Szenarien für Entwicklung, Absicherung und Test von automatisierten Fahrzeugen

G. Bagschik, T. Menzel, A. Reschka* und M. Maurer†

Zusammenfassung:

Die Norm ISO 26262 stellt in der Fassung von 2011 den Stand der Technik für eine funktional sichere Entwicklung von sicherheitskritischen elektrischen/elektronischen Systemen für Kraftfahrzeuge dar. Dazu gehören Fahrerassistenzsysteme und Fahrzeugführungssysteme. Im Entwicklungsprozess der Norm ISO 26262 kann in mehreren Prozessschritten eine szenarienbasierte Sichtweise zur Generierung der von der Norm geforderten Arbeitsergebnisse für die funktionale Absicherung der Systeme genutzt werden. Szenarienbasierte Ansätze werden dafür in mehreren Prozessschritten für unterschiedliche Betrachtungen verwendet, woraus sich widersprüchliche Anforderungen an die Darstellung der Szenarien ergeben. Dieser Beitrag definiert aufbauend auf vorherigen Veröffentlichungen zur Begriffsdefinition die Anforderungen an Darstellungsweisen von Szenarien und sich daraus ergebende Abstraktionsebenen und zeigt auf, wie sich diese Szenarien entlang des Entwicklungsprozesses nach Norm ISO 26262 ineinander überführen lassen.

Schlüsselwörter: Automatisierte Fahrzeuge, Funktionale Sicherheit, ISO 26262, Szenarien, Testprozess

1 Einleitung

Fahrerassistenzsysteme und teilautomatisierte Fahrzeugführungssysteme nach den Definitionen von Gasser et al. [2012] gehören in den oberen Fahrzeugklassen bereits zur Standardausstattung. Den nächsten Schritt stellt die Einführung hochautomatisierter und vollautomatisierter Systeme dar. Eine große Herausforderung für die Einführung von Fahrzeugführungssystemen liegt in der konzeptionellen und technischen Entwicklung, der Verifikation und der Validierung eines Sicherheitskonzeptes.

Die Norm ISO 26262 ist ein Leitfaden für die Entwicklung von sicherheitskritischen elektrischen/elektronischen Systemen und legt damit auch einen Rahmen für die Entwicklung automatisierter Fahrzeugführungssysteme unter dem Aspekt der funktionalen Sicherheit fest. In dem von der Norm ISO 26262 vorgeschlagenen Entwicklungsprozess kann die Beschreibung von Szenarien helfen Anforderungen zu formulieren, die benötigten Hard- und Softwarekomponenten zu konzeptionieren und das funktionale Sicherheitskonzept im Testprozess zu validieren und verifizieren. Bereits in der Gefährdungsanalyse und Risikobewertung und spätestens bei der Erstellung von Testfällen werden Szenarien

*G. Bagschik, T. Menzel und A. Reschka sind wissenschaftliche Mitarbeiter am Institut für Regelungstechnik der Technischen Universität Braunschweig (Email: {bagschik, menzel, reschka}@ifr.ing.tu-bs.de).

†M. Maurer ist Professor und Institutsleiter an selbigem Institut (Email: maurer@ifr.ing.tu-bs.de).

zur Beschreibung der Eingangsdaten des Entwicklungsgegenstandes benötigt. Daraus ergeben sich für die Darstellung von Szenarien in den Entwicklungsphasen unterschiedliche Anforderungen, die in diesem Beitrag analysiert werden.

Der Ansatz, der in diesem Beitrag dargestellt wird, stellt eine Definition von Szenarien auf unterschiedlichen Abstraktionsebenen vor. Auf diese Weise können Szenarien von Beginn des Entwicklungsprozesses an bereits in der Konzeptphase identifiziert werden und im weiteren Verlauf detailliert und konkretisiert werden. Dies erlaubt einen strukturierten Ansatz ausgehend von der Definition des Entwicklungsgegenstandes, über eine Gefährdungsanalyse und Risikobewertung, bis hin zur Ableitung von Testfällen für die Validierung und Verifikation des Gesamtsystems. Aus diesem Grund stellen die Autoren in diesem Beitrag ausgehend von der Definition des Begriffs Szenario nach Ulbrich et al. [2015] eine erweiterte Definition vor und führen die Abstraktionsebenen der funktionalen, logischen und konkreten Szenarien ein.

1.1 Bisherige Arbeiten

Ulbrich et al. [2015] haben die Begriffe Szene, Situation und Szenario aus diversen Quellen verglichen und eine einheitliche Definition für automatisierte Fahrzeugführungssysteme und Fahrerassistenzsysteme vorgeschlagen.

Bagschik et al. [2016] haben aufbauend auf diesen Definitionen eine Vorgehensweise zur Generierung potenziell gefährlicher Szenarien für eine Gefährdungsanalyse und Risikobewertung nach dem Entwicklungsprozess der Norm ISO 26262 erarbeitet. Diese Vorgehensweise nutzt eine abstrahierte Beschreibung der Verkehrsteilnehmer sowie der Szenerie und kombiniert diese mit einer Modellierung von funktionalen Fehlern für einen eingeschränkten Anwendungsfall des vollautomatisierten Fahrens im Projekt *automatisch fahrerlos fahrendes Absicherungsfahrzeug für Arbeitsstellen auf Bundesautobahnen* (aFAS).

Schuldt et al. [2013] motivieren einen szenarienbasierten Testprozess und stellen eine systematische Testfallgenerierung mittels eines 4-Ebenen-Modells vor.

Bach et al. [2016] motivieren eine modellbasierte Szenariendarstellung mit räumlichen und zeitlichen Beziehungen als durchgängige Darstellungsweise im Entwicklungsprozess der Norm ISO 26262. Die Darstellung wurde prototypisch für ein ACC-System auf Autobahnen implementiert und die Ergebnisse wurden vorgestellt.

Bergenhem et al. [2015] argumentieren, dass vollständige Anforderungen für automatisierte Fahrzeuge nur durch einen durchgängigen, nachverfolgbaren und verifizierbaren Prozess der Anforderungserstellung im Sinne des V-Modells erreicht werden können [Verein Deutscher Ingenieure (VDI), 2004].

Die genannten Veröffentlichungen verwenden Szenarien auf unterschiedlichen Abstraktionsebenen für die Entwicklung und Absicherung automatisierter Fahrzeuge. Dabei wird der Begriff *Szenario* nicht einheitlich definiert, was ein gemeinsames Verständnis für die Nutzung von Szenarien im Entwicklungsprozess der Norm ISO 26262 erschwert. Dieser Beitrag schlägt daher eine erweiterte Definition des Begriffs Szenario vor.

1.2 Aufbau des Beitrags

In diesem Beitrag werden im nächsten Abschnitt Anforderungen an die Darstellung und Verwendung von Szenarien im Entwicklungsprozess der Norm ISO 26262 abgeleitet und analysiert. Danach folgt eine Definition verschiedener Abstraktionsebenen für Szenarien

im Entwicklungsprozess und wie diese Abstraktionsebenen ineinander überführt werden können.

2 Motivation und Problemstellung

Die Norm ISO 26262 stellt derzeit in der Fassung von 2011 [ISO, 2011] den Stand der Technik für die funktionale sichere Entwicklung[1] sicherheitskritischer E/E-Systeme dar. Abbildung 1 zeigt die Übersicht der Prozessschritte aus der Norm ISO 26262 und markiert (rot), in welchen Prozessschritten Szenarien genutzt werden können, um die geforderten Arbeitsergebnisse (vgl. englisch *work products*) zu erbringen. Der Begriff des Szenarios wurde von Ulbrich et al. [2015] in verschiedenen Disziplinen untersucht und es wurde eine Definition für das automatisierte Fahren vorgeschlagen. Dieser Beitrag folgt der Definition des Szenarios von Ulbrich et al. [2015]. Go und Carroll [2004] stellen heraus, dass Szenarien in den meisten Anwendungen aus den gleichen Bestandteilen zusammengesetzt sind. Dabei können Szenarien jedoch in unterschiedlichen Detailgraden spezifiziert und dargestellt werden. Die Darstellung von Szenarien kann informativ, semi-formal oder formal erfolgen [Go und Carroll, 2004]. Diese Unterscheidung gibt einen Hinweis auf mehrere Detailgrade im Entwicklungsprozess der Norm ISO 26262.

Da Szenarien im Entwicklungsprozess nach Norm ISO 26262 von der Konzeptphase über die technische Entwicklung bis zum Test und der Validierung des Gesamtsystems verwendet werden, ist es notwendig, die aus den Prozessschritten resultierenden Anforderungen an Szenarien zu definieren. Die Anforderungen ermöglichen eine einheitliche Definition von Detailgraden für die Verwendung von Szenarien. Die folgenden Abschnitte orientieren sich an den Arbeitsergebnissen der Norm ISO 26262 und leiten Anforderungen an die Darstellungsweisen von Szenarien in den markierten Prozessschritten ab.

2.1 Szenarien in der Konzeptphase und Entwicklungsphase

In der Konzeptphase (Teil 3) der Norm ISO 26262 werden vor der technischen Entwicklung der Entwicklungsgegenstand (vgl. englisch *item*) definiert, der Sicherheitslebenszyklus initiiert, eine Gefährdungsanalyse und Risikobewertung durchgeführt und resultierend aus der Analyse ein funktionales Sicherheitskonzept erstellt. In der Beschreibung des Entwicklungsgegenstandes (vgl. englisch *item definition*) sollen funktionale Konzepte und Systemgrenzen, die Einsatzumgebung, die rechtlichen Rahmenbedingungen und die Abhängigkeiten zu anderen Entwicklungsgegenständen beschrieben werden. Aus diesen Informationen lassen sich mögliche Betriebsszenarien für den Entwicklungsgegenstand ableiten. Reschka [2017] schlägt vor, für diese Szenarien sichere Fahrzustände festzulegen und das Sollverhalten des zu entwickelnden Systems zu beschreiben. Die Betriebsszenarien sind in diesem Prozessschritt abstrakt gehalten und für den menschlichen Sprachgebrauch (textuelle Beschreibung, Experten- und Entwicklergespräche) zu formulieren.

Der nächste Prozessschritt, in dem in der Norm ISO 26262 Szenarien zur Erbringung der Arbeitsergebnisse gefordert werden, ist die Gefährdungsanalyse und Risikobewertung (GuR). Diese setzt sich aus den Teilschritten *Situationsanalyse und Gefährdungsidentifikation* und *Klassifikation von gefährlichen Ereignissen* zusammen. In der Situations-

[1] Die gesamte Systementwicklung für automatisierte Fahrzeuge umfasst zusätzlich parallele Entwicklungsprozesse, die andere Aspekte, wie beispielsweise die Funktionsentwicklung, des Systems behandeln.

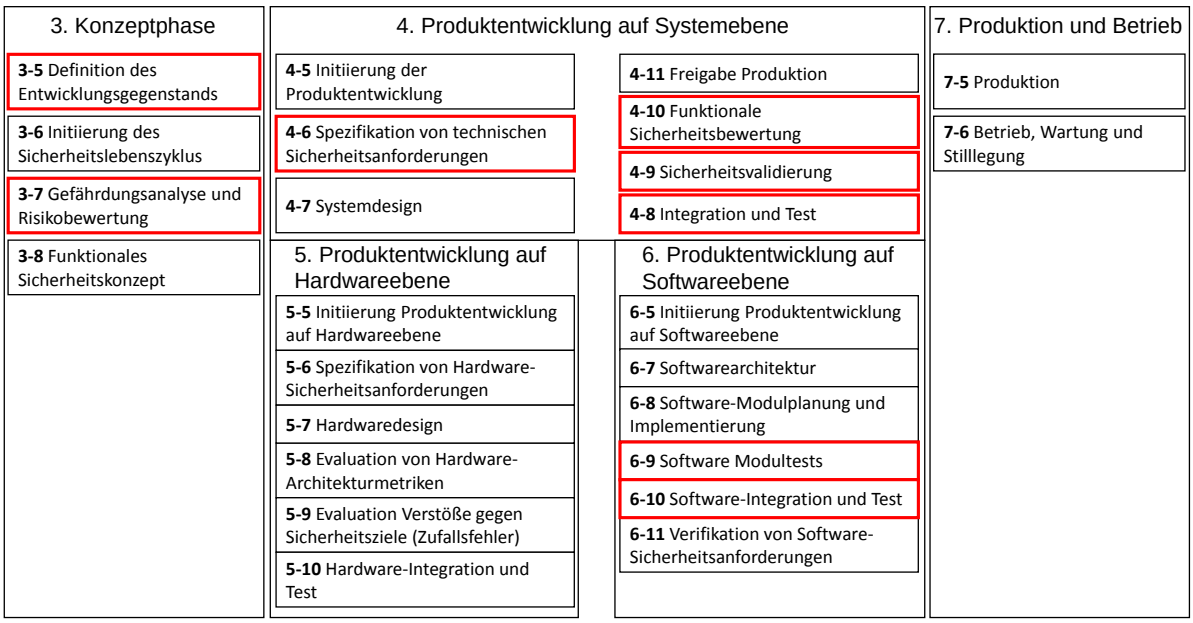

Abbildung 1: Prozessübersicht der Norm ISO 26262. Rot markierte Phasen nutzen Szenarien zur Erbringung der Arbeitsergebnisse.

analyse nach Norm ISO 26262 sollen alle Betriebssituationen[2] und -zustände, in denen ein funktionales Fehlverhalten (vgl. englisch *malfunctioning behavior*) Schaden verursachen kann, identifiziert werden. Das funktionale Fehlverhalten kann dabei als Abweichung vom definierten Sollverhalten interpretiert werden. Gefährliche Szenarien, welche aus der Kombination von Betriebsszenarien und funktionalem Fehlverhalten bestehen, werden anschließend mit dem Sicherheitsintegritätslevel für Automobile (ASIL) bewertet. Die Darstellung der gefährlichen Szenarien muss somit andere Verkehrsteilnehmer und das stationäre Umfeld beinhalten, um die Parameter Auftretenswahrscheinlichkeit des Betriebsszenarios, mögliche Schadensschwere und Beherrschbarkeit des gefährlichen Szenarios[3] der ASIL-Klassifikation ermitteln zu können. Die Analyse der gefährlichen Szenarien wird nach derzeitigem Stand der Technik von Experten durchgeführt, weshalb diese Szenarien sprachlich formuliert werden müssen. Da menschliche Experten je nach Fachgebiet und Expertise unterschiedlich detaillierte Begriffe für die Beschreibung eines Szenarios verwenden, muss ein einheitliches Vokabular für die funktionale Betrachtungsweise im Prozessschritt der Gefährdungsanalyse und Risikobewertung definiert werden. Weiterhin können die definierten Begriffe des Vokabulars, zum Beispiel durch Ontologien, formal geordnet werden, um ein allgemeines Verständnis unter Experten zu gewährleisten. Somit können sprachlich gefasste Szenarien aus Kombinatorik der geordneten Begriffe erzeugt und der Interpretationsraum für Experten verkleinert werden.

Nachdem die gefährlichen Szenarien analysiert wurden und ein funktionales Sicherheitskonzept erstellt wurde, werden in Prozessschritt 4-6 technische Sicherheitsanforderungen festgelegt. Technische Anforderungen können gegenüber funktionalen Anforderungen

[2]Die Autoren weisen darauf hin, dass der Begriff *Betriebssituation* aus dem Sprachgebrauch der Norm ISO 26262 nach Definition von Ulbrich et al. [2015] als *Betriebsszenario* bezeichnet werden müsste.

[3]Die Beherrschbarkeit eines Szenarios umfasst die Beherrschbarkeit durch den Fahrer im eigenen Fahrzeug und die Beherrschbarkeit durch andere Verkehrsteilnehmer.

quantifiziert werden. Beispielsweise kann die funktionale Anforderung, einen Sicherheitsabstand einzuhalten, durch den einzuhaltenden Abstand in Metern im Zustandsraum formuliert werden. Jedes gefährliche Szenario kann von der sprachlichen und semi-formalen Darstellungsweise der *Konzeptphase* (3) für die *Produktentwicklung auf Systemebene* (4) in physikalische Zustandsgrößen überführt werden. Eine Auflistung dieser Zustandsgrößen ist eindeutig, aber für den menschlichen Experten aufgrund der Detailtiefe nicht mehr intuitiv zu verarbeiten. Um die Anzahl der Szenarien zu reduzieren, können Zustandsgrößen in Wertebereichen zusammengefasst und somit sichere und unsichere Wertebereiche festgelegt werden. Diese Detaillierung der sprachlichen Elemente zu einer oder mehreren Zustandsgrößen führt dazu, dass Anforderungen an das zu entwickelnde System validierbar formuliert werden können, sodass in Prozessschritt 4-9 der Norm ISO 26262 eine Sicherheitsvalidierung durchgeführt werden kann.

2.2 Szenarien im Testprozess und in der Absicherung

Nach der technischen Entwicklung wird geprüft, ob das implementierte System die in den vorherigen Prozessschritten gestellten Anforderungen erfüllt. Für diese Verifikation müssen Tests systematisch geplant, spezifiziert, durchgeführt, evaluiert und dokumentiert werden [ISO, 2011, Teil 8, Abschnitt 9.2].

Eine Testfallspezifikation muss in diesem Rahmen unabhängig von der Testmethode folgende Informationen enthalten:

1. Eindeutige Kennung
2. Referenz auf das Testobjekt
3. Vorbedingungen und Konfiguration[4]
4. Umgebungsbedingungen
5. Eingangsdaten mit zeitlichem Verlauf
6. Erwartetes Verhalten formuliert in Wertebereichen

Eine große Herausforderung der Testfallerstellung liegt in der Spezifikation der Eingangsdaten. Die Eingangsdaten müssen den zeitlichen Verlauf aller Parameter beinhalten, die das Verhalten des Testobjektes maßgeblich beeinflussen. Zeitgleich dürfen die Eingangsparameter keine Widersprüche[5] aufweisen, sondern müssen aufgrund der Komplexität, im Sinne von interagierenden Komponenten, aktueller Systeme konsistente Eingangsdaten in Form eines Szenarios darstellen [vgl. Ulbrich et al., 2015].

Informationen über die Einsatzumgebung des zu testenden Systems sowie die auftretenden Betriebsszenarien werden bereits im Rahmen der Beschreibung des Entwicklungsgegenstandes in der Konzeptphase der Norm ISO 26262 zusammengestellt. Diese Informationen können als Grundlage für die Erstellung konsistenter Eingangsdaten bei der Spezifikation von Testfällen genutzt werden. Die Szenarien der Beschreibung des Entwicklungsgegenstandes liegen auf einer abstrakten sprachlich gefassten Ebene vor und

[4] Im Sinne einer Systemvariante

[5] Hiermit sind unbeabsichtigte Widersprüche gemeint. Fehlerinjektionen können später als Testmethode gezielt eingesetzt werden.

müssen für die Verwendung im Rahmen eines Testfalls zunächst weiter detailliert und konkretisiert werden.

Der Detaillierungsschritt kann im Rahmen der *Spezifikation von technischen Sicherheitsanforderungen* erfolgen [Teil 4, Abschnitt 6 ISO, 2011]. Die technischen Sicherheitsanforderungen beschreiben unter anderem, wie der Entwicklungsgegenstand auf äußere Anregungen, die eine Einhaltung der Sicherheitsziele beeinflussen können, reagieren soll. Die technischen Anforderungen detaillieren die sprachlich gefassten Anforderungen im Parameterraum (inklusive Parameterbereiche) und geben somit an, in welchen Bereichen die Funktionalität des Systems gegeben sein muss. Dieser Parameterraum muss im Verifikationsprozess systematisch geprüft und somit bei der Erstellung von Testfällen berücksichtigt werden. Zudem müssen die Szenarien im Detaillierungsschritt in eine formale Darstellung überführt werden, um später eine reproduzierbare Testdurchführung gewährleisten zu können. In den Szenarien müssen alle Parameter zur Ausführung im jeweiligen Prüfverfahren (Simulation, Feldtest, etc.) beschrieben sein. Im Detaillierungsschritt steht somit die Überführung der Szenarien von einer informativen Beschreibung mit geordneten Begriffen in eine formale Beschreibung auf Basis physikalischer Systemzustandsgrößen inklusive zugehöriger Wertebereiche im Vordergrund.

Zur Generierung der Eingangsdaten eines Testfalls müssen aus den Parameterbereichen der spezifizierten Szenarien in einem Konkretisierungsschritt die zu prüfenden Parameterstufen ausgewählt werden. Schuldt et al. [2013] schlagen für die Identifikation einer repräsentativen Stichprobe Äquivalenzklassenbildung, Grenzwertanalysen und kombinatorische Verfahren vor. Diese Verfahren erlauben eine systematische Generierung von Testfällen, geben jedoch noch keinen Hinweis auf die Testraumabdeckung. Die Testraumabdeckung muss im Testkonzept als Produkt der Auswahl der Szenarien, der zu verwendenden Prüfmethoden und der Quantisierung des Konkretisierungsschrittes ermittelt werden. Die im Konkretisierungsschritt systematisch ermittelten und formal beschriebenen Szenarien stellen widerspruchsfreie Eingangsdaten für den Entwicklungsgegenstand dar und können im Rahmen eines Testfalles zur Verifikation genutzt werden.

2.3 Anforderungen an Szenarien

Aus den oben genannten Prozessschritten der Norm ISO 26262 lassen sich die folgenden Anforderungen an Szenarien im Entwicklungsprozess formulieren (Konzeptphase [K], Systementwicklung [S], Testprozess [T]):

K1 Szenarien müssen aus der sprachlich gefassten Definition eines Entwicklungsgegenstands in eine semi-formale Darstellung überführt werden können.

K2 Szenarien müssen für menschliche Experten in einheitlicher Fachsprache formuliert werden können.

S1 Szenarien müssen Parameterbereiche für Zustandsgrößen abbilden können.

S2 Szenarien müssen eine formale Ordnung für die Darstellung in Parameterbereichen bereitstellen (zum Beispiel Dateiformat).

T1 Szenarien müssen so detailliert beschrieben werden, dass sie mit Prüfverfahren ausgeführt werden können.

T2 Szenarien müssen eindeutig definiert werden und dürfen keine Interpretationsmöglichkeiten aufweisen (Reproduzierbarkeit).

T3 Szenarien müssen effizient maschinen-lesbar dargestellt werden.

Aus den oben genannten Anforderungen ergeben sich Widersprüche hinsichtlich der Darstellungsweise von Szenarien. Die Anforderungen K1 und T3 drücken den Bedarf für eine abstrakte sprachliche (K1) und im Gegensatz dazu eine effizient maschinen-lesbare (T3) Repräsentation der Szenarien aus. Da natürliche Sprache für Maschinen schwer zu verarbeiten ist und Menschen effiziente (meist binarisierte) Datenformate nicht lesen können, ergibt sich eine Notwendigkeit nach mehreren Darstellungsweisen der Szenarien. Ebenso ergibt sich aus den Anforderungen S1 und T2 eine gegensätzliche Sichtweise auf die Darstellung von Szenarien. Wenn Bereiche für Zustandsgrößen angegeben werden können (S1), lässt dies einen gewissen Spielraum bei der Festlegung von konkreten Größen, die für die Ausführung in unterschiedlichen Prüfverfahren notwendig sind (T2). Daraus ergibt sich neben den Forderungen nach einer sprachlichen und einer maschinen-lesbaren Darstellung noch eine Unterscheidung des Detailgrades bei letzterer Darstellung.

3 Szenarien für Entwicklung, Absicherung und Test

Wie im vorherigen Abschnitt hergeleitet, ergeben sich widersprüchliche Anforderungen an die Darstellungsweise von Szenarien im Entwicklungsprozess der Norm ISO 26262. Im folgenden Abschnitt werden drei Abstraktionsebenen für Szenarien vorgeschlagen und es wird dargestellt, wie sich diese Ebenen im Verlauf des Entwicklungsprozesses ineinander überführen lassen.
Abbildung 2 zeigt die Unterteilung der Abstraktionsebenen in *funktionale*, *logische* und *konkrete* Szenarien, die in den folgenden Abschnitten definiert werden.

3.1 Funktionale Szenarien

Funktionale Szenarien bilden die erste und somit abstrakteste Ebene von Szenarien, welche in der Konzeptphase der Norm ISO 26262 zur Definition des Entwicklungsgegenstands und der Gefährdungsanalyse und Risikobewertung genutzt werden können. Die Darstellung von funktionalen Szenarien basiert auf einer sprachlichen Beschreibung. Funktionale Szenarien können somit Expertenwissen abbilden und sind intuitiv lesbar. Die Autoren schlagen folgende Definition für funktionale Szenarien vor:

> Funktionale Szenarien stellen Betriebsszenarien des Entwicklungsgegenstands auf semantischer Ebene dar. Die Entitäten und Beziehungen zwischen den Entitäten der Anwendungsdomäne werden in sprachlich gefassten Szenarien ausgedrückt. Die Szenarien sind widerspruchsfrei. Das Vokabular der funktionalen Szenarien ist spezifisch für den Anwendungsfall und die -domäne und kann unterschiedliche Detailgrade aufweisen.

Die Darstellung funktionaler Szenarien auf semantischer Ebene beinhaltet eine sprachliche und widerspruchsfreie Beschreibung der Entitäten (Bestandteile der Szenarien) und der Beziehungen und Interaktionen zwischen den Entitäten. Funktionale Szenarien lassen

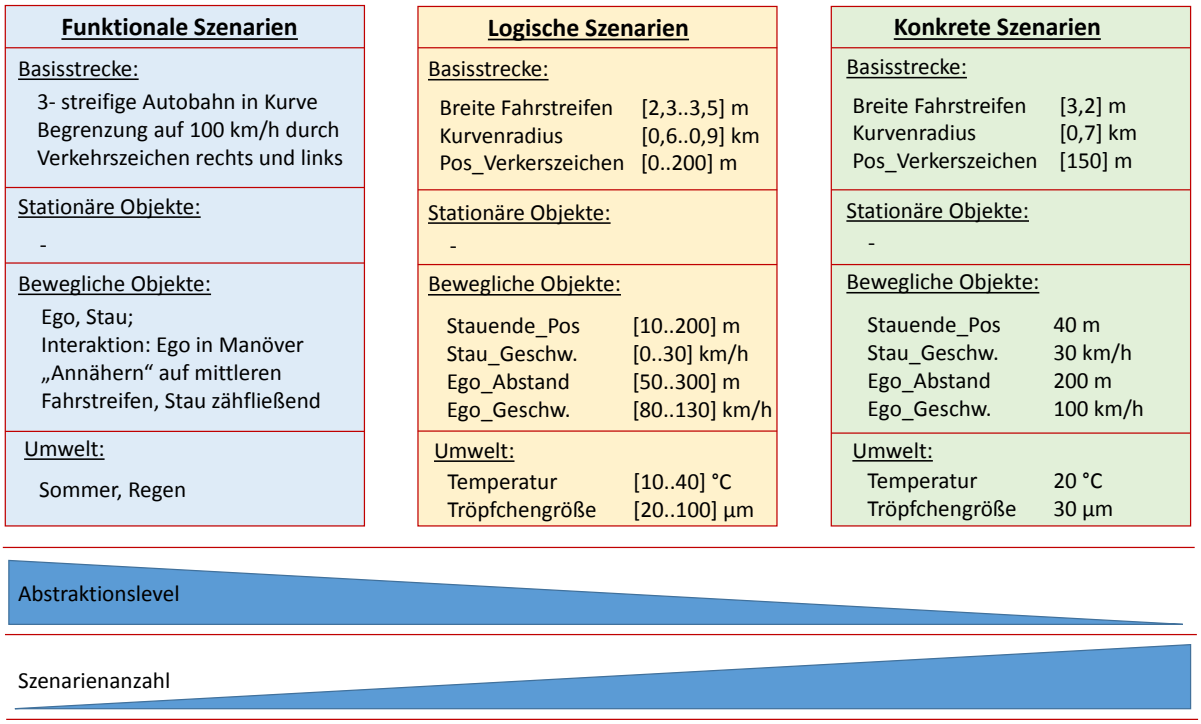

Abbildung 2: Abstraktionsebenen von Szenarien anhand eines Beispielszenarios im Entwicklungsprozess nach Norm ISO 26262

sich somit durch ein Vokabular, das Entitäten (Fahrzeug A, Fahrzeug B) und deren Beziehung zueinander (Fahrzeug A überholt Fahrzeug B) einheitlich definiert, beschreiben.

Der Detailgrad dieser Szenarien lässt sich nicht eindeutig definieren, da dieser durch die aktuelle Entwicklungsphase, den Fokus der Betrachtung und die daraus resultierende Wahl des Vokabulars maßgeblich beeinflusst wird. Wird ein umfangreiches Vokabular zur Beschreibung aller Entitäten gewählt, kann eine große Anzahl von Szenarien aus dem Vokabular erzeugt werden. Für die widerspruchsfreie Erstellung von funktionalen Szenarien müssen die Begriffe des Vokabulars eindeutig voneinander trennbar sein. Quellen für die Beschreibung der Domäne können beispielsweise Normen und Richtlinien (Richtlinien zur Anlage von Autobahnen, Straßenverkehrsordnung, etc.) sein, in denen Entitäten des Verkehrsgeschehens benannt und differenzierbar definiert sind. Für den jeweiligen Anwendungsfall (Was tut der Entwicklungsgegenstand?) kann ein (firmen-)eigenes Vokabular genutzt werden, welches jedoch über Entwicklungsstände einheitlich definiert sein muss. Somit können bereits erstellte Szenarien für weitere Entwicklungen nachverfolgbar genutzt werden.

3.2 Logische Szenarien

Logische Szenarien stellen in der Definition dieses Beitrags eine Detaillierung der funktionalen Szenarien im physikalischen Zustandsraum dar. Somit lassen sich funktionale Szenarien in Parameter der Entitäten (absolute Parameter) und Parameter der Beziehungen (relative Parameter) überführen. Die Autoren schlagen folgende Definition für logische Szenarien vor:

> Logische Szenarien stellen Betriebsszenarien durch Entitäten und Beziehungen dieser Entitäten mithilfe von Parameterbereichen im Zustandsraum dar. Für die einzelnen Parameterbereiche können optional statistische Verteilungen angegeben werden. Zusätzlich können optional die Beziehungen der Parameterbereiche zueinander mithilfe von Korrelationen oder numerischen Bedingungen modelliert werden. Logische Szenarien enthalten eine formale Beschreibung von Szenarien.

Für eine schrittweise Detaillierung von Szenarien im Entwicklungsprozess werden logische Szenarien bereits formalisiert im Zustandsraum, jedoch in Wertebereichen der Parameter, angegeben. Für eine genauere Beschreibung der Parameterbereiche können statistische Verteilungen (Normalverteilung, Gleichverteilung etc.) modelliert werden. Beziehungen zwischen Parameterbereichen können zusätzlich durch numerische Bedingungen (z.B. bei Überholvorgängen muss Geschwindigkeit A größer Geschwindigkeit B sein) oder Korrelationsfunktionen (z.B. Fahrstreifenbreite in Abhängigkeit des Kurvenradius) näher spezifiziert werden.

3.3 Konkrete Szenarien

Konkrete Szenarien beschreiben die Entitäten und Beziehungen der Entitäten mithilfe von eindeutigen Parametern im Zustandsraum. Jedes logische Szenario kann durch Konkretisierung der Parameterbereiche zu jeweils einem festen Wert in ein konkretes Szenario überführt werden. Die Autoren schlagen daher folgende Definition für konkrete Szenarien vor:

> Konkrete Szenarien stellen Betriebsszenarien eindeutig durch Entitäten und Beziehungen dieser Entitäten mithilfe von festen Werten im Zustandsraum dar.

Aus einem logischen Szenario mit wertkontinuierlichen Parameterbereichen können durch infinitesimale Abtastung und Kombination der Wertebereiche theoretisch beliebig viele konkrete Szenarien abgeleitet werden. Die Konkretisierung erfolgt anhand der Identifikation und Kombination repräsentativer Diskretisierungsstufen der Parameter. Nur konkrete Szenarien können direkt in einen Testfall überführt und mit dem Fahrzeugführungssystem ausgeführt werden.

3.4 Einordnung in den Entwicklungsprozess

Funktionale, logische und konkrete Szenarien lassen sich durch Detaillierung und Überführung in den Zustandsraum sowie Konkretisierung von Wertebereichen zu festen Parametern ineinander überführen. Abbildung 3 zeigt einen schematischen Entwicklungsprozess nach dem V-Modell mit der Zuordnung der in diesem Beitrag definierten Szenarien.

Die funktionalen Szenarien werden vor der technischen Entwicklung zur Definition des Entwicklungsgegenstandes und der Gefährdungsanalyse und Risikobewertung genutzt. Durch die Detaillierung und die Überführung der sprachlich gefassten Szenarien in den Zustandsraum können technische Anforderungen durch valide und nicht valide Wertebereiche

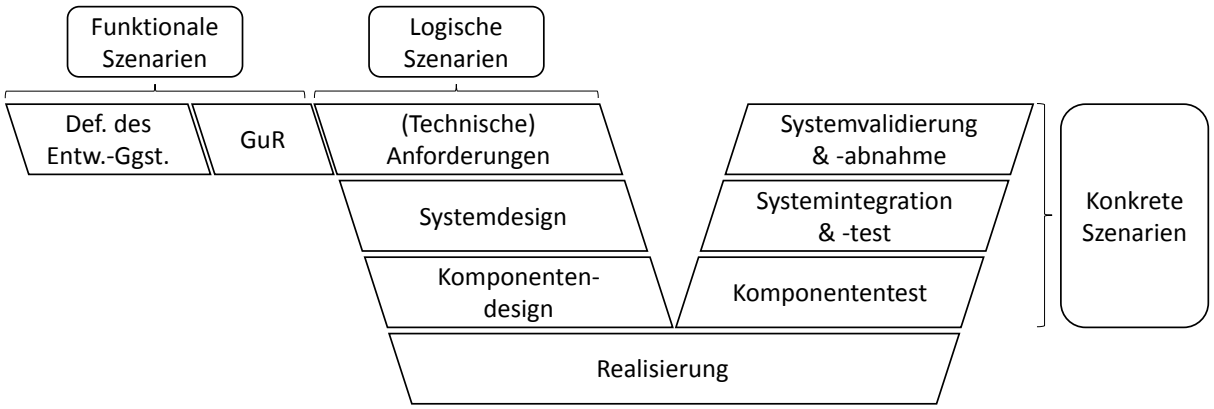

Abbildung 3: Funktionale, logische und konkrete Szenarien im V-Modell-basierten Entwicklungsprozess; Abkürzung: GuR - Gefährdungsanalyse und Risikobewertung

formuliert werden. Konkrete Szenarien dienen als Grundlage für ausführbare Testfälle und müssen vorher, wie bereits von Ulbrich et al. [2015] formuliert, um das erwartete Sollverhalten des Testgegenstands und die zu verwendende Testinfrastruktur erweitert werden. Das Sollverhalten kann dabei aus den funktionalen (Betriebs-)Szenarien und der Definition des Entwicklungsgegenstandes abgeleitet werden. Ein weiterer Unterschied zwischen Szenarien und Testfällen besteht darin, dass das resultierende Verhalten des Testgegenstandes in einem Testfall nicht bekannt ist und erst durch die Ausführung eintritt. In Szenarien ist das Verhalten aller Teilnehmer zumindest durch ihre Ziele und Werte definiert. Diesen Aspekt und die damit zusammenhängende Transformation der Szenarien zu Testfällen wird im Entwicklungsprozess durch die Erstellung des Testkonzepts und die Identifikation von Testfällen erreicht.

4 Zusammenfassung und Ausblick

In diesem Beitrag wurde der Entwicklungsprozess der Norm ISO 26262 hinsichtlich der Umsetzbarkeit einer szenarienbasierten Entwicklung betrachtet. Zu diesem Zweck wurden die Prozessschritte identifiziert, in welchen Szenarien zur Erbringung der Ergebnisse des jeweiligen Prozessschrittes genutzt werden können. Weiterführend wurden Anforderungen an die Darstellungen von Szenarien definiert und Widersprüche hinsichtlich der aus unterschiedlichen Prozessschritten resultierenden Anforderungen aufgezeigt. Auf dieser Grundlage haben die Autoren unterschiedliche Abstraktionsebenen von Szenarien eingeführt, um alle Anforderungen erfüllen zu können. Des Weiteren wurden Definitionen für die eingeführten Abstraktionsebenen vorgeschlagen und in den Entwicklungsprozess der Norm ISO 26262 eingeordnet.

Aufbauend auf den eingeführten Abstraktionsebenen werden zukünftig Methoden und Werkzeuge benötigt, um die Darstellungen von Szenarien entlang des Prozesses der Norm ISO 26262 ineinander zu überführen. Dabei lassen sich bestehende Ansätze zur Szenarienmodellierung in die vorgeschlagenen Abstraktionsebenen einordnen. Anschließend kann der Bedarf nach fehlenden Darstellungsweisen und Methoden zur Detaillierung und Konkretisierung identifiziert werden.

5 Danksagung

Dieser Beitrag entstand im Rahmen von *PEGASUS - Projekt zur Etablierung von generell akzeptierten Gütekriterien, Werkzeugen und Methoden sowie Szenarien und Situationen zur Freigabe hochautomatisierter Fahrfunktionen*, gefördert vom Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages.

Literatur

Bach, J., Otten, S. und Sax, E. (2016). Model based scenario specification for development and test of automated driving functions. In *2016 IEEE Intelligent Vehicles Symposium (IV)*, Seiten 1149–1155, Göteborg.

Bagschik, G., Reschka, A., Stolte, T. und Maurer, M. (2016). Identification of Potential Hazardous Events for an Unmanned Protective Vehicle. In *2016 IEEE Intelligent Vehicles Symposium (IV)*, Seiten 691–697, Göteborg.

Bergenhem, C., Johansson, R., Söderberg, A., Nilsson, J., Tryggvesson, J., Törngren, M. und Ursing, S. (2015). How to Reach Complete Safety Requirement Refinement for Autonomous Vehicles. In *CARS 2015 - Critical Automotive Applications: Robustness & Safety*, Paris.

Gasser, T., Arzt, C., Ayoubi, M., Bartels, A., Bürkle, L., Eier, J., Flemisch, F., Häcker, D., Hesse, T., Huber, W., Lotz, C., Maurer, M., Ruth-Schumacher, S., Schwarz, J. und Vogt, W. (2012). In *Rechtsfolgen zunehmender Fahrzeugautomatisierung: gemeinsamer Schlussbericht der Projektgruppe*, Ausgabe 83 von *Berichte der Bundesanstalt für Straßenwesen*. Wirtschaftsverlag NW Verlag für neue Wissenschaft, Bergisch Gladbach.

Go, K. und Carroll, J. M. (2004). The Blind Men and the Elephant: Views of Scenario-based System Design. *interactions*, 11(6):44–53.

ISO (2011). *26262 – Road vehicles – Functional Safety*.

Reschka, A. (2017). *Fertigkeiten- und Fähigkeitengraphen als Grundlage für den sicheren Betrieb von automatisierten Fahrzeugen in städtischer Umgebung*. Dissertation, Technische Universität Braunschweig, Braunschweig. angekündigt.

Schuldt, F., Saust, F., Lichte, B., Maurer, M. und Scholz, S. (2013). Effiziente systematische Testgenerierung für Fahrerassistenzsysteme in virtuellen Umgebungen. In *AAET - Automatisierungssysteme, Assistenzsysteme und eingebettete Systeme für Transportmittel*, Seiten 114 – 134, Braunschweig.

Ulbrich, S., Menzel, T., Reschka, A., Schuldt, F. und Maurer, M. (2015). Definition der Begriffe Szene, Situation und Szenario für das automatisierte Fahren. In *10. Workshop Fahrerassistenzsysteme FAS 2015*, Seiten 105 – 117, Walting im Altmühltal.

Verein Deutscher Ingenieure (VDI) (2004). VDI-Richtlinien - Entwicklungsmethodik für mechatronische Systeme.