Generische Strukturierung von Sicherheitsnachweisen von Fahrcomputern für automatisierte Fahrzeugsysteme des Level 3

L. Schnieder^{1,2} · R. S. Hosse¹

Eingegangen: 8. Februar 2019 / Angenommen: 13. Februar 2020 / Online publiziert: 6. März 2020
© Der/die Autor(en) 2020

Zusammenfassung

Die Entwicklung sicherheitsrelevanter elektronischer Steuerungssysteme für automatisierte Fahrzeugsysteme des Level 3 ist eine komplexe und anspruchsvolle Entwurfs- und Nachweisaufgabe. Dieser Beitrag zeigt auf, dass eine erfolgreiche Entwicklung sicherheitsrelevanter elektronischer Steuerungssysteme für Kraftfahrzeuge ein gegenläufiger Prozess ist. Top-Down-Entwurfsvorgaben im Sinne einer Vorgabe konkreter Sicherheitsanforderungsstufen können zumeist erst bei der Entwicklung einer konkreten Anwendung auf Fahrzeugebene getroffen werden. Um die Innovationsdynamik in der Automobilindustrie nicht zu hemmen, sind auch „Bottom-up“ entstehende generische Produkte und Anwendungen mit wohl dokumentierten Annahmen erforderlich. Dieser Beitrag stellt Anforderungen an generische Sicherheitsnachweise auf und zeigt, wie diese über das Konzept „sicherheitsbezogener Anwendungsregeln“ miteinander bruchlos verknüpft werden können. Grundlage hierfür ist ein eindeutig definierter Anwendungskontext sowie eine verbindlich festgelegte Systemdefinition. Hierfür wird gezeigt, welchen Beitrag die Verwendung einer semi-formalen Notation für die generische Strukturierung funktionaler Sicherheitsanforderungen von Fahrcomputern für automatisierte Fahrzeugsysteme des Level 3 leisten kann.

Generic structure of safety cases for automated vehicle systems of level 3

Abstract

The development of safety-relevant electronic control systems for automated vehicle systems of level 3 is a complex and demanding design and verification task. This article shows that the successful development of safety-related electronic control systems for motor vehicles requires both a top-down as well as a bottom-up approach. Top-down design specifications in the sense of specifying safety requirements with an automotive safety Integrity Level attached to them can usually only be made when a specific application is developed by the original equipment manufacturer (OEM) at the vehicle level. In order not to inhibit the dynamics of innovation in the automotive industry, bottom-up generic products and applications with well-documented assumptions are also required. This article sets out requirements for generic safety evidence and shows how these can be seamlessly linked using the concept of “safety-related application conditions”. The basis for this is a clearly defined application context and a binding system definition. For this, it is shown what contribution the use of a semi-formal notation for the generic structuring of functional safety requirements of driving computers for level 3 automated vehicle systems can make.

1 Problemstellung und Motivation

In der Entwicklung sicherheitsrelevanter elektronischer Steuerungssysteme für Kraftfahrzeuge werden von den an der Entwicklung beteiligten Unternehmen gezielt Maßnahmen zur Vermeidung systematischer Fehler und zufälliger Ausfälle umgesetzt. Ausgangspunkt der Systementwicklung ist in der Regel ein strenger „Top-Down“-Entwurfsprozess, an dessen Beginn die Vorgabe von Zielgrößen (Automotive Safety Integrity Level, ASIL) für

✉ L. Schnieder
Lars.schnieder@ese.de

¹ Technische Universität Dresden, Fakultät Verkehrswissenschaften, 01062 Dresden, Deutschland

² ESE Engineering und Software-Entwicklung GmbH, Am Alten Bahnhof 16, 38122 Braunschweig, Deutschland

Abb. 1 Begriffliche Abgrenzung eines Fahrcomputers für automatisierte Fahrzeugsysteme des Level 3 (Bildnachweis: eigene Darstellung in Anlehnung an ISO 26262-10)

die Systementwicklung steht. Die ASIL bestimmen den Umfang der umzusetzenden Maßnahmen zur Vermeidung systematischer Fehler sowie zufälliger Ausfälle eines zu entwickelnden sicherheitsrelevanten elektronischen Steuerungssystems. Diese Vorgehensweise eines strengen „Top-Down“-Entwurfsprozesses ist nicht immer möglich:

- *Längere „time to market“ funktional sicherer Subsysteme hemmt Innovationsdynamik in der Automobilindustrie:* Eine strenge hierarchische Vorgabe auf Systemebene abgeleiteter Sicherheitsziele durch den Original Equipment Manufacturer (OEM) samt Kaskadierung auf die verschiedenen Ebenen der Systemarchitektur ist aus Zeitgründen nicht immer möglich. Zukünftig werden sich die Innovationszyklen in der Automobilindustrie in einem dynamischen Wettbewerbsumfeld weiter verkürzen.
- *Fehlende Nutzung von Synergiepotenzialen sprengt das Zielkostengefüge der Fahrzeugplattformen:* Eine Umsetzung der im Einzelfall von einem OEM heruntergebrochenen Sicherheitsziele durch die Lieferanten ist für alle Beteiligten der Wertschöpfungskette nicht wirtschaftlich. Für jeden spezifischen Anwendungsfall fallen Aufwände für das Engineering des spezifischen Systems samt der Durchführung der entsprechenden Bestätigungsmaßnahmen an. Dies verteuert die zu integrierenden Zulieferanteile. Hier helfen klare technische Abgrenzungen (Hardware-Software-Interface, HSI der ISO 26262-4) sowie die verbindliche Festlegung von Rollen und Verantwort-

lichkeiten in einer verteilten Entwicklung (Development Interface Agreement, DIA der ISO 26262-8).

- *Unklare Voraussetzungen einer rechtssicheren Typgenehmigung automatisierter Fahrzeugsysteme:* Bislang spielen Erfahrungen eine große Rolle in der Entwicklung von Kraftfahrzeugen. Technische Regelwerke (bspw. UNECE-Regelungen) dokumentieren diese Erfahrungen. Da beim hochautomatisierten Fahren das Fahrzeug selbsttätig und ohne Einwirkung des Fahrers fährt, sind die bestehenden Normen zur funktional sicheren Entwicklung sicherheitsrelevanter elektronischer Steuerungssysteme im Lichte des deutschen Produkthaftungsgesetzes (ProdHaftG) eine notwendige, aber nicht hinreichende Bedingung. Zukünftig sind für eine rechtssichere Typgenehmigung über die funktionale Sicherheit hinaus weitere Nachweise zu erbringen. Beispiele hierfür ist der Nachweis der Sicherheit der Sollfunktion (Safety of the Intended Functionality, SOTIF nach ISO PAS 21448) sowie der Angriffssicherheit (Automotive Cybersecurity nach ISO/SAE 21434).

Die zuvor dargestellten Herausforderungen erfordern ein anderes Vorgehen in der Entwicklung sicherheitsrelevanter Steuerungssysteme für Kraftfahrzeuge. Die internationale Norm für die Entwicklung funktional sicherer elektronischer Steuerungssysteme für Kraftfahrzeuge sieht deshalb vor, dass Komponenten, welche in sicherheitsrelevanten Systemen im Kraftfahrzeug eingesetzt werden sollen auch außerhalb ihres spezifischen Anwendungskontexts entwickelt werden können (Safety Element out

of Context, SEooC nach ISO 26262-10). Dieser Beitrag stellt dar, unter welchen Rahmenbedingungen generische Sicherheitsnachweise in der Entwicklung sicherheitsrelevanter Steuerungssysteme für Kraftfahrzeuge zum Einsatz kommen.

2 Generizität von Sicherheitsnachweisen

Unter Generizität wird die Eigenschaft eines anwendungsunabhängigen Elements verstanden, Klassen von Anwendungen (auf Ebene eines Items nach ISO 26262) realisieren zu können. Abb. 1 stellt die Betrachtungseinheit eines Fahrcomputers (controller) für das hochautomatisierte Fahren dar.

Aus dieser Abstraktion heraus können – in Anlehnung an die in anderen Verkehrsmoden etablierte Vorgehensweise der Sicherheitsnachweisführung (vgl. [1]) – verschiedene Kategorien an Sicherheitsnachweisen differenziert werden:

- Generischer Produktsicherheitsnachweis (unabhängig von der Anwendung):** Ein generisches Element kann für unterschiedliche, unabhängige Anwendungen wiederverwendet werden. Ein Beispiel für ein generisches Element ist ein Fahrcomputer (vgl. Controller in Abb. 1). Dieser kann später in der Entwicklung eines Items integriert
- Generischer Anwendungssicherheitsnachweis (für eine Klasse von Anwendungen):** Eine generische Anwendung kann für eine Klasse/Art von Anwendungen mit gemeinsamen Funktionen wiederverwendet werden. Ein Beispiel hierfür wäre eine – unabhängig von einem spezifischen Fahrzeug – entwickelte Assistenzanwendung, welche eine Zusammenführung von Sensorik, Regel-funktion und Aktorik mit dem Zweck der Erbringung einer konkreten Automatisierungsaufgabe (= Regelstrecke) darstellt. Die auf dieser Ebene entwickelte generische Software kann in der nächsten Integrationsstufe durch Daten, Algorithmen oder beides konfiguriert werden, um damit die ausführbare Software für die spezifische Anwendung anzufertigen. Die Ebene des generischen Anwendungssicherheitsnachweises ist in Abb. 1 die Ebene der E/E-Komponente als Verknüpfung von Sensoren, Aktoren und Steuergerät.
- Spezifischer Anwendungssicherheitsnachweis (für eine spezifische Anwendung):** Eine spezifische Anwendung wird in einem konkreten Fahrzeug integriert. Es ist wichtig, für jede spezifische Anwendung zu zeigen, dass die Umgebungsbedingungen und die Randbedingungen (u. a. ASIL-Qualifizierung) der eingesetzten generischen Anwendungen berücksichtigt wurden. Darüber hinaus muss gezeigt werden, dass die anwendungsspezifische

Abb. 2 Abhängigkeit zwischen den Sicherheitsnachweisen (Bildnachweis: eigene Darstellung in Anlehnung an ISO 26262-10)

Konfiguration korrekt und vollständig durchgeführt worden ist. Der spezifische Anwendungssicherheitsnachweis ist in Abb. 1 das Item also die Ebene des Systems, bzw. System Arrays.

Für alle drei Kategorien ist die grundsätzliche Struktur des Sicherheitsnachweises im Wesentlichen identisch. Allerdings sind zwischen den Sicherheitsnachweisen bestehende Abhängigkeiten zu beachten. Dies wird im nächsten Abschnitt beschrieben.

3 Generizität von Sicherheitsnachweisen

Bereits heute sieht die ISO 26262 die Möglichkeit einer Betrachtung generischer Elemente vor. Dies wird in der ISO 26262 als so genanntes „Safety Element out of Context“ (SEooC) gehandhabt. In diesem Sinne verfügt ein SEooC abstrakt gesprochen über die prinzipielle Fähigkeit, in späteren Integrationsstufen zu einem ASIL-qualifizierten Produkt zu führen (vgl. Abb. 2).

Dies führt zu einer Schnittstelle zwischen verschiedenen Sicherheitsnachweisen auf unterschiedlichen Betrachtungsebenen des Systems. Dies wird nachfolgend durch die Differenzierung des unterlagerten Sicherheitsnachweises vom integrierenden Sicherheitsnachweis beschrieben:

- *Unterlagerter Sicherheitsnachweis:* Das SEooC wird auf der Grundlage von Annahmen entwickelt. Diese Annahmen umfassen die unterstützte Klasse möglicher Anwendungen sowie mögliche Anwendungsbedingungen (u.a. Umweltbedingungen), sowie möglicher externer Schnittstellen des Betrachtungsgegenstands. Im Falle eines Fahrcomputers für automatisierte Fahrzeugsysteme des Level 3 ist der unterlagerte Sicherheitsnachweis ein generischer Produktsicherheitsnachweis. Ein solcher generischer Produktsicherheitsnachweis exportiert an übergeordnete Sicherheitsnachweise „sicherheitsbezogene Anwendungsregeln“. Hierunter fallen die folgenden Aspekte:
 - Regeln, Bedingungen und Einschränkungen, die bei der Integration des betrachteten Teilsystems beachtet werden müssen. Dies gilt vor allem bezüglich zu entwickelnder SEooC-externer Sicherheitsmaßnahmen des zu integrierenden Systems.
 - Eine Beschreibung der Konfigurationsmöglichkeiten programmierbarer Systeme, um diese an spezielle Anwendungen anzupassen,
 - Einzuhaltende Vorsichtsmaßnahmen bei der Herstellung, Installation, Prüfung und Inbetriebnahme sowie Regeln und Methoden für die Instandhaltung und Fehlersuche

- Anweisungen für die Handhabung des Systems sowie sicherheitsrelevante Warnungen und Vorsichtsmaßnahmen.

- *Integrierender Sicherheitsnachweis:* Zum Zeitpunkt der Integration eines SEooC muss die Gültigkeit der in der Entwicklung des SEooC getroffenen Annahmen bestätigt werden. Dies sind vor allem die Anforderungen hinsichtlich des Anwendungskontexts (beispielsweise Schnittstellen) oder aber Annahmen hinsichtlich der konkreten Umsetzung von Sicherheitsanforderungen. In dieser Hinsicht integriert die Ebene eines generischen Anwendungssicherheitsnachweises mehrere Teilsysteme, die jeweils über generische Produktsicherheitsnachweise die Einhaltung der an sie gestellten Sicherheitsanforderungen dokumentieren. Im Zuge der Integration werden bereits erste „sicherheitsbezogene Anwendungsregeln“ geschlossen. Im Zuge der Integration neu entstehende „sicherheitsbezogene Anwendungsregeln“ werden wiederum über „sicherheitsbezogene Anwendungsregeln“ an die Ebene des spezifischen Anwendungssicherheitsnachweises weitergeleitet und müssen dort behandelt werden.

Die Rolle des Sicherheitsnachweises in der hochgradig verteilten Systementwicklung in der Automobilindustrie ist zuvor dargestellt worden. Aus dieser Rolle heraus resultieren besondere Anforderungen an die Ausgestaltung der Gefährdungsanalyse und der Sicherheitsnachweisführung. Dies wird im nächsten Abschnitt dargestellt.

4 Anforderungen an die Gefährdungsanalyse und Sicherheitsnachweisführung

In der Entwicklung eines sicherheitsrelevanten elektronischen Steuerungssystems für Kraftfahrzeuge müssen verschiedene Entwurfsaufgaben strukturiert bearbeitet werden. Hierfür sind methodische Vorgehensweisen erforderlich, die den Bearbeiter zu einer vollständigen Bearbeitung der Entwurfsaufgabe zwingen. Die methodische Vorgehensweise sollte hierbei die grundlegenden Wirkzusammenhänge im Systemkontext offenbaren. Der Sicherheitsnachweis hat also – auch für den Bearbeiter selbst – eine Funktion der Unterstützung im Systementwurf:

- *Entwurfsunterstützungsfunktion:* Der Sicherheitsnachweis muss eine klare Systemgrenze für die Sicherheitsbetrachtung berücksichtigen. Sicherheitsbezogene elektronische Steuerungssysteme für Kraftfahrzeuge müssen im Zusammenwirken verschiedener technischer Komponenten (Sensor, Aktor, Regler in ihrem Zusammenwirken mit der Regelstrecke) beschrieben sein. Gleiches gilt

für die Mensch-Maschine-Interaktion welche für automatisierte Fahrzeugsysteme des Level 3 nach wie vor kennzeichnend ist.

Bereits zuvor ist deutlich geworden, dass eine zentrale Aufgabe des Sicherheitsnachweises die strukturierte Darlegung der die Entwicklung eines sicherheitsrelevanten elektronischen Steuerungssystems für Kraftfahrzeuge leitenden Sicherheitserwägungen ist. Der Sicherheitsnachweis hat somit eine Dokumentationsfunktion. Dies führt zur folgenden Anforderung an die Darstellung im Sicherheitsnachweis:

- **Dokumentationsfunktion:** Der Sicherheitsnachweis erfordert ein umfassendes technisches Verständnis des zu entwickelnden Systems. Gleichzeitig ist ein Expertenwissen zu den anwendbaren Regeln der Technik (Normen und Standards) sowie der Anwendung von Sicherheitsmechanismen im Entwurf sicherheitsrelevanter elektronischer Steuerungssysteme für Kraftfahrzeuge erforderlich. Die zentralen Darstellungen im Sicherheitsnachweis müssen daher zentrale entwurfsleitende Annahmen umfassend (d. h. vollständig) dokumentieren.

Die Automobilindustrie ist geprägt von einer hochgradig differenzierten Aufgabenteilung entlang der Wertschöpfungskette. Sicherheitsnachweise fixieren den genauen Funktionsumfang sowie die entwurfsleitenden Annahmen. Ein Sicherheitsnachweis dient also auch der Kommunikation zu einem unbeteiligten Dritten darüber, auf welcher Grundlage eine höhere Integrationsstufe (generische Anwendung, spezifische Anwendung) aufsetzen kann. Die Kommunikationsfunktion des Sicherheitsnachweises führt zur folgenden Anforderung an die Darstellung im Sicherheitsnachweis:

- **Kommunikationsfunktion:** Die Darstellung im jeweiligen Sicherheitsnachweis muss für einen Dritten nachvollziehbar sein. Hierfür kommen natürlichsprachliche Darstellungen an die Grenzen ihrer semantischen Ausdrucksfähigkeit. So führen insbesondere sprachliche Mehrdeutigkeiten zu Missverständnissen. Es ist also sinnvoll, im Entwurf und der Nachweisführung semiformale Notationen zu verwenden, um diesen Spielraum unterschiedlicher Deutungen einzuengen [2].

5 Methoden zur Durchführung von Gefährdungsanalyse für generische Produkte

Ziel der ISO 26262 ist die Vermeidung von E/E-Ausfällen. Die Norm legt einen Sicherheitslebenszyklus fest und beschreibt, wie ein auf die Funktionale Sicherheit ausgerichtetes Systems Engineering aussehen soll. Eine zentra-

le Aufgabe in der Konzeptphase ist die Durchführung einer Risikoanalyse (Hazard Analysis and Risk Assessment, HARA). Die Risikoanalyse umfasst die beiden Teilaufgaben der *Risikoidentifikation* und der *Risikobewertung*. Während die Risikobewertung durch Nutzung der Risikoparameter in ISO 26262-3 klar festgelegt ist, lässt die Norm eine Wahlfreiheit für die anzuwendende Methode zur Risikoidentifikation. Konventionelle Ansätze der Risikoidentifikation sind Fehlerbaumanalysen (Fault Tree Analysis, FTA), die Fehlermöglichkeits- und Einflussanalyse (FMEA, vgl. [3] und [4]) sowie die Durchführung einer Hazard and Operability Study (HAZOP, vgl. [5]). Diese Ansätze haben jedoch Einschränkungen bei der Risikoidentifikation in komplexen (Mensch-Maschine)Systemen. Dementsprechend gibt es die Notwendigkeit, die Wirksamkeit anderer Ansätze für Risikoidentifikation zu untersuchen. STAMP/STPA (Theoretic Accident Model and Processes/Systems Theoretic Process Analysis/STPA) hat sich in der Literatur als geeigneter Ansatz herausgestellt. Qualitative Vergleiche der Ergebnisse mittels konventioneller Methoden (bspw. FMEA) durchgeführter Gefährdungsanalysen mit den Ergebnissen einer mit STAMP/STPA durchgeführten Gefährdungsanalysen zeigen, dass diese Methode für die Nutzer anwendbar ist und zu vergleichbaren Ergebnissen führt [6]. Weitergehendes Potenzial zeigt sich hinsichtlich einer Einbettung von STAMP/STPA in einen ganzheitlichen modellbasierten Entwurfsprozess softwareintensiver sicherheitskritischer Systeme für Automotive-Anwendungen [7], bzw. der Prozessindustrie [8]. Aus Sicht der Autoren adressiert STAMP/STPA die zuvor genannten Anforderungen an den Sicherheitsnachweis für Automotive-Anwendungen:

- **Entwurfsunterstützungsfunktion:** Die konsequente Umsetzung von STAMP/STPA (vgl. [9]) erzwingt eine umfassende gedankliche Auseinandersetzung mit allen für die Entwicklung funktional sicherer Anwendungen für Kraftfahrzeuge relevanten Aspekte.
- **Dokumentationsfunktion:** Die Ergebnisse der im Entwurf getroffenen Entscheidungen werden dokumentiert. Dies ermöglicht im Falle produkthaftungsrechtlicher Fragestellungen (vgl. hierzu [10]) die Darlegung der Erfüllung einschlägiger Rechtspflichten (Erfüllung der *Konstruktionspflicht*). Durch eine erfolgreiche Beweislastumkehr können Haftungsrisiken wirksam abgewendet werden.
- **Kommunikationsfunktion:** Die verwendete semi-formale Notation der Regelstrukturen vereinfacht die Kommunikation. Eine eindeutige Festlegung von Inhalten schafft zum einen ein klares Verständnis in der organisationsübergreifenden Zusammenarbeit in der Automobilindustrie. Zum anderen wird auch entlang des Sicherheitslebenszyklus die Kommunikation zwischen verschiedenen Rollen (u. a. dem Gutachter) vereinfacht.

Abb. 3 Vorgehensmodell der STPA (eigene Darstellung in Anlehnung an ISO 26262)

Abb. 4 Beschreibung des Systemumfangs STPA/STAMP (eigene Darstellung)

6 Durchführung einer semi-formalen Gefährdungsanalyse eines generischen Produkts

Die zuvor definierten Anforderungen werden durch die Methode STAMP/STPA (Systems-Theoretic Accident Model and Processes, Systems-Theoretic Process Analysis) angepasst an die ISO 26262 umgesetzt. Das methodische Vorgehen folgt dabei dem Vorgehensmodell in Abb. 3. Hierbei ist auf der linken Seite der für die Konzeptphase der Systementwicklung relevante Ausschnitt aus dem Sicherheitslebenszyklus zu dargestellt. Bei einem Fahrcomputer handelt es sich nicht um ein Item im Sinne der ISO 26262. ISO 26262-3 ist somit nicht anwendbar. Allerdings sollte für die Ableitung von Annahmen zur Entwicklung des SEooCs eine übergeordnete HARA der (potentiell später) integrierenden Items vorgenommen werden.

Auf der rechten Seite ist die Vorgehensweise von STAMP/STPA nach [9] dargestellt. Aus der Gegenüberstellung ergeben sich erforderliche Ergänzungen in der Vorgehensweise nach [9] insbesondere hinsichtlich der Bewertung der erkannten Gefährdungen nach Schwere (Severity), Auftreten (Exposure) und Kontrollierbarkeit (Controllabili-

ty). Die Pfeile zwischen den beiden Vorgehensweisen verdeutlichen, dass STAMP/STPA die Erstellung zentraler Dokumentationsartefakte einer Systementwicklung nach ISO 26262 sowohl methodisch als auch hinsichtlich des gewählten Beschreibungsmittels (Regelstrukturen) unterstützt. So setzt beispielsweise die Entwicklung sicherheitsrelevanter elektronischer Steuerungssysteme für Kraftfahrzeuge voraus, dass zunächst einmal eindeutig bestimmt wird, was Gegenstand der Entwicklung des funktional sicheren Systems sein soll. Die hierfür einschlägige internationale Norm spricht hierbei von einer *Item Definition* (vgl. [11]).

Nachfolgend wird dargestellt, wie der eigentliche Scope einer Systementwicklung durch die semi-formale Notation der STPA/STAMP-Analyse fixiert werden kann. Gegenstand der hier durchzuführenden Identifikation generischer funktionaler Sicherheitsanforderungen ist ein Fahrzeugcomputer, welcher für die Anwendung hochautomatisierter Fahrfunktionen geeignet ist. Die STPA sieht zur Beschreibung des Items vor, die sog. hierarchischen Regelungsstrukturen als semi-formale Beschreibungsmethode zu verwenden. Um diese Struktur zu erstellen, ist zuerst notwendig die logischen im System enthaltenen Komponenten zu identifizieren und deren Wirkzusammenhänge zu

Tab. 1 Betriebsmodi eines Fahrzeugcomputers

ID	Operating Mode	Comment
OM_1	Vehicle Computer Off	e.g. no power to Vehicle Computer ECU
OM_2	Vehicle Computer passive	e.g. On/Standby mode, not having an influence on the driving process
OM_3	Vehicle Computer active	e.g. active ADAS/HAD Driving Mode(s)
OM_4	Vehicle Computer degraded operation	e.g. fail safe mode
OM_5	Vehicle Computer emergency operation	–
OM_6	Vehicle Computer service mode	–

Tab. 2 Gefährdungen eines automatisierten Fahrzeugs

ID	Hazard
HZ_1	Loss of vehicle lateral motion control
HZ_2	Unintended vehicle lateral motion/unintended yaw
HZ_3	Insufficient deceleration of vehicle
HZ_4	Unintended vehicle longitudinal deceleration
HZ_5	Insufficient acceleration of vehicle
HZ_6	Unintended acceleration

beschreiben. Dies ist exemplarisch in der folgenden Abb. 4 erfolgt.

Die Regelstruktur des Fahrcomputers sieht dabei eine Differenzierung zwischen sog. *Basisfunktionalitäten* (z.B. Betriebssystem, AUTOSAR, etc.) und *spezifischen Applikationen* zur Durchführung der operativen Fahraufgabe (z.B. Objekterkennung, Trajektorienplanung, Aktuatomodelle, etc.) vor. Die Sensorsignale können entweder direkt oder über andere fahrzeuginterne Kommunikationssysteme an den Fahrzeugcomputer gegeben werden. Nach Verarbeitung der Sensorinformationen durch die spezifischen Applikationen, gibt der Fahrcomputer die Aktuatorbefehle

direkt/indirekt an die Fahrzeugaktuatoren (Lenkung, Bremse, Antrieb) und übernimmt so die operative Regelung des Fahrzeugs. Um nun die notwendigen Sicherheitsziele für Fahrcomputer zu bestimmen, ist gemäß ISO eine Definition u.a. der Betriebsmodi, der kompletten Funktionalität und Schnittstellen des SEooC des Items, hier der Fahrcomputers, notwendig (analog zur „Item Definition“ aus ISO 26262-3). Diese sind gemäß ISO wie in Tab. 1 dargestellt zu definieren.

Je nach Automatisierungslevel muss der Fahrzeugcomputer einen „fail operational mode“ ermöglichen, also der Fehlerfall muss ebenfalls abgesichert sein. Die Gefährdungen auf Fahrzeugebene bei denen ein potentieller Schadensfall eintreten kann, sind in Tab. 2 dargestellt.

Da bisher nicht eindeutig ist, welche spezifische Assistenz der Fahrzeugcomputer übernimmt (z.B. Spurhaltefunktion, Spurwechselfunktion, etc.) sind die hier definierten Gefährdung sehr generisch gehalten und beziehen sich ausschließlich auf unerwünschte Reaktionen auf Fahrzeuglevel. Um nun generische funktionale Sicherheitsanforderungen und die entsprechende ASIL Einstufung für Fahrzeugcomputer zu identifizieren, schlägt die STPA die Iden-

Tab. 3 UCAs eines Fahrcomputers

ID	System level control action	Unsafe control action (UCA)
UCA1.1	Provide data to the vehicle/driver	Required control action by Vehicle Computer is not provided
UCA1.2		Provided control action by Vehicle Computer is wrong
UCA1.3		Provided control action by Vehicle Computer is not required
UCA1.4		Required control action by Vehicle Computer is provided too early/too long/out of order
UCA1.5		Required control action by Vehicle Computer is applied too long
UCA1.6		Required control action by Vehicle Computer is stopped too soon
UCA2.1	Provide data to application software	Required Data by Vehicle Computer to ADAS/HAD Software Application are not provided
UCA2.2		Provided Data by Vehicle Computer to ADAS/HAD Software Application are wrong
UCA2.3		Provided Data by Vehicle Computer to ADAS/HAD Software Application are not required
UCA2.4		Required Data by Vehicle Computer to ADAS/HAD Software Application are provided too early/too late/out of order
UCA2.5		Required Data Transfer by Vehicle Computer to ADAS/HAD Software Application are applied too long
UCA2.6		Required Data Transfer by Vehicle Computer to ADAS/HAD Software Application is stopped too soon
UCA3.1	Operation mode change	Required change of operation mode is not performed
UCA3.2		Change to the wrong operation mode is performed
UCA3.3		Performed change of operation mode is not required

Tab. 4 Generische funktionale Sicherheitsanforderungen für Fahrzeugcomputer

ID	Functional Safety Requirement (FSR)	ASIL SAE L ≤ 2	ASIL SAE L ≤ 3
FSR_1	Data transfer to the vehicle must be ensured	ASIL C	ASIL D
FSR_2	Corruption of data transferred to the vehicle must be prevented	ASIL D	ASIL D
FSR_3	Timing constraints of data transferred to the vehicle according to specification must be ensured	ASIL D	ASIL D
FSR_4	Unintended transfer of data to the vehicle must be prevented	ASIL D	ASIL D

tifikation der sog. Unsafe Control Actions (UCA) vor. Hierunter sind verschiedene unerwünschte Regelungsaktionen zu verstehen, welche potentiell eine der Gefährdungen hervorrufen können. Basierend auf der generischen Regelungsstruktur eines Fahrzeugcomputers ergeben sich 13 UCAs, welche es im Nachgang durch eine Szenariobetrachtung im Rahmen der Hazard Analysis and Risk Assessment (nach ISO 26262) zu analysieren, zu bewerten und an die Entwicklung in Form von funktionalen Sicherheitsanforderungen zu geben sind (vgl. Tab. 3).

Sicherheitsziele nehmen in der Entwicklung von sicherheitsrelevanten Steuerungssystemen für Kraftfahrzeuge eine zentrale Rolle ein. In der Regel werden die Gefährdungen auf Grundlage von Szenarienkatalogen bestimmt [12] und gemäß den Merkmalen Schweregrad, Kontrollierbarkeit und Exposure (Zeitdauer oder Häufigkeit des Auftretens einer zu betrachtenden Situation) bewertet [13]. Für jedes der erkannten gefährlichen Ereignisse wird ein Sicherheitsziel formuliert. Jedem der funktionalen Sicherheitsanforderungen wird eine Sicherheitsintegritätsstufe (ASIL, Automotive Safety Integrity Level) zugeordnet. Das im weiteren Verlauf der Systementwicklung aufgestellte Funktionale Sicherheitskonzept formuliert, welche Funktionen zur Erreichung der Sicherheitsziele des Items erforderlich sind. Für den Fahrcomputer ergeben sich die in Tab. 4 dargestellten funktionalen Sicherheitsanforderungen samt zugehöriger ASIL Einstufungen. Demnach beschreiben die vier funktionalen Sicherheitsanforderungen die Schnittstelle vom Fahrcomputer für die Anwendung einer Assistenzfunktion im Level 2 und Level 3. Hierin fließen gleichzeitig die UCAs aus der STPA fließen, um direkt funktionalen Sicherheitsanforderungen hinreichend zu präzisieren. Damit sind generische funktionale Sicherheitsanforderungen für Fahrzeugcomputer im Umfeld des hochautomatisierten Fahrens definiert und im Sinne eines Safety Element out of Context normkonform in die ISO 262626 eingebunden.

7 Zusammenfassung und Ausblick

Dieser Beitrag zeigt auf, dass „Top-Down“-Entwurfsansätze von spezifischen Anwendungen (im Fahrzeug) und

„Bottom-up“ Lösungen generischer Produkte, bzw. generischer Anwendungen kein Widerspruch in sich darstellen. Die Komponentenhersteller generischer Produkte stellen ein marktgerechtes Produkt mit wohl definierten Annahmen bereit. Diese Annahmen müssen bei der Integration in „überlagerte“ generische Anwendungen und spezifische Systemausprägungen (konkretes Fahrzeug) im Sinne einzuhaltender „sicherheitsbezogener Anwendungsregeln“ nachgewiesen werden. Damit dieser Nachweis gelingt, müssen Anforderungen klar und eindeutig gefasst werden. Hierfür wurde in diesem Beitrag das Beschreibungsmittel der Regelstrukturen, die in übergeordneten methodischen Rahmen von STPA/STAMP eingebettet sind, vorgestellt. Dieser Ansatz ist für die in diesem Beitrag dargestellte generische Strukturierung funktionaler Sicherheitsanforderungen für automatisierte Fahrzeugsysteme des Level 3 erfolgversprechend.

Funding Open Access funding provided by Projekt DEAL.

Open Access Dieser Artikel wird unter der Creative Commons Namensnennung 4.0 International Lizenz veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.

Die in diesem Artikel enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen.

Weitere Details zur Lizenz entnehmen Sie bitte der Lizenzinformation auf <http://creativecommons.org/licenses/by/4.0/deed.de>.

Literatur

1. DIN EN 50129:2019-06 (2019) Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsbezogene elektronische Systeme für Signaltechnik (Deutsche Fassung EN 50129:2018)
2. Schnieder E (1999) Methoden der Automatisierung – Beschreibungsmittel, Modellkonzepte und Werkzeuge für Automatisierungssysteme. Springer Vieweg, Braunschweig

3. IEC 60812:2006 (2006) Analysis techniques for system reliability-procedure for failure mode and effects analysis (FMEA)
4. MIL-STD-1629A (1980) Procedures for performing a failure mode, effects and criticality analysis. U.S. Department of Defense, Washington, DC
5. McDermid JA, Nicholson M, Pumfrey DJ, Fenelon P (1995) Experience with the application of HAZOP to computer-based systems. In: Proceedings of the 10th Annual Conference on Computer Assurance (COMPASS'95), Systems Integrity, Software Safety and Process Security, S 37–48
6. Sardar MS, Beer A, Felderer M, Höst M (2019) Comparison of the FMEA and STPA safety analysis methods—a case study. *Softw Qual J* 27:349–387
7. Abdulkhaleq A (2017) A system-theoretic safety engineering approach for software-intensive systems. Dissertation Universität Stuttgart
8. Becker U (2018) STPA guided systems engineering. In: Gallina B et al (Hrsg) SAFECOMP 2018 Workshops, LNCS 11094, S 164–176
9. Leveson N (2012) Engineering a safer world: applying systems thinking to safety by Nancy Leveson. MIT Press, Cambridge, MA
10. Klindt T, Handorn B (2010) Haftung eines Herstellers für Konstruktions- und Instruktionsfehler. *Neue Juristische Wochenschrift* 63(16):1105–1108
11. ISO 26262-3:2018 (2018) Road vehicles—functional safety—part 3: concept phase
12. SAE 2980:2018 (2018) Surface vehicle recommended practice. Considerations for ISO 26262 ASIL hazard classification
13. VDA 702:2015 (2015) Situationskatalog E-Parameter nach ISO 26262-3