver or a superordinated system function)	Vehicle moves unintentionally in lateral direction	city traffic	city traffic in general	E4	Driver notices unintentional steering manoveur	Intervention of the driver with hand wheel torque against the assist torque to compensate for additional Steering Assist Torque and keep the lane	C3	The vehicle leaves the intended path which may lead to a collision with other road users or obstacles	S3	D	Unintended provision of steering assist torque shall be prevented	EPS shall be deactivated (No steering assist functions active)
C.5	Steering assist	F05 – Steady Steering Assist Torque is requested but provided Steering Assist Torque is unsteady and varies including a violation of limits	Vehicle moves unintentionally in lateral direction	city traffic	city traffic in general	E4	Driver notices unintentional steering manoveur	Intervention of the driver with hand wheel torque against the assist torque to compensate for additional Steering Assist Torque and keep the lane	C3	The vehicle leaves the intended path which may lead to a collision with other road users or obstacles	S3	D	Oscillating provision of steering assist torque shall be prevented	EPS shall be deactivated (No steering assist functions active)
C.6.1	Steering assist	F06 – Steering Assist Torque is provided in the wrong direction	Steering ability of the vehicle is impaired	city traffic	city traffic in general	E4	Steering of the vehicle is more difficult	Stronger steering required; an average driver is still able to steer	C1	Vehicle could collide with other road users or obstacles (eg when swerving or changing lanes) due to steering behavior which the driver is not used to	S3	B	Provision of steering assist torque in reverse direction of the driver intent (hand wheel torque) shall be overridable	EPS shall be deactivated (No steering assist functions active)
C.6.2	Steering assist	F06 – Steering Assist Torque is provided in the wrong direction	Steering ability of the vehicle is blocked	city traffic	city traffic in general	E4	Steering of the vehicle is blocked	No steering intervention by the driver possible	C3	Driving direction cannot be influenced by the driver which could lead to a collision with other road users or obstacles	S3	D	Blocking of the steering system shall be prevented	EPS shall be deactivated (No steering assist functions active)
C.6.3	Steering assist	F06 – Steering Assist Torque is provided in the wrong direction	Vehicle steers against the intended direction	city traffic	city traffic in general	E4	Vehicle steers against the desired steering direction	No steering intervention by the driver possible	C3	The vehicle leaves the intended path which may lead to a collision with other road users or obstacles	S3	D	Provision of steering assist torque in reverse direction of the driver intent (hand wheel torque) shall be overridable	EPS shall be deactivated (No steering assist functions active)
C.7	Steering assist	F07 – The Steering Assist Torque is provided too late	Vehicle steers more than requested	city traffic	city traffic in general	E4	Driver notices unintentional steering manoveur	Intervention of the driver with hand wheel torque against the assist torque to compensate the additional Steering Assist Torque and keep the lane	C2	Assistance function does not start, driver steers himself, then assistance function starts delayed which may lead to a collision with other road users or obstacles	S3	C	Delayed provision of steering assist torque shall be prevented	EPS shall be deactivated (No steering assist functions active)
R.1	Steering assist	F01 – Steering Assist Torque request is not fulfilled (no torque provided)	Steering ability of the vehicle is impaired	country road, speed up to 80km/h, not divided to opposing lane	free driving with or without opposing traffic, road may be winding	E4	Steering by the driver is impaired and more difficult	Controllable in general by the driver.	C0	Vehicle could collide with other road users or obstacles (eg when swerving or changing lanes) due to steering behavior which the driver is not used to	S3	-	Sudden loss of steering assist torque shall be prevented	EPS shall be deactivated (No steering assist functions active)
R.2	Steering assist	F02 – Provided Steering Assist Torque exceeds the requested value and limits	Vehicle steers more than requested	country road, speed up to 80km/h, not divided to opposing lane	free driving with or without opposing traffic, road may be winding	E4	Stronger steering of the vehicle than expected by the driver	Additional hand wheel torque by the driver to compensate for additional Steering Assist Torque	C2	The vehicle leaves the intended path which may lead to a collision with other road users or obstacles	S3	C	Too high (excessive) provision of steering assist torque shall be prevented	EPS shall be deactivated (No steering assist functions active)
R.3	Steering assist	F03 – Provided Steering Assist Torque is less than the requested value and limits	Vehicle steers less than requested	country road, speed up to 80km/h, not divided to opposing lane	free driving with or without opposing traffic, road may be winding	E4	Driver notices a too little steerings assist torque	Controllable in general by the driver	C0	Driving behavior does not change due to easily compensatable missing steering assist torque	S0	-	Less provision of steering assist torque shall be prevented	EPS shall be deactivated (No steering assist functions active)
R.4	Steering assist	F04 – Steering Assist Torque is applied without a request (eg from the driver or a superordinated system function)	Vehicle moves unintentionally in lateral direction	country road, speed up to 80km/h, not divided to opposing lane	free driving with or without opposing traffic, road may be winding	E4	Driver notices unintentional steering manoveur	Intervention of the driver with hand wheel torque against the assist torque to compensate for additional Steering Assist Torque and keep the lane	C3	The vehicle leaves the intended path which may lead to a collision with other road users or obstacles	S3	D	Unintended provision of steering assist torque shall be prevented	EPS shall be deactivated (No steering assist functions active)
R.5	Steering assist	F05 – Steady Steering Assist Torque is requested but provided Steering Assist Torque is unsteady and varies including a violation of limits	Vehicle moves unintentionally in lateral direction	country road, speed up to 80km/h, not divided to opposing lane	free driving with or without opposing traffic, road may be winding	E4	Driver notices unintentional steering manoveur	Intervention of the driver with hand wheel torque against the assist torque to compensate for additional Steering Assist Torque and keep the lane	C3	The vehicle leaves the intended path which may lead to a collision with other road users or obstacles	S3	D	Oscillating provision of steering assist torque shall be prevented	EPS shall be deactivated (No steering assist functions active)
R.6.1	Steering assist	F06 – Steering Assist Torque is provided in the wrong direction	Steering ability of the vehicle is impaired	country road, speed up to 80km/h, not divided to opposing lane	free driving with or without opposing traffic, road may be winding	E4	Driver notices unintentional steering manoveur	Additional hand wheel torque by the driver to compensate the impaired Steering Assist Torque	C1	Vehicle could collide with other road users or obstacles (eg when swerving or changing lanes) due to steering behavior which the driver is not used to	S3	B	Provision of steering assist torque in reverse direction of the driver intent (hand wheel torque) shall be overridable	EPS shall be deactivated (No steering assist functions active)
R.6.2	Steering assist	F06 – Steering Assist Torque is provided in the wrong direction	Steering ability of the vehicle is blocked	country road, speed up to 80km/h, not divided to opposing lane	free driving with or without opposing traffic, road may be winding	E4	Steering of the vehicle is blocked	No steering intervention by the driver possible	C3	Driving direction cannot be influenced by the driver which could lead to a collision with other road users or obstacles	S3	D	Blocking of the steering system shall be prevented	EPS shall be deactivated (No steering assist functions active)
R.6.3	Steering assist	F06 – Steering Assist Torque is provided in the wrong direction	Vehicle steers against the intended direction	country road, speed up to 80km/h, not divided to opposing lane	free driving with or without opposing traffic, road may be winding	E4	Vehicle steers against the desired steering direction	No steering intervention by the driver possible	C3	The vehicle leaves the intended path which may lead to a collision with other road users or obstacles	S3	D	Provision of steering assist torque in reverse direction of the driver intent (hand wheel torque) shall be overridable	EPS shall be deactivated (No steering assist functions active)
R.7	Steering assist	F07 – The Steering Assist Torque is provided too late	Vehicle steers more than requested	country road, speed up to 80km/h, not divided to opposing lane	free driving with or without opposing traffic, road may be winding	E4	Driver notices unintentional steering manoveur	Intervention of the driver with hand wheel torque against the assist torque to compensate the additional Steering Assist Torque and keep the lane	C2	Assistance function does not start, driver steers himself, then assistance function starts delayed which may lead to a collision with other road users or obstacles	S3	C	Delayed provision of steering assist torque shall be prevented	EPS shall be deactivated (No steering assist functions active)
F.1.1	Steering assist	F06 – Steering Assist Torque is provided in the wrong direction	Steering ability of the vehicle is impaired	Freeway or other controlled access highway with roadway devided by a median	dense traffic with speed of approx 80km/h	E4	Driver notices unintentional steering manoveur	Additional hand wheel torque by the driver to compensate the impaired Steering Assist Torque	C1	Vehicle could collide with other road users or obstacles (eg when swerving or changing lanes) due to steering behavior which the driver is not used to	S3	B	Provision of steering assist torque in reverse direction of the driver intent (hand wheel torque) shall be overridable	EPS shall be deactivated (No steering assist functions active)
F.1.2	Steering assist	F06 – Steering Assist Torque is provided in the wrong direction	Steering ability of the vehicle is blocked	Freeway or other controlled access highway with roadway devided by a median	dense traffic with speed of approx 80km/h	E4	Steering of the vehicle is blocked	No steering intervention by the driver possible	C3	Driving direction cannot be influenced by the driver which could lead to a collision with other road users or obstacles	S3	D	Blocking of the steering system shall be prevented	EPS shall be deactivated (No steering assist functions active)
F.1.3	Steering assist	F06 – Steering Assist Torque is provided in the wrong direction	Vehicle steers against the intended direction	Freeway or other controlled access highway with roadway devided by a median	dense traffic with speed of approx 80km/h	E4	Vehicle steers against the desired steering direction	No steering intervention by the driver possible	C3	The vehicle leaves the intended path which may lead to a collision with other road users or obstacles	S3	D	Provision of steering assist torque in reverse direction of the driver intent (hand wheel torque) shall be overridable	EPS shall be deactivated (No steering assist functions active)

Safety Goal		ASIL
SG01	Sudden loss of steering assist torque shall be prevented	QM
SG02	Too high (excessive) provision of steering assist torque shall be prevented	C
SG03	Less provision of steering assist torque shall be prevented	QM
SG04	Unintended provision of steering assist torque shall be prevented	D
SG05	Oscillating provision of steering assist torque shall be prevented	D
SG06	Provision of steering assist torque in reverse direction of the driver intent (hand wheel torque) shall be overridable	D
SG07	Delayed provision of steering assist torque shall be prevented	C

Anhang 2 - HAZOP

Potential malfunctions based on the functional behavior of the EPS / HAZOP														
	Guideword	**NO / NOT**	**MORE**	**LESS**	**AS WELL AS**	**PART OF**	**Unintended**	**Interrupt / Frozen**	**OTHER THAN**	**REVERSE**	**EARLY**	**LATE**	**BEFORE**	**AFTER**
Function	**Description**	Complete negation of the design intent, no part of the intention is achieved	Quantitative increase	Quantitative decrease	Qualitative increase, all the design intention is achieved together with additions	Qualitative decrease, only some of the design intention is achieved	Activation without request	Partly negation of the design intent	Complete substitution, where no part of the original intention is achieved but something quite different happens	Logical opposite of the design intent	Relative to the clock time happens earlier	Relative to the clock time happens later	Relating to order or sequence, before it is expected	Relating to order or sequence, after it is expected
Steering assist	Provides steering assist depending on vehicle speed	Steering Assist Torque request is not fulfilled (no torque provided)	Provided Steering Assist Torque exceeds the requested value and limits	Provided Steering Assist Torque is less than the requested value and limits	n.a	n.a	Steering Assist Torque is applied without a request (e.g. from the driver or a superordinated system function)	Steady Steering Assist Torque is requested but provided torque is unsteady and varies including a violation of limits	n.a	Steering Assist Torque is provided in the wrong direction	n.a	The Steering Assist Torque is provided too late	n.a	n.a
Consequence	Consequences at vehicle level	Driver needs to apply more force to steer	Potential lane departure	Increased steering effort by the driver	n.a	n.a	Active risk of a dangerous situation for the driver and the environment	Active risk of a dangerous situation for the driver and the environment	n.a	Active risk of a dangerous situation for the driver and the environment	n.a	Active risk of a dangerous situation for the driver and the environment	n.a	n.a

F01 – Steering Assist Torque request is not fulfilled (no torque provided)
F02 – Provided Steering Assist Torque exceeds the requested value and limits
F03 – Provided Steering Assist Torque is less than the requested value and limits
F04 – Steering Assist Torque is applied without a request (e.g. from the driver or a superordinated system function)
F05 – Steady Steering Assist Torque is requested but provided torque is unsteady and varies including a violation of limits
F06 – Steering Assist Torque is provided in the wrong direction
F07 – The Steering Assist Torque is provided too late

Anhang 3 – Situationskatalog und Situationsanalyse

Situation Catalog

No.	Situational category (operating mode)	Situation/ critical operation phase	Relvant for EPS/ Steering system	E-class based on duration (e.g. 10%)	E-class based on frequency (e.g. 2 times a day)	Worst case
S.0	Workshop	Maintanence by worker (e.g. checking oil level, changing oil, changing wheels, changing starter battery, jump-starting)	yes	E1	E1	E1
S.1	city traffic	city traffic in general	yes	E4	E4	E4
S.1.1	city traffic	car driving in front steps out of lane / turns	no	E2	E4	E4
S.1.2	city traffic	bicycle driving behind car	no	E2	E2	E2
S.2	country road, speed up to 80km/h, not divided to opposing lane	free driving with or without opposing traffic, road may be winding	yes	E4	E4	E4
S.2.1	country road, speed up to 80km/h, not divided to opposing lane	passing an intersection or a side road	no	E2	E4	E4
S.2.2	country road, speed up to 80km/h, not divided to opposing lane	passing, critical point where passing vehicle cannot move back in behind passed vehicle	no	E2	E2	E2
S.3	Freeway or other controlled access highway with roadway devided by a median	dense traffic with speed of approx. 80km/h	yes	E3	E4	E4
S.3.1	Freeway or other controlled access highway with roadway devided by a median	approaching unexpected traffic jam	no	E1	E2	E2
S.3.2	Freeway or other controlled access highway with roadway devided by a median	free driving with high speed (>180km/h)	no	E2	E3	E3

Situation Analysis

No.	Situational category	Operating Situations / Considered Malfunctions (Failures)	Exposure	F01 – Steering Assist Torque request is not fulfilled (no torque provided)	F02 – Provided Steering Assist Torque exceeds the requested value and limits	F03 – Provided Steering Assist Torque is less than the requested value and limits	F04 – Steering Assist Torque is applied without a request (e.g. from the driver or a superordinated system function)	F05 – Steady Steering Assist Torque is requested but provided torque is unsteady and varies including a violation of limits	F06 – Steering Assist Torque is provided in the wrong direction	F07 – The Steering Assist Torque is provided too late
S.0	Workshop	Maintanence by worker e.g. checking axle parts, oil level, changing oil, changing wheels, changing starter battery, jump-starting,	E2	-	-	-	A.1	-	-	-
S.1	city traffic	city traffic in general	E4	C.1	C.2	C.3	C.4	C.5	C.6.1 C.6.2 C.6.3	C.7
S.1.1	city traffic	car driving in front steps out of lane / turns	E4	covered by (city traffic in general)	covered by (city traffic in general)	covered by (city traffic in general)	covered by (city traffic in general)	covered by (city traffic in general)	covered by (city traffic in general)	covered by (city traffic in general)
S.1.2	city traffic	bicycle driving behind car	E2	covered by (city traffic in general)	covered by (city traffic in general)	covered by (city traffic in general)	covered by (city traffic in general)	covered by (city traffic in general)	covered by (city traffic in general)	covered by (city traffic in general)
S.2	country road, speed up to 80km/h, not divided to opposing lane	free driving with or without opposing traffic, road may be winding	E4	R.1	R.2	R.3	R.4	R.5	R.6.1 R.6.2 R.6.3	R.7
S.2.1	country road, speed up to 80km/h, not divided to opposing lane	passing an intersection or a side road	E4	covered by (free driving with or without opposing traffic, road may be winding)	covered by (free driving with or without opposing traffic, road may be winding)	covered by (free driving with or without opposing traffic, road may be winding)	covered by (free driving with or without opposing traffic, road may be winding)	covered by (free driving with or without opposing traffic, road may be winding)	covered by (free driving with or without opposing traffic, road may be winding)	covered by (free driving with or without opposing traffic, road may be winding)
S.2.2	country road, speed up to 80km/h, not divided to opposing lane	passing, critical point where passing vehicle cannot move back in behind passed vehicle	E2	covered by (free driving with or without opposing traffic, road may be winding)	covered by (free driving with or without opposing traffic, road may be winding)	covered by (free driving with or without opposing traffic, road may be winding)	covered by (free driving with or without opposing traffic, road may be winding)	covered by (free driving with or without opposing traffic, road may be winding)	covered by (free driving with or without opposing traffic, road may be winding)	covered by (free driving with or without opposing traffic, road may be winding)
S.3	Freeway or other controlled access highway with roadway devided by a median	dense traffic with speed of approx. 80km/h	E4	-	-	-	-	-	F.1.1 F.1.2 F.1.3	-
S.3.1	Freeway or other controlled access highway with roadway devided by a median	approaching unexpected traffic jam	E2	-	-	-	-	-	covered by (dense traffic with speed of approx. 80km/h)	-
S.3.2	Freeway or other controlled access highway with roadway devided by a median	free driving with high speed (>180km/h)	E3	-	-	-	-	-	covered by (dense traffic with speed of approx. 80km/h)	-

Anhang 4 - System - FMEA

System - FMEA

System: Function/ Task:	Created by:	Date:	Reviewed:	Responsible person:
Electric power steering Provide steering and steering assist	Berke Ertugrul	13.03.2022	28.03.2022 07.04.2022	Berke Ertugrul

Potential Failure	Potential Effects of Failures	Potential Causes of Failure	Prevention controls	Detection controls	Current status					Recommended actions	Responsibility	Improved			
					O	S	D	RPN	SxO		Actions taken	O	S	D	RPN
excessive provision of steering assist torque	loss of lateral vehicle stability	Motor supplies too much torque to the pump	correct design of the motor, with the corresponding equations regarding the magnetic field and number of windings	Torque measurement of the motor/ recording the motor curve	3	10	3	90	30						
excessive provision of steering assist torque	loss of lateral vehicle stability	Pump input torque / pump generates too much pressure	correct selection of the pump with the corresponding formulas regarding the moment/ pressure	Absorption of the pressure via the pump torque	3	10	3	90	30						
excessive provision of steering assist torque	loss of lateral vehicle stability	too large cylinder	construction must consider exactly how the cylinder is to be designed at the beginning, e.g. exact formulas to calculate	Steering torque absorption via pump pressure	3	10	3	90	30						
excessive provision of steering assist torque	loss of lateral vehicle stability	too high motor current	correct design of the electrical circuit	Corresponding measurements	3	10	3	90	30						
excessive provision of steering assist torque	loss of lateral vehicle stability	wrong sensor signals	correct design of the corresponding sensors	Component test	4	10	2	80	40						
excessive provision of steering assist torque	loss of lateral vehicle stability	wrong Can signals	use of known security measures e.g. end to end protection	Integration test	5	10	2	100	50						
excessive provision of steering assist torque	loss of lateral vehicle stability	wrong software calculation	Coding guideline, reuse of well known code	Correct software tests	6	10	2	120	60						

O=Occurence Probability of Failure		S=Severity Severity of Effect		D=Detection Opportunity for Detection		RPN=Risk priority number RPN = O x S x D	
Very Low	1	Very Low	1	Very High	1	No risk and no need for action	1
Low	2-3	Low	2-3	High	2-3	Minimal acceptable risk, there is no	2<50
Moderate	4-6	Moderate	4-6	Moderate	4-6	Medium risk, action should be	50<125
High	7-8	High	7-8	Low	7-8	High risk and urgent need for action	125<1000
Very High	9-10	Very High	9-10	Very Low	9-10		

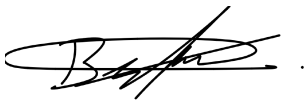
Haftungsausschluss

Diese Arbeit dient ausschließlich zur Qualifikation im generischen Studiengang *Sicherheitstechnik*. Diese Arbeit ersetzt kein Gutachten einer oder eines Sachverständigen. Die Prüfer dieser Arbeit sind keine Sachverständigen des diskutierten Anwendungsgebiets. Die Prüfer weisen darauf hin, dass eine Begutachtung der Betrachtungseinheit inklusive deren Dokumentation durch Sachverständige zwingend erforderlich ist.

Ehrenwörtliche Erklärung

Hiermit versichere ich, dass die vorliegende Arbeit von mir selbstständig und ohne unerlaubte Hilfe angefertigt worden ist, insbesondere dass ich alle Stellen, die wörtlich oder annähernd wörtlich aus Veröffentlichungen entnommen sind, durch Zitate als solche gekennzeichnet habe. Ich versichere auch, dass die von mir eingereichte schriftliche Version mit der digitalen Version übereinstimmt. Weiterhin erkläre ich, dass die Arbeit in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde oder Prüfungsstelle vorgelegen hat. Ich erkläre mich damit einverstanden, dass die Arbeit der Öffentlichkeit zugänglich gemacht wird. Ich erkläre mich damit einverstanden, dass die Digitalversion dieser Arbeit zwecks Plagiatsprüfung auf die Server externer Anbieter hochgeladen werden darf. Die Plagiatsprüfung stellt keine Zurverfügungstellung für die Öffentlichkeit dar.

Velbert, 29. April 2022



Berke Ertugrul