SOTIF
BEDEUTUNG DER SOLLFUNKTION IN DER SERIENENTWICKLUNG

Herr Dr.-Ing. René S. Hosse[1], Herr Dipl.-Ing. (FH) Peter Krumbach[2]

[1] Director Assessment Service Center, Prokurist
Fa. ESE Engineering and Software-Entwicklung GmbH,
Part of DB E.C.O. Group
Am Alten Bahnhof 16
D-38122 Braunschweig
rene.hosse@ese.de

[2] Senior Functional Safety Manager
Fa. ESE Engineering and Software-Entwicklung GmbH,
Part of DB E.C.O. Group
Moosacher Strasse 82
D-80809 München
peter.krumbach@ese.de

Keywords: Automotive, Safety, SOTIF, Sollfunktion, Funktionale Sicherheit, Serienentwicklung

ABSTRACT

Der größte Teil von Verletzungen im Automobil geschehen augenscheinlich in der Bedienung und Nutzung der Soll-Funktionen und nicht im Zusammenhang mit dem Auftreten von Fehlfunktionen. Weder zufällige Hardwarefehler, noch systematische Fehler in Fahrzeugsystemen sind signifikant für Unfälle oder Verletzungen im Fahrzeug wie z.B., Klemmen, Stoßen, Verbrennungen oder eine Fehlbedienung. Fahrunfälle sind nur selten einem Fahrzeugfehler geschuldet und entstehen erst durch das Zusammenspiel aus Fahrer, Fahrzeug und Fahrumgebung. Konsequent sollte sich das Verhältnis der Entwicklungsaufwendungen zur sicherheitsorientierten Systementwicklung in den drei Disziplinen Funktionale Sicherheit, Gebrauchssicherheit und Automotive Cybersecurity in einem erforderlichen, der Unfallhäufigkeit geschuldeten, entsprechenden Verhältnis stehen. So macht es den Anschein, dass in dem methodischen Vorgehen und in der Auslegung der Sollfunktion ein Aufholbedarf gegenüber der Funktionalen Sicherheit (ISO 26262) ansteht. Dieser Beitrag motiviert einen verstärkten ingenieurwissenschaftlichen Einsatz bei der Auslegung und Entwicklung der Sollfunktion im Hinblick auf den Faktor Mensch und zeigt die Anwendungsmöglichkeiten der aktuellen Norm ISO 21448 (Road vehicles: Safety of the intended functionality).

1 MOTIVATION

Seit 2011 ist die Norm ISO 26262 zur sicherheitsgerichteten Entwicklung von elektrisch/elektronischen Komponenten in der Automobilindustrie eingeführt und findet in der Second Edition aus dem Jahr 2018 ihre Novellierung und Weiterentwicklung. Im Zuge dessen hat sich insbesondere der Fokus der darin betrachteten Gefährdungen (engl. Hazards) dahingehend weiterentwickelt, dass systematische und zufällige Fehler als Gefährdungsursache herangezogen werden, vgl. Tabelle 1. Der vorhersehbare Fehlgebrauch ist größtenteils aus der Norm verschwunden, welcher noch in der 2011er Version betrachtet werden sollte, vgl. ISO26262:2011 Part 3 [ISO26262].

Insbesondere der vorhersehbare Fehlgebrauch und die Auslegung der eigentlichen Sollfunktion stellen die Hauptursache von Verletzungen und Unfällen dar. So sind Unfälle, bei denen es aufgrund von technischen Fehlern zu Sachschäden oder Verletzungen kam, sehr gering, wenn auch die Entwicklung der Automobilindustrie einen Großteil der Entwicklungskosten und zeitlichen

Aufwendungen auf die sog. Funktionale Sicherheit gemäß ISO 26262 legt. Zur Untermauerung der Entwicklungsaufwendungen „Sichere Sollfunktion kontra Vermeidung sowie Beherrschung von Fehlfunktionen“ wird hier eine Statistik aus der DESTATIS herangezogen, siehe Abbildung 1. Die Statistik zeigt, dass die fahrzeugbezogenen Ursachen (Funktionale Sicherheit) mit nur einem Prozent die geringste Anzahl als Unfallursache ausmachen. Wohingegen das Bedienen der Sollfunktion im Kontext der menschlichen Fehlbedienung oder das falsche Einschätzen der Leistungsgrenzen im Fahrzeug mit fast 90% die Hauptursache am Unfallgeschehen im Straßenverkehr ausmacht.

Tabelle 1: Vergleich der Anforderungen an die Gefährdungs- und Risikoanalyse zwischen ISO 26262:2011 und ISO 26262:2018

ISO 26262:2011		ISO 26262:2018[a]	
3–7.4.2.2.1	The hazards shall be determined systematically ~~by using adequate techniques~~	3–6.4.2.2	The hazards shall be determined systematically **based on the possible malfunctioning behaviour of the item**
3–7.4.2.2.2	Hazards shall be defined ~~in terms of the conditions or behaviour that can be observed~~ at the vehicle level	3–6.4.2.3	Hazards **caused by malfunctioning behaviour of the item** shall be defined at the vehicle level

Der Normentwurf ISO PAS 21448 übernimmt den aus der Novellierung der ISO 26262 entfallenen Fokus auf die Auslegung der Sollfunktion und den vorhersehbaren Fehlgebrauch und stellt einen ersten Ansatz für einen strukturierten Entwicklungsprozess vor, bei dem auf Basis fundierter Methoden Maßnahmen für einen sicheren Fahrzeugbetrieb auch unter Einfluss von vorhersehbarem Fehlgebrauch und eine dem Einsatzzweck entsprechenden Auslegung der Sollfunktion stattfindet.

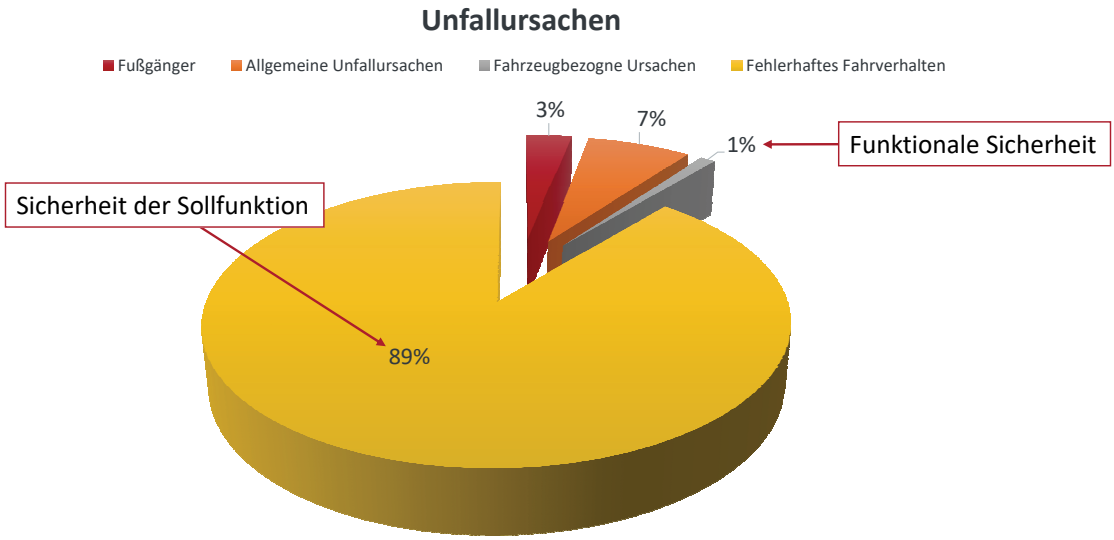

Abbildung 1: Unfallursachen gemäß destatis 2021

2 DIFFERENZIERUNG ZWISCHEN FUNKTIONALER SICHERHEIT, SOTIF, CYBERSECURITY

Aus der Perspektive der Ingenieurwissenschaft heraus wird Sicherheit in der Regel definiert als „Freiheit von nicht akzeptierten Risiken“. Bei näherer Betrachtung bedarf jedoch dieser abstrakte Sicherheitsbegriff einer Konkretisierung, da sich in gegenwärtigen Standardisierungsaktivitäten für den umfassenden Begriff der „Sicherheit“ verschiedene Teilbegriffe herauskristallisiert haben, die jeweils für sich genommen unterschiedliche Beiträge zum übergeordneten Ziel „sicherer“ Fahrzeuge

leisten können. Folgende Abbildung zeigt die Begrifflichkeiten „Funktionale Sicherheit“, „Sicherheit der Sollfunktion“ und „Cybersecurity“ in ihren Abhängigkeiten und aktuell bekannten Einstufungen der Normentwürfe. Folgend wird kurz auf die grundlegenden Abgrenzungen eingegangen:

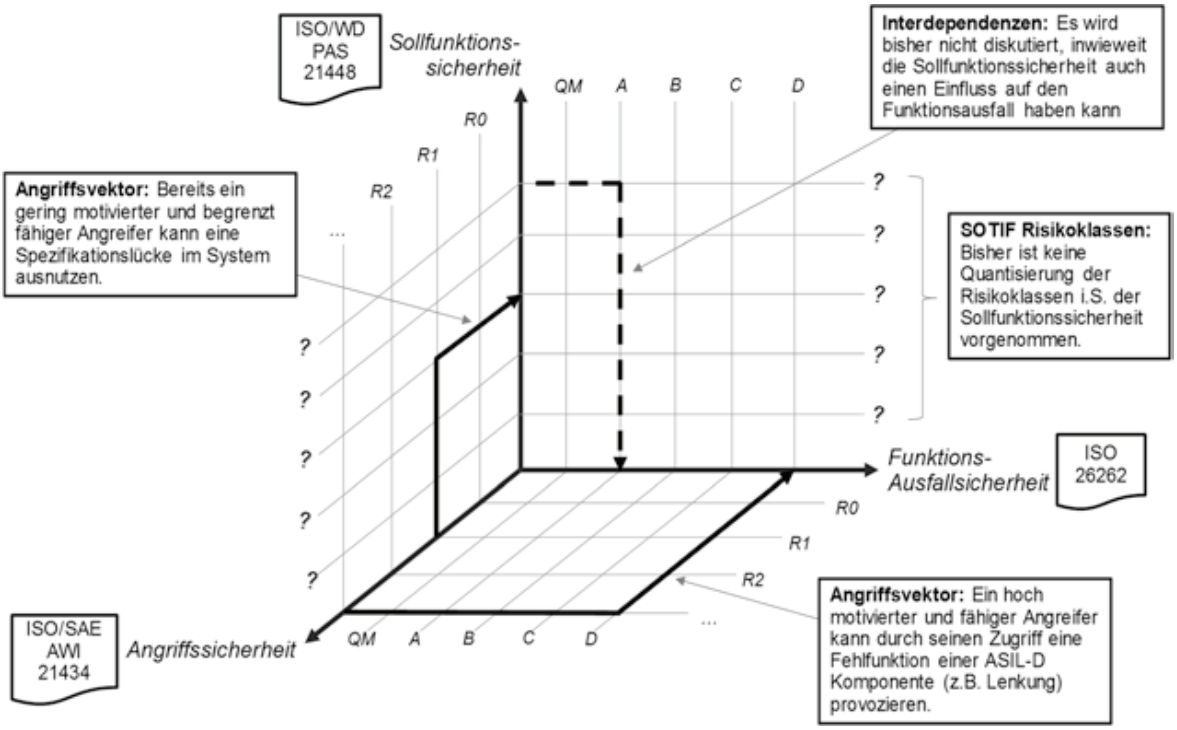

Abbildung 2: Zusammenhang der Funktionalen Sicherheit, Sicherheit der Sollfunktion und Cybersecurity

2.1 Funktionale Sicherheit gemäß ISO 26262

Funktionale Sicherheit ist der Teil der Sicherheit, der von der korrekten Funktion des sicherheitsbezogenen Systems und anderen risikomindernden Maßnahmen (d. h. identifizierten Gefährdungen und aus diesen abgeleitete Sicherheitsfunktionen) abhängt. Ziel ist es, den potenziellen Funktionsausfall im Sinne zufälliger und systematischer Fehler zu bewerten und geeignete Maßnahmen zur Fehlervermeidung umzusetzen. Auf diese Weise wird das Restrisiko auf ein gesellschaftlich akzeptiertes Maß reduziert. Die Funktionale Sicherheit wird umfassend in der ISO 26262 beschrieben.

Definition 3.67
functional safety: absence of unreasonable risk (3.176) due to hazards (3.75) caused by malfunctioning behaviour (3.88) of E/E systems (3.40) [ISO 26262]

2.2 Cybersecurity gemäß ISO 21434

Cybersecurity zielt auf die Verhinderung der Kompromittierung von Sicherheitsfunktionen ab. Hierbei steht der Schutz des betrachteten sicherheitsrelevanten elektronischen Steuerungssystems vor Gefahren aus der Systemumwelt im Vordergrund. Bedrohungsvektoren wirken von außen auf das betrachtete sicherheitsrelevante elektronische Steuerungssystem ein und können dessen korrekte Funktionsweise negativ beeinflussen. Aktuell wird auch von der sog. Operational Technology als Fokus der Cybersecurity gesprochen. Hier findet eine Differenzierung von dem Begriff der klassischen IT Security statt, welche den Fokus auf den Schutz von örtlich fest installierter IT Infrastruktur thematisiert.

Definition 3.1.8 CYBERSECURITY
Road Vehicle Cybersecurity Condition in which assets (3.1.1) are sufficiently protected against threat scenarios to electrical or electronic components of road vehicles and their functions. [ISO 21434]

Normativ wird für die Automobilindustrie dieser Aspekt der Sicherheit in dem Normungsvorhaben der ISO 21434 abgehandelt und steht in einer ersten Version zur Verfügung. Der Gegenstand der Cybersecurity wird in diesem Beitrag nicht weiter behandelt.

2.3 Sicherheit der Sollfunktion (SOTIF) gemäß ISO 21448

Die *Gebrauchssicherheit* betrachtet die vom betrachteten System zu erbringende Sicherheit der Sollfunktion, oder auch Sollfunktionssicherheit. Hierbei dürfen bei bestimmungsgemäßem Gebrauch oder zu erwartendem Fehlgebrauch keine intolerablen Personengefährdungen vom betrachteten System ausgehen und die Funktion muss entsprechend dem Einsatzzweck ausreichend leistungsfähig sein (Performance). Es können Gefährdungen durch eine unvollständige Spezifikation oder einen zu erwartenden (Fehl-)Gebrauch der Funktionen entstehen.

Der Gegenstand der Sollfunktionssicherheit wird aktuell im internationalen Normungsvorhaben der ISO 21448 erarbeitet, weiter ausdifferenziert und bildet die Grundlage der in diesem Artikel getroffenen Empfehlungen zur konsequenteren Umsetzung der in der Norm formulierten Entwicklungsmethoden.

Definition: 3. 10 Safety Of The Intended Functionality SOTIF
absence of unreasonable risk due to hazards resulting from functional insufficiencies of the intended functionality or from reasonably foreseeable misuse by persons [ISO 21448]

3 ABGRENZUNG ZWISCHEN „ZU ERWARTENDER FEHLGEBRAUCH“ UND „MISSBRAUCH“

Der häufig (50-mal) in der ISO PAS 21448 zitierte Begriff des „misuse“ stellt im Kontext der Produkthaftung eine große Herausforderung dar. In der europäischen und nordamerikanischen Rechtsprechung sowie in der gesellschaftlichen Akzeptanz ist die Unterscheidung von Missbrauch zu Fehlgebrauch ein wichtiger Faktor:

- Bei dem *Missbrauch* einer Funktion wird dem Nutzer eine böse Absicht unterstellt. Der Nutzer handelt bewusst entgegen der Bedienungsanleitung und hebelt die Funktionsauslegung aus.
- Beim *Fehlgebrauch* ist eher von einer „unabsichtlichen“ Fehlhandlung auszugehen. Ein Missbrauch steht hier also im Gegensatz zum Fehlgebrauch außerhalb des Fokus der Produkthaftung und ist in der Auslegung der Funktion auch nur schwer zu verhindern, schwer zu beherrschen und nach Schadenseintritt schwer zu belegen.

Die Herausforderung besteht folglich darin, die Unterscheidung von Fehlgebrauch und Missbrauch des Funktionsnutzers zu definieren und im Schadensfall zu belegen. In der folgenden Darstellung werden Schlagworte aus einschlägigen Normen zum Thema Missbrauch und Fehlgebrauch, entsprechend eingruppiert.

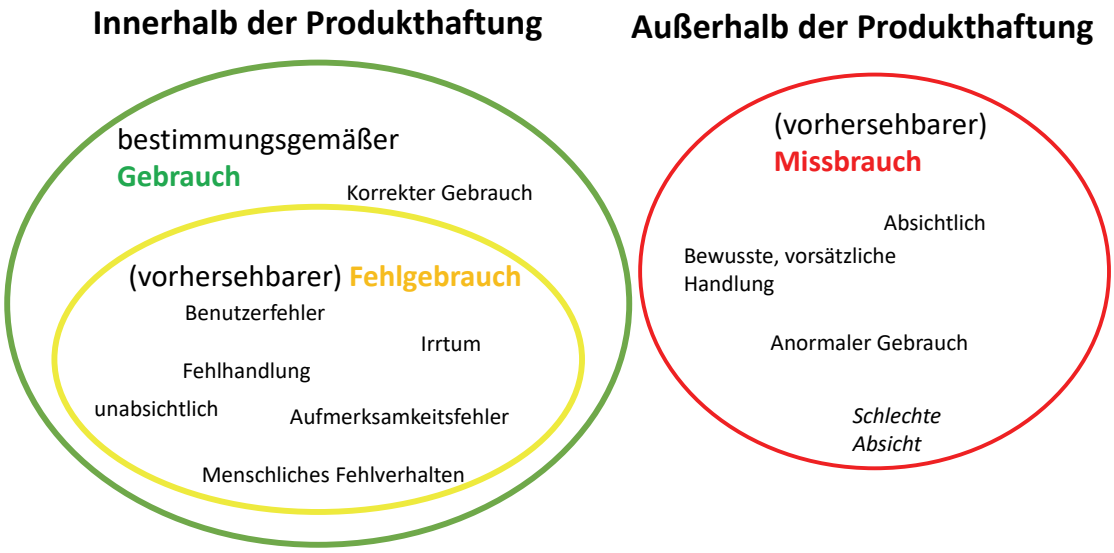

Abbildung 3: Gruppierung der Begrifflichkeiten Fehlgebrauch und Missbrauch, nach (Johner 2021)

Ein weiterer Ansatz, die Unterscheidungsmerkmale des Fehlgebrauchs zum Missbrauch zu identifizieren, wird im folgenden Ablaufdiagramm dargestellt: Dieses Ablaufdiagramm wird in der Medizintechnik herangezogen, um den bestimmungsgemäßen, den Fehl-, oder Missbrauch zu ermitteln (Johner 2021).

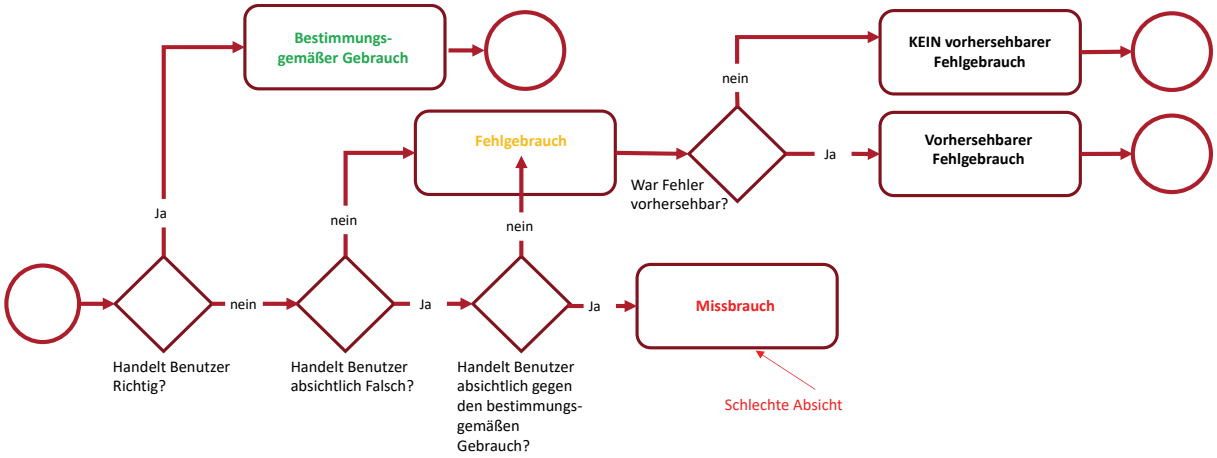

Figure 4: Ablaufdiagramm zur Unterscheidung von Fehlgebrauch und Missbrauch in Anlehnung an (Johner 2021)

Basierend auf den zuvor getroffenen Differenzierungen zwischen Fehlgebrauch und Missbrauch steht der vorhersehbare Fehlgebrauch im Fokus der Sollfunktion, da dieser insbesondere produkthaftungsrechtliche Konsequenzen für die Hersteller beinhaltet.

4 NORMVORHABEN ISO 21448

Während bei der Konzeption eines Fahrzeugs die sog. fahrererlebbaren Funktionen im Vordergrund stehen und Ausgangslage für weitere Entwicklungs- und Analysetätigkeiten darstellen (z.B. Hazard Analysis and Risk Assessment gemäß ISO 26262), stellen genau diese fahrererlebbaren Funktionen ebenso die Ausgangslage für SOTIF dar, vgl. Abbildung 5.

"[ISO 21448] is intended to be applied to intended functionality where proper situational awareness is critical to safety, and where that situational awareness is derived from complex sensors and processing algorithms; especially emergency intervention systems (e.g. emergency braking systems) and Advanced Driver Assistance Systems (ADAS) with levels 1 and 2 on the OICA/SAE standard J3016 automation scales." [ISO 21448]

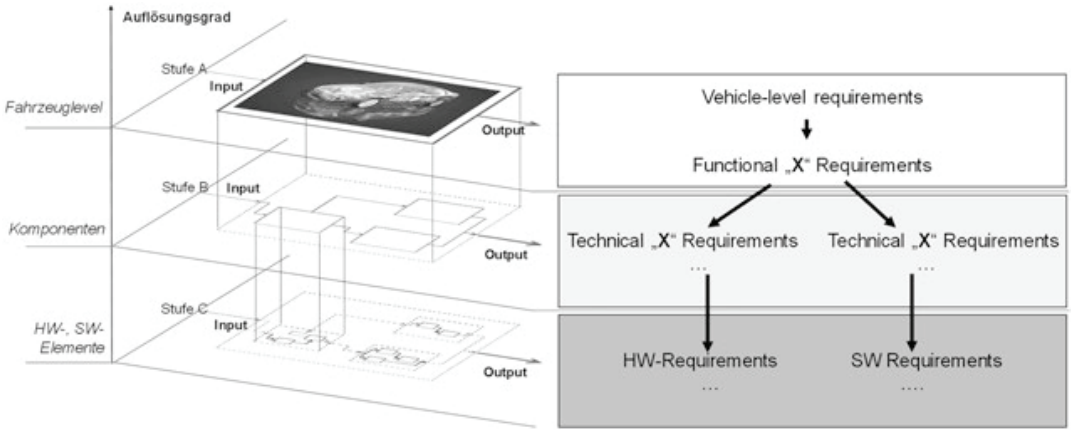

Abbildung 5: Betrachtungslevel von SOTIF

Gemäß der o.g. Definition wird wiederum eine Einschränkung von SOTIF auf Funktionen gelegt, welche eine dezidierte Umfeldwahrnehmung zur Funktionserfüllung nutzen. Damit wird das Potenzial, welches ein stringentes SOTIF Vorgehen für die Funktionsqualität und Nutzerakzeptanz beinhaltet, nicht ausgeschöpft.

Der im aktuellen Normvorhaben vorgeschlagene Lebenszyklus sieht wie folgt aus:

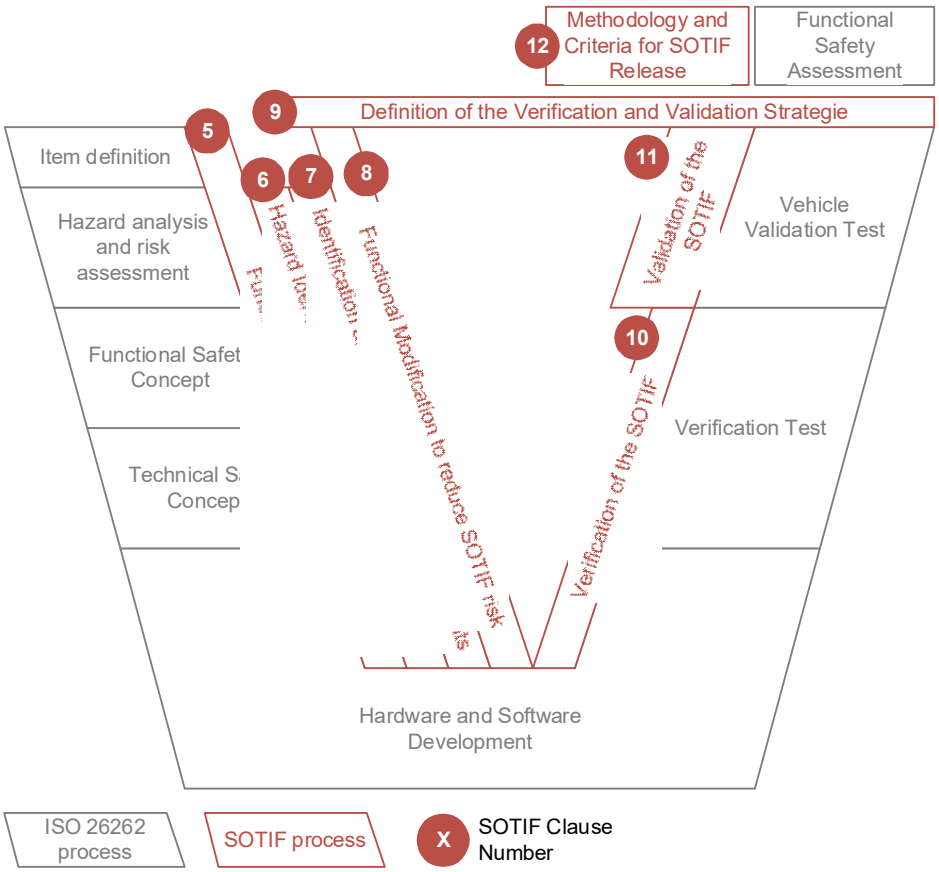

Abbildung 6: SOTIF Lebenszyklus gemäß ISO 21448

Wie bereits deutliche wurde, fokussiert sich SOTIF auf die Entwicklungsaktivitäten in der Konzeptphase, sowie in der Systementwicklung und insb. auf die Verifikations- und Validierungsstrategien. Es gibt keine separaten Anforderungen an die Entwicklung von Hardware, Software oder mechanischen Komponenten der Funktion.

Insgesamt schafft der SOTIF Standard somit eine Abrundung des normativen Kontexts im Bezug auf die Erfüllung der Sicherheit einer Funktion. Durch SOTIF sind insgesamt höhere Qualitäten in der Sollfunktion zu erwarten und gerade im Bereich der Fahrerassistenzen sollte dies zu einer gesteigerten Nutzerakzeptanz führen. Auf der anderen Seite wird anhand des Standards auch deutlich, dass bisher eine Quantifizierung des SOTIF Risikos, vergleichbar mit einer ASIL Einstufung (Automotive Safety Integrity Level) nach ISO 26262, nicht enthalten ist. Das aus der Sollfunktion entstehende Risiko für die Sicherheit gibt folglich keine Vorgaben an die Entwicklungsaktivitäten im Rahmen der Systementwicklung.

Die Chancen, welche sich auf Basis des neuartigen Verständnisses durch SOTIF ergeben, liegen auf der Hand: Wie die Statistiken zeigen, liegt ein Großteil der Unfälle in der Sollfunktion, welche bisher nur spärlich strukturiert seitens der ISO 26262 erarbeitet werden und insb. durch die Novellierung vollständig entfallen sind. Der Fokus der Aktivitäten von SOTIF liegt primär in der Konzeptphase. Eine höhere Qualität in der Auslegung der Sollfunktion und der damit einhergehenden Gefährdungs- und Risikoanalyse generiert umfangreich neue Anforderungen für die Entwicklung, welche sicherlich zufriedenstellend durch den sicherheitsgerichteten Prozess gemäß ISO 26262 in den eigentlichen Entwicklungsaktivitäten abgehandelt werden können.

Gleichfalls treibt das Normungsgremium einen Entwicklungsansatz zu standardisieren, welcher wenig in der Praxis erprobt ist und selbst grundlegende Analysemethoden seitens der Fachliteratur noch nicht vollständig erarbeitet sind. Daher empfehlen die Autoren die folgenden Konzepte zur Erarbeitung der Sollfunktion anzusetzen.

5 KONZEPT ZUR STRUKTURIERTEN ERARBEITUNG DER SOLLFUNKTION

5.1 Integration des Menschen als Funktionsbestandteil in die SOTIF-Analyse

Da SOTIF den Fokus auf den vorhersehbaren Fehlgebrauch legt und gezeigt werden konnte, dass ein Großteil der Unfallursachen in der Sollfunktion und nicht im Funktionsausfall liegt, bedarf es einer stringenteren Integration des Menschen als integralen Funktionsbestandteil in den Betrachtungen der Konzeptphase.

Dies kann primär im Rahmen der sog. SOTIF-Analyse erfolgen und gemäß folgender schematischer Darstellung erarbeitet werden:

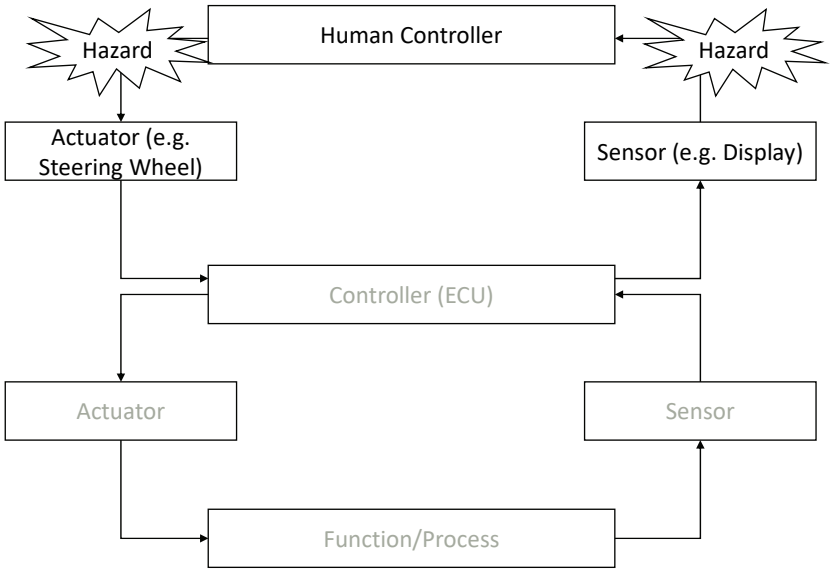

Figure 7: Integration des Menschen in die Funktionsbeschreibung

Die Gefährdungs- und Risikoanalyse gemäß der ISO 26262 erarbeitet die möglichen Gefährdungen einer Funktion auf Basis der fahrererlebbaren Funktionen. Hierbei wird die vom Fahrzeug bereitgestellte Funktion analysiert. Es wird wiederum nicht betrachtet, welche Funktionalität der Fahrer bzw. der Funktionsnutzer aufbringen muss, damit es zu einer sicherheitsgerechten Funktionserfüllung kommt.

Die Integration des Funktionsnutzers als Teil der Funktion ermöglicht den vorhersehbaren Fehlgebrauch systematisch zu erarbeiten und hier ebenso Sicherheitsziele (oder SOTIF-Ziele) zu definieren. Ein oben benanntes Vorgehen würde direkt mit Anforderungen an die Ausgestaltung und Umsetzung der Funktion einhergehen und damit auch den möglichen Ausfall des Funktionsnutzers (Fehlgebrauch) als Entwicklungsziel berücksichtigen.

5.2 Quantifizierung des Risikos der Sollfunktion in Anlehnung an die ISO 26262 der ASIL Einstufung über E, C und S.

In der ISO PAS 21448 wird die Einstufung der Gefährdung der Funktion über Szenarien in Anlehnung an die ISO 26262 Band 3 und im Zusammenhang mit der Anwendung einer HARA beschrieben. Die Bewertung des E-Wertes, also die Exposition, benötigt jedoch eine Fallunterscheidung:

- E (keine Fallunterscheidung vorhanden)
- C (ab Automatisierungslevel L3 für hochautomatisiertes Fahren immer „3“)
- S (ggf. Sachschaden oder Funktionsverhalten im Sinne Nutzerakzeptanz)

Der Grad der Gefährdung kann in Anlehnung an das methodische Vorgehen einer HARA nach ISO 26262 eingestuft werden, indem die Kennzahlen der Schadensschwere „S“ sowie die Kontrollierbarkeit der Schadenabwehr „C“ bewertet werden. Eine Häufigkeit der Funktionsnutzung oder eine Quantifizierung über das Befinden in der gefährlichen Situation (Exposition) „E“ ist jedoch schwer anzuwenden.

Wenn die Sollfunktion hinsichtlich ihrer Gefährdung bewertet wird, geht die Betrachtung davon aus, dass diese Funktion gerade genutzt wird (immer = E4). Sollte beispielsweise eine automatische Notbremsfunktion (AEB) in ihrer Sollfunktion bewerten werden, wird ein Szenario beschrieben, in dem die Funktion zur Wirkung kommt. Liegt in dem Fall eine Performance-Grenze in einem Verzögerungswert der Bremse vor, für ein hergeleitetes Szenario, in dem das Ego-Fahrzeug nicht rechtzeitig zum Stehen kommt (zu dicht für die Delta-Geschwindigkeit), wird diese Eintrittswahrscheinlichkeit <u>immer</u> in dem beschriebenen Szenario so sein. Da wäre es gegen die empfundene Sicherheitskultur die Aufenthaltswahrscheinlichkeit in der Situation (E-Wert) zur Herabsetzung der Gefährdung heran zu ziehen.

Eine stringente Quantifizierung des E-Wertes ist damit massiv erschwert und kann nicht in dem vom Normvorhaben vorgenommen Vorgehen umgesetzt werden.

5.3 Erweiterung des Scopes auf alle Funktionen (Bestandsfunktionen) im Fahrzeug

Ein Ungleichgewicht zwischen sollfunktionsresultierenden Unfällen und den von Systemfehlern basierten Unfällen rechtfertigt die Bestandsfunktionen, und nicht ausschließlich Funktionen mit umfassender Umfeldwahrnehmung, in einem methodischen Vorgehen in Anlehnung an die SOTIF zu durchleuchten.

Die ISO PAS 21448 weist im Kapitel „Scope“ jedoch darauf hin, dass sie in ihrer Anwendung für primär teilautomatisierte Funktionen eine Anwendung findet. Besonders im Fokus sollten auch innerhalb der Funktionalen Sicherheit alle elektronischen (Bestands-)Funktion in einer HARA bewertet werden.

9 ZUSAMMENFASSUNG

Der Beitrag stellt die Motivation und Zielsetzung der Sicherheit der Sollfunktion (SOTIF) dar und beschreibt das Normvorhaben der ISO PAS 21448. Weiterhin bewerten die Autoren den Stand des Normvorhabens sowie die darin getroffenen Methoden und Vorgehensmodelle. Nach der Betrachtung erfolgt ein Konzept zur Erweiterung des im Normvorhaben getroffenen Entwicklungsvorgehens. Die

Autoren heben hierbei hervor, dass SOTIF verstärkt und methodisch fundiert in der Konzeptphase einer Funktionsentwicklung integriert werden kann und direkt Anforderungen an die Funktionsentwicklung stellt. Weiterhin sprechen sich die Autoren dafür aus, eine an die Sollfunktion angepasste Risikoeinstufung vorzunehmen und insb. die Exposition zu überdenken, sowie die Unterscheidungsmerkmale zwischen vorhersehbaren Fehlgebrauch und Missbrauch besser auszuformulieren. Der Beitrag endet in der Empfehlung, die Sicherheit der Sollfunktion nicht nur für Assistenzfunktionen anzuwenden, sondern vor dem Hinblick der primären Unfallursachen, welche in der Sollfunktion liegen, auch für Bestandsfunktionen durchzuführen.

REFERENCES

[Johner Institut 2021] Johner Institut: Johner Institut GmbH, Villa Rheinburg, Reichenaustr. 1, 78467 Konstanz

[destatis 2021] Statistisches Bundesamt: “Unfallursachen im Verkehr”, 2021, Berlin.

[ISO 26262] Road Vehicles: Functional Safety, 2018.

[ISO 21448] Road Vehicles: Safety of the Intended Functionality, 2019.

[ISO 21443] Road Vehicles: Cybersecurity, 2020.