

	DIN 70065	
ICS 43.040.99 Kraftfahrzeuge – Anforderungen an ein "Steer-by-Wire (SbW)-System" Road vehicles – Requirements for a "Steer-by-Wire (SbW)-system" Véhicule routiers – Exigences pour un système de direction électrique Gesamtumfang 112 Seiten DIN-Normenausschuss Auto und Mobilität (NAAutomobil)		

Inhalt

	Seite
Vorwort	6
Einleitung	7
1 Anwendungsbereich	8
2 Normative Verweisungen	8
3 Begriffe	8
4 Verzeichnis der Symbole	12
5 Herleitung von Sicherheitszielen	13
5.1 Systemabgrenzung	13
5.2 SbW-Fehlfunktionen	15
5.3 Sicherheitsziele	16
5.3.1 Allgemeines	16
5.3.2 Sicherheitsziel SZ1	17
5.3.3 Sicherheitsziel SZ2	18
5.3.4 Sicherheitsziel SZ3	18
5.3.5 Sicherheitsziel SZ4	19
5.3.6 Sicherheitsziel SZ5	20
6 Anforderungen an die Systemverfügbarkeit	22
6.1 Allgemeine Verfügbarkeitsanforderungen	22
6.2 Verfügbarkeitsanforderungen nach Fehlerfall	22
6.3 Verfügbarkeitsanforderungen an mechanische Systemumfänge	24
7 Kontrollierbarkeit im Erstfehlerfall	24
7.1 Einleitung und Allgemeines zur Kontrollierbarkeit	24
7.2 Fehlerbilder	24
7.2.1 Allgemeines	24
7.2.2 Fehlfunktionen	24
7.2.3 Fehlerquelle	25
7.2.4 Fehlerausprägung	25
7.2.5 Fehlercharakteristiken mit den zugehörigen physikalischen Größen	25
7.2.6 Fehlerbild mit Verlust des aktiv generierten Handmoments	27
7.3 Fehlerbildmatrix	27
7.4 Bewertung der Kontrollierbarkeit im Fehlerfall	29
7.5 Beschreibung von Fahrmanövern und Versuchsdurchführung zur Bewertung der Kontrollierbarkeit im Fehlerfall	32
8 Mindestanforderungen an das Betriebsverhalten nach Fehlerfall	33
8.1 Einleitung und allgemeine Beschreibung des Degradationskonzepts	33
8.2 Degradationen und Transitionen	35
8.2.1 Normalzustand N	35
8.2.2 Transition x-2 und Degradation 2	35
8.2.3 Transition 2-3 und Degradation 3	36
8.2.4 Transition x-Notbremsung	36
8.2.5 Transition N-1 und Degradation 1	36
8.2.6 Transition x-3	36
8.3 Allgemeine Anforderungen des Degradationskonzeptes	37
8.3.1 Kontrollierbarkeit während Degradationen und Transitionen	37
8.3.2 Bordnetz	37
8.3.3 Verkürzte Transitionen	37
8.3.4 Definition Fahrzeug-Querbeschleunigung	38
8.3.5 Uneingeschränkte Weiterfahrt vor einer automatisierten Geschwindigkeitsreduktion	38
8.3.6 Übersteuern der automatisierten Geschwindigkeitsreduktion und der Geschwindigkeitslimitierung	39
8.3.7 Überbremsen der automatisierten Geschwindigkeitsreduktion	39

8.4	Abgrenzung zu anderen Systemen und der Infrastruktur des Fahrzeuges	39
8.5	Mindestanforderungen an die Degradationen und Transitionen	40
8.5.1	Allgemeines	40
8.5.2	Systemintegrität und Geschwindigkeitseinschränkungen	40
8.5.3	Anforderungen an die Sicherheitsintegrität	48
8.5.4	Zeitliche Nutzungseinschränkungen	48
8.5.5	Rücküberführung und deren Bedingungen	50
8.5.6	Anforderungen an das Warnkonzept	53
8.5.7	Mindestanforderungen an die Querführung und Kontrollierbarkeit des Fahrzeugs	54
8.6	Manöversequenzen und deren Anforderungen	56
8.6.1	Allgemeine Erläuterungen	56
8.6.2	Ziele der Manöversequenzen und zugehörige Manöver	56
8.6.3	Generelle Anforderungen	59
Anhang A (normativ) Fahrmanöver zur Bewertung der Kontrollierbarkeit		60
A.1	Einleitung	60
A.2	Anforderungen an die Versuchskonfiguration	60
A.2.1	Einleitende Hinweise	60
A.2.2	Konfiguration des Versuchsfahrzeugs	60
A.2.3	Allgemeine Anforderungen an die Versuchsdurchführung	60
A.2.4	Systeme zur Fahrzeugstabilisierung	61
A.2.5	Alternative Systeme zur Fahrzeugquerführung	61
A.2.6	Definition der Handhaltung in der Versuchsdurchführung	61
A.3	Fahrmanöver	62
A.3.1	Fahrmanöver: Geradeausfahrt	62
A.3.2	Fahrmanöver: Stationäre Kreisfahrt	65
A.3.3	Fahrmanöver: Slalom	67
A.3.4	Methodiken zur Auswertung der objektiven fahrdynamischen Kenngrößen	69
Anhang B (normativ) Prüfungen zum Nachweis der Fahrzeugquerführung und Kontrollierbarkeit in den Degradationen und Transitionen		72
B.1	Einleitung	72
B.2	Anforderungen an die Versuchskonfigurationen	72
B.2.1	Einleitende Hinweise	72
B.2.2	Konfiguration des Versuchsfahrzeugs	72
B.2.3	Konfiguration der Fahrzeugsysteme	73
B.3	Allgemeine Anforderungen an die Versuchsdurchführung	74
B.3.1	Umgebungsbedingungen	74
B.3.2	Allgemeine Toleranzen für die Versuchsdurchführung und die Akzeptanzkriterien	74
B.3.3	Automatisierte Geschwindigkeitsreduktion	75
B.3.4	Manöver zum Nachweis der Lenkleistung nach thermischer Belastung	75
B.3.5	Übertragbarkeit von Ergebnissen	75
B.3.6	Verkürzte Transition x-2	75
B.3.7	Markierung und Anpassung der Fahrstreifenbreite	76
B.3.8	Systeme zur Fahrzeugstabilisierung	76
B.3.9	Systeme zur alternativen Fahrzeugquerführung	76
B.3.10	Definition der Handhaltung in der Versuchsdurchführung	76
B.3.11	Ermittlung fahrdynamischer Größen	76
B.4	Fahrmanöver	77
B.4.1	Fahrmanöver: Achten-Fahren	77
B.4.2	Fahrmanöver: Automatisiertes Anhalten bei Einfahrt in den Kreis	79
B.4.3	Fahrmanöver: Automatisiertes Anhalten im einfachen Spurwechsel	80
B.4.4	Fahrmanöver: Automatisiertes Anhalten in einer Geraden	82
B.4.5	Fahrmanöver: Automatisiertes Anhalten im Kreis	84
B.4.6	Fahrmanöver: Automatisierte Verzögerung im Slalom	86
B.4.7	Fahrmanöver: Doppelter Spurwechsel	88
B.4.8	Fahrmanöver: Lenkwinkelrampe	90
B.4.9	Fahrmanöver: Slalom	92
B.4.10	Immobilisieren des Fahrzeugs	94

B.4.11 Übersicht der Akzeptanzkriterien 94

B.5 Dokumentation der Ergebnisse 96

Anhang C (informativ) Entwicklungsverantwortung 98

C.1 Beispielhafte Systemaufteilung 98

C.2 Entwicklungsverantwortung zwischen OEM und Lieferanten 99

C.3 Beispielhafte Systemarchitekturen 100

Anhang D (informativ) Erfahrungswerte aus Versuchsreihen während der Normerstellung 103

D.1 Allgemeines 103

D.2 Matrix Erfahrungswerte 104

D.3 Hinweise zur Probandenstudie 105

Anhang E (informativ) Erläuterungen zum Degradationskonzept 106

E.1 Allgemeine Darstellung der Geschwindigkeitslimitierung 106

E.2 Zeitlicher Verlauf der Geschwindigkeitslimitierung mit 3 Beispielszenarien 107

E.3 Typische Systemfehler und auszulösende Transitionen 109

E.3.1 Beispielarchitektur 1 mit redundantem Lenkradaktuator analog Bild C.3 109

E.3.2 Beispielarchitektur 2 mit drittem Lenkwinkelsensor analog Bild C.4 110

E.3.3 Beispielarchitektur 3 mit zusätzlicher Redundanz zur Fahrzeugquerführung 111

Literaturhinweise 112

Bilder

Bild 1 — Definition „Item“ für SbW 14

Bild 2 — Möglichkeit 1: Definition System(e) „SbW“ nach ISO 26262 15

Bild 3 — Möglichkeit 2: Definition System(e) „SbW“ nach ISO 26262 15

Bild 4 — Weiterfahrzeit bei reduzierter Sicherheitsintegrität 23

Bild 5 — Übersichtsdiagramm des Degradationskonzeptes (ohne Transition x-3) 35

Bild 6 — Übersichtsdiagramm des Degradationskonzeptes (mit Transition x-3) 37

Bild A.1 — Versuchsaufbau Fahrmanöver Geradeausfahrt 63

Bild A.2 — Versuchsaufbau Fahrmanöver Kreisfahrt 66

Bild A.3 — Versuchsaufbau Fahrmanöver Slalom 68

Bild A.4 — Auswertung der objektiven fahrdynamischen Kenngröße (exemplarisch für die Stör-Giergeschwindigkeit in der Geradeausfahrt) 70

Bild A.5 — Methodik zur Auswertung der objektiven fahrdynamischen Kenngröße (exemplarisch für die Stör-Giergeschwindigkeit im Slalom) 71

Bild B.1 — Versuchsaufbau Fahrmanöver „Achten-Fahren“ 77

Bild B.2 — Versuchsaufbau Fahrmanöver Automatisiertes Anhalten bei Einfahrt in den Kreis 79

Bild B.3 — Versuchsaufbau Fahrmanöver Automatisiertes Anhalten im einfachen Spurwechsel 81

Bild B.4 — Versuchsaufbau Fahrmanöver Automatisiertes Anhalten in einer Geraden 83

Bild B.5 — Versuchsaufbau Fahrmanöver Automatisiertes Anhalten im Kreis 85

Bild B.6 — Versuchsaufbau Fahrmanöver Automatisierte Verzögerung im Slalom 87

Bild B.7 — Versuchsaufbau Fahrmanöver Doppelter Spurwechsel nach ISO 3888-2:2011 89

Bild B.8 — Prinzip-Bild der Trajektorie bei einer Lenkwinkelrampe 91

Bild B.9 — Versuchsaufbau Fahrmanöver Slalom 93

Bild C.1 — Beispielhafte Systemaufteilung SbW: 1Item = 1 System 98

Bild C.2 — Beispielhafte Systemaufteilung SbW: 1 Item = 2 System 99

Bild C.3 — Beispielarchitektur mit redundantem Handmoment für Item SbW 101

Bild C.4 — Beispielarchitektur ohne redundantes Handmoment für Item SbW 102

Bild E.1 — Zeitlicher Verlauf der Geschwindigkeitslimitierung 106

Bild E.2 — Zeitlicher Verlauf eines Fahrprofils (Beispiel 1) 107

Bild E.3 — Zeitlicher Verlauf eines Fahrprofils (Beispiel 2) 108

Bild E.4 — Zeitlicher Verlauf eines Fahrprofils (Beispiel 3) 109

Tabellen

Tabelle 1 — Fehlerbildmatrix	28
Tabelle 2 — Kombinationen ausgewählter Fehlerbilder mit Fahrmanövern	30
Tabelle 3 — Anforderungen Sicherheitsintegrität	48
Tabelle 4 — Übersicht der Manöversequenzen	54
Tabelle 5 — Ziele der Manöversequenzen	56
Tabelle 6 — Übersicht der Manöversequenzen und ihrer Manöver	58
Tabelle A.1 — Toleranzen für Versuchsdurchführung	60
Tabelle A.2 — Parameter Fahrmanöver Geradeausfahrt	62
Tabelle A.3 — Fehlerbilder im Fahrmanöver Geradeausfahrt	64
Tabelle A.4 — Parameter Fahrmanöver Kreisfahrt	65
Tabelle A.5 — Fehlerbilder im Fahrmanöver Kreisfahrt	67
Tabelle A.6 — Parameter Fahrmanöver Slalom	67
Tabelle A.7 — Fehlerbilder im Fahrmanöver Slalom	68
Tabelle B.1 — Toleranzen für Versuchsdurchführung und Akzeptanzkriterien	74
Tabelle B.2 — Versuchsvarianten „Achten-Fahren“	78
Tabelle B.3 — Versuchsvarianten Automatisiertes Anhalten bei Einfahrt in den Kreis	80
Tabelle B.4 — Versuchsvarianten Automatisiertes Anhalten im einfachen Spurwechsel	82
Tabelle B.5 — Automatisiertes Anhalten in einer Geraden	83
Tabelle B.6 — Versuchsvarianten Automatisiertes Anhalten im Kreis	85
Tabelle B.7 — Automatisierte Verzögerung im Slalom	87
Tabelle B.8 — Versuchsvarianten Doppelter Spurwechsel	89
Tabelle B.9 — Versuchsvarianten Lenkwinkelrampe	91
Tabelle B.10 — Versuchsvarianten Slalom	93
Tabelle B.11 — Relevante Manöver für Immobilisierung	94
Tabelle B.12 — Zusammenfassung der Akzeptanzkriterien	95
Tabelle B.13 — Dokumentation Fahrzeug	96
Tabelle B.14 — Allgemeine Versuchsinformationen	96
Tabelle B.15 — Messsignale	96
Tabelle C.1 — Aufteilung Entwicklungsverantwortung	99
Tabelle D.1 — Übersicht Erfahrungswerte	104
Tabelle E.1 — Typische Systemfehler und auszulösende Transition — Beispielarchitektur 1	110
Tabelle E.2 — Typische Systemfehler und auszulösende Transition — Beispielarchitektur 2	110
Tabelle E.3 — Typische Systemfehler und auszulösende Transition — bei weiterer Redundanz zur Fahrzeugquerführung	111

Vorwort

Dieses Dokument wurde vom Arbeitskreis NA 052-00-33-18 AK „Sicherheitsanforderungen an ein Steer-by-Wire Lenksystem“ im DIN-Normenausschuss Auto und Mobilität (NAAutomobil) erarbeitet.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. DIN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Einleitung

SbW-Systeme stellen die nächste Technologiegeneration im Bereich Fahrzeuglenkung dar. Diese ermöglichen neue Interieurkonzepte und sind Wegbereiter für weitere Innovationen im Bereich der Fahrzeugtechnik. Dabei gewinnt im Rahmen des automatisierten Fahrens die mechanische Entkopplung zwischen dem Lenkrad und den gelenkten Rädern an Bedeutung. Bisher existieren keine Erfahrungen aus einer flächendeckenden Verbreitung dieser Technologie im Markt für PKW-Großserien.

Im Vergleich zu konventionellen Lenksystemen ergeben sich aus der SbW-Technologie zusätzliche Anforderungen an ein Sicherheitskonzept im Fahrzeug für den sicheren Betrieb.

Dieses Dokument stellt eine von Fahrzeugherstellern und Systemlieferanten erarbeitete Beschreibung notwendiger Sicherheitsaspekte dar.

Dieses Dokument berücksichtigt

- die Beschreibung und Abgrenzung eines SbW-Systems,
- grundlegende Sicherheitsziele,
- allgemeine Verfügbarkeitsanforderungen,
- Anforderungen an die Kontrollierbarkeit im Erstfehlerfall und
- Anforderungen an das Betriebsverhalten nach einem Fehlerfall.

1 Anwendungsbereich

Dieses Dokument legt notwendige, aber nicht hinreichende Sicherheitsanforderungen für die Verwendung von SbW-Systemen in Personenkraftwagen und leichten Nutzfahrzeugen für die Serienanwendung fest.

Dieses Dokument ersetzt nicht die vollständige Anwendung der Normenreihe ISO 26262 und deren Umsetzung in sicherheitsrelevante Maßnahmen.

Dieses Dokument definiert Anforderungen für das manuelle Fahren, bei dem der Fahrer das Lenkrad festhält.

ANMERKUNG Das missbräuchliche, freihändige Fahren wird nicht betrachtet.

Das Dokument enthält keine Anforderungen für die Verwendung von automatisierten Querführungsfunktionen.

Die Anforderungen berücksichtigen Systeme die aus Radaktor, Lenkradaktor sowie einem Lenkrad zur Lenkwunscheingabe bestehen. Abweichende Konzepte sind durch den Anwender auf Übertragbarkeit zu überprüfen.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ISO 3888-2:2011, *Passenger cars — Test track for a severe lane-change manoeuvre — Part 2: Obstacle avoidance*

ISO 15037-1:2019, *Road vehicles — Vehicle dynamics test methods — Part 1: General conditions for passenger cars*

ISO 26262 (alle Teile), *Road vehicles — Functional safety*

ISO 26262-1:2018, *Road vehicles — Functional safety — Part 1: Vocabulary*

ISO 26262-5:2018, *Road vehicles — Functional safety — Part 5: Product development at the hardware level*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO 26262-1 und die folgenden Begriffe.

DIN und DKE stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- DIN-TERMinologieportal: verfügbar unter <https://www.din.de/go/din-term/>
- DKE-IEV: verfügbar unter <https://www.dke.de/DKE-IEV>

3.1**Degradation****Degradationszustand****DEG**

Betriebszustand des Fahrzeugs im Rahmen des Degradationskonzepts

Anmerkung 1 zum Begriff: Bedingt durch den Betriebszustand des Lenksystems oder unterstützender Systeme kann ein Degradationszustand zu Nutzungseinschränkungen des Fahrzeuges führen, z. B. Geschwindigkeitsbeschränkungen. Der Normalzustand oder Normalbetrieb wird im Dokument als Degradationszustand behandelt.

3.2**Degradationskonzept**

Summe der Betriebszustände des Fahrzeuges einschließlich der Betriebszustände des Lenksystems und der unterstützenden Fahrzeugsysteme nach Erst- und Folgefehlern

Anmerkung 1 zum Begriff: Zu den Betriebszuständen gehören sowohl die Transitions- als auch die Degradationszustände nach Fehlern, sowie der fehlerfreie Normalzustand.

3.3**Expertenfahrer**

Person, die ein überdurchschnittliches fahrdynamisches Wissen, Können und Bewertungsvermögen aufweist und über regelmäßige Fahrpraxis verfügt

3.4**Fahrstreifen**

lateral begrenzte Fläche für die Fortbewegung des Fahrzeuges, innerhalb der die Fahraufgabe zu bewältigen ist

3.5**Fahrzeugquerführung**

Fähigkeit eines fahrenden Kraftfahrzeugs, im Bereich des verfügbaren Kraftschlusses zwischen Reifen und Fahrbahnoberfläche die Lenkwinkelvorgabe des Fahrers in eine vom Fahrer erwartbare Krümmung der Fahrzeugtrajektorie umzusetzen

Anmerkung 1 zum Begriff: Eine Trajektorienänderung kann über das SbW-System hinaus auch durch andere fahrzeugseitige Systeme (z. B. Bremse, Antrieb usw.) realisiert werden.

3.6**Fahrzyklus**

Zeitspanne von Beginn bis Ende einer Fahrt

Anmerkung 1 zum Begriff: In diesem Dokument wird der Begriff im Zusammenhang mit der Rücküberführung zwischen den Degradationszuständen genutzt.

3.7**Fehler**

anormaler Zustand, der zur Beeinträchtigung einer Funktion des Items oder zum Versagen des Items führt

Anmerkung 1 zum Begriff: Die Fehlerwirkung kann durch Sicherheitsmechanismen abgeschwächt werden.

Anmerkung 2 zum Begriff: Ohne Abschwächungsmaßnahmen für die Fehlerwirkung durch geeignete Sicherheitsmechanismen kann die Fehlerwirkung zu einer Fehlfunktion führen.

[QUELLE: ISO 26262-1:2018, 3.54, modifiziert — „fault“ in die deutsche Sprache übersetzt, ursprüngliche Anmerkungen zum Begriff gestrichen und durch neue ersetzt]

3.8

Fehlfunktion

unbeabsichtigtes Verhalten aufgrund einer Manifestierung der Fehlerwirkung eines Fehlers

[QUELLE: ISO 26262-1:2018, 3.50, modifiziert — „failure“ in die deutsche Sprache übersetzt, Anmerkung 1 zum Begriff gestrichen]

3.9

Fehlergutprüfung

Diagnosemaßnahme, die einen vorab erkannten Fehler als nicht mehr vorhanden bestätigt

3.10

Lenkbarkeit

Fähigkeit des SbW-Systems, die Lenkwinkelvorgabe des Fahrers in eine auslegungskonforme Lenkbewegung der Räder des Kraftfahrzeuges umzusetzen

3.11

Lenkradaktuator

LA

Komponente(n) zum Erfassen des Lenkradwinkels und zum Einstellen eines Handmoments

3.12

Handmoment

Drehmoment am Lenkrad

Anmerkung 1 zum Begriff: Ein aktiv generiertes Handmoment entsteht, wenn mindestens eine Antriebseinheit des Lenkradaktuators aktiv ist. Ein passiv generiertes Handmoment entsteht, wenn keine Antriebseinheit des Lenkradaktuators aktiv ist und der Fahrer eine Lenkbewegung durchführt. Das Handmoment dient unter anderem zur Darstellung des Lenkgefühls.

3.13

Immobilisierung

Vorgang, bei dem ein stillstehendes Fahrzeug gegen Wegrollen gesichert wird

3.14

Kontrollierbarkeit

Fähigkeit des Fahrzeugs, durch rechtzeitige Reaktion der beteiligten Personen ein bestimmtes Unheil oder einen Schaden abwenden zu können, möglicherweise mit Unterstützung durch externe Maßnahmen

Anmerkung 1 zum Begriff: Im Kontext dieses Dokuments wird als beteiligte Person ausschließlich der Fahrer betrachtet.

[QUELLE: ISO 26262-1:2018, 3.25, modifiziert — „controllability“ in die deutsche Sprache übersetzt, ursprüngliche Anmerkungen zum Begriff gestrichen und Anmerkung 1 zum Begriff ergänzt]

3.15

Manöver

spezifizierter Fahrversuch

3.16

Manöversequenz

MP, en: Mission-Profile

spezifische Abfolge von Manövern

3.17**Normalbetrieb****N**

Zustand des Lenksystems und der unterstützenden Fahrzeugsysteme ohne sicherheitskritische Fehler

Anmerkung 1 zum Begriff: Geringe, nicht sicherheitskritische Abweichungen innerhalb des nominalen Applikationsbereichs sind zulässig. Die Abweichung des Verhaltens des Lenksystems und des Fahrzeugs relativ zum Nominalverhalten liegt innerhalb des vom Fahrer zu erwartenden Bereichs.

3.18**Normalfahrer**

Person, welche nicht über besondere Fähigkeiten zur Führung eines Fahrzeugs verfügt

Anmerkung 1 zum Begriff: Wird benutzt zur Abgrenzung vom Expertenfahrer.

3.19**passive Rückfallebene (des Lenkradaktuators)**

Betriebszustand bei dem kein aktives Handmoment generiert wird

3.20**Radaktor****RA**

Komponente(n) zum Einstellen des geforderten Radlenkwinkels an der Vorderachse

3.21**Sicherheitsmechanismus**

technische Lösung implementiert durch E/E-Funktionen oder -Elemente oder durch andere Technologien, um Fehler zu erkennen und abzumindern beziehungsweise zu tolerieren oder Fehlfunktionen zu kontrollieren beziehungsweise zu vermeiden, um die gewünschte Funktionalität zu erhalten oder einen sicheren Zustand zu erreichen beziehungsweise zu erhalten

[QUELLE: ISO 26262-1:2018, 3.142, modifiziert — „safety mechanism“ in die deutsche Sprache übersetzt, Anmerkungen zum Begriff gestrichen]

3.22**Sicherheitsintegrität**

Fähigkeit des Gegenstandes oder des Elementes, angenommene Sicherheitsanforderungen mit einem zugeordneten ASIL zu erfüllen

[QUELLE: ISO 26262-1:2018, 3.2, modifiziert — „ASIL capability“ in die deutsche Sprache übersetzt, Anmerkung 1 zum Begriff gestrichen]

3.23**Systemintegrität**

Eigenschaften des SbW-Systems einschließlich der Sicherheitsintegrität zur Erfüllung von Anforderungen an die Funktion und an die Verfügbarkeit

Anmerkung 1 zum Begriff: Anforderungen an die Funktion betreffen z. B. Lenkleistung, Handmoment und Synchronität. Anforderungen an die Verfügbarkeit betreffen z. B. Redundanzen zur Erhaltung der Lenkfähigkeit.

Anmerkung 2 zum Begriff: Eine Beeinträchtigung der Lenkleistungsfähigkeit oder ein Verlust einer Redundanz kann die Sicherheitsintegrität reduzieren.

3.24

Transition**TR**

Übergang zwischen den Degradationszuständen

Anmerkung 1 zum Begriff: Eine Transition stellt in sich einen zeitlich eingeschränkten Lenksystem- und Fahrzeugzustand dar. Bedingt durch den Systemzustand des Lenksystems oder unterstützender Systeme kann eine Transition zu Nutzungseinschränkungen des Fahrzeuges führen, z. B. Geschwindigkeitsbeschränkungen.

3.25

Versuchskonfiguration

Kombination der Konfiguration des Versuchsfahrzeugs (siehe Anhang B, B.2.2) und der Konfigurationen der jeweiligen Fahrzeugsysteme (siehe Anhang B, B.2.3) für die Versuche zum Nachweis der Lenkbarkeit bzw. der Fahrzeugquerführung und Kontrollierbarkeit in den Degradationen und Transitionen

3.26

Warnkonzept

technische Maßnahmen zur Warnung des Fahrers und des Umfelds im Fehlerfall

3.27

Warnsymbol

standardisiertes Symbol zur Rückmeldung des Fehler- bzw. Degradationszustands des SbW-Systems an den Fahrer

4 Verzeichnis der Symbole

Größe	Symbol	Einheit
Fahrzeugquerbeschleunigung	a_y	m/s^2
Fahrzeuglängsbeschleunigung	a_x	m/s^2
Abstand	a	m
Fahrzeugbreite	B	m
Fahrstreifenbreite	b	m
Radstand	L	m
Pylonen-Abstand	d	m
Kreisradius	R/R_i	m
Streckenlänge	S	m
Fahrzeuggeschwindigkeit	v_x	km/h
Fahrzeuggeschwindigkeit zu Beginn des Manövers	$v_{x \text{ Start}}$	km/h
Fahrzeuggeschwindigkeit am Ende des Manövers	$v_{x \text{ Ziel}}$	km/h
Stör-Giergeschwindigkeit	$\Delta\dot{\psi}$	$^\circ/\text{s}$
Stör-Querbeschleunigung	Δa_y	m/s^2
Fehlerdauer	t_{Fehler}	s

5 Herleitung von Sicherheitszielen

5.1 Systemabgrenzung

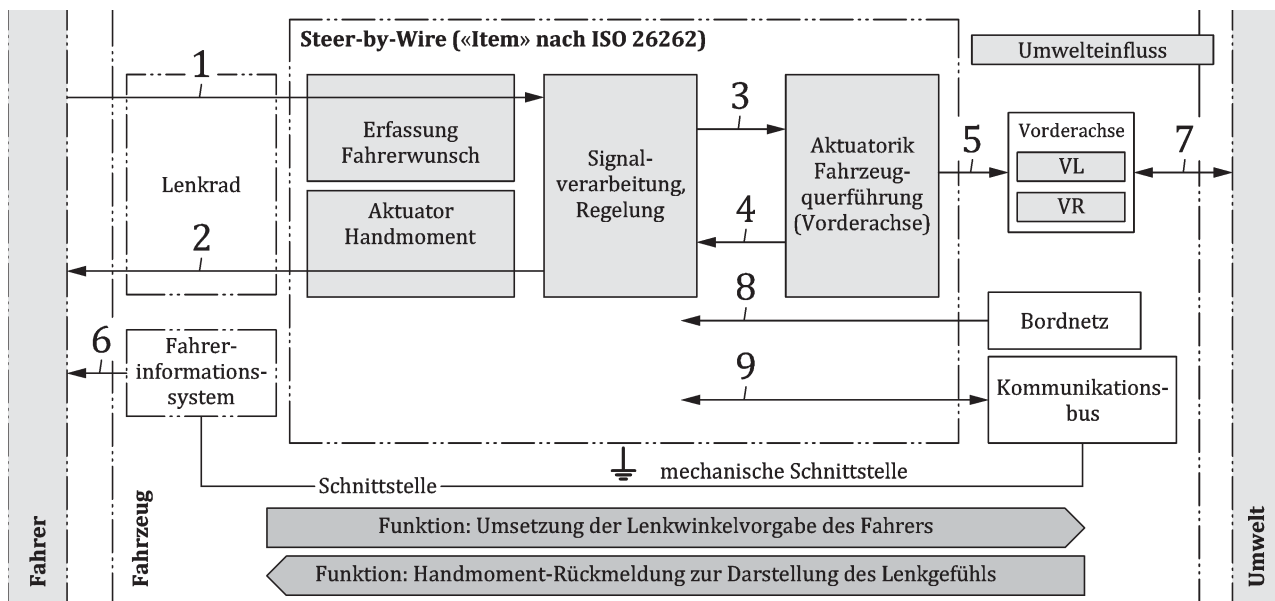
SbW ist ein Lenksystem, bei dem der Lenkbefehl des Fahrers über eine Sensorik erfasst und zur Stellung der Radlenkwinkel ausschließlich elektrisch an die Aktuatorik übertragen wird. Mittels eines Lenkradaktuators wird dem Fahrer das Lenkgefühl dargestellt.

Im Vergleich zu konventionellen Lenksystemen (z. B. elektromechanische Lenkung, Überlagerungslenkung) besteht bei einem SbW-System keine mechanische Verbindung zwischen dem Lenkrad und den gelenkten Rädern. Aus diesem konzeptionellen Unterschied resultieren zusätzliche Sicherheitsanforderungen und Anforderungen an die Ausfallsicherheit des Lenksystems im Fahrzeug.

Für ein SbW-System muss trotz eines elektrischen Fehlers im SbW-System oder in anderen unterstützenden Systemen im Fahrzeug (z. B. Bordnetz, Fahrzeugkommunikation) die Lenkbarkeit bzw. die Fahrzeugquerführung des Fahrzeuges während der Fahrt aufrechterhalten werden.

Zur Abgrenzung des in diesem Dokument betrachteten Item „SbW“, nach ISO 26262-1:2018, 3.84, wird die Übersicht aus Bild 1 verwendet, welche die funktionalen Elemente und Schnittstellen des Items „SbW“ zum Fahrzeug beispielhaft darstellt. Außerdem sind die Wirkketten der zwei Hauptfunktionen eines SbW-Systems gezeigt:

- Umsetzung der Lenkwinkelvorgabe des Fahrers; und
- Handmoment-Rückmeldung zur Darstellung des Lenkgefühls.



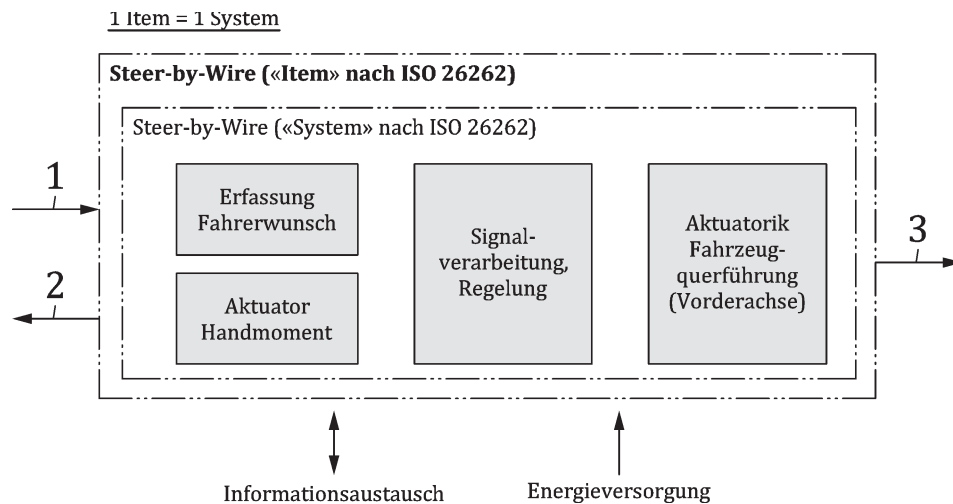
Legende

- 1 Lenkwinkelvorgabe Fahrer über Lenkrad und Erfassung Fahrerwunsch
- 2 Handmoment Fahrer über Aktuator Handmoment und Lenkrad (Rückmeldung Lenkgefühl einschließlich haptischer Warnung)
- 3 Vorgabe Radlenkwinkel
- 4 Messgrößen Aktuatoren
- 5 Radlenkwinkel (Übertragung durch die mechanische Verbindung über Spurstange und Lenkgestänge zu den Vorderrädern)
- 6 Visuelle oder akustische Informationen und Warnungen des SbW-Systems
- 7 Wechselwirkung Rad – Straße
- 8 Energieversorgung
- 9 Informationsaustausch

Bild 1 — Definition „Item“ für SbW

Ein SbW-System mit dem beschriebenen Funktionsumfang ist als ein „Item“ entsprechend der Definition nach ISO 26262-1 und ISO 26262-5 anzusehen.

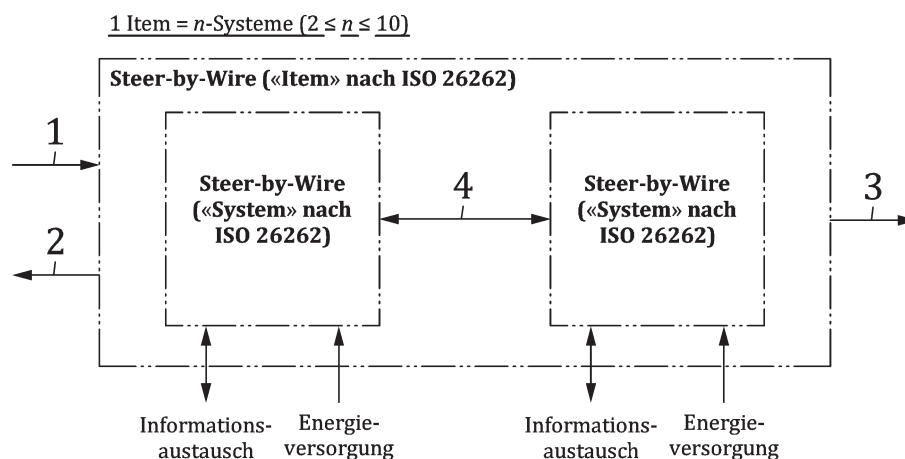
Es besteht die Möglichkeit das „Item“ SbW als ein System oder eine Kombination aus mehreren Systemen nach ISO 26262-1 und ISO 26262-5 zu betrachten, siehe Bild 2 und Bild 3.



Legende

- 1 Lenkwinkelvorgabe Fahrer
- 2 Handmoment Fahrer (Rückmeldung Lenkgefühl einschließlich Warnkonzept)
- 3 Radlenkwinkel

Bild 2 — Möglichkeit 1: Definition System(e) „SbW“ nach ISO 26262



Legende

- 1 Lenkwinkelvorgabe Fahrer
- 2 Handmoment Fahrer (Rückmeldung Lenkgefühl einschließlich Warnkonzept)
- 3 Radlenkwinkel
- 4 Informationsaustausch zwischen den Systemen

ANMERKUNG Die Definition „1 Item = n -Systeme ($2 \leq n \leq 10$)“ folgt den Vorgaben nach ISO 26262 (alle Teile).

Bild 3 — Möglichkeit 2: Definition System(e) „SbW“ nach ISO 26262

Eine beispielhafte Aufteilung in physische Systemarchitektur(en) für beide Varianten und für die Aufteilung der Entwicklungsverantwortung zwischen Erstausrüster (OEM, en: original equipment manufacturer) und Lieferanten ist in Anhang C dargestellt.

5.2 SbW-Fehlfunktionen

Die Funktionen der in diesem Dokument betrachteten „Item-Definition“ sind:

- Umsetzung der Lenkwinkelvorgabe des Fahrers; und
- Handmoment-Rückmeldung zur Darstellung des Lenkgefühls.

In diesem Dokument werden folgende SbW-Fehlfunktionen ohne weitere Detaillierung betrachtet:

- Selbstlenker;
- Ausfall der Lenkbarkeit;
- Verlust des Handmoments;
- Blockieren der Lenkung; und
- Asynchronität zwischen Lenkradwinkel und Radlenkwinkel.

5.3 Sicherheitsziele

5.3.1 Allgemeines

Aus den oben aufgeführten SbW-Fehlermodi sind folgende Sicherheitsziele und deren Kritikalitätsbewertung hergeleitet:

- SZ1: Ein Selbstlenken muss während der Fahrt verhindert werden.
- SZ2: Ein Ausfall der Lenkbarkeit muss während der Fahrt verhindert werden.
- SZ3: Ein Verlust des Handmomentes an den Fahrer muss während der Fahrt verhindert werden.
- SZ4: Ein ungewolltes Blockieren des Lenkrads während der Fahrt muss verhindert werden.
- SZ5: Eine unaufgeforderte, (unbeherrschbare) Asynchronität zwischen den SbW-Aktuatoren muss während der Fahrt verhindert werden.

ANMERKUNG 1 Im Kontext der Sicherheitsziele bedeutet "während der Fahrt", dass das Fahrzeug in einem Zustand ist, bei dem der Fahrer die laterale und longitudinale Kontrolle über das Fahrzeug hat. Die Kritikalität (ASIL-Einstufung) einer Sicherheitszielverletzung ist geschwindigkeitsabhängig. Bei sehr niedrigen Geschwindigkeiten (z. B. 10 km/h mit entsprechendem Warnkonzept) ist das Risiko aufgrund der deutlich reduzierten kinetischen Energie wesentlich kleiner als bei höheren Geschwindigkeiten.

ANMERKUNG 2 In diesem Dokument wird die Kritikalität der Sicherheitsziele für E/E-Fehler mit Automotive Safety Integrity Level (ASIL) nach ISO 26262 (alle Teile) bewertet.

ANMERKUNG 3 Die SbW Fehlfunktion „Blockieren der Lenkung“ aus 5.2 kann durch ein Blockieren des Lenkradaktuators (SZ4) oder durch ein Blockieren des Radaktuators (SZ2) verursacht werden.

Die aufgeführten Sicherheitsziele sind nicht aus einer vollständigen Gefahrenanalyse und Risikobeurteilung nach ISO 26262 (alle Teile) (en: hazard analysis & risk assessment, HARA) hergeleitet, sondern basieren auf den generischen Fehlermodi. Daher stellen die aufgeführten Sicherheitsziele nur einen Mindestumfang dar.

Dieses Dokument entbindet den Anwender nicht von der Durchführung einer vollständigen HARA für ein konkretes SbW-System.

Mechanische Fehler, die zu einer Verletzung der Sicherheitsziele führen können, müssen entsprechend ihrer Kritikalität berücksichtigt werden.

5.3.2 Sicherheitsziel SZ1

5.3.2.1 Erläuterung

Selbstlenken ist eine ungewollten Lenkwinkeländerung (Radaktuator und/oder Lenkradaktuator) verursacht durch eine fehlerhafte Kraft des Radaktuators oder ein fehlerhaftes Moment des Lenkradaktuators. Das Sicherheitsziel ist mit ASIL D eingestuft.

ANMERKUNG Mögliche Ursachen für eine fehlerhafte Kraft oder das fehlerhafte Moment umfassen Fehler in der Wirkkette: Sensorik, Kommunikation, Steuerung und Aktuatorik. Dabei kann die Art der fehlerhaften Aktuatoransteuerung unterschiedlichen Fehlerbildern folgen, z. B. falsche Amplitude, falsche Richtung, überlagernd, oszillierend.

5.3.2.2 Akzeptanzkriterien

Bei Fehlern in einem SbW-System, welche zur Verletzung eines Sicherheitsziels führen können, müssen diese in geeigneter Weise abgeschwächt werden, sodass ein Verbleib im Fahrstreifen sichergestellt ist (siehe Abschnitt 7).

5.3.2.3 Sicherer Zustand Fahrzeug

Auf Fahrzeugebene ist der sichere Zustand erreicht, wenn die Fahrzeuggeschwindigkeit auf ≤ 10 km/h mit entsprechender Warnung reduziert ist.

ANMERKUNG UNECE R79 Rev. 4, 5.3.3.1, verweist auf die Schwelle ≤ 10 km/h im Fehlerfall. Das Degradationskonzept geht situationsabhängig über den sicheren Zustand hinaus und beschreibt falls möglich auch die Überführung des Fahrzeugs in den Fahrzeugstillstand.

Bei der Überführung des Fahrzeugs in den sicheren Zustand sind die Anforderungen des Degradationskonzepts zu erfüllen (siehe Abschnitt 8).

Der sichere Zustand auf Fahrzeugebene kann nur unter Berücksichtigung von Systemen außerhalb des SbW-Systems oder durch den Fahrer erreicht und sichergestellt werden.

5.3.2.4 Sicherer Zustand SbW-System

Auf Ebene des SbW-Systems ist für die Funktion "Umsetzung der Lenkwinkelvorgabe des Fahrers" der sichere Zustand das Aufrechterhalten der Funktion, bis der sichere Zustand auf Fahrzeugebene erreicht ist. Fehler sind zu isolieren oder abzuschalten. Verbleibende notwendige Redundanzen sind zu aktivieren oder aufrecht zu erhalten.

Auf Ebene des SbW-Systems kann für die Funktion "Handmoment-Rückmeldung zur Darstellung des Lenkgefühls" der sichere Zustand innerhalb des SbW-Systems erreicht werden. Fehler sind zu isolieren oder abzuschalten. Entweder sind verbleibende notwendige Redundanzen zu aktivieren bzw. aktiv zu halten oder es sind alternative Mitigationsmaßnahmen umzusetzen.

ANMERKUNG Mitigationsmaßnahmen sind beispielsweise erhöhte Reibung oder Dämpfung.

Um andere Sicherheitsziele nicht zu verletzen, müssen folgende zusätzliche Maßnahmen beachtet werden:

- Verbleibende redundante Steuerungs- und Energiekanäle sind zu aktivieren bzw. aktiv zu halten.
- Minimale Lenkleistung nach dem Degradationskonzept muss sichergestellt werden.

5.3.3 Sicherheitsziel SZ2

5.3.3.1 Erläuterung

Ein Ausfall der Lenkbarkeit ist ein Fehler im SbW-System, der zum Verlust der Umsetzung der Fahrerlenkwinkelvorgabe führt, und bei dem diese Funktion nicht durch andere Systeme ausreichend kompensiert werden kann. Das Sicherheitsziel ist mit ASIL D eingestuft

ANMERKUNG Mögliche Fehlerursachen für einen Ausfall der Lenkbarkeit betreffen die Wirkkette: Sensorik, Kommunikation, Steuerung, Aktuatorik, Energieversorgung, sowie mechanische Komponenten.

5.3.3.2 Akzeptanzkriterien

Bei Fehlern in einem SbW-System, welche zur Verletzung eines Sicherheitsziels führen können, müssen diese in geeigneter Weise abgeschwächt werden, sodass ein Verbleib im Fahrstreifen sichergestellt ist (siehe Abschnitt 7). Die minimale Lenkleistung muss nach dem Degradationskonzept sichergestellt werden (siehe Abschnitt 8).

5.3.3.3 Sicherer Zustand — Fahrzeug

Auf Fahrzeugebene ist der sichere Zustand erreicht, wenn die Fahrzeuggeschwindigkeit auf $\leq 10\text{ km/h}$ mit entsprechender Warnung reduziert ist.

ANMERKUNG 1 UNECE R79 Rev. 4, 5.3.3.1, verweist auf die Schwelle $\leq 10\text{ km/h}$ im Fehlerfall. Das Degradationskonzept geht situationsabhängig über den sicheren Zustand hinaus und beschreibt falls möglich auch die Überführung des Fahrzeugs in den Fahrzeugstillstand.

Der sicherere Zustand mit entsprechender Warnung ist eine ausreichende Risikominderung im Sinne der Normenreihe ISO 26262. Das verbleibende Restrisiko eines Ausfalls der Lenkbarkeit bei Geschwindigkeiten $\leq 10\text{ km/h}$ mit entsprechender Warnung ist nicht mit einem ASIL zu bewerten.

Bei Weiterfahrt im sicheren Zustand ist eine minimale Manövrierfähigkeit des Fahrzeugs vorzuhalten. Bei vollständigem Verlust der Lenkbarkeit bzw. der Fahrzeugquerführung ist das Fahrzeug, wenn technisch möglich, automatisiert in den Stillstand abzubremsen.

ANMERKUNG 2 Bisherige Erfahrungen weisen darauf hin, dass Fahrer zuerst versuchen durch mehr Lenkradbewegung das Fahrzeug zu kontrollieren, anstatt direkt zu bremsen. Die Reaktion des Fahrers, das Fahrzeug in den Stillstand zu bremsen, könnte daher verzögert sein.

Bei der Überführung des Fahrzeugs in den sicheren Zustand sind die Anforderungen des Degradationskonzepts zu erfüllen (siehe Abschnitt 8).

Der sichere Zustand auf Fahrzeugebene kann nur unter Berücksichtigung von Systemen außerhalb des SbW-Systems oder durch den Fahrer erreicht und sichergestellt werden.

5.3.3.4 Sicherer Zustand SbW-System

Auf Ebene des SbW-Systems ist für die Funktion „Umsetzung der Lenkwinkelvorgabe des Fahrers“ der sichere Zustand das Aufrechterhalten der Funktion, bis der sichere Zustand auf Fahrzeugebene erreicht ist. Fehler sind zu isolieren oder abzuschalten. Verbleibende notwendige Redundanzen sind zu aktivieren oder aufrecht zu erhalten.

5.3.4 Sicherheitsziel SZ3

5.3.4.1 Erläuterung

Der Verlust des Handmoments ist ein Fehler im SbW-System, der zum Verlust der Handmomentrückmeldung zur Darstellung des Lenkgefühls führt. Das Sicherheitsziel ist mit Minimum ASIL B eingestuft. Die Kritikalität

für den Verlust des Handmoments kann je nach System Design und Übertragungsfunktion unterschiedlich sein (z. B. Unterschiede in Reibung, Lenkübersetzung).

ANMERKUNG Mögliche Fehlerursachen für einen Verlust des Handmoments betreffen die Wirkkette: Sensorik, Kommunikation, Steuerung, Aktuatorik, Energieversorgung, sowie mechanische Komponenten. Dabei kann die Auswirkung von Fehlern sowohl zu einem Teilverlust bis hin zum Komplettverlust des Handmomentes führen.

5.3.4.2 Akzeptanzkriterien

Es müssen zwei Aspekte beim Verlust des Handmoments bezüglich der Kontrollierbarkeit berücksichtigt werden.

Zum einen müssen Fehler in einem SbW-System, welche zur Verletzung eines Sicherheitsziels führen können, in geeigneter Weise abgeschwächt werden, sodass ein Verbleib im Fahrstreifen sichergestellt ist (siehe Abschnitt 7).

Zum anderen muss die Kontrollierbarkeit des Fahrzeugs mit den verbleibenden Ersatzfunktionen (zum Beispiel Redundanz, Reibung, Dämpfung) für das Weiterfahren sichergestellt sein (siehe Abschnitt 8).

5.3.4.3 Sicherer Zustand — Fahrzeug

Auf Fahrzeugebene ist der sichere Zustand erreicht, wenn die allgemeine Kontrollierbarkeit (C0-Kontrollierbarkeit) gegeben ist oder wenn die Fahrzeuggeschwindigkeit auf ≤ 10 km/h mit entsprechender Warnung reduziert ist.

ANMERKUNG UNECE R79 Rev. 4, 5.3.3.1, verweist auf die Schwelle ≤ 10 km/h im Fehlerfall. Das Degradationskonzept geht situationsabhängig über den sicheren Zustand hinaus und beschreibt falls möglich auch die Überführung des Fahrzeugs in den Fahrzeugstillstand.

Bei der Überführung des Fahrzeugs in den sicheren Zustand sind die Anforderungen des Degradationskonzepts zu erfüllen (siehe Abschnitt 8).

Wenn der sichere Zustand nicht durch eine allgemeine Kontrollierbarkeit erreicht wird, kann der sichere Zustand auf Fahrzeugebene nur unter Berücksichtigung von Systemen außerhalb des SbW-Systems oder durch den Fahrer erreicht und sichergestellt werden.

5.3.4.4 Sicherer Zustand SbW-System

Auf Ebene des SbW-Systems kann für die Funktion „Handmoment-Rückmeldung zur Darstellung des Lenkgefühls“ der sichere Zustand innerhalb des SbW-Systems erreicht werden. Fehler sind zu isolieren oder abzuschalten. Entweder sind verbleibende notwendige Redundanzen zu aktivieren bzw. aktiv zu halten oder es sind alternative Mitigationsmaßnahmen umzusetzen.

ANMERKUNG Mitigationsmaßnahmen sind beispielsweise erhöhte Reibung oder Dämpfung.

5.3.5 Sicherheitsziel SZ4

5.3.5.1 Erläuterung

Ein Verlust der Lenkbarkeit durch ein ungewolltes zu hohes Handmoment, welches entgegen der Lenkbewegung des Fahrers wirkt (Schwergängigkeit bis hin zum Blockieren des Lenkradaktuators), muss verhindert werden. Dies umfasst sowohl die elektromechanische als auch die mechanische Schwergängigkeit bis hin zum Blockieren. Das Sicherheitsziel ist mit ASIL D eingestuft.

ANMERKUNG 1 Mögliche elektromechanische Fehlerursachen für ein zu hohes Handmoment betreffen die Wirkkette: Sensorik, Kommunikation, Steuerung, Aktuatorik. Beispiele sind z. B. Simulation des dynamischen Endanschlags (End-Stop) bei einem falschen Lenkwinkel oder Phasenkurzschluss im Lenkradaktuator.

ANMERKUNG 2 Mögliche mechanische Fehlerursachen für ein zu hohes Handmoment betreffen die mechanischen Komponenten, z. B. mechanischer Endanschlag, erhöhte Reibung (Schwergängigkeit).

ANMERKUNG 3 SZ4 unterscheidet sich vom SZ1 dadurch, dass durch Fehler keine aktive Lenkbewegung am Lenkrad-aktuator hervorgerufen wird. Vielmehr wird die Lenkbewegung des Fahrers verhindert bzw. das Handmoment wird bis hin zum Blockieren erhöht.

5.3.5.2 Akzeptanzkriterien

Es müssen zwei Aspekte beim ungewollten Blockieren des Lenkrads bezüglich der Kontrollierbarkeit berücksichtigt werden.

Zum einen müssen Fehler in einem SbW-System, welche zur Verletzung eines Sicherheitsziels führen können, in geeigneter Weise abgeschwächt werden, sodass ein Verbleib im Fahrstreifen sichergestellt ist (siehe Abschnitt 7).

Zum anderen muss die Kontrollierbarkeit des Fahrzeugs mit den verbleibenden Ersatzfunktionen (zum Beispiel Redundanz, Reibung, Dämpfung) für das Weiterfahren sichergestellt sein (siehe Abschnitt 8).

5.3.5.3 Sicherer Zustand — Fahrzeug

Auf Fahrzeugebene ist der sichere Zustand erreicht, wenn die allgemeine Kontrollierbarkeit (C0-Kontrollierbarkeit) gegeben ist oder wenn die Fahrzeuggeschwindigkeit auf ≤ 10 km/h mit entsprechender Warnung reduziert ist.

ANMERKUNG UNECE R79 Rev. 4, 5.3.3.1, verweist auf die Schwelle ≤ 10 km/h im Fehlerfall. Das Degradationskonzept geht situationsabhängig über den sicheren Zustand hinaus und beschreibt falls möglich auch die Überführung des Fahrzeugs in den Fahrzeugstillstand.

Bei der Überführung des Fahrzeugs in den sicheren Zustand sind die Anforderungen des Degradationskonzepts zu erfüllen (siehe Abschnitt 8).

Wenn der sichere Zustand nicht durch eine allgemeine Kontrollierbarkeit erreicht wird, kann der sichere Zustand auf Fahrzeugebene nur unter Berücksichtigung von Systemen außerhalb des SbW-Systems oder durch den Fahrer erreicht und sichergestellt werden.

5.3.5.4 Sicherer Zustand SbW-System

Auf Ebene des SbW-Systems kann für die Funktion „Handmoment-Rückmeldung zur Darstellung des Lenkgefühls“ der sichere Zustand innerhalb des SbW-Systems erreicht werden. Fehler sind zu isolieren oder abzuschalten. Entweder sind verbleibende notwendige Redundanzen zu aktivieren bzw. aktiv zu halten oder es sind alternative Mitigationsmaßnahmen umzusetzen.

ANMERKUNG Mitigationsmaßnahmen sind beispielsweise erhöhte Reibung oder Dämpfung.

5.3.6 Sicherheitsziel SZ5

5.3.6.1 Erläuterung

Eine unaufgeforderte und unkontrollierbare Lenkwinkeländerung oder Lenkwinkelabweichung aufgrund von Asynchronitäten zwischen Lenkradwinkel und Radlenkwinkel muss verhindert werden. Das Sicherheitsziel ist mit ASIL D eingestuft

ANMERKUNG 1 Ursachen, die zu einer Asynchronität führen können, sind z. B.:

- Lenkleistungslimitierung des Radaktuators bei sehr schnellen Lenkbewegungen;
- Laufzeitverzögerungen;

- Riemensprung;
- fehlerhaftes Umschalten zwischen Lenkübersetzungen (z. B. Sport, Normal, Comfort);
- ungewollte Änderungen mit maximalen Gradienten in der variablen Lenkübersetzung, ggf. durch Fahrzeuggeschwindigkeitsänderungen;
- Abbau von existierenden Lenkwinkelabweichungen;
- Radaktuator und Lenkradaktuator sind vor Fahrtbeginn nicht synchronisiert; und
- Behinderung des Radaktuators durch externe Einflüsse (z. B. sehr tiefe Spurrillen, Bordstein).

Eine detaillierte Betrachtung von Situationen und eine damit einhergehende Aufteilung in mehrere Sicherheitsziele ggf. mit unterschiedlichem ASIL ist möglich. Hierfür ist dann die Unabhängigkeit nachzuweisen.

ANMERKUNG 2 Der Unterschied zwischen SZ5 zu SZ1, SZ2 & SZ4 ist, dass die Lenkbarkeit nicht vollständig verloren wird, aber die Beeinträchtigung der Lenkbarkeit durch die Asynchronität zu nicht kontrollierbaren Trajektorien-Abweichungen führen kann.

ANMERKUNG 3 Sowohl der Aufbau als auch der Abbau von Asynchronitäten führt möglicherweise zu einer reduzierten Kontrollierbarkeit.

5.3.6.2 Akzeptanzkriterium für SZ5

Bei der Entwicklung eines SbW-Systems muss darauf geachtet werden, dass trotz einer möglicherweise vorhandenen Asynchronität die Kontrollierbarkeit sichergestellt ist. Bei Fehlern in einem SbW-System, welche zur Verletzung eines Sicherheitsziels führen können, müssen diese in geeigneter Weise abgeschwächt werden, sodass ein Verbleib im Fahrstreifen sichergestellt ist. Maximale Asynchronitäten, sowie die Steuerungsstrategien zum Auf- und Abbau von Asynchronitäten, müssen für den Fahrer kontrollierbar sein.

Eine partielle Betrachtung der Asynchronität im SbW-Lenkssystem erfolgt in Abschnitt 8.

ANMERKUNG Die Asynchronität wird bei der Bewertung der Kontrollierbarkeit im Erstfehlerfall in Abschnitt 7 nicht weiter betrachtet, da ein generisches Fehlerbild nicht definiert werden kann.

Es wird empfohlen, dass der Normanwender einen Prüfkatalog erstellt, der die Spezifikation von „worst case-scenarios“ (z. B. tiefe Spurrillen, Bordsteinkanten, Leistungseinschränkungen, Umschalten zwischen Lenkmodi) beinhaltet.

5.3.6.3 Sicherer Zustand — Fahrzeug

Auf Fahrzeugebene ist der sichere Zustand erreicht, wenn die Fahrzeuggeschwindigkeit auf ≤ 10 km/h mit entsprechender Warnung reduziert ist.

ANMERKUNG UNECE R79 Rev. 4, 5.3.3.1, verweist auf die Schwelle ≤ 10 km/h im Fehlerfall. Das Degradationskonzept geht situationsabhängig über den sicheren Zustand hinaus und beschreibt falls möglich auch die Überführung des Fahrzeugs in den Fahrzeugstillstand.

Bei der Überführung des Fahrzeugs in den sicheren Zustand sind die Anforderungen des Degradationskonzepts zu erfüllen (siehe Abschnitt 8).

Der sichere Zustand auf Fahrzeugebene kann nur unter Berücksichtigung von Systemen außerhalb des SbW-Systems oder durch den Fahrer erreicht und sichergestellt werden.

5.3.6.4 Sicherer Zustand SbW-System

Auf Ebene des SbW-Systems ist für die Funktion „Umsetzung der Lenkwinkelvorgabe des Fahrers“ der sichere Zustand das Aufrechterhalten der Funktion, bis der sichere Zustand auf Fahrzeugebene erreicht ist. Fehler sind zu isolieren oder abzuschalten. Entweder sind verbleibende notwendige Redundanzen zu aktivieren bzw. aktiv zu halten oder es sind alternative Mitigationsmaßnahmen (z. B. Regelstrategien zur Abschwächung der Asynchronität und zur Aufrechterhaltung der Kontrollierbarkeit) umzusetzen.

6 Anforderungen an die Systemverfügbarkeit

6.1 Allgemeine Verfügbarkeitsanforderungen

Bei der Herleitung der Systemverfügbarkeit müssen unter anderem die folgenden Anforderungen erfüllt werden:

- Aus den Sicherheitszielen der HARA müssen sicherheitsrelevante Verfügbarkeitsanforderungen abgeleitet werden.

ANMERKUNG 1 Klassifizierungsbeispiele können „fail safe“ und „fail operational“ sein.

- Für das Erreichen der sicheren Zustände der Sicherheitsziele muss eine ausreichende sicherheitsrelevante Verfügbarkeit vorhanden sein. Dies kann über E/E-Redundanz erreicht werden, wie in den Beispielarchitekturen im Anhang C, Abschnitt C.3, beschrieben.

ANMERKUNG 2 In diesem Dokument betrifft diese Anforderung die Sicherheitsziele 2 und 3.

ANMERKUNG 3 Die Beispielarchitekturen im Anhang C, Abschnitt C.3, setzen eine ausreichende Integrität der E/E-Elemente und ihrer notwendigen Diagnosen voraus.

- Die zum Erreichen des sicheren Zustandes unter Berücksichtigung des Degradationskonzepts nötige Energie muss zur Verfügung gestellt werden. Dabei muss der Energiebedarf der relevanten Fahrzeugsysteme während der Überführung in den sicheren Zustand berücksichtigt werden.
- Die zur Lenkbarkeit bzw. Fahrzeugquerführung und Kontrollierbarkeit geforderte Systemintegrität (z. B. Lenkleistung, Handmoment) in den Degradationen und Transitionen zur Überführung in den sicheren Zustand muss verfügbar sein und ist in Abschnitt 8 definiert.

Im Rahmen der Betrachtung der sicherheitsrelevanten Verfügbarkeit des SbW-Systems werden nach Item-Definition weitere Funktionalitäten wie z. B. Energieversorgung und Kommunikation auf Fahrzeugebene in diesem Dokument nicht berücksichtigt.

Hinsichtlich der Verfügbarkeit auf Fahrzeugebene sind alternative Möglichkeiten zur Fahrzeugquerführung zulässig und können weitere Potenziale bieten.

ANMERKUNG 4 Alternative Möglichkeiten zur Fahrzeugquerführung sind z. B. einseitige Bremsengriffe oder eine Hinterradlenkung.

6.2 Verfügbarkeitsanforderungen nach Fehlerfall

Im Falle eines Fehlers, der die Sicherheitsintegrität des SbW-Systems reduziert, muss die Lenkbarkeit und Kontrollierbarkeit des Fahrzeugs ausreichend lange aufrechterhalten bleiben, sodass der Fahrer das Fahrzeug in einen sicheren Zustand (siehe Abschnitt 5) bringen kann.

Die verfügbare Weiterfahrzeit sollte dem Fahrer ein sicheres Anhalten im Sinne eines sicheren Verlassens der Fahrsituation und Erreichen eines sicheren Abstellpunktes ermöglichen.

Für die Bestimmung der Weiterfahrzeit sind die folgenden Aspekte zu berücksichtigen:

- Für die Ermittlung der minimalen Weiterfahrzeit sind mögliche Umweltbedingungen, welche für ein sicheres Anhalten bzw. für das Erreichen eines sicheren Abstellpunkts relevant sind, zu berücksichtigen. Im Besonderen sind u. a. maximale Längen von Brücken, Tunneln, Baustellen und die Abstände von Autobahnabfahrten zu betrachten.

ANMERKUNG 1 Begründete Ausnahmen sind zulässig (z. B. im Falle von geringem Ladezustand im Energiespeicher).

- Bei der Festlegung der maximal zulässigen Weiterfahrzeit sind die Anforderungen an die „Emergency Operation“ nach ISO 26262 (alle Teile) anzuwenden.
- Ein Sicherheitsfaktor zur Ermittlung der maximal zulässigen Weiterfahrzeit ist zu definieren.
- Ein Sicherheitsfaktor der Größenordnung 10 wird empfohlen.
- Die maximal zulässige Obergrenze für die Weiterfahrzeit ist das kürzeste „Emergency Operation Tolerance Time Interval“ (EOTTI) nach ISO 26262 (alle Teile) mit Berücksichtigung des definierten Sicherheitsfaktors.

ANMERKUNG 2 Bei der Definition des Sicherheitsfaktors sind die Analysen und Maßnahmen der Normenreihe ISO 26262 hinsichtlich Fehler gleicher Art (z. B. Bauteilalterung, systematische Qualitätsprobleme in der Herstellung) sowie systematische Fehler zu berücksichtigen.

In Bild 4 ist die angestrebte minimale Weiterfahrzeit und beispielhafte Umweltbedingungen mit Zeiten und Fahrstrecken angegeben und es ist die maximal mögliche Weiterfahrzeit dargestellt.

Die Weiterfahrzeit soll dem Fahrer ermöglichen, einen sicheren Abstellpunkt zu erreichen. Ein früheres Anhalten durch den Fahrer muss jederzeit gegeben sein.

Möglicherweise wird die angestrebte Weiterfahrzeit durch die Verfügbarkeit der unterstützenden Systeme (z. B. Energiebordnetz) eingeschränkt. Dies muss bei der Auslegung der Weiterfahrzeit berücksichtigt werden.

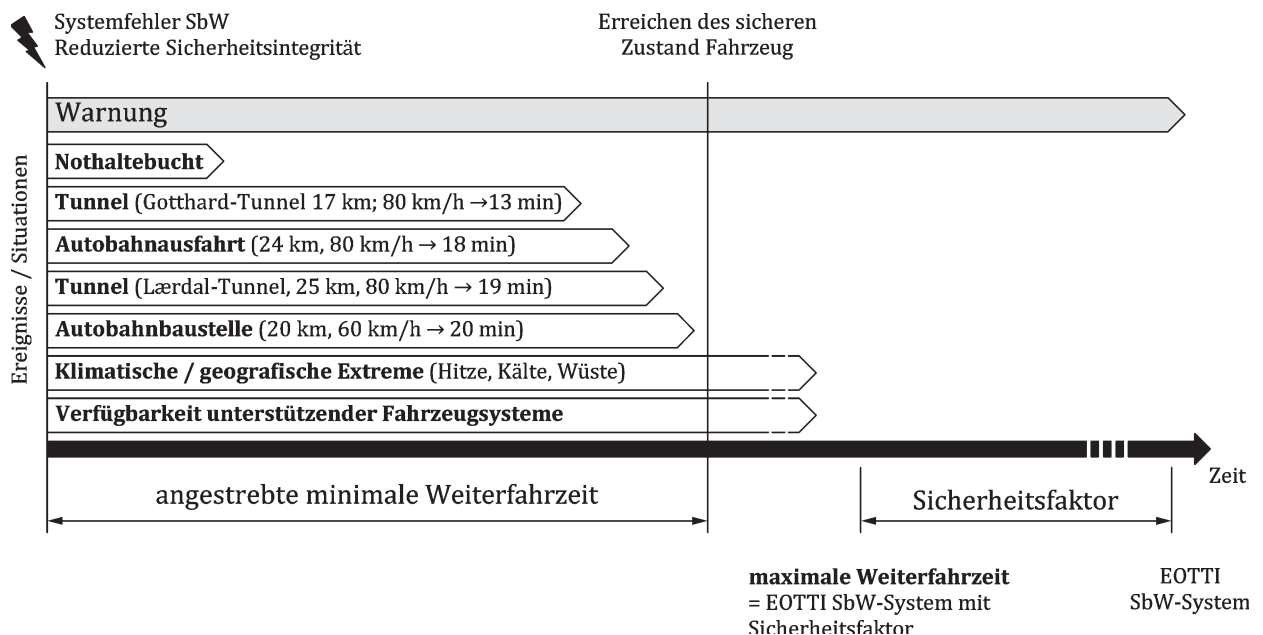


Bild 4 — Weiterfahrzeit bei reduzierter Sicherheitsintegrität

ANMERKUNG 3 Extreme klimatische und geografische Bedingungen (Hitze, Kälte, Wüste) können bei der Ermittlung der Weiterfahrzeit berücksichtigt werden.

6.3 Verfügbarkeitsanforderungen an mechanische Systemumfänge

Mechanische Fehler können bei SbW-Systemen kritische Gefährdungen hervorrufen. Es können die gleichen Methodiken wie bei konventionellen Lenksystemen zur Absicherung der Systemauslegung und Verifikation der Mechanik angewendet werden.

ANMERKUNG 1 Methodiken zur Absicherung der Systemauslegung sind z. B. Robustheits- und Zuverlässigkeitsanalysen.

ANMERKUNG 2 Mechanische Teilkomponenten im SbW-System können gegenüber konventionellen Lenksystemen veränderte Sicherheitseinstufungen erfordern.

7 Kontrollierbarkeit im Erstfehlerfall

7.1 Einleitung und Allgemeines zur Kontrollierbarkeit

In diesem Abschnitt werden die Anforderungen an die Bewertung der Kontrollierbarkeit des Fahrzeugs im Erstfehlerfall definiert. Die Anforderungen berücksichtigen die in 5.3 definierten Sicherheitsziele und stellen einen Mindestumfang von Anforderungen an die Bewertung der Kontrollierbarkeit dar. Der Anwender der Norm muss die Kontrollierbarkeitsbewertung für ein konkretes SbW-System basierend auf einer vollständigen HARA für eventuell zusätzliche Sicherheitsziele und Sicherheitsanforderungen entsprechend erweitern.

7.2 Fehlerbilder

7.2.1 Allgemeines

Die im folgenden erläuterten Fehlerbilder sind während der Entwicklung eines SbW-Systems zu überprüfen, um Systemfehler und deren Auswirkung auf Fahrzeug-Umgebungs-Ebene oder Fahrzeug-Fahrer-Ebene im Hinblick auf die Kontrollierbarkeit des Fahrzeugs zu bewerten. Insgesamt werden 11 Fehlerbilder betrachtet (siehe Tabelle 1).

ANMERKUNG Jedes der folgenden Fehlerbilder führt möglicherweise ohne geeigneten Sicherheitsmechanismus zur Verletzung eines Sicherheitsziels.

Ein Fehlerbild im Kontext der Bewertung der Kontrollierbarkeit setzt sich zusammen aus der Fehlfunktion, der Fehlerquelle, der Fehlerausprägung und der Fehlercharakteristik mit zugehöriger physikalischer Beschreibung.

7.2.2 Fehlfunktionen

Den Sicherheitszielen aus 5.3 liegen folgende Fehlfunktionen zu Grunde:

- Selbstlenker;
- Ausfall der Lenkbarkeit;
- Verlust des Handmoments;
- Blockieren der Lenkung; und
- Asynchronität zwischen Lenkradwinkel und Radlenkwinkel.

Die Asynchronität zwischen Lenkradwinkel und Radlenkwinkel wird im Rahmen der Kontrollierbarkeit im Erstfehlerfall nicht betrachtet, da ein generisches Fehlerbild nicht definiert werden kann. Betrachtungen zur Bewertung der Kontrollierbarkeit bei Weiterfahrt im Fehlerfall erfolgen in Abschnitt 8.

7.2.3 Fehlerquelle

Für die Bewertung der Kontrollierbarkeit des Fahrzeugs bei den Fehlfunktionen aus 7.2.2 werden als Fehlerquellen der Radaktuator und Lenkradaktuator betrachtet. Die Auswirkungen von Fehlern auf das SbW-System wie z. B. Fehler im Energiebordnetz oder im Kommunikationsnetzwerk werden auch den Fehlerquellen Radaktuator und Lenkradaktuator zugeordnet.

7.2.4 Fehlerausprägung

7.2.4.1 Reversibler Fehler

Reversible Fehler sind Fehler, deren Fehlerwirkungen von systemeigenen Sicherheitsmechanismen zeitlich begrenzt werden müssen, um die Kontrollierbarkeit sicherzustellen. Die im Hinblick auf die Kontrollierbarkeit zulässige Fehlerdauer muss in Abhängigkeit von der anliegenden Fehlfunktion, der Fehlerquelle und der Fehlercharakteristik bestimmt werden.

7.2.4.2 Irreversibler Fehler

Irreversible Fehler sind Fehler, deren Fehlerwirkungen von systemeigenen Sicherheitsmechanismen nicht oder nicht vollständig kompensiert werden und zeitlich nicht begrenzt sind. Die Fehlerdauer muss mindestens 2 s betragen, wobei die erlaubte physikalische Größe der Fehlercharakteristik (siehe 7.2.5) bestimmt werden muss.

ANMERKUNG Die Fehlerdauer von 2 s wurde definiert, da sich nach dieser Zeit der Fahrer an die Fehlerwirkung adaptiert hat und die Kontrollierbarkeit trotz weiterhin bestehender Fehlerwirkung gegeben ist.

7.2.5 Fehlercharakteristiken mit den zugehörigen physikalischen Größen

7.2.5.1 Blockieren

Beim Blockieren wirkt ein Moment entgegen der Lenkrad- bzw. Lenkbewegung, sodass eine Lenkrad- bzw. Lenkbewegung verhindert wird. Beim Blockieren wird ausschließlich eine reversible Fehlerausprägung betrachtet.

Die vorgegebene physikalische Größe beim Blockieren am Lenkradaktuator ist der eingefrorene Lenkradwinkel.

Die vorgegebene physikalische Größe beim Blockieren am Radaktuator ist der eingefrorene Radlenkwinkel.

Die gesuchte physikalische Größe im Hinblick auf die Kontrollierbarkeit ist die zulässige Fehlerdauer.

Beim Blockieren muss die vorgegebene physikalische Größe (Lenkradwinkel oder Radlenkwinkel) über die Fehlerdauer konstant gehalten werden.

7.2.5.2 Oszillation

Die Oszillation beschreibt einen oszillierenden rechteckigen Momentenverlauf am Lenkradaktuator oder einen oszillierenden rechteckigen Radlenkwinkelverlauf am Radaktuator. Bei der Oszillation wird ausschließlich eine irreversible Fehlerausprägung betrachtet.

ANMERKUNG 1 Die Oszillation wurde als Ersatz-Fehlercharakteristik gewählt, um stochastische Fehler abzubilden.

ANMERKUNG 2 Eine rechteckige Oszillation stellt durch ihren sprungförmigen Charakter den kritischsten Fall von Oszillationen dar.

Die vorgegebenen physikalischen Größen bei der Oszillation sind die Fehlerdauer $t_{\text{Fehler}} \geq 2 \text{ s}$ und die Fehlerfrequenz.

Die Frequenz der Oszillation muss so gewählt werden, dass sowohl der Einfluss der Eigenfrequenz des Fahrzeugs als auch die Frequenz der verstärkenden Kompensation des Fahrers berücksichtigt werden.

ANMERKUNG 3 Typische Größenordnungen für die Frequenz der Oszillation liegen bei 1,2 Hz bis 1,5 Hz.

Die gesuchte physikalische Größe ist die Handmomenten-Amplitude am Lenkradaktuator oder die Radlenkwinkel-Amplitude am Radaktuator.

Die Oszillation muss die vorgegebene physikalischen Größe (Handmoment, Radlenkwinkel) additiv überlagern.

7.2.5.3 Sprung

Der Sprung beschreibt eine sprungartige Änderung im Handmoment durch den Lenkradaktuator oder eine sprungartige Änderung im Radlenkwinkel durch den Radaktuator. Beim Sprung werden sowohl reversible als auch eine irreversible Fehlerausprägungen betrachtet. Um die sprungartige Änderung zu realisieren, muss die maximal mögliche Dynamik des jeweiligen Aktuators angefordert werden.

Reversibler Sprung

Die vorgegebene physikalische Größe bei einem reversiblen Sprung im Lenkradaktuator ist die maximal mögliche Handmomentanforderung.

Die vorgegebene physikalische Größe bei einem reversiblen Sprung am Radaktuator ist die maximal mögliche Radlenkwinkelanforderung. Eine weitere mögliche Fehlercharakteristik des reversiblen Sprungs ist der sprungartige Verlust des Moments am Radaktuator. Hier ist die vorgegebene physikalische Größe das Motor-moment von 0 Nm.

Die gesuchte physikalische Größe im Hinblick auf die Kontrollierbarkeit des reversiblen Sprungs ist die zulässige Fehlerdauer.

Beim reversiblen Sprung muss die vorgegebene physikalische Größe (Handmoment oder Radlenkwinkel) ersetzt werden.

Irreversibler Sprung

Die vorgegebene physikalische Größe des irreversiblen Sprungs im Lenkradaktuator oder Radaktuator ist die Fehlerdauer $t_{\text{Fehler}} \geq 2 \text{ s}$.

Die gesuchte physikalische Größe bei einem irreversiblen Sprung im Lenkradaktuator ist die maximal kontrollierbare Handmomentanforderung.

Die gesuchte physikalische Größe bei einem irreversiblen Sprung im Radaktuator ist die Radlenkwinkelanforderung.

Beim irreversiblen Sprung muss die vorgegebene physikalische Größe (Handmoment oder Radlenkwinkel) additiv überlagert werden.

7.2.5.4 Schwergängigkeit

Eine Schwergängigkeit ist ein passiv erzeugtes Moment, das in Abhängigkeit der Lenkradwinkelgeschwindigkeit der Lenkbewegung entgegenwirkt. Bei der Schwergängigkeit wird ausschließlich eine irreversible Fehlerausprägung am Lenkradaktuator betrachtet.

Die vorgegebene physikalische Größe der Schwergängigkeit am Lenkradaktuator ist die Fehlerdauer von $t_{\text{Fehler}} \geq 2 \text{ s}$.

Die gesuchte physikalische Größe ist das maximal kontrollierbare Handmoment in Abhängigkeit der Lenkradwinkelgeschwindigkeit.

Bei der Schwergängigkeit muss die vorgegebene physikalische Größe (Handmoment) ersetzt werden.

ANMERKUNG Eine Schwergängigkeit entsteht beispielsweise durch einen elektrischen Defekt im Lenkradaktuator oder durch mechanische Reibung.

7.2.6 Fehlerbild mit Verlust des aktiv generierten Handmoments

Ein Verlust der vom Lenkradaktuator aktiv generierten Handmomente führt nicht unbedingt zu einem Verlust der Kontrollierbarkeit des Fahrzeugs. Wenn dabei aufgrund von systemimmanenter Reibung oder Dämpfung des Lenkradaktuators passiv generierte Handmomente verbleiben, können diese dazu beitragen, dass die Kontrollierbarkeit bei einem solchen Fehlerbild (siehe 7.4) gegeben ist.

Allerdings ist dieses Fehlerbild deutlich kritischer zu betrachten, wenn dem Verlust des aktiv generierten Handmoments ein Selbstlenker vorausgeht, in dessen Folge die Antriebseinheit des Lenkradaktuators durch Abschalten in einen sicheren Zustand versetzt wird.

Dem Fehlerbild 11 (siehe Tabelle 1) liegt dementsprechend die Annahme zugrunde, dass bei einem nicht redundant ausgeführten Lenkradaktuator auf die reversible Fehlerausprägung des Selbstlenkers nach Fehlerbild 7 (Phase 1) unmittelbar ein irreversibler Verlust des aktiv generierten Handmoments folgt (Phase 2).

Die vorgegebene physikalische Größe in Phase 1 ist in Analogie zum Fehlerbild 7 die maximale Handmomenten-Amplitude in der Fehlfunktion Selbstlenker. Die gesuchte physikalische Größe im Hinblick auf die Kontrollierbarkeit des Fahrzeugs bei der Fehlfunktion Selbstlenker ist die zulässige Fehlerdauer.

Zusätzlich zum Fehlerbild 7 sind die physikalischen Wechselwirkungen mit der Ausprägung der verbleibenden passiv generierten Handmomente zu berücksichtigen. Eine schwache Ausprägung der passiv generierten Handmomente führt in der Regel zu sehr kleinen Werten für die zulässige Fehlerdauer in der Phase 1. Wenn die Fehlerdauer beispielsweise aus technischen Gründen nicht weiter eingeschränkt werden kann, muss durch zusätzliche Maßnahmen sichergestellt werden, dass die Kontrollierbarkeit des Fahrzeugs bei dem Fehlerbild 11 sichergestellt ist.

Im geschlossenen Regelkreis Fahrer-Fahrzeug-Umgebung folgt auf eine externe Störung zunächst die Wahrnehmung der Störung durch den Fahrer und dann die Kompensation der Störung durch den Fahrer. Beim Fehlerbild 11 kompensiert der Fahrer nicht nur die direkten Folgen eines Handmomentsprungs in Form einer Abweichung des Lenkradwinkels, sondern gleichzeitig eine Veränderung des gewohnten Zusammenhangs zwischen Handmomentänderung und Lenkwinkeländerung. Ziel der zusätzlichen Maßnahmen ist es, mit Hilfe von passiv generiertem Handmoment, beispielsweise in Form von Reibung oder Dämpfung im Lenkradaktuator die Anforderungen an die kompensatorischen Fähigkeiten des Fahrers zu verringern und dadurch die Kontrollierbarkeit des Fahrzeugs im Fall des Fehlerbilds 11 sicherzustellen.

7.3 Fehlerbildmatrix

Durch Kombination von Fehlfunktionen, Fehlerquellen, Fehlerausprägungen und den Fehlercharakteristiken wurden 11 Fehlerbilder zusammengestellt, die im Hinblick auf die Kontrollierbarkeit des Fahrzeugs von besonderer Bedeutung sind. Diese sind in Tabelle 1 gezeigt, wobei jede Zeile ein Fehlerbild beschreibt.

Bei der Zusammenstellung der Fehlerbilder wurde davon ausgegangen, dass der Radaktuator entsprechend der Beispielarchitektur redundant ausgeführt ist (siehe Anhang C, Abschnitt C.3).

Die Kontrollierbarkeit des Fahrzeugs bei diesen Fehlerbildern muss, wie in 7.4 beschrieben, bewertet werden.

Tabelle 1 — Fehlerbildmatrix

Fehler- bild	Fehlfunktion	Fehlerquelle	Fehler- ausprägung	Fehler- charakteristik	Vorgegebene physikalische Größe	Gesuchte physikalische Größe
1	Blockieren der Lenkung	Lenkradaktuator	irreversibel	Schwer- gängigkeit ^a	$t_{\text{Fehler}} \geq 2 \text{ s}$	Handmoment entgegen der Lenk- bewegung des Fahrers in Abhängigkeit der Lenkradwinkelgeschwindigkeit
2	Blockieren der Lenkung	Lenkradaktuator	reversibel	Blockieren ^a	eingefrorener Lenkradwinkel	t_{Fehler}
3	Ausfall Lenkbarkeit	Radaktuator	reversibel	Blockieren ^a	eingefrorener Radlenkwinkel	t_{Fehler}
4	Ausfall Lenkbarkeit	Radaktuator	reversibel	Sprung ^b	Motormoment	t_{Fehler}
5	Selbstlenker	Lenkradaktuator	irreversibel	Sprung ^c	$t_{\text{Fehler}} \geq 2 \text{ s}$	Handmomenten-Amplitude
6	Selbstlenker	Lenkradaktuator	irreversibel	Oszillation ^c	$t_{\text{Fehler}} \geq 2 \text{ s}$	Handmomenten-Amplitude, Fehlerfrequenz
7	Selbstlenker	Lenkradaktuator	reversibel	Sprung ^a	max. Handmomenten-Amplitude (aktiv) mit max. Dynamik	t_{Fehler}
8	Selbstlenker	Radaktuator	irreversibel	Sprung ^c	$t_{\text{Fehler}} \geq 2 \text{ s}$	Radlenkwinkel-Amplitude
9	Selbstlenker	Radaktuator	irreversibel	Oszillation ^c	$t_{\text{Fehler}} \geq 2 \text{ s}$	Radlenkwinkel-Amplitude, Fehlerfrequenz
10	Selbstlenker	Radaktuator	reversibel	Sprung ^a	max. Radlenkwinkel-Amplitude (aktiv) mit max. Dynamik	t_{Fehler}
11	Selbstlenker mit anschließendem Verlust des aktiv generierten Handmoments	Lenkradaktuator	irreversibel	Sprung ^a	Phase 1: Selbstlenker	
					max. Handmomenten-Amplitude (aktiv) mit max. Dynamik	t_{Fehler}
					Phase 2: Verlust Handmoment	
					$t_{\text{Fehler}} \geq 2 \text{ s}$	min. passiv generiertes Handmoment
^a Physikalische Größe wird durch Fehlerwert ersetzt.						
^b Physikalische Größe wird durch Fehlerwert 0 Nm ersetzt.						
^c Physikalische Größe wird mit Fehlerwert additiv überlagert.						

7.4 Bewertung der Kontrollierbarkeit im Fehlerfall

Die Kontrollierbarkeit des Fahrzeugs unter der Einwirkung der nach 7.3 ausgewählten Fehlerbilder des SbW-Systems muss anhand der in 7.5 festgelegten Fahrmanöver bewertet werden.

Die Bewertung der Kontrollierbarkeit muss im geschlossenen Regelkreis Fahrer-Fahrzeug-Umgebung erfolgen. Auf diese Weise wird die Reaktion des Fahrers auf das Fehlerbild während des Fahrmanövers berücksichtigt.

Die Bewertung der Kontrollierbarkeit muss anhand der Bewertungsstufen C0 (allgemein kontrollierbar), C1 (einfach kontrollierbar), C2 (normal kontrollierbar) und C3 (schwierig kontrollierbar oder nicht kontrollierbar) nach ISO 26262 (alle Teile) erfolgen.

ANMERKUNG 1 Neben der Auftretenswahrscheinlichkeit und dem möglichen Schadensausmaß berücksichtigt die ASIL-Einstufung von sicherheitskritischen Funktionen die Kontrollierbarkeit bei potenziellen Fehlern als Einstufungskriterium. Zusätzlich wird die Kontrollierbarkeit als Bewertungskriterium für die Wirksamkeit von Sicherheitsmechanismen zur Abschwächung von Fehlerwirkungen herangezogen (siehe ISO 26262 (alle Teile)).

Für die Bewertung müssen Fehlerbild-Fahrmanöver-Kombinationen herangezogen werden, die im Hinblick auf die Kontrollierbarkeit des Fahrzeugs im Fehlerfall von besonderer Relevanz sind.

Tabelle 2 gibt für die in 7.3 ausgewählten Fehlerbilder und die in 7.5 festgelegten Fahrmanöver einen Überblick über diese Kombinationen.

Tabelle 2 — Kombinationen ausgewählter Fehlerbilder mit Fahrmanövern

Fehler- bild	Fehlfunktion	Fehlerquelle	Fehler- ausprägung	Fehlercharakteristik	Manöver		
					Geradeaus- fahrt	Kreis- fahrt	Slalom
1	Blockieren der Lenkung	Lenkradaktuator	irreversibel	Schwergängigkeit ^a	—	—	X
2	Blockieren der Lenkung	Lenkradaktuator	reversibel	Blockieren ^a	—	—	X
3	Ausfall der Lenkbarkeit	Radaktuator	reversibel	Blockieren ^a	—	—	X
4	Ausfall der Lenkbarkeit	Radaktuator	reversibel	Sprung ^b	—	X	X
5	Selbstlenker	Lenkradaktuator	irreversibel	Sprung ^c	X	—	X
6	Selbstlenker	Lenkradaktuator	irreversibel	Oszillation ^c	X	X	—
7	Selbstlenker	Lenkradaktuator	reversibel	Sprung ^a	X	—	—
8	Selbstlenker	Radaktuator	irreversibel	Sprung ^c	X	X	—
9	Selbstlenker	Radaktuator	irreversibel	Oszillation ^c	X	X	—
10	Selbstlenker	Radaktuator	reversibel	Sprung ^a	X	—	—
11	Selbstlenker mit anschließendem Verlust des aktiv generierten Handmoments	Lenkradaktuator	irreversibel	Sprung ^a	X ^d	X	—
^a Physikalische Größe wird durch Fehlerwert ersetzt. ^b Physikalische Größe wird durch Fehlerwert 0 Nm ersetzt. ^c Physikalische Größe wird mit Fehlerwert additiv überlagert. ^d Versuch bei 120 km/h und einer Fahrstreifenbreite von 3,25 m.							

Mittels der Bewertung der Kontrollierbarkeit müssen für jedes Fehlerbild Grenzwerte für die physikalischen Größen der Fehlerbilder nach Tabelle 1 festgelegt und bestätigt werden.

Die Grenzwerte müssen system- und fahrzeugspezifisch bestätigt werden, weil davon auszugehen ist, dass die gesuchten physikalischen Größen der Fehlerbilder über verschiedene Fahrzeugtypen hinweg betrachtet, stark variieren.

Die Grenzwerte für die physikalischen Größen gelten als bestätigt, wenn das zugehörige Fehlerbild keine besonderen Anforderungen an die Kontrollierbarkeit stellt, also wenn die Bewertung unterhalb der Schwelle zwischen den Bewertungsstufen C0 und C1 nach ISO 26262 (alle Teile) liegt.

Wenn die Bewertung der Kontrollierbarkeit für eine Fehlerbild-Fahrmanöver-Kombination nicht unterhalb dieser Schwelle liegt, müssen die zugehörigen Grenzwerte für die physikalischen Größen so weit reduziert werden, bis die Schwelle unterschritten ist.

In jedem Fall muss die Kontrollierbarkeit als nicht ausreichend angesehen werden, wenn das Fahrzeug während des Fahrmanövers die vorgegebenen Fahrstreifengrenzen infolge des Fehlerbilds überfährt.

Die so ermittelten Grenzwerte für die physikalischen Größen der Fehlerbilder sollten die Grundlage bilden für die Anforderungen an die Sicherheitsmechanismen des SbW-Systems.

Die Bewertung der Kontrollierbarkeit muss in Form einer subjektiven Bewertung durch Expertenfahrer erfolgen.

ANMERKUNG 2 Das Risiko einer Fehleinschätzung wird reduziert, wenn die subjektive Bewertung von mehreren Expertenfahrern vorgenommen wird.

Die subjektive Bewertung der Kontrollierbarkeit muss für jede Fahrmanöver-Fehlerbild-Kombination im geschlossenen Regelkreis Fahrer-Fahrzeug-Umgebung anhand von objektiven fahrdynamischen Kenngrößen plausibilisiert werden.

Die objektiven fahrdynamischen Kenngrößen müssen dabei den Grad der querdynamischen Störung widerspiegeln, der durch das Fehlerbild im geschlossenen Regelkreis Fahrer-Fahrzeug-Umgebung hervorgerufen wird. Hierzu zählt sowohl die Fehlerwirkung als auch die Kompensation des Fahrers als Reaktion auf das anliegende Fehlerbild. Geeignete Kenngrößen sind somit die Störung des Giergeschwindigkeits- und des Querbeschleunigungsverlaufs gegenüber den entsprechenden Verläufen ohne Einwirkung eines Fehlerbilds.

Die Bewertung der Kontrollierbarkeit des Fahrzeugs im Fehlerfall anhand objektiver fahrdynamischer Kenngrößen sollte in Analogie zu der subjektiven Bewertung idealerweise von mehreren Expertenfahrern vorgenommen werden.

ANMERKUNG 3 Bei mehreren Expertenfahrern wird berücksichtigt, dass das Verhalten des geschlossenen Regelkreises Fahrer-Fahrzeug-Umgebung unter der Einwirkung eines Fehlerbilds von der individuellen Leistungsfähigkeit des Fahrers bei der Kompensation von Störungen abhängt.

Eine erprobte Methode zur Bewertung der Kontrollierbarkeit anhand von objektiven fahrdynamischen Kenngrößen ist im Anhang A, A.3.4, beschrieben.

Die Bewertung der Kontrollierbarkeit anhand objektiver fahrdynamischer Kenngrößen erfordert geeignete Referenzwerte beziehungsweise Obergrenzen für diese Kenngrößen.

Für die ausgewählten Fehlerbild-Fahrmanöver-Kombinationen nach Tabelle 2 liegen Erfahrungswerte für die Obergrenzen vor, die im Jahr 2022 im Rahmen einer während der Normerstellung durchgeführten Versuchsreihe unter Beteiligung von 12 Unternehmen der Automobilindustrie ermittelt wurden, siehe Anhang D.

Die Erfahrungswerte für die Obergrenzen der fahrdynamischen Kenngrößen Stör-Giergeschwindigkeit und Stör-Querbeschleunigung sind in der Tabelle D.1 jeweils in Form eines Bereichs angegeben, der sich aus der Betrachtung über verschiedene PKW-Fahrzeugsegmente und SbW-Ausführungsformen hinweg ergeben hat.

Für die nach 7.2.5 festgelegten physikalischen Größen der Fehlerausprägung sollten die fahrdynamischen Kenngrößen Stör-Giergeschwindigkeit und Stör-Querbeschleunigung für die Fehlerbild-Fahrmanöver-Kombinationen nach Tabelle 2 anhand der in Anhang A, A.3.4, enthaltenen Vorgaben system- und fahrzeug-spezifisch ermittelt werden.

Wenn die subjektive Bewertung der Kontrollierbarkeit durch Expertenfahrer unterhalb der Schwelle zwischen den Bewertungsstufen C0 und C1 liegt und die genannten objektiven fahrdynamischen Kenngrößen die Bereiche für die Obergrenzen nach Tabelle D.1 nach oben hin nicht überschreiten, gilt die subjektive Bewertung als plausibilisiert.

Wenn die subjektive Bewertung der Kontrollierbarkeit durch Expertenfahrer unterhalb der Schwelle zwischen den Bewertungsstufen C0 und C1 liegt, aber die genannten objektiven fahrdynamischen Kenngrößen die Bereiche für die Obergrenzen nach Tabelle D.1 nach oben hin überschreiten, gilt die subjektive Bewertung als nicht abschließend plausibilisiert. In diesem Fall sollte die subjektive Bewertung der Kontrollierbarkeit mit einer angemessenen Anzahl von Fahrern verifiziert werden.

Nach der Verifizierung einer subjektiven Bewertung der Kontrollierbarkeit mit einer angemessenen Anzahl von Fahrern kann der Normanwender die Tabelle D.1 um die neu ermittelten Obergrenzen erweitern.

Der subjektiven Bewertung der Kontrollierbarkeit muss gegenüber der Bewertung anhand von objektiven fahrdynamischen Kenngrößen nach Tabelle D.1 ein Vorrang eingeräumt werden.

Nach einem Erstfehler muss die Kontrollierbarkeit von möglichen Folgefehlern nach 8.3.1 neu bewertet werden.

7.5 Beschreibung von Fahrmanövern und Versuchsdurchführung zur Bewertung der Kontrollierbarkeit im Fehlerfall

Die in 7.3 beschriebenen Fehlerbilder und deren Auswirkungen auf die Kontrollierbarkeit des Fahrzeugs werden im folgenden Fahrmanövern zugeordnet. Die Zuordnung erfolgt unter Berücksichtigung der Kritikalität der Fehlerausprägung im geschlossenen Regelkreis Fahrer-Fahrzeug-Umgebung.

Folgende Fahrmanöver und Fahrzeuggeschwindigkeiten bzw. Querbeschleunigungen müssen mindestens für die Bewertung der Kontrollierbarkeit des Fahrzeugs im Fehlerfall in Fahrversuchen gewählt werden:

- Geradeausfahrt mit 80 km/h, Fahrstreifenbreite 2,5 m oder 120 km/h, Fahrstreifenbreite 3,25 m;
- Kreisfahrt, 80 m bis 100 m Radius mit einer minimalen Querbeschleunigung von 5 m/s^2 , Fahrstreifenbreite 3 m;
- 18 m Slalom mit einer Querbeschleunigung von mindestens 5 m/s^2 , Fahrstreifenbreite 2,75 m.

Hierbei werden insbesondere Fehlerbild-Fahrmanöverkombinationen beschrieben in welchen die Ausprägung der Fehlerwirkung einen signifikanten Einfluss auf die Bewältigung der Fahraufgabe hinsichtlich der Kontrollierbarkeit hat.

ANMERKUNG 1 Die ausgewählten Fahrmanöver sowie die vorgegebenen Fahrzeuggeschwindigkeiten bzw. Querbeschleunigungen entsprechen dem Stand der Technik und wurden nach der Auftretenswahrscheinlichkeit im Straßenverkehr (E1 Grenze im Zeitbereich), abgeleitet aus der VDA-Empfehlung 702 SitKat [3], sowie der Kritikalität hinsichtlich der Bewältigung der Fahraufgabe ausgewählt. Einige Fehlerbilder sind erfahrungsgemäß bei erhöhten Querbeschleunigungen vom Expertenfahrer präziser bewertbar. Die Definition der Fahrstreifenbreiten in den jeweiligen Fahrmanövern ist abgeleitet aus der Richtlinie für die Anlage von Autobahnen [1] sowie der ISO 3888-1. Des Weiteren wurde bei der Auswahl der Fahrmanöver die Durchführbarkeit auf Prüfgeländen und Versuchsstrecken berücksichtigt.

ANMERKUNG 2 Die Übertragbarkeit der Bewertung der Kontrollierbarkeit durch den Expertenfahrer auf die Kontrollierbarkeit durch Normalfahrer ist durch eine Probandenstudie [4] gestützt.

Begründete Anpassungen der Fahrstreifenbreiten und des Slalom-Pylonenabstands sind zulässig, siehe Anhang A, A.2.3.3.

Während der Durchführung der vorgegebenen Fahrmanöver müssen die in Tabelle 1 beschriebenen Fehlerbilder bei einem definierten Fahrzustand des Versuchsfahrzeugs und einer vorgeschriebenen Handhaltung des Fahrers aufgeschaltet werden. Um eine Adaption des Expertenfahrers an die Fehlerwirkung zu verhindern, muss die genaue Position der Fehleraufschaltung in dem definierten Rahmen des jeweiligen Fahrmanövers variiert werden. Für jede Fahrmanöver-Fehlerbild Kombination müssen je Variation des Fehlerbildes mindestens 4 Versuche durchgeführt werden, die eine aussagekräftige Bewertung der Kontrollierbarkeit ermöglichen.

BEISPIEL Variationen des Fehlerbilds sind Fehlerdauer und/oder Aufschaltzeitpunkt des Fehlers.

Eine weitere Variation des Fehlerbildes muss vorgenommen werden, um die Kontrollierbarkeit des Fahrzeugs im Fehlerfall in beide Fahrtrichtungen zu prüfen.

Die gewählten Fahrmanöver sowie die vorgegebenen Fahrzeuggeschwindigkeiten bzw. Querbeschleunigungen stellen einen Mindestumfang dar und müssen system- und fahrzeugspezifisch bewertet und gegebenenfalls erweitert werden.

ANMERKUNG 3 In den jeweiligen Fahrmanövern werden minimal zu fahrende Geschwindigkeiten bzw. Querbeschleunigungen vorgegeben. Die Auswirkung der Fehlerbilder wird prägnanter mit höheren Geschwindigkeiten bzw. Querbeschleunigungen. Die Anzahl der Versuche je Variation des Fehlerbilds je Fahrmanöver-Fehlerbild Kombination wurde in Orientierung an die ISO 17361:2017 gewählt.

Die Versuchsdurchführung ist im Anhang A beschrieben.

8 Mindestanforderungen an das Betriebsverhalten nach Fehlerfall

8.1 Einleitung und allgemeine Beschreibung des Degradationskonzepts

Während Abschnitt 7 die Kontrollierbarkeit bei Fehlerauftritt betrachtet, werden in diesem Abschnitt die Anforderungen an das System und das Fahrzeug bei Weiterfahrt nach Abschwächung der Fehler behandelt.

Das hier beschriebene Degradationskonzept berücksichtigt die in 5.3 definierten Sicherheitsziele. Der Anwender muss das Degradationskonzept für ein konkretes SbW-System basierend auf einer vollständigen HARA für eventuell zusätzliche Sicherheitsziele und Sicherheitsanforderungen entsprechend erweitern. Außerdem muss der Anwender das Degradationskonzept und die in diesem Abschnitt definierten Anforderungen in seinem übergeordneten Sicherheitskonzept des Fahrzeugs berücksichtigen.

Das hier definierte Degradationskonzept beschreibt den Zustand des Fahrzeugs nach Fehlern mittels Degradationen und Transitionen. Die Überführung des Fahrzeugs von einer Degradation zur nächsten Degradation wird als Transition bezeichnet. Die Bedingungen für einen Zustandswechsel zwischen den Degradationen und Transitionen werden als Transitionsbedingungen bezeichnet.

Degradationen sind:

- Normalbetrieb N;
- Degradation 1: eingeschränkte Weiterfahrt;
- Degradation 2: Kriechfahrt;
- Degradation 3: Fahrzeugstillstand.

Transitionen sind:

- Transition N-1: Geschwindigkeitsreduktion (optional);
- Transition x-2 Phase A: Geschwindigkeitsreduktion;
- Transition x-2 Phase B: zeitlich eingeschränkte Weiterfahrt;
- Transition x-2 Phase C: automatisierte Geschwindigkeitsreduktion;
- Transition 2-3: automatisierte Geschwindigkeitsreduktion;
- Transition x-3: sicheres Anhalten am Straßenrand;
- Transition x-Notbremsung: automatisierte Notbremsung.

Kritische Fehler reduzieren die System- und die Sicherheitsintegrität. Um den Verlust der Sicherheitsintegrität zu vermeiden, muss das Fahrzeug bei kritischen Fehlern in einen sicheren Betriebszustand überführt werden. Sichere Fahrzeugzustände sind nach 5.3 die Degradation 2 mit einer Fahrzeuggeschwindigkeit ≤ 10 km/h und die Degradation 3 jeweils mit entsprechender Warnung.

Das Degradationskonzept als ein erweiterter Teil von bestehenden Fahrzeugsicherheitskonzepten, beschreibt unter anderem Anforderungen an die sicherheitsbezogene Verfügbarkeit. Eine Standardisierung bietet den Vorteil, dass sich Fahrzeuge nach Auftreten von Fehlern herstellerübergreifend ähnlich, nachvollziehbar und konsistent verhalten.

Für die Umsetzung sind dabei neue Aspekte zu berücksichtigen, die über den Bereich des Lenksystems hinausgehen:

- automatisierte Verzögerung (z. B. mittels Bremse oder Antrieb);
- automatisierte Notbremsung; und
- weitere Systeme zur Fahrzeugquerführung.

Falls das Fahrzeug weitere Systeme zur Fahrzeugquerführung besitzt (z. B. Bremse, Antrieb, Hinterachslenkung), können diese, ggf. auch in Kombination, als zusätzliche Redundanz für eine erweiterte Verfügbarkeit vorgesehen werden.

In Bild 5 wird das Degradationskonzept dargestellt.