Markus Ettinger, BSc

# Methoden und Prozesse zur Abarbeitung des Safety Lifecycle der Funktionalen Sicherheit in der Konzeptphase der Fahrzeugentwicklung bei Magna Steyr

Masterarbeit

zur Erlangung des akademischen Grades Dipl.-Ing.

Technische Universität Graz

Studienrichtung: Wirtschaftsingenieurwesen-Maschinenbau

Institut für Technische Informatik

Betreuer: Dipl.-Ing. Dr.techn. Christian Kreiner

Magna Steyr

Betreuer: Dipl.-Ing. Helmut Schoby

Graz, August 2016

# Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbstständig verfasst, andere als die angegebenen Quellen/Hilfsmittel nicht benutzt, und die den benutzten Quellen wörtlich und inhaltlich entnommenen Stellen als solche kenntlich gemacht habe. Das in TUGRAZonline hochgeladene Textdokument ist mit der vorliegenden Masterarbeit identisch.

# Statutory Declaration

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitly indicated all material which has been quoted either literally or by content from the sources used. The text document uploaded to TUGRAZonline is identical to the present master‘s thesis.

| | |
|---|---|
| Datum/Date | Unterschrift/Signature |

# Sperrvermerk

Diese Diplomarbeit enthält vertrauliche Daten der Firma Magna Steyr. Sie ist daher bis August 2018 für die Öffentlichkeit gesperrt. Veröffentlichungen und Vervielfältigungen jeglicher Art – auch auszugsweise – sind bis zu diesem Zeitpunkt ausdrücklich untersagt.

# Danksagung

An dieser Stelle möchte ich mich bei Magna Steyr und bei Herrn Dipl.-Ing. Dr. Wilhelm Dietrich bedanken, dass mir die Möglichkeit gegeben wurde, diese Masterarbeit in einem der größten Unternehmen der Steiermark verfassen zu können. Mein besonderer Dank geht an Herrn Dipl.-Ing. Helmut Schoby, der mir jederzeit mit fachlichen Ratschlägen zur Seite stand und von dem ich auch persönlich sehr viel lernen konnte. Außerdem möchte ich mich bei Frau Dipl.-Ing. Alexandra Schwarzböck und allen Fachbereichsvertreterinnen und Fachbereichsvertretern aus dem Kernteam der Funktionalen Sicherheit dafür bedanken, dass sie mich mit vielen Hinweisen und Anregungen bei der Erstellung der Templates so tatkräftig unterstützt haben.

Mein Dank gilt auch Herrn Dipl.-Ing. Dr. Christian Kreiner, der mich seitens des Institutes für Technische Informatik betreut hat und der bei der systematischen Herangehensweise der Erstellung dieser Masterarbeit eine große Hilfe war. Der interessierten Leserin und dem interessierten Leser möchte ich an dieser Stelle auch die von Dipl.-Ing. Dr. Kreiner abgehaltene Lehrveranstaltung „Fehlertolerante Rechnersysteme“ ans Herz legen, in der wesentliche Elemente der Funktionalen Sicherheit mit praktischem Bezug bearbeitet werden.

Abschließend möchte ich ein paar Worte an meine Familie und meine Freundin richten. Eurer Unterstützung ist es zu verdanken, dass ich mich in den letzten Jahren voll auf mein Studium und nun auch auf das Verfassen dieser Arbeit konzentrieren konnte. Ohne euch wäre all dies nicht möglich gewesen, vielen Dank dafür!

# Kurzfassung

Die ISO 26262 ist die im Automobilbereich gültige Norm der Funktionalen Sicherheit und stellt spezielle Anforderungen an die sicherheitsgerechte Entwicklung und Produktion von Straßenfahrzeugen. In diesem Zusammenhang sehen sich Fahrzeughersteller und Zulieferfirmen auch mit einem erhöhten Dokumentationsaufwand konfrontiert. In der Norm werden diese geforderten Dokumente auch als „Work Products“ bezeichnet.

Im Zuge dieser Arbeit wurden Vorlagen zu einigen der normativ geforderten Work Products aus der Konzeptphase des „Functional Safety Lifecycle“ der ISO 26262 erstellt. Zur Verdeutlichung der Zusammenhänge werden zuerst einige wesentliche Teile und Begriffe der Norm genauer beschrieben. Zusätzlich werden einige Methoden erläutert, wie Teile der Work Products in der Theorie und Praxis erstellt werden können. Nach einer Analyse der internen Ausgangssituation der Funktionalen Sicherheit wird in weiterer Folge genauer auf die Inhalte der einzelnen Vorlagen und die Vorgehensweise bei der Erstellung Bezug genommen. Ein wichtiges Thema, das unmittelbaren Einfluss auf die Vorlagen hat, ist das Anforderungsmanagement auf unterschiedlichen Abstraktionsebenen. In dieser Arbeit wird eine Systematik vorgestellt, wie Anforderungen eindeutig identifiziert und beschrieben werden können. Diese Systematik wird in allen Vorlagen angewendet und ermöglicht die Nachverfolgbarkeit der Anforderungen über die Schnittstellen der Vorlagen hinweg. Damit die praktische Verwendbarkeit gewährleistet werden kann, wurden die fertigen Vorlagen intern vorgestellt und zur Ausarbeitung von zwei Systemen verwendet. Dadurch war es möglich die Vorlagen weiter zu optimieren und gezielt an die internen Bedürfnisse anzupassen.

Konkret wurden acht Vorlagen für Work Products aus dem Functional Safety Lifecycle der Funktionalen Sicherheit für Straßenfahrzeuge erstellt. Wichtige Kriterien bei der Erstellung waren die Berücksichtigung der internen Voraussetzungen, sowie die einfache und praktische Anwendbarkeit. Die erstellten Vorlagen können generisch eingesetzt werden und stellen eine Basis dar, um in Zukunft auch weitere Work Products nach einem ähnlichen Schema abbilden zu können.

# Abstract

The ISO 26262 is the valid standard for functional safety in the automotive industry. It has specific requirements concerning the functional safety related to the development and production of road vehicles. In this context, vehicle manufacturers and suppliers are facing a higher effort of documentation. The documents that are demanded by the standard are called work products.

Within this work several templates regarding some work products of the concept phase of the functional safety lifecycle of the ISO 26262 have been created. For clarification of the correlations some essential parts and terms of the standard are described at the beginning. Additionally some methods are described, how some parts of the work products can be established in theory and practice. After an analysis of the internal initial situation of the functional safety, the contents of the templates and how they have been created is described. An important issue that had an immediate influence on the creation of the templates is the requirements management on different levels of abstraction. In this work a method is described, how requirements can be identified and described unambiguously. This method is applied in all templates to enable traceability of the requirements via the interfaces of the different templates. To make sure that the practical usability is guaranteed, the templates have been presented and internally been used to elaborate two items. Therefore it was possible to optimize the templates and adapt them to the internal necessities.

During this thesis there have been created eight templates for work products of the functional safety lifecycle for road vehicles. Important criteria for creation were the consideration of the internal prerequisites as well as the easy and practical usability of the templates. The created templates can be used generically and constitute a basis, how further work products according the same scheme can be created.

# Inhaltsverzeichnis

# Abbildungsverzeichnis

# Abkürzungsverzeichnis

| | |
|---|---|
| **AG** | Aktiengesellschaft |
| **ALM** | Application lifecycle management |
| **ASIL** | Automotive safety integrity level |
| **AUTOSAR** | Automotive open system architecture |
| **BPMN** | Business Process Model and Notation |
| **C** | Kontrollierbarkeit |
| **CC** | Concept Confirmation |
| **DIA** | Development interface agreement |
| **E** | Expositionshäufigkeit |
| **E/E** | elektrisch/elektronisch |
| **ECU** | Electric control unit |
| **EPB** | Electric parking brake |
| **ER-FSI** | Engineering Responsible Functional Safety Item |
| **ER-FSM** | Engineering Responsible Functional Safety Manager |
| **FB** | Functional block |
| **FC** | Functional concept |
| **FFBD** | Functional flow block diagram |
| **FMEA** | Fehlermöglichkeits- und -einflussanalyse |
| **FSC** | Functional safety concept |
| **FSM** | Functional safety manager |
| **FTA** | Fault tree analysis |
| **FTTI** | Fault tolerant time interval |
| **FUSA** | Functional safety |
| **FUSI** | Funktionale Sicherheit |
| **GSN** | Goal structuring notation |
| **GuR** | Gefahren- und Risikoanalyse |
| **HARA** | Hazard analysis and risk assessment |
| **HW** | Hardware |
| **IDE** | Item Definition |
| **IEC** | International Electrotechnical Commission |
| **ISO** | International Organization for Standardization |
| **KG** | Kommanditgesellschaft |

| | |
|---|---|
| **LS** | Launch Sign-Off |
| **MS** | Magna Steyr |
| **MSDS** | Magna Steyr Development System |
| **MSE** | Magna Steyr Engineering |
| **OEM** | Original equipment manufacturer |
| **PP** | Pilot Production |
| **PPS** | Preliminary Product Specification |
| **PS** | Process Stability |
| **PTO** | Production Try Out |
| **PV** | Product Vision |
| **S** | Schadensaumaß |
| **SOP** | Start Of Production |
| **SW** | Software |
| **SWOT** | Strengths, weaknesses, opportunities and threads |
| **SysML** | Systems modeling language |
| **TA** | Target Agreement |
| **TC** | Technical concept |
| **TCL** | Tool confidence level |
| **TD** | Tool error detection |
| **TI** | Tool impact |
| **TSC** | Technical safety concept |
| **UML** | Unified Modeling Language |

# 1. Einleitung

Einleitend wird die Ausgangssituation, sowie die Aufgabenstellung und Zielsetzung dieser Masterarbeit näher erläutert.

## 1.1 Ausgangssituation

Da aufgrund der im Automobilbereich gültigen Norm der Funktionalen Sicherheit für Straßenfahrzeuge (ISO 26262), hinsichtlich der sicherheitsgerechten Fahrzeugentwicklung, erhöhte Anforderungen gestellt werden, sehen sich Fahrzeughersteller und Zulieferfirmen in diesem Zusammenhang auch mit einem erhöhten Dokumentationsaufwand konfrontiert. In der Norm werden diese geforderten Dokumente auch als Work Products bezeichnet. Um den Aufwand der Dokumentation zu reduzieren und die entsprechenden Vorschriften an den Produktentstehungsprozess erfüllen zu können, müssen Methoden, Werkzeuge und Vorlagen zur Verfügung gestellt werden, die ein strukturiertes und einheitliches Vorgehen aller beteiligten Fachbereiche ermöglichen.

Bei Magna Steyr werden Work Products der Funktionalen Sicherheit derzeit in jedem Projekt unterschiedlich und ohne durchgängige Systematik erstellt. In diesem Zusammenhang besteht folgende Problematik:

- Keine einheitliche Dokumentation
- Struktur von Fachbereich zu Fachbereich unterschiedlich
- Keine durchgehende Toolunterstützung
- Schnittstellen zwischen den Dokumenten
- Erhöhter Dokumentationsaufwand

## 1.2 Aufgabenstellung und Ziele

Die Ziele dieser Arbeit umfassen daher unter anderem die Einarbeitung in die ISO 26262 sowie in die funktionsorientierte Entwicklung bei Magna Steyr. Darauf aufbauend wird die aktuelle Situation der Funktionalen Sicherheit bei Magna Steyr erfasst und abgebildet.

Der praktische Teil der vorliegenden Masterarbeit umfasst die Erstellung von Templates für gewisse Work Products aus dem Functional Safety Lifecycle, damit diese dann im Zuge der Fahrzeugentwicklung während der Konzeptphase bei Magna Steyr verwendet werden können. Aus dieser Aufgabenstellung resultieren folgende Anforderungen an die Templates:

- Für Review-pflichtige Work Products
- Fokus auf der Konzeptphase der Fahrzeugentwicklung
- Integration der Funktionsentwicklung
- Anforderungen der ISO 26262 müssen erfüllt sein
- Templates in Form von Excel-Dokumenten
- Einheitlicher Aufbau und Struktur
- Einfach und praktisch anwendbar

## 1.3 Vorgehensweise und Aufbau

Im Anschluss an die Einleitung wird in Kapitel 2 zuerst ein kurzer Überblick über das Engineering Center von Magna Steyr und seine Tätigkeitsbereiche gegeben. Um sich in den Bereich der Funktionalen Sicherheit grundsätzlich einzuarbeiten, wurden einerseits Fachliteratur und andererseits ausgewählte Kapitel der ISO 26262 herangezogen. Bei der Literaturrecherche wurde auf die Managementthemen der Funktionalen Sicherheit besonderer Wert gelegt, wobei auch die grundsätzliche Beschreibung von Fahrzeugfunktionen ein wichtiges Thema war. Zum besseren Verständnis der Thematik wird daher der Begriff der Funktionalen Sicherheit und die Vorgehensweise nach dem V-Modell in Kapitel 3 zuerst allgemein beschrieben.

In weiterer Folge wird der Fokus auf die Anwendung im Automobilbereich gelegt. Davon sind im Speziellen solche Unternehmen betroffen, die sich mit der Entwicklung und Produktion von Straßenfahrzeugen beschäftigen. Aus diesem Grund werden in

Abschnitt 3.1 kurz die ISO 26262 und ihre wesentlichen Inhalte beschrieben. Darauf aufbauend wird in Abschnitt 3.2 genauer auf die wesentlichen Teile der Konzeptphase des Functional Safety Lifecycle Bezug genommen. Auf einige Möglichkeiten, wie Teile der Work Products in der Theorie und Praxis erstellt werden können, wird in Kapitel 4 eingegangen.

Die Erhebung der Ausgangssituation in Bezug auf die Funktionale Sicherheit bei Magna Steyr und die erstellten Templates werden in Kapitel 5 und 6 vorgestellt. Um sich ein möglichst breites Bild der Ausgangssituation der Funktionalen Sicherheit bei Magna Steyr zu machen, wurden zu diesem Zweck Einzelgespräche mit einigen Fachbereichsvertretern aus dem Kernteam der Funktionalen Sicherheit durchgeführt. Die Ergebnisse dieser Gespräche wurden in Form einer SWOT-Analyse zusammengefasst und firmenintern vorgestellt. Eine genauere Beschreibung findet sich dazu in Kapitel 5. Die erstellten Templates werden in Kapitel 6 näher beschrieben. Hier wird unter anderem genauer auf die Ursachen für die Auswahl der zu erstellenden Templates, die Grundlagen der Erstellung sowie die wichtigsten Inhalte Bezug genommen. Damit die praktische Verwendbarkeit gewährleistet werden kann, wurden die fertigen Vorlagen intern vorgestellt und zur Ausarbeitung von zwei Systemen verwendet. Dadurch war es möglich die Vorlagen zu optimieren und gezielt an die internen Bedürfnisse anzupassen.

Abschließend werden die wichtigsten Ergebnisse noch einmal zusammengefasst und ein Ausblick auf die zukünftige Themen im Zusammenhang mit der Funktionalen Sicherheit gemacht.

Es wird darauf hingewiesen, dass zum Zweck der leichteren Lesbarkeit auf eine gendergerechte Formulierung verzichtet wird. Des Weiteren werden die in dieser Arbeit verwendeten Begriffe „Produkt“ und „Fahrzeug“ synonym verwendet. Gleiches gilt auch für die Begriffe „Templates“ und „Vorlagen“.

# 2. Magna Steyr Engineering

In diesem Abschnitt wird das Unternehmen Magna Steyr Engineering kurz vorgestellt.

## 2.1 Rechtliche Grundlagen

Die Magna Steyr Engineering AG & Co KG ist eine Kommanditgesellschaft, deren eingetragener Komplementär (haftender Gesellschafter) die Magna Steyr Fahrzeugtechnik AG ist. Als Kommanditist ist die Magna Steyr Fahrzeugtechnik AG & Co KG tätig.

## 2.2 Organisationsstruktur

Die Organisation gliedert sich bei Magna Steyr in „Business Units“ und „Functional Departments“, was überblicksweise in Abbildung 1 dargestellt ist. Die Business Units haben hauptsächlich die Aufgabe, Produkte zu entwickeln und herzustellen. Die Functional Departements stellen dabei die zur Leistungserstellung notwendigen Unterstützungseinrichtungen zur Verfügung. Dies umfasst beispielsweise das Personalwesen oder das Qualitätsmanagement.

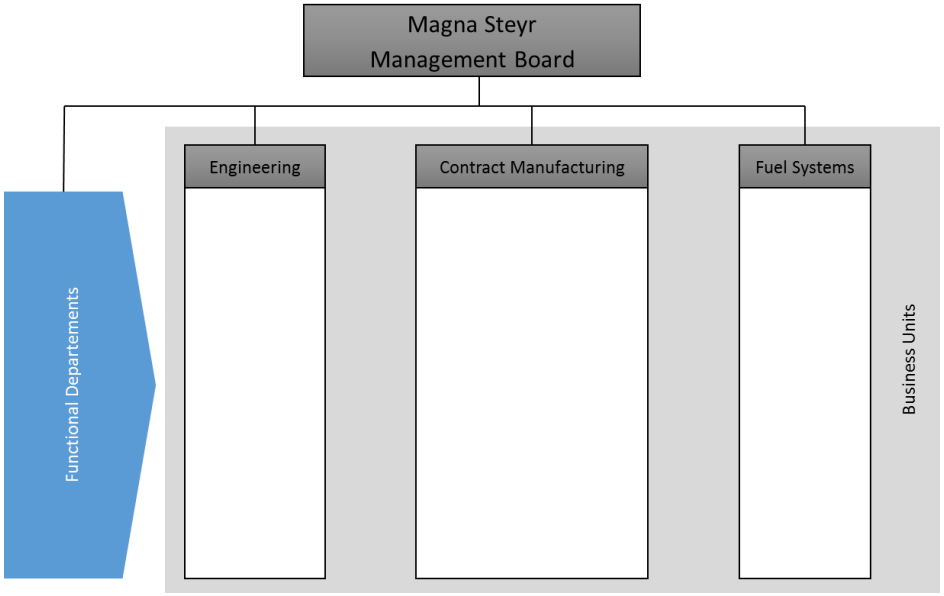


Abbildung 1: Organisation Magna Steyr

## 2.3 Tätigkeitsfeld

Der Schwerpunkt der Tätigkeit des Magna Steyr Engineerings liegt auf der Entwicklung und Integration von Modulen und Systemen bis hin zur Entwicklung von Gesamtfahrzeugen. Durch das globale Netzwerk mit 21 Entwicklungszentren welche auf 8 Ländern verteilt sind, kann gezielt auf die besonderen Produkt- und Marktanforderungen von Kunden weltweit eingegangen werden.

# 3. Funktionale Sicherheit

In diesem Kapitel soll nun zuerst der Begriff der Funktionalen Sicherheit und die Zusammenhänge allgemein beschrieben werden. Der Begriff kann folgendermaßen interpretiert werden:

> *„Funktionale Sicherheit ist die Abwesenheit eines unzumutbaren Risikos in einer Gefahrensituation, hervorgerufen durch eine Fehlfunktion eines elektrischen und oder elektronischen Systems.“* (ISO 26262-1, 2011, S. 8)

Dementsprechend betrifft die Funktionale Sicherheit grundsätzliche alle Bereiche, wo elektrische, elektronische oder programmierbare elektronische (= softwarebasierte) Systeme eingesetzt werden, um gewisse Funktionen oder Funktionalitäten von technischen Geräten zu ermöglichen. Der diesbezügliche Stand der Technik wurde 1998 erstmals in dem generischen Standard IEC 61508 festgehalten. In diesem Standard wird ein Vorgehensmodell beschrieben, um Geräte so zu entwickeln und herzustellen, dass durch sie im Betrieb keine unverhältnismäßige Gefährdung für den Anwender oder die Umwelt ausgeht. In Anlehnung an die IEC 61508 zeigt Abbildung 2 den Zusammenhang, wie durch Risikominderung das Risiko, das von einem System ausgeht, über das tolerierbare Maß bis hin zu einem angestrebten Restrisiko reduziert werden kann. Diese Risikominderung kann entweder durch eigene sicherheitsbezogenen Maßnahmen realisiert werden oder von externen Einrichtungen ausgehen.

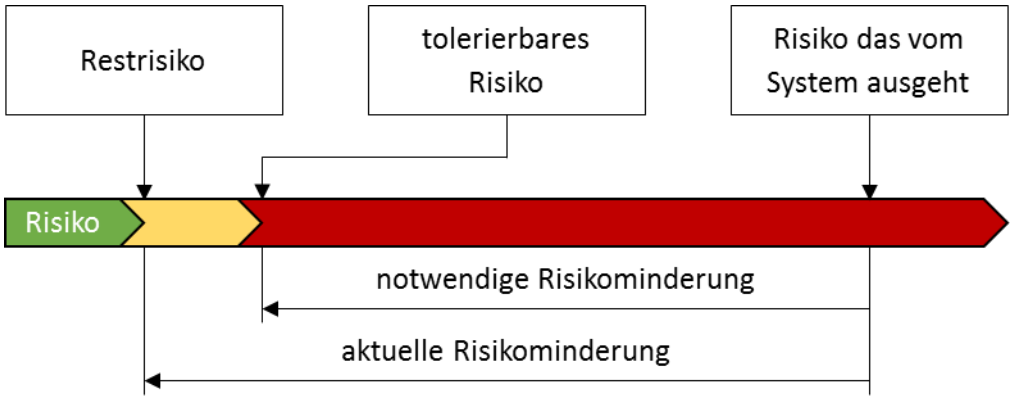


Abbildung 2: Risikominderung

Das tolerierbare Risiko kann dabei nicht grundsätzlich definiert werden, sondern hängt je nach Einsatzgebiet des Gerätes von unterschiedlichen Faktoren ab. Beispielsweise liegt bei kleineren Elektrogeräten der Fokus in erster Linie auf einer möglichen Gefährdung des Anwenders durch das System. Bei größeren Anlagen spielt aber auch die Gefährdung der Umwelt eine wesentliche Rolle. Dies ist vor allem für Geräte die in Kernkraftwerken oder einer ähnlichen Umgebung eingesetzt werden zutreffend. In jedem Fall gilt, dass die Reduktion der Gefährdung von Menschenleben oberste Priorität ist.

Ausgehend von führenden Automobilherstellern wurde seit 2003 an einer speziellen Adaption der IEC 61508 für den Automobilsektor gearbeitet, um der steigenden Anwendung und zunehmenden Komplexität von E/E-Systemen in Straßenfahrzeugen Rechnung zu tragen. In den Normungsgremien waren während der Erstellung des entsprechenden Standards viele Experten aus allen Teilbereichen der Fahrzeugtechnik involviert. Im November 2011 wurde die vorläufig gültige Version mit der Bezeichnung ISO 26262:2011 veröffentlicht.

Wie von Schmidt et al. beschrieben, steht beim branchenübergreifenden Standard IEC 61508 die konkrete Anlagensicherheit durch ein bestimmtes Kontrollsystem im Vordergrund. Die Minderung des Risikos beruht hier also auf bestimmten Sicherheitsfunktionen. Die ISO 26262 geht im Gegensatz dazu davon aus, dass die Fahrzeugsicherheit von dem Verhalten des Kontrollsystems selbst abhängig ist. Wesentliches Unterscheidungsmerkmal ist auch, dass die ISO 26262 gezielt auf die Massenproduktion von Fahrzeugen gerichtet ist. (Schmidt, Rau, Helmig, & Bauer, 2011, S. 1)

Die Norm bezieht sich dabei auf sicherheitsrelevante Systeme, die aus ein oder mehreren E/E-Systemen aufgebaut sind und in seriengefertigten Personenkraftwagen bis 3.500kg verwendet werden. Sonderanfertigungen und Prototypen, wie sie beispielsweise für Menschen mit Beeinträchtigungen hergestellt werden, sind von der Anwendung der Norm explizit ausgenommen. Des Weiteren stehen Fahrzeuge, deren Entwicklung zeitlich noch vor der Veröffentlichung des Standards begonnen hat, ebenfalls nicht im Fokus der Norm. (ISO 26262-1, 2011, S. 1) Allerdings muss in diesem Zusammenhang darauf hingewiesen werden, dass bereits Draft-Versionen

einer Norm praktische Relevanz haben und insofern keine zeitliche Abgrenzung gemacht werden kann.

In Anlehnung an die IEC 61508 wird die Kritikalität eines Systems in der ISO 26262 durch den sogenannten „Automotive Safety Integrity Level“ angegeben, der als ASIL abgekürzt wird. Dieser ASIL-Wert wird im Rahmen der Gefahren- und Risikoanalyse ermittelt. In diesem Zusammenhang gilt, je kritischer die Auswirkung einer möglichen Fehlfunktion eines Systems, desto höher ist auch der ASIL-Wert in Bezug auf diese entsprechende Fehlfunktion. Wie diese Bewertung zustande kommt und welche Einflussfaktoren es gibt wird in Kapitel 3.2.3 dieser Arbeit genauer beschrieben.

Straßenfahrzeuge gehören derzeit bereits zu den komplexesten Geräten auf die man im Alltag stoßen kann. Im Hinblick auf aktuelle Forschungsthemen im Automobilbereich (x-by-wire, car-2-x-communication, autonomes Fahren, etc.) wird diese Komplexität weiter zunehmen. In diesem Zusammenhang ist der in der Praxis bisher angewendete bauteilorientierte Entwicklungsansatz nicht mehr in der Lage, die Entwicklung solcher komplexen Systeme effizient umzusetzen.

Ein Schlüssel zur erfolgreichen Umsetzung stellt ein Umdenken hin zu einem funktionsorientierten Entwicklungsansatz dar. Dabei tritt die Frage danach, was ein Fahrzeug können soll beziehungsweise welche Funktionen ein Fahrzeug erfüllen muss, in den Vordergrund. Wie diese Fahrzeugfunktionen konkret umgesetzt und realisiert werden sollen, spielt am Anfang dieses funktionsorientierten Entwicklungsprozesses eine eher untergeordnete Rolle, um die Kreativität der Entwickler nicht negativ zu beeinflussen. Dadurch sind der Entwicklung innovativer Fahrzeugkonzepte grundsätzlich keine Grenzen gesetzt. Solche kundenerlebbaren Funktionen werden zunächst auf oberster Ebene und unabhängig von einer technischen Umsetzung festgelegt. Ein Vorteil der sich aus dieser Denkweise ergibt ist, dass es dadurch ermöglicht wird, diese Funktionen auch in unterschiedlichen Fahrzeugprojekten realisieren zu können (Kaiser, Augustin, & Baumann, 2013, S. 4). Wie von Björn Dietrich beschrieben, ist die Grundprämisse eines funktionsorientierten Entwicklungsansatzes die Abstimmung aller beteiligten Teams über ihre Entwicklungsaktivitäten. Dieser Grundgedanke findet sich in entsprechenden Vorgehensmodellen in vielen Bereichen der Technik wieder. (Dietrich, 2010, S. 83)

Das Vorgehensmodell gemäß dem funktionsorientierten Entwicklungsansatz ist in Abbildung 3 dargestellt.

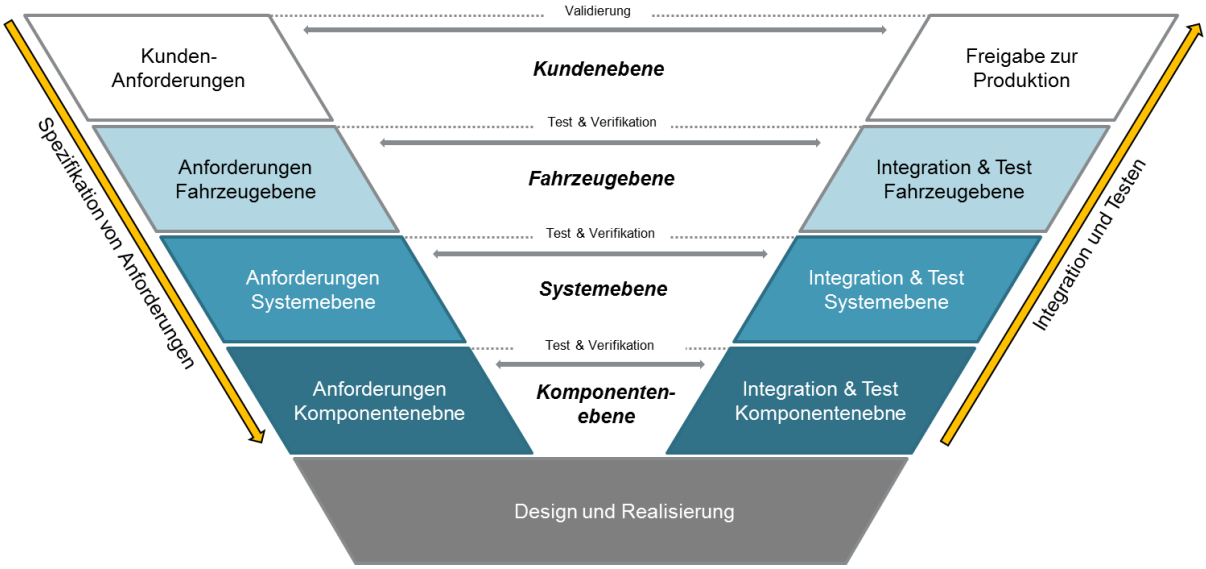


Abbildung 3: V-Modell in der Automobilbranche

Allgemein gilt, dass diese sogenannten V-Modelle aus einem absteigenden, sowie aus einem aufsteigenden Ast bestehen. Dies weist auf den Detaillierungsgrad der Entwicklung hin, wobei die einzelnen Ebenen im V-Modell über diesen Detaillierungsgrad Auskunft geben. Je tiefer die Ebene im V-Modell, desto detaillierter die Anforderung. Eine entsprechende Darstellung wird auch in der ISO 26262 angewendet und ist in Abbildung 4 ersichtlich. Auf dem absteigenden Ast wird ein System immer detaillierter ausgearbeitet bis die einzelnen Elemente des Systems bestimmt und entwickelt werden. Am aufsteigenden Ast werden diese Elemente wieder den zugehörigen Systemen zugeordnet und schlussendlich in das Fahrzeug integriert. Dadurch entsteht, vor allem für sicherheitsrelevante Funktionen die Notwendigkeit, alle Aktivitäten im Produktentstehungsprozess aufeinander abzustimmen. Neben dem Functional Safety Lifecycle, dem zentralen Vorgehensmodell der ISO 26262, sind zusätzliche Unterstützungsprozesse notwendig, die die Rahmenbedingungen einer erfolgreichen funktionalen Entwicklung darstellen. Diese Unterstützungsprozesse umfassen beispielsweise das Anforderungsmanagement, Konfigurationsmanagement, Change Management sowie die Dokumentation der notwendigen Unterlagen. Demzufolge kommt dem Management der funktionalen Sicherheit (Kapitel 2 der Norm), sowie den beteiligten Unterstützungsprozessen (Kapitel 8 der Norm) in der Praxis eine wesentliche Bedeutung zu.

## 3.1 Funktionale Sicherheit für Straßenfahrzeuge - ISO 26262

Nachdem die Thematik der Funktionalen Sicherheit allgemein beschrieben wurde, wird nun konkret auf die Anwendung im Automobilbereich eingegangen. Zu diesem Zweck wird einleitend ein kurzer Überblick über den Aufbau der ISO 26262 und die Inhalte des Functional Safety Lifecycle gegeben. Außerdem werden einige grundsätzliche Merkmale der Norm, rechtliche Aspekte und in diesem Zusammenhang wichtige Begriffe genauer beschrieben.

### 3.1.1 Aufbau der Norm

Die Norm ist in übergeordnete Kapitel und dazu gehörende Abschnitte eingeteilt. Diese Gliederung ist in Abbildung 4 dargestellt. An dieser Stelle wird auch noch einmal auf die schattierten „Vs“ hingewiesen, welche das Vorgehensmodell in den einzelnen Kapiteln der Produktentwicklung auf System-, Hard- und Softwareebene kennzeichnen.

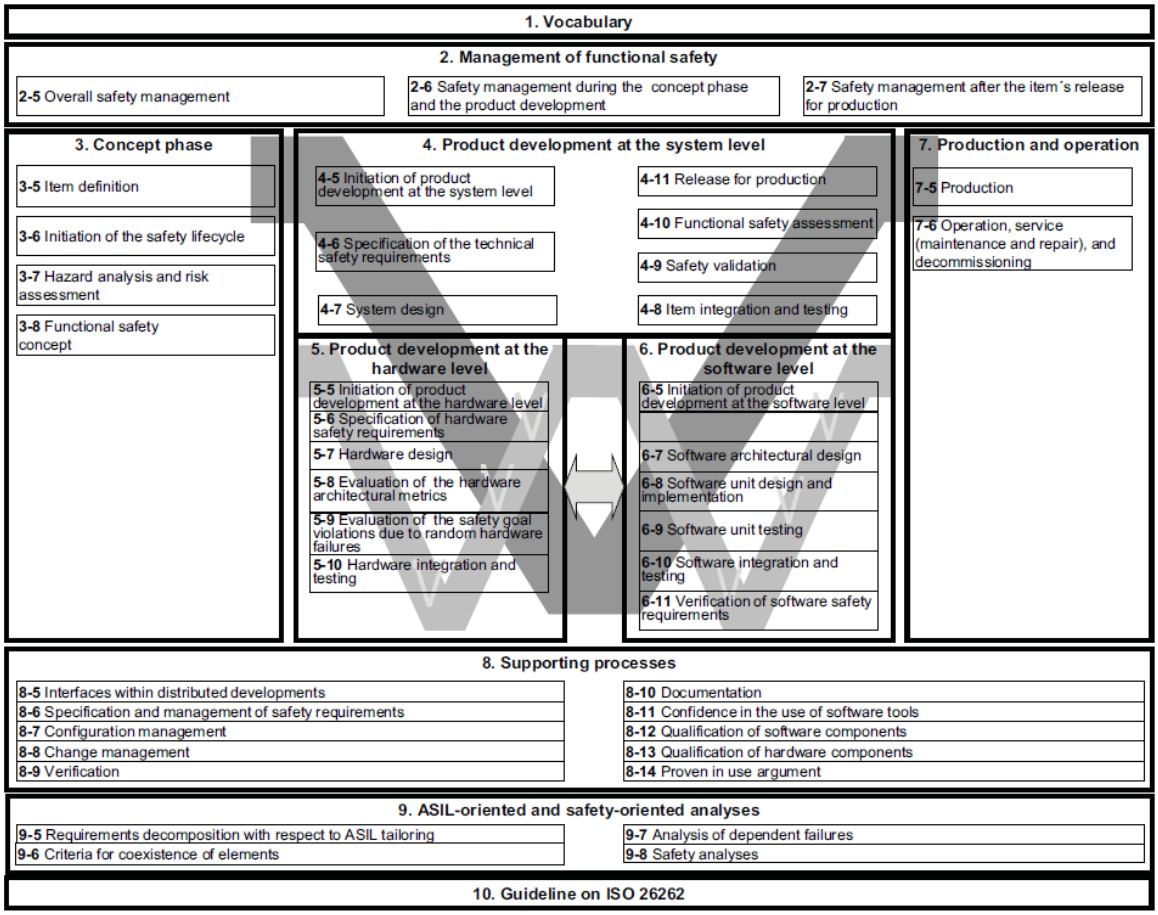


Abbildung 4: Übersicht der ISO 26262 (Quelle: ISO 26262)

Die ISO 26262 besteht aus insgesamt 10 Kapiteln (ISO 26262-1, 2011, S. 4):

- Part 1: Vocabulary
- Part 2: Management of functional safety
- Part 3: Concept phase
- Part 4: Product development at the system level
- Part 5: Product development at the hardware level
- Part 6: Product development at the software level
- Part 7: Production and operation
- Part 8: Supporting processes
- Part 9: Automotive Safety Integrity Level- and safety-oriented analyses
- Part 10: Guideline on ISO 26262 (informative)

In Kapitel 1 der Norm werden alle Begriffe und Abkürzungen erläutert, die im Zusammenhang mit der Norm verwendet werden. Das zweite Kapitel umfasst einige Grundlagen des Managements der Funktionalen Sicherheit. In diesem Kapitel werden Maßnahmen beschrieben die während der Konzeptphase und der konkreten Produktentwicklung getroffen werden müssen, um eine effiziente Anwendung des Functional Safety Lifecycles zu gewährleisten. Außerdem werden hier auch notwendige Maßnahmen im Zusammenhang mit dem Management der Funktionalen Sicherheit, das nach der Freigabe zur Produktion durchgeführt werden soll, genauer erläutert. Der bereits erwähnte Functional Safety Lifecycle verteilt sich auf die Kapitel 3 bis 7 und umfasst folgende Bereiche des Produktlebenszyklus: die Konzeptphase, die Produktentwicklung auf System-, Hard- und Softwareebene, sowie die Produktion und den Einsatz des Produktes selbst. Kapitel 8 der Norm fasst einige notwendige Unterstützungsprozesse wie zum Beispiel das Konfigurationsmanagement, das Change Management oder Anforderungen an die Dokumentation von Arbeitsergebnissen zusammen. Kapitel 9 gibt einen Überblick über sicherheitsorientierte Analysemethoden. Das abschließende Kapitel 10 liefert eine Guideline hinsichtlich der Anwendung der Norm und stellt den informativen Teil dar.

### 3.1.2 Sicherheitslebenszyklus

Wie bereits erwähnt, wird der Sicherheitslebenszyklus der ISO 26262 auch als Functional Safety Lifecycle bezeichnet. Er beschreibt eine Vorgehensweise und Struktur wie bei der Entwicklung und Produktion in Bezug auf die Funktionale Sicherheit vorgegangen werden soll. Auf den Functional Safety Lifecycle wird in Kapitel 3.2 dieser Arbeit genauer eingegangen.

### 3.1.3 Merkmale

Die Norm fordert, egal ob es sich um einen OEM oder Zulieferer handelt, eine grundsätzliche Systematik bei der Entwicklung und Produktion von Fahrzeugen oder einzelnen Komponenten einzuhalten. Ziel ist es dabei nicht, möglichst neue oder andere Vorgehensweisen einzusetzen, sondern die in der Praxis bewährten Maßnahmen zur Sicherstellung von funktional sicheren Geräten auf allen Ebenen der Produktentwicklung (System, Hard- und Softwareebene) zu etablieren. Diese Systematik stellt aber keine grundsätzliche Einschränkung auf nur sicherheitsrelevante Produkte dar, sondern kann auch bei nicht-sicherheitskritischen Produkten angewendet werden.

Eine wesentliche Anforderung der Norm ist die Überprüfung von Dokumenten, die im Laufe des Produktlebenszyklus erstellt wurden. Wie bereits eingangs erwähnt, werden solche Dokumente in der Norm als Work Products bezeichnet. Die Dokumentation reicht von der Planung der einzelnen Sicherheitsaktivitäten in einem „Safety Plan“, über die Durchführung einer Gefahren- und Risikoanalyse in Form einer „Hazard analysis and risk assessment“ bis hin zu einer Sammlung von Argumenten für die Erreichung eines funktional sicheren Produktes in einem „Safety Case“. Je nach Relevanz und Auswirkung auf die weiteren Schritte des Sicherheitslebenszyklus, müssen einige dieser Work Products eben, normativ gefordert, überprüft werden. Diese Überprüfungen werden, unter anderem, im Rahmen von „Verification-Reviews“ und „Confirmation measures“ durchgeführt. Je nach Kritikalität eines Systems muss dies teilweise mit einer notwendigen Unabhängigkeit des Begutachters erfolgen. Die Ergebnisse solcher Begutachtungen werden in Reports zusammengefasst und dokumentiert. Da diese Überprüfungen einen zentralen Bestandteil der Norm darstellen und während aller Phasen des Sicherheitslebenszyklus durchgeführt

werden müssen, wird nun auf die genaue Bedeutung und die jeweiligen Unterschiede dieser Überprüfungsaktivitäten genauer eingegangen.

### 3.1.4 Confirmation measures

Die Confirmation measures dienen der Beurteilung, ob ein System grundsätzlich als funktional sicher gilt oder nicht. Dies erfordert unter anderem (ISO 26262-10, 2011, S. 13):

- Die angemessene Definition, Adaptierung und Ausführung der notwendigen Sicherheitsaktivitäten während des Sicherheitslebenszyklus.
- Die richtigen Inhalte der Work Products in Bezug auf die jeweiligen Anforderungen nach ISO 26262.

In Bezug auf die Confirmation measures werden das Review, das Audit der Funktionalen Sicherheit sowie das Assessment der Funktionalen Sicherheit unterschieden. Allgemein gilt, dass die jeweilige Überprüfungsaktivität von einer fachkundigen Person mit einer ausreichenden Unabhängigkeit vom Entwicklungsteam durchgeführt werden muss. Der Grad der Unabhängigkeit richtet sich dabei nach der Kritikalität die von einem System ausgeht die, wie eingangs erwähnt, durch den ASIL-Wert angegeben wird.

Die notwendige Unabhängigkeit der überprüfenden Person ist nun von der höchsten ASIL-Einstufung einer Fehlfunktion des Systems abhängig. Einen Übersicht über die normativ geforderten Confirmation measures, sowie die jeweils notwendige Unabhängigkeit der Person welche die Überprüfung durchführt, liefert Abbildung 5.

| Confirmation measures | Degree of independency[a] applies to ASIL | | | | Scope |
|---|---|---|---|---|---|
| | A | B | C | D | |
| Confirmation review of the hazard analysis and risk assessment of the item (see ISO 26262-3:2011, Clauses 5 and 7, and, if applicable, ISO 26262-8:2011, Clause 5)<br>Independence with regard to the developers of the item, project management and the authors of the work product | I3 | I3 | I3 | I3 | The scope of this review shall include the correctness of the determined ASILs and quality management (QM) ratings of the identified hazardous events for the item, and a review of the safety goals |
| Confirmation review of the safety plan (see 6.5.1)<br>Independence with regard to the developers of the item, project management and the authors of the work product | — | I1 | I2 | I3 | Applies to the highest ASIL among the safety goals of the item |
| Confirmation review of the item integration and testing plan (see ISO 26262-4)<br>Independence with regard to the developers of the item, project management and the authors of the work product | I0 | I1 | I2 | I2 | Applies to the highest ASIL among the safety goals of the item |
| Confirmation review of the validation plan (see ISO 26262-4)<br>Independence with regard to the developers of the item, project management and the authors of the work product | I0 | I1 | I2 | I2 | Applies to the highest ASIL among the safety goals of the item |
| Confirmation review of the safety analyses (see ISO 26262-9:2011, Clause 8)<br>Independence with regard to the developers of the item, project management and the authors of the work products | I1 | I1 | I2 | I3 | Applies to the highest ASIL among the safety goals of the item |
| Confirmation review of the software tool criteria evaluation report and the software tool qualification report[b] (see ISO 26262-8:2011, Clause 11)<br>Independence with regard to the persons performing the qualification of the software tool | — | I0 | I1 | I1 | Applies to the highest ASIL of the requirements that can be violated by the use of the tool |
| Confirmation review of the proven in use arguments (analysis, data and credit), of the candidates (see ISO 26262-8:2011, Clause 14)<br>Independence with regard to the author of the argument | I0 | I1 | I2 | I3 | Applies to the ASIL of the safety goal or requirement related to the considered behaviour, or function, of the candidate |
| Confirmation review of the completeness of the safety case (see 6.5.3)<br>Independence with regard to the authors of the safety case | I0 | I1 | I2 | I3 | Applies to the highest ASIL among the safety goals of the item |
| Functional safety audit in accordance with 6.4.8<br>Independence with regard to the developers of the item and project management | — | I0 | I2 | I3 | Applies to the highest ASIL among the safety goals of the item |
| Functional safety assessment in accordance with 6.4.9<br>Independence with regard to the developers of the item and project management | — | I0 | I2 | I3 | Applies to the highest ASIL among the safety goals of the item |

[a] The notations are defined as follows:
- —: no requirement and no recommendation for or against regarding this confirmation measure;
- I0: the confirmation measure should be performed; however, if the confirmation measure is performed, it shall be performed by a different person;
- I1: the confirmation measure shall be performed, by a different person;
- I2: the confirmation measure shall be performed, by a person from a different team, i.e. not reporting to the same direct superior;
- I3: the confirmation measure shall be performed, by a person from a different department or organization, i.e. independent from the department responsible for the considered work product(s) regarding management, resources and release authority.

[b] A software tool development is outside the item's safety lifecycle whereas the qualification of such a tool is an activity of the safety lifecycle.

Abbildung 5: Übersicht der „Confirmation measures“ (Quelle: ISO 26262)

Die vorige Übersicht umfasst alle normativ geforderten Confirmation measures. Falls manche dieser Überprüfungsaktivitäten berechtigterweise nicht durchgeführt werden müssen, muss eine Begründung dafür im Safety Plan vermerkt werden. Im Folgenden werden die einzelnen Confirmation measures näher beschrieben.

#### 3.1.4.1 Confirmation review

Bei einem Confirmation-Review geht es darum, den Nachweis zu erbringen, dass ein bestimmtes Work Product den jeweiligen Anforderungen der ISO 26262 entspricht. Diese Art von Review umfasst dabei die Überprüfung der Korrektheit hinsichtlich Formvorschriften, Inhalt, Angemessenheit und Vollständigkeit in Bezug auf die Anforderungen der Norm. Hierbei wird genauer zwischen allgemeinen und spezifischen Anforderungen unterschieden. Allgemeine Anforderungen betreffen Richtlinien zum grundsätzlichen Aufbau von Dokumenten. Dies umfasst beispielsweise die Beschreibung des Zweckes eines Dokumentes, die durchgehende Versionsverwaltung, die Dokumentation von fortlaufenden Änderungen in einer Historie oder ähnliches. Die spezifischen Anforderungen sind vom jeweiligen Work Product abhängig.

#### 3.1.4.2 Functional safety audit

Bezogen auf die ISO 26262 überprüft das Audit der Funktionalen Sicherheit die implementierten Prozesse, die notwendig sind, um die einzelnen Aktivitäten des Sicherheitslebenszyklus durchzuführen. Ein solches Audit wird normativ dann gefordert, wenn eine Fehlfunktion im Rahmen der Gefahren- und Risikoanalyse mit ASIL B, ASIL C oder D bewertet wurde.

#### 3.1.4.3 Functional safety assessment

Wurde eine Fehlfunktion eines Items mit ASIL B, ASIL C oder D bewertet, sieht die Norm außerdem die Durchführung eines „Functional safety assessement“ vor. Ein solches Assessment beinhaltet folgende Punkte (ISO 26262-10, 2011, S. 13):

- Eine Überprüfung der Angemessenheit und der Effektivität der Sicherheitsmaßnahmen, die während der Item-Entwicklung durchgeführt wurden.

- Confirmation-Reviews der vom jeweiligen Safety Plan geforderten Work Products, hinsichtlich der normgerechten Erstellung und der spezifischen Anforderungen der ISO 26262.
- Ein oder mehrere Audits der Funktionalen Sicherheit um die Implementierung der notwendigen Prozesse zu überprüfen.

Für den Fall, dass es nachträglich zu Änderungen des Items kommt, ist vorgesehen, dass ein Assessment der Funktionalen Sicherheit auch wiederholt oder aktualisiert werden kann. Wenn der höchste ASIL aller Fehlfunktionen eines Items mit A bewertet wurde, muss kein eigenes Assessment durchgeführt werden, allerdings sind auch weiterhin die in diesem Fall geforderten Überprüfungsaktivitäten durchzuführen.

### 3.1.5 Verification-Reviews

Die Verifikation von Work Products in Bezug auf die Funktionale Sicherheit kann grundsätzlich folgende Punkte umfassen (ISO 26262-10, 2011, S. 13):

- Verification-Reviews um die Spezifikation oder Implementierung von abgeleiteten Sicherheitsanforderungen aus übergeordneten Sicherheitsanforderungen hinsichtlich der Vollständigkeit und Richtigkeit zu überprüfen.
- Die Ausführung von Testfällen oder die Erhebung von Testergebnissen um den Nachweis der Erfüllung von Sicherheitsanforderungen zu erbringen.

Die Verification-Reviews dienen dementsprechend der Überprüfung hinsichtlich der Vollständigkeit und korrekten Spezifikation oder Implementierung von Sicherheitsanforderungen in den einzelnen Work Products. Abbildung 6 liefert eine Übersicht der normativ geforderten Verification-Reviews.

| Verification review subject | Highest ASIL among the safety goals of the item | | | | Clause in which required or recommended |
|---|---|---|---|---|---|
| | A | B | C | D | |
| Hazard analysis and risk assessment of the item (see ISO 26262-3:2011, Clauses 5 and 7, and, if applicable, ISO 26262-8:2011, Clause 5) | required[a] | | | | ISO 26262-3:2011, Clause 7 |
| Safety goals | required | | | | ISO 26262-3:2011, Clause 7 |
| Functional safety concept | required | | | | ISO 26262-3:2011, Clause 8 |
| Technical safety requirements specification | required | | | | ISO 26262-4:2011, Clause 6 |
| System design | required | | | | ISO 26262-4:2011, Clause 7 |
| Hardware safety requirements | required | | | | ISO 26262-5:2011, Clause 6 |
| Hardware design | required | | | | ISO 26262-5:2011, Clause 7 |
| Results of the applied methods with regard to the evaluation of the hardware architectural metrics | b | recommended | required | required | ISO 26262-5:2011, Clause 8 |
| Analysis of the potential safety goal violations due to random hardware failures, considering the applied evaluation method | b | recommended | required | required | ISO 26262-5:2011, Clause 9 |
| Software safety requirements and the refined hardware-software interface requirements | required | | | | ISO 26262-6:2011, Clauses 6 and 11 |
| Software architectural design | required | | | | ISO 26262-6:2011, Clause 7 |
| Software unit design and implementation | required | | | | ISO 26262-6:2011, Clause 8 |
| Software component qualification report | required for the qualified software components | | | | ISO 26262-8:2011, Clause 12 |
| Hardware component qualification report | required for the qualified hardware components | | | | ISO 26262-8:2011, Clause 13 |
| Safety analyses | required | | | | ISO 26262-9:2011, Clause 8 |

[a] The scope of this review also includes hazardous events rated as QM.

[b] No requirement and no recommendation for or against.

Abbildung 6: Übersicht der „Verification-Reviews“ (Quelle: ISO 26262)

In Bezug auf die Verification-Reviews gilt das Vier-Augen-Prinzip, sodass das Review von einer fachkundigen Person durchzuführen ist, die nicht dem Autor des eigentlichen Dokumentes entspricht.

### 3.1.6 Rechtliche Aspekte

Bei der ISO 26262 handelt es sich nicht um ein bindendes Gesetz, sondern um den aktuellen Stand der Wissenschaft und Technik auf dem Gebiet der Entwicklung und Produktion von Straßenfahrzeugen. Demensprechend ist es denkbar, dass auch ohne explizite Anwendung des Vorgehensmodells der Norm ein gleichwertiges Sicherheitsniveau eines Produktes erreicht werden kann.

Wie jedoch von Schmidt et al. beschrieben wird, bestimmt die Umsetzung der Anforderungen der Norm allerdings wesentlich die zivilrechtliche und strafrechtliche Verantwortlichkeit der Hersteller sicherheitsrelevanter Systeme, insbesondere die von Fahrzeugherstellern (Schmidt, Rau, Helmig, & Bauer, 2011, S. 2). Die einheitliche Meinung von Experten legt also die Anwendung der Norm dringend nahe. Vor allem bei der Entwicklung und Fertigung von verteilten Systemen, an der teilweise eine größere Kette von Zuliefern beteiligt ist, spielt die Trennung der einzelnen Aufgaben und Verantwortungen eine wichtige Rolle. Dies wird beispielsweise in der normativ geforderten Leistungsschnittstellenvereinbarung („Development interface agreement“) klar geregelt. Außerdem kann im Falle eines Rechtsstreites durch die Überprüfungsaktivitäten und die teilweise notwendige Unabhängigkeit des Bestätigungsvermerks eine Vorgehensweise dem Stand der Technik entsprechend nachgewiesen werden. Dieser Nachweis wird ohne Anwendung der Norm nur schwer möglich sein und kann unter Umständen zu ungeklärten Haftungen der einzelnen Zulieferfirmen führen.

Die Frage der Haftung stellt sich vor allem dann, wenn es wirklich zu einem Verstoß im Sinne der Produkthaftung kommen sollte. So ein Fall würde beispielsweise dann eintreten, wenn die Ursache für einen Unfall auf eine Fehlfunktion eines Fahrzeuges zurückzuführen ist und aus diesem Grund der Hersteller des Produktes für die entstandenen Schäden haftet. In diesem Zusammenhang kann es unter Umständen auch zu einer persönlichen Haftung kommen. Nachdem die Entwicklung von Straßenfahrzeugen nicht von Einzelpersonen alleine bewerkstelligt werden kann, wird eine Zusammenarbeit von Experten einzelner Fachbereiche immer notwendig sein. Dies stellt auch sicher, dass eine Entwicklung unter der Aufsicht fachkundiger Personen stattfindet. Aus diesem Grund sollten alle erforderlichen Dokumente und Freigaben auch von allen involvierten Entscheidungsträgern unterzeichnet werden, um eine mögliche persönliche Haftung auf die verantwortlichen Personen aufzuteilen. Eine weitere denkbare Variante ist, dass die Verantwortlichen, respektive der Manager der Funktionalen Sicherheit, nur eine Empfehlung zur Freigabe aussprechen und dem Geschäftsführer zur Unterschrift vorlegen. Auf diese Weise können die Beteiligten teilweise geschützt werden, außer es kann grob fahrlässiges Verhalten vorgeworfen werden.

### 3.1.7 Wichtige Begriffe

In diesem Abschnitt werden einige wichtige Begriffe der Funktionalen Sicherheit erwähnt und deren Bedeutung kompakt zusammengefasst. Aufgrund der Vielzahl an Begriffen die im Zusammenhang mit der Norm vorkommen, wurde bei dieser Auswahl auf solche Rücksicht genommen, die für die erstellten Templates relevant sind.

#### 3.1.7.1 Item

Im Kontext der ISO 26262 wird ein System oder eine gemeinsame Anordnung von mehreren Systemen, die eine Funktion auf Fahrzeugebene ermöglichen, als Item bezeichnet (ISO 26262-1, 2011, S. 16). Die funktionalen und nicht-funktionalen Anforderungen die ein Item erfüllen soll, werden in der sogenannten Item Definition festgelegt. Darauf wird in Kapitel 3.2.1 genauer eingegangen.

#### 3.1.7.2 System

Ein System setzt sich aus einzelnen Elementen zusammen. Es verbindet zumindest einen Sensor, einen Controller und einen Aktuator miteinander, wobei der Sensor und der Aktuator auch außerhalb des betrachteten Systems angeordnet sein können (ISO 26262-1, 2011, S. 23). Aus welchen Elementen ein Item also grundsätzlich aufgebaut sein kann, ist in Abbildung 7 dargestellt.

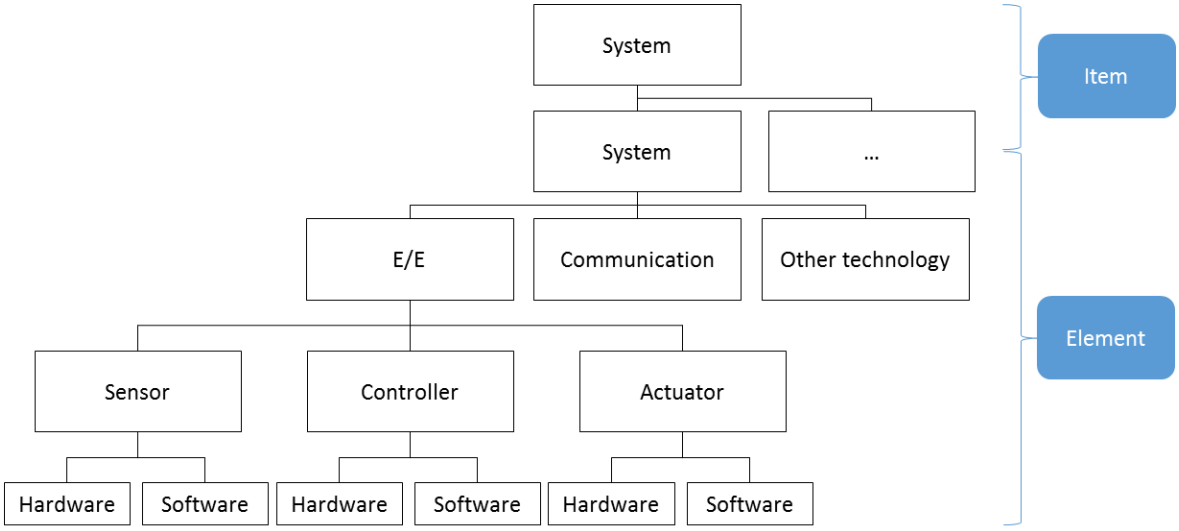


Abbildung 7: Unterteilung eines Items

Ein Element kann wiederum ein System, ein Teil eines Systems, eine einzelne Komponente, eine Hardware- oder eine Softwareeinheit bedeuten.

### 3.1.7.3 Fehlertoleranzzeit

In der Funktionalen Sicherheit werden einige Begriffe verwendet, die eine zeitliche Unterteilung der Phasen vom normalen Betrieb bis hin zum Auftreten einer Gefahr für den Anwender eines Systems ermöglichen. Diese zeitliche Einteilung ist in Anlehnung an die ISO 26262 in Abbildung 8 dargestellt.

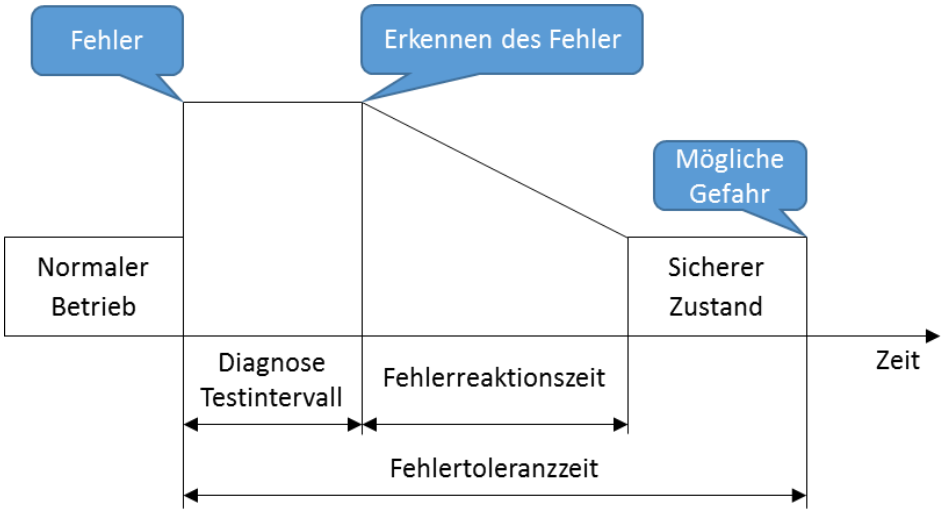


Abbildung 8: Fehlertoleranzzeit und Fehlerreaktionszeit

Die Fehlertoleranzzeit bezeichnet die Dauer vom Eintreten eines Fehlers bis zu dem Zeitpunkt, zu dem eine mögliche Gefährdung besteht. Die Fehlertoleranzzeit wird gemäß der englischen Übersetzung auch als FTTI abgekürzt. Sie wird bereits während der Gefahren- und Risikoanalyse für eine Gefahrensituation festgelegt und ist dementsprechend ein Teil eines Sicherheitszieles. Das Diagnose-Testintervall beschreibt die Dauer vom Eintreten eines Fehlers bis zum Erkennen des Fehlers. Die Fehlerreaktionszeit ist die Zeitspanne, vom Erkennen eines Fehlers bis zum Erreichen des sicheren Zustandes eines System. Der sichere Zustand hängt dabei vom jeweiligen System ab und wird im Zuge der Gefahren- und Risikoanalyse ebenfalls als Teil eines Sicherheitszieles definiert. Die beschriebenen Zeiten wirken sich dabei in wesentlichem Maße auf die Architektur des sicherheitsrelevanten Systems aus.

### 3.1.7.4 Störung, Fehler und Ausfall

Die Ursachen für den Ausfall eines Systems sind hierarchisch gegliedert. Eine Störung (fault) kann zu einem Fehler (error) führen, der wiederum den Ausfall (failure) eines Systems bedeuten kann. Dies ist überblicksweise in Abbildung 9 dargestellt. Das Beispiel in dieser Abbildung ist an die ISO 26262 angelehnt. Ein Fehler führt allerdings noch nicht zwangsläufig dazu, dass auch eine Gefahr für den Anwender besteht. Erst wenn es zu einem Fehler und dadurch zu einem Ausfall eines Systems während einer Gefahrensituation kommt, besteht ein Risiko für den Anwender. Damit dieses Risiko reduziert werden kann, muss vor Eintreten der Gefahrensituation ein sicherer Zustand des Systems erreicht werden. Eine zentrale Aufgabe der Funktionalen Sicherheit ist es also, schon beim Auftreten von Fehlern einen sicheren Zustand herbeizuführen, beziehungsweise den sicheren Zustand beizubehalten.

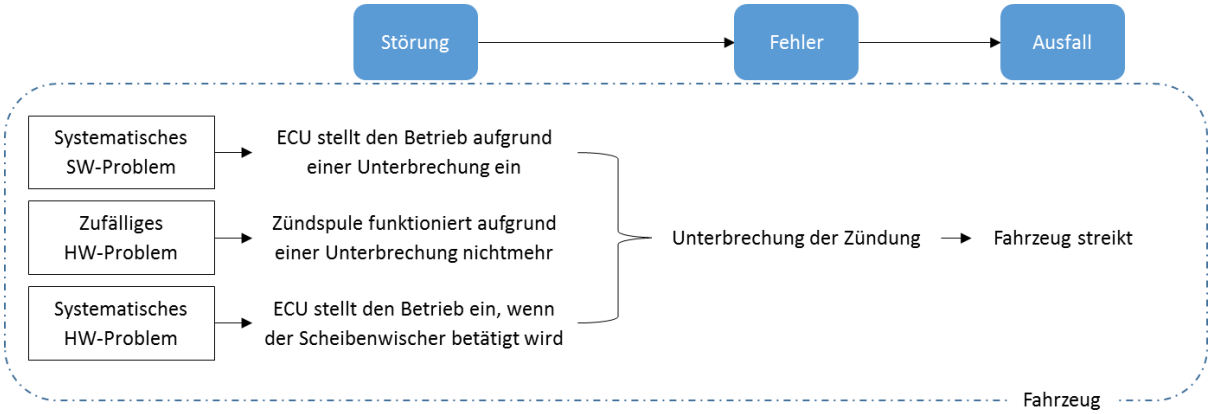


Abbildung 9: Zusammenhang Störung - Fehler - Ausfall

Folgende Ursachen für eine Störung, einen Fehler oder einen Ausfall können unterschieden werden: Systematische Softwareprobleme, zufällige Hardwareprobleme und systematische Hardwareprobleme. Systematische Probleme werden wesentlich vom Design und der Spezifikation eines Systems beeinflusst. Zufällige Hardwareprobleme sind physikalischen Ursprungs und können beispielsweise durch Korrosion, Abnützung oder Ähnliches hervorgerufen werden. Wie in Abbildung 9 dargestellt, kann die gleiche Ausfallwirkung unter Umständen auch auf unterschiedliche Störungen zurückgeführt werden.

#### 3.1.7.5 Sicherer Zustand

Wie in Abbildung 8 ersichtlich, muss das System beim Auftreten eines Fehlers während einer Gefahrensituation in einen sicheren Zustand übergehen. Dieser sichere Zustand ist davon abhängig, welche Funktionen das System im normalen Betrieb ausführt. Bei manchen Systemen kann es reichen, das System abzuschalten und die Funktionsfähigkeit einzuschränken (z.B. Power steering). Bei anderen Systemen wird ein sicherer Zustand durch ein Abschalten, beziehungsweise Einschränken der Funktionsfähigkeit nicht erreicht werden können (z.B. Steer-by-wire). In diesem Fall muss die Funktionsfähigkeit, zumindest kurzfristig bis die Gefahrensituation vorbei ist, weiter aufrechterhalten werden können. Redundante Systeme, beziehungsweise fehlertolerante Systeme können in diesem Zusammenhang Abhilfe schaffen.

#### 3.1.7.6 Sicherheitsziele

Die Sicherheitsziele, oder auch „Safety Goals“, bezeichnen in der Funktionalen Sicherheit die oberste Sicherheitsanforderung in Bezug auf ein Item. Die Formulierung der Sicherheitsziele wird im Rahmen der Gefahren- und Risikoanalyse durchgeführt . Ein Sicherheitsziel beinhaltet unter anderem den sicheren Zustand, die FTTI und andere physikalische Beschreibungen (z.B. die maximal gewünschte Beschleunigung) die zur ASIL-Einstufung benötigt werden. Im Laufe der Entwicklung werden auf den einzelnen Ebenen des V-Modells aus den obersten Sicherheitszielen immer detaillierte Sicherheitsanforderungen abgeleitet. Diese umfassen:

- Sicherheitsziele
- Funktionale Sicherheitsanforderungen
- Technische Sicherheitsanforderungen
- Sicherheitsanforderungen auf Hard- und Softwareebene

Da die korrekte Spezifikation und Formulierung dieser Sicherheitsanforderungen in der Praxis einen wichtigen Beitrag bei der Entwicklung darstellt, wird darauf in Kapitel 6.2.5 und 6.2.6 dieser Arbeit genauer eingegangen.

#### 3.1.7.7 Fehlermöglichkeits- und -einflussanalyse

Die Fehlermöglichkeits- und -einflussanalyse ist eine Methode zur Optimierung von Systemen, beziehungsweise zur Minimierung von Risiken in Bezug auf Produkte und Prozesse und wird auch als FMEA abgekürzt. Sie stellt keine spezifische Anforderung der ISO 26262 dar, sondern ist ein in der Praxis vielfach eingesetztes Verfahren um bereits frühzeitig mögliche Fehler in Systemen erkennen zu können. In Anlehnung an Wolfgang Danzer kann die FMEA dabei folgende Prozesse unterstützen (2016, S. 94):

- Die Absicherung von Funktionsanforderungen
- Die Minimierung von Gewährleistungs- und Kulanzkosten
- Die Nachweisführung zur Entlastung im Produkthaftungsfall
- Den Wissensaufbau im Unternehmen

Diese Analysemethode kann dabei präventiv bereits in einer frühen Phase der Entwicklung durchgeführt werden, um so früh wie möglich potenzielle Fehler von vornherein ausschließen zu können und die Zuverlässigkeit von Produkten zu verbessern. Die frühe Anwendung ist auch vor allem darauf zurückzuführen, dass die Korrektur von Fehlern im weiteren Verlauf der Entwicklung immer kostenintensiver wird. Im Kontext der Funktionalen Sicherheit kann die FMEA zur Identifikation möglicher Gefahrensituationen eingesetzt werden und kann diesbezüglich als Überprüfungsmöglichkeit der Gefahren- und Risikoanalyse gesehen werden. Auf die Gefahren- und Risikoanalyse wird im weiteren Verlauf dieser Arbeit noch genauer eingegangen.

#### 3.1.7.8 Fehlerbaumanalyse

Eine weitere Methode, um mögliche Fehler in Bezug auf ein System zu analysieren, ist die Fehlerbaumanalyse. Sie wird gemäß ihrer englischen Abkürzung in der Praxis auch als FTA bezeichnet. Bei der FTA wird zuerst ein ungewolltes Verhalten eines Systems beschrieben und dann Schritt für Schritt mögliche Ursachen analysiert. Dementsprechend ist die FTA eine Analysemethode bei der deduktiv vorgegangen wird. Ein Fehlerbaum kann zuerst qualitativ und in weiterer Folge auch quantitativ ausgeführt sein. Ein quantitativer Fehlerbaum ermöglicht es, die Wahrscheinlichkeit des Eintretens von gewissen Ereignissen rechnerisch zu ermitteln.

#### 3.1.7.9 Safety Manager

Dem „Safety Manager“ obliegt, je nach der organisatorischen Gliederung im Unternehmen, die Verantwortung aller sicherheitsrelevanten Tätigkeiten, die entweder projektunabhängig oder –spezifisch sein können. In Anlehnung an Philip Stirgwolt vereint ein Safety Manager mehrere Funktionen und erfüllt dabei folgende Aufgaben (Stirgwolt, 2013, S. 4):

- „Tailoring“ der Produktentwicklung gemäß den Anforderungen des Items
  (vgl. „Quality Manager“)
- Erstellung eines Safety Plan für den gesamten Sicherheitslebenszyklus
  (vgl. „Project Manager“)
- Verwaltung des Safety Plans während des Sicherheitslebenszyklus
  (vgl. „Configuration Manager“)
- Im Zuge des Assessment Plans der Funktionalen Sicherheit, die Überprüfung, ob die durchgeführten Arbeiten auch mit den freigegebenen Prozessen übereinstimmen
  (vgl. Auditor)
- Erstellung des Safety Case, der die Konformität von Prozess- und Produktmerkmalen nachvollziehbar darstellt
  (vgl. „Requirement Manager“)

Die Norm legt dabei nicht fest, ob diese Aufgaben direkt vom Projektleiter, von einem eigenen Safety Manager oder in Zusammenarbeit von mehreren Personen erledigt werden. Dies kann je nach Umfang eines Entwicklungsprojektes unterschiedlich sein. In jedem Fall spielt das Management der Funktionalen Sicherheit eine zentrale Rolle bei der Planung und Bereitstellung von notwendigen Ressourcen, um sicherheitsgerechte Entwicklungen zu ermöglichen.

#### 3.1.7.10 Leistungsschnittstellenvereinbarung

Die Leistungsschnittstellenvereinbarung, auch als „Development Interface Agreement“ (DIA) bezeichnet, stellt eine Vereinbarung zwischen dem Auftraggeber und Auftragnehmer dar, in der die Verantwortlichkeiten über die einzelnen Aktivitäten, Nachweise oder Work Products festgehalten werden (ISO 26262-1, 2011, S. 11).

#### 3.1.7.11 Safety Plan

Die Planung, Terminierung und Verfolgung der sicherheitsrelevanten Aktivitäten in Bezug auf ein Item stellt in der Praxis eine der wichtigsten Managementaufgaben der Funktionalen Sicherheit dar. Diese Planung wird in einem sogenannten „Safety Plan“ festgehalten. Je nach Umfang des Items ist es möglich, dass dieser Plan entweder direkt in einem übergreifenden Projektplan integriert ist, oder ein eigenes Dokument darstellt. Folgender Auszug umfasst einige Anforderungen, die an einen Safety Plan gestellt werden (ISO 26262-2, 2011, S. 17f):

- Die Planung der Aktivitäten und Abläufe, um Funktionale Sicherheit zu erreichen
- Die Umsetzung von projektunabhängigen Sicherheitsaktivitäten in das projektspezifische Safety Management
- Falls erforderlich, die Definition aller angepassten Sicherheitsaktivitäten
- Die Planung der Gefahren- und Risikoanalyse
- Die Planung der Entwicklungsaktivitäten, inklusive der Entwicklung und Implementierung des Funktionalen Sicherheitskonzeptes, sowie die Produktentwicklung auf System-, Hardware- und Softwareebene
- Die Planung der Leistungsschnittstellenvereinbarung
- Die Planung der Reviews, sowie die Initiierung von Audits und Assessments der Funktionalen Sicherheit

Die Planung einer Sicherheitsaktivität soll außerdem folgende Punkte umfassen (ISO 26262-2, 2011, S. 18):

- Die Zielsetzung der Sicherheitsaktivität
- Die Abhängigkeiten von anderen Aktivitäten oder Informationen
- Die Ressourcen, die für die Durchführung verantwortlich ist
- Die Ressourcen, die für die Durchführung der Aktivität notwendig sind
- Den Beginn und die Dauer der Aktivität
- Identifizierung des mit der Aktivität in Zusammenhang stehenden Work Products

#### 3.1.7.12 Safety Case

Dem Safety Case kommt in der Praxis eine wesentliche Bedeutung zu, weil er die gesammelten Nachweise beinhaltet, dass ein System bei bestimmungsgemäßem Gebrauch und unter vorhergesehenen Umständen ein akzeptables Sicherheitsniveau erreicht. Der Safety Case stützt sich in erster Linie darauf, dass die Anforderungen, die an ein System gestellt werden, auch erfüllt werden. Um zu belegen dass die jeweilige Anforderung erfüllt wird, werden Nachweise erbracht, die durch eine entsprechende Argumentation mit der Anforderung verknüpft werden. Solche Nachweise können beispielsweise durch Work Products erbracht werden.

Zu diesem Zweck wird auch der Safety Case auf seine Vollständigkeit hin überprüft. Diese Überprüfung umfasst laut Norm folgende Punkte (ISO 26262-2, 2011, S. 27):

- Bestätigung, dass die Work Products, auf die im Safety Case referenziert wird, zugänglich sind und in ausreichendem Umfang ausgeführt wurden, damit die Erreichung der Funktionalen Sicherheit des Items angemessen evaluiert werden kann.
- Bestätigung, dass die Work Products aus dem Safety Case
    - von einem zum anderen verfolgbar sind,
    - keine Wiedersprüche innerhalb oder zwischen den Work Products aufweisen, und
    - entweder keine offenen Fragen beinhalten die zu einer Verletzung des Safety Goals führen, oder nur vorläufig offene Fragen beinhalten, für die es eine bereits geplante Lösung gibt.

## 3.2 Functional Safety Lifecycle

In diesem Kapitel wird nun der Sicherheitslebenszyklus der ISO 26262, der Functional Safety Lifecycle, vorgestellt. Abbildung 10 zeigt den Ablauf des Functional Safety Lifecylce und die Zuordnung der Kapitel der Norm zu den einzelnen Phasen.

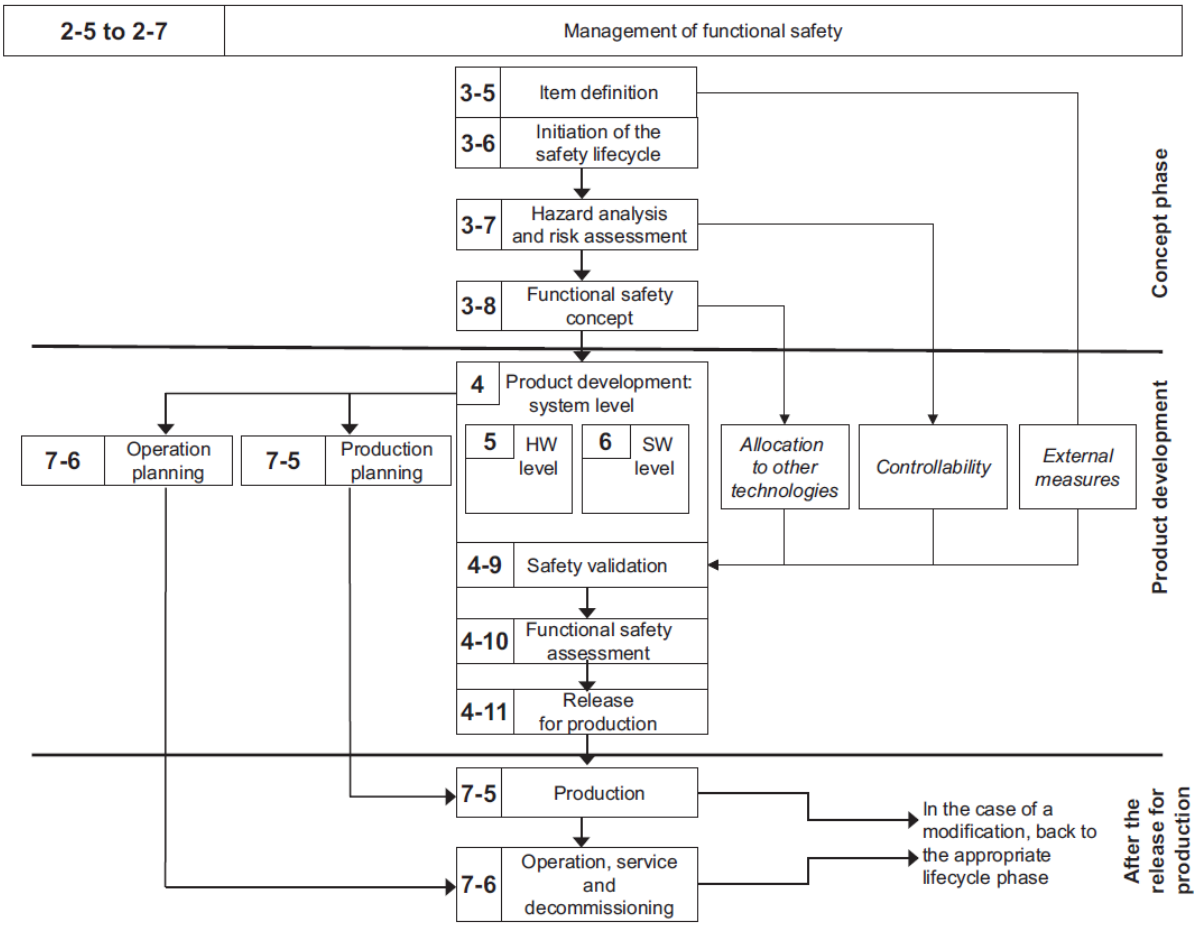


Abbildung 10: Übersicht des Functional Safety Lifecycle (Quelle: ISO 26262)

Übergeordnet findet sich das Management der Funktionalen Sicherheit wieder, das während aller Phasen des Lebenszyklus zur Anwendung kommt. Die Konzeptphase umfasst die Item Definition, die Initiierung des Sicherheitslebenszyklus, die Gefahren- und Risikoanalyse sowie das Funktionale Sicherheitskonzept. Nachdem die Konzeptphase abgeschlossen, ist wird mit der eigentlichen Entwicklungsphase fortgefahren. Hier werden zuerst die Anforderungen auf Produktebene beschrieben und später auf Hard- und Softwareebene genauer spezifiziert. Die Entwicklungsphase endet mit der Produktionsfreigabe.

Die letzte Phase nach der Freigabe zur Produktion beinhaltet die eigentliche Produktion, sowie den Betrieb, das Service und die Außerbetriebnahme des

Produktes. Während dieser abschließenden Phase sollen unter anderem Felddaten erhoben werden und mit den getroffenen Annahmen aus früheren Phasen der Entwicklung abgeglichen werden. Falls es hier zu Abweichungen kommen sollte, müssen die Ursachen dafür genauer erfasst werden und eventuell notwendige Anpassungen vorgenommen werden, um mögliche Gegenmaßnahmen einleiten zu können.

In weiterer Folge werden nur mehr die Teile des Functional Safety Lifecycle genauer beschrieben, die während der Konzeptphase der Fahrzeugentwicklung durchzuführen sind.

### 3.2.1 Item Definition

Wie bereits erwähnt beschreibt das Item ein System oder eine Anordnung von Systemen, um eine oder mehrere Funktionen auf Fahrzeugebene zu realisieren. Die Item Definition soll nun das Item unter Berücksichtigung der kundenerlebbaren Funktionen, vorhandenen Schnittstellen, relevanten Umgebungsbedingungen, rechtlichen Anforderungen, Gefahren oder ähnlichem soweit beschreiben, dass alle weiteren Aktivitäten in späteren Phasen des Functional Safety Lifecycle durchgeführt werden können. Sofern es bereits bestehende Informationen bezüglich des Items gibt (Produktidee, Projektskizzen, relevante Patente, Ergebnisse von Vor-Testläufen etc.), sollen diese Informationen ebenfalls berücksichtigt werden.

Die Daten, die festgelegt werden müssen, umfassen also sowohl die funktionalen und nicht-funktionalen Anforderungen des Items, als auch die Abhängigkeiten zwischen dem Item und der Umgebung. Diese Informationen beinhalten laut Norm unter anderem (ISO 26262-3, 2011, S. 10):

- Das funktionale Konzept, das den Zweck und die Funktion, inklusive der Betriebsart und den möglichen Betriebszuständen beschreibt
- Die Randbedingungen im Betrieb und der Umgebung
- Rechtliche Anforderungen, Gesetze, Bestimmungen, nationale und internationale Vorgaben
- Wenn anwendbar, das Verhalten, das durch ähnliche Funktionen, Items oder Elemente erreicht wird

- Potentielle Konsequenzen des Verhaltens des Items im Falle eines Ausfalles, inklusive bekannter Fehlerzustände und Gefahren

Außerdem soll die Umgebung des Items, die Schnittstellen und die Annahmen über mögliche Interaktion mit anderen Items und Elementen betrachtet werden, wobei folgende Aspekte berücksichtigt werden sollen (ISO 26262-3, 2011, S. 10):

- Die einzelnen Elemente des Items
- Die Annahmen betreffend der Effekte des Item-Verhaltens auf andere Items oder Elemente, beziehungsweise die Umgebung des Items
- Interaktionen des Items mit anderen Items oder Elementen
- Die von anderen Items, Elementen oder der Umgebung geforderte Funktionsfähigkeit des Items
- Die Anordnung und Verteilung von Funktionen innerhalb der betroffenen Systeme oder Elemente
- Betriebsszenarien welche die Funktionalität des Items beeinflussen

### 3.2.2 Initiierung des Safety Lifecycle

Auf Basis der Item Definition wird entschieden, ob das jeweilige Item eine komplette Neuentwicklung darstellt, oder ob es sich um eine Modifikation eines bereits entwickelten Items handelt. Wenn es sich bei dem Item um eine Modifikation eines bereits existierenden Items handelt, kann der Safety Lifecycle, entsprechend der Änderungen im Vergleich zum bestehenden Item, angepasst werden. In diesem Zusammenhang spricht die Norm auch vom so genannten „Tailoring“. Zum Zweck der Ermittlung der Änderungen ist es daher notwendig eine Einflussanalyse durchzuführen. Durch diese Einflussanalyse wird festgestellt, welchen Einfluss die Modifikationen auf das Item haben und welcher Änderungsbedarf in Bezug auf bereits erstellte Work Products besteht. Dieser gesamte Ablauf ist in Abbildung 11 dargestellt.

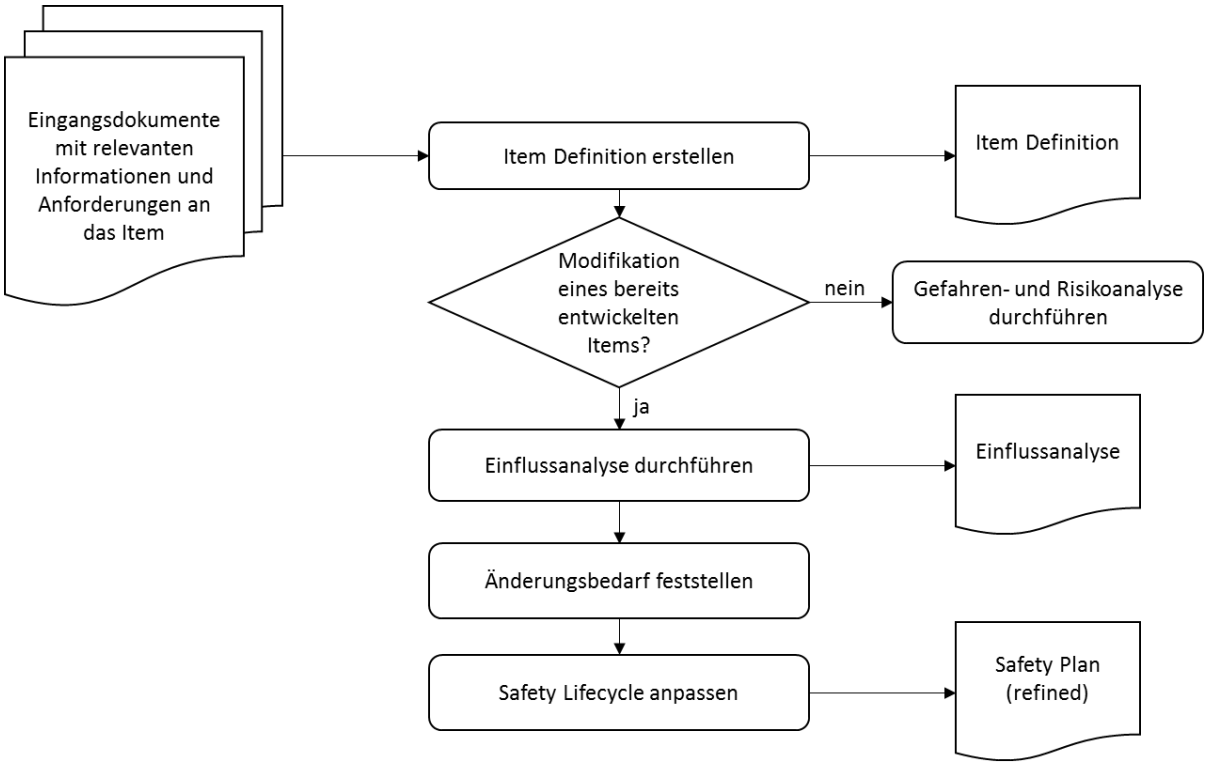


Abbildung 11: Initiierung des Safety Lifecycle

Sofern es sich bei dem Item um eine komplette Neuentwicklung und keine Modifikation handelt, muss auch keine Einflussanalyse durchgeführt werden. In diesem Fall wird gleich mit dem nächsten Schritt in der Konzeptphase des Safety Lifecycle, der Gefahren- und Risikoanalyse, fortgefahren.

### 3.2.3 Gefahren- und Risikoanalyse

In der Gefahren- und Risikoanalyse sollen alle möglichen Gefahren und Risiken eines Items analysiert werden, zu denen es während des Betriebes kommen kann. Diese Analyse dient also der Identifizierung und Klassifizierung von möglichen Gefährdungen und Risiken, welche durch Fehlfunktionen von E/E-Systemen ausgelöst werden können. Die Klassifizierung erfolgt dabei anhand von drei unterschiedlichen Bewertungsklassen. Die Faktoren, die dabei Berücksichtigung finden, sind das Schadensausmaß (S), die Kontrollierbarkeit (C) sowie die Expositionshäufigkeit (E). Je nach Faktor gibt eine dazugehörige Zahl Auskunft darüber, wie groß der Einfluss auf das Gesamtrisiko ist. Durch die Kombination dieser Faktoren wird der „Automotive Safety Integrity Level“, kurz ASIL, abgeleitet. Der ASIL stellt also ein Maß für die Kritikalität einer Fehlfunktion dar. Abbildung 12 zeigt, wie aus den jeweiligen Faktoren der entsprechende ASIL bestimmt wird.

| Severity class | Probability class | Controllability class | | |
|---|---|---|---|---|
| | | C1 | C2 | C3 |
| S1 | E1 | QM | QM | QM |
| | E2 | QM | QM | QM |
| | E3 | QM | QM | A |
| | E4 | QM | A | B |
| S2 | E1 | QM | QM | QM |
| | E2 | QM | QM | A |
| | E3 | QM | A | B |
| | E4 | A | B | C |
| S3 | E1 | QM | QM | A |
| | E2 | QM | A | B |
| | E3 | A | B | C |
| | E4 | B | C | D |

Abbildung 12: Übersicht ASIL Ermittlung (Quelle: ISO 26262)

In Anlehnung an Wolfgang Danzer, besteht die Gefahren- und Risikoanalyse zusammenfassend aus folgenden Punkten (2016, S. 92):

- Situationsanalyse, um relevante Betriebszustände und Situationen von Fehlfunktionen, auch unter Berücksichtigung möglicher zu erwartender Missbrauchsfälle zu beschreiben.
- Bewertung des Schadensausmaßes entsprechend den Bewertungsklassen S0 (keine Verletzung) bis S3 (lebensbedrohliche Verletzung).
- Bewertung der Expositionshäufigkeit und damit der Auftretenshäufigkeit von Situationen im Fahrzeug, entsprechend den Bewertungsklassen E0 (nahezu unmöglich) bis E4 (hohe Wahrscheinlichkeit).
- Bewertung der Kontrollierbarkeit und damit der Erwartung, dass Gefährdung durch Beteiligte abgewandt werden kann, entsprechend den Bewertungsklassen C0 (im Allgemeinen kontrollierbar) bis C3 (schwer zu kontrollieren bis unkontrollierbar).
- Berechnung des ASIL als Summe der drei Bewertungsklassen (SEC = 10: ASIL D, SEC = 9: ASIL C, SEC = 8: ASIL B, SEC = 7: ASIL A, SEC ≤ 6: keine Zusatzanforderungen an die Absicherung aufgrund der Gefahren- und Risikoanalyse).

Für jede Fehlfunktion wird in weiterer Folge mindestens ein Sicherheitsziel definiert. Dieses sogenannte Safety Goal erbt den ASIL der dazugehörenden Fehlfunktion. Das Safety Goal stellt nun die oberste Sicherheitsanforderung dar. Einer Fehlfunktion können mehrere Safety Goals zugeordnet werden, umgekehrt kann aber auch ein Safety Goal an mehrere Fehlfunktionen gerichtet sein (ISO 26262-1, 2011, S. 20).

Damit ein System im Hinblick auf mögliche Gefahren und Risiken so umfassend wie möglich betrachtet werden kann, empfiehlt es sich die entsprechenden Analysen in einem interdisziplinären Team durchzuführen. Das bedeutet, dass das Team nicht nur aus Personen einer einzigen Fachrichtung besteht, sondern dass es sich aus Experten unterschiedlicher Fachbereiche zusammensetzt. Dadurch werden möglicherweise einige zusätzliche Fragen aufgeworfen, die auf eine unterschiedliche Betrachtungsweise der Beteiligten zurückzuführen ist.

Wie bereits angesprochen bedeutet eine höhere ASIL-Einstufung in Bezug auf eine Fehlfunktion, dass umfassendere Maßnahmen zur Erreichung der Funktionalen Sicherheit des Items notwendig sind. Dies betrifft sowohl den Aufwand in der Entwicklung als auch den Dokumentationsaufwand. Hinzu kommt, dass die Gefahren- und Risikoanalyse sowohl ein Confirmation- als auch ein Verification-Review durchlaufen muss. Das Confirmation-Review ist dabei sogar immer von einer zum Entwicklungsteam unabhängigen organisatorischen Einheit oder überhaupt von einem unabhängigen Dienstleister durchzuführen.

### 3.2.4 Funktionales Sicherheitskonzept

Sicherheitskonzepten kommt in der Praxis eine wesentliche Bedeutung zu, wenn es darum geht, unverhältnismäßige Risiken durch Fehlfunktionen von E/E-Systemen zu vermeiden. Für Hans-Leo Ross stellen Sicherheitskonzepte die Planungsgrundlage für die zu implementierenden Sicherheitsmechanismen und Sicherheitsaktivitäten dar, die im Rahmen einer sicherheitsrelevanten Produktrealisierung in Betracht gezogen werden müssen (Ross, 2014, S. 107). Sicherheitskonzepte können funktionaler und technischer Natur sein.

Ausgehend von der Item Definition und den Sicherheitszielen aus der Gefahren- und Risikoanalyse umfasst das Funktionale Sicherheitskonzept die Ermittlung der funktionalen Sicherheitsanforderungen, sowie die Zuordnung dieser Anforderungen zu den jeweiligen Elementen der vorläufigen Systemarchitektur des Items, oder zu externen Maßnahmen. Um die Sicherheitsziele zu erfüllen, beinhaltet es Sicherheitsmaßnahmen und Sicherheitsmechanismen, die durch Architekturelemente des Items ausgeführt werden und in den funktionalen Sicherheitsanforderungen spezifiziert werden (ISO 26262-3, 2011, S. 18).

Laut Norm beinhaltet das funktionale Sicherheitskonzept folgende Punkte (ISO 26262-3, 2011, S. 18):

- Fehlererkennung und Ausfallsminderung
- Übergang in einen sicheren Zustand
- Fehlertoleranzmechanismen (mit und ohne Degradation)
- Fehlererkennung und Fahrerwarnung
- Entscheidungslogik, um die am besten geeignete Steueranforderung auszuwählen

Wie die Item Definition wird auch das funktionale Sicherheitskonzept lösungsneutral formuliert, damit wiederum die Anwendbarkeit auf unterschiedliche technische Architekturen ermöglicht wird. Ein Beispiel für eine entsprechende lösungsneutrale Formulierung wäre das Warnen des Fahrers durch Visualisierung. Wie die Umsetzung dann in weiterer Folge durchgeführt wird, durch eine Anzeige am Armaturenbrett oder durch eine Einblendung auf der Windschutzscheibe, spielt erst auf der technischen Ebene eine Rolle.

### 3.2.5 Spezifikation der technischen Sicherheitsanforderungen

Die Spezifikation der technischen Sicherheitsanforderungen fällt zwar normativ nicht mehr in den Bereich der Konzeptphase, stellt aber die Schnittstelle zur Phase der eigentlichen Produktentwicklung dar und wird daher an dieser Stelle ebenfalls mitbetrachtet.

Wenn die Sicherheitsziele formuliert sind und das Funktionale Sicherheitskonzept ausgearbeitet wurde, erfolgt unter Berücksichtigung der vorläufigen Architektur die Spezifikation der technischen Sicherheitsanforderungen. Dabei besteht ein direkter Zusammenhang zwischen den funktionalen und technischen Sicherheitsanforderungen. Die technischen Sicherheitsanforderungen definieren dabei Anforderungen, die auf Elemente der E/E-Architektur allokiert werden. Wie der Zusammenhang der Work Products aus dem Safety Lifecycle und der jeweils dazu gehörenden Anforderungen in der Praxis aussieht, ist in Abbildung 13 dargestellt.

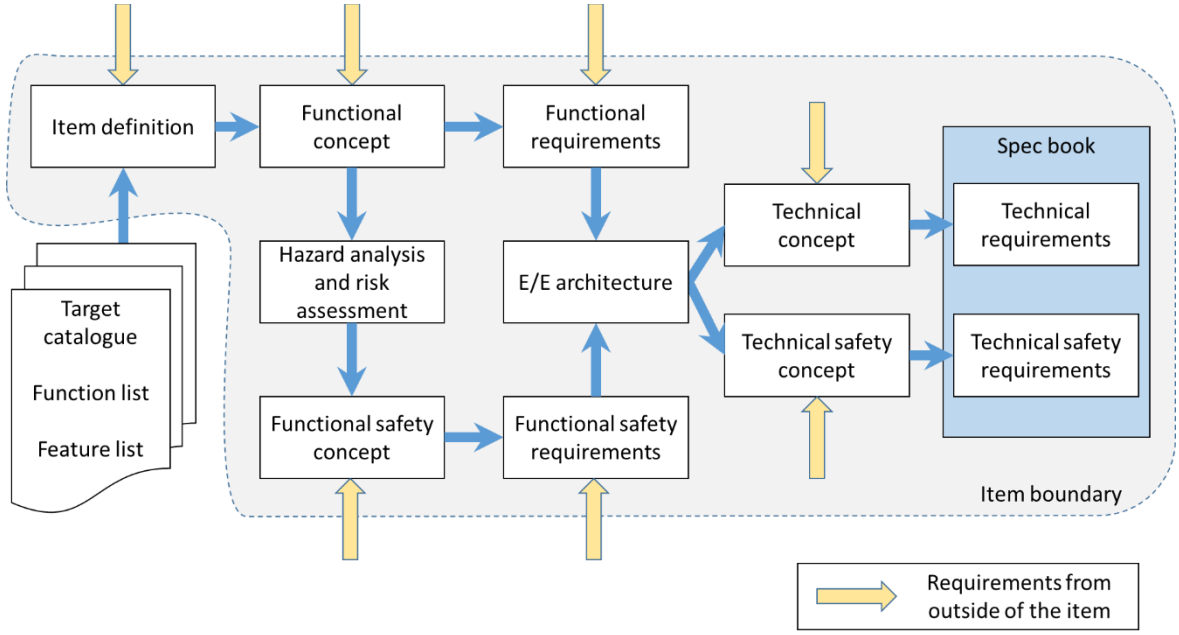


Abbildung 13: Zusammenhang der Anforderungen

Die technischen Anforderungen beziehungsweise technischen Sicherheitsanforderungen werden schlussendlich zur Spezifikationen für die Lastenhefte bei der Angebotserstellung herangezogen.

# 4. Möglichkeiten der Erstellung

Die Dokumentenanforderungen der Norm sind, was die Art der Dokumentation und Erstellung der Dokumente und Work Products betrifft, eher auf einen ausreichenden Informationsgehalt ausgerichtet, als auf das Layout und Erscheinungsbild (ISO 26262-8, 2011, S. 27). Auch müssen die Dokumente nicht zwangsläufig immer in physischer Form vorliegen, außer dies wird explizit durch die Norm gefordert. Die Norm fordert (ISO 26262-8, 2011, S. 28), dass die Dokumente

- präzise und prägnant,
- in einer klaren Art und Weise strukturiert,
- für die beabsichtigten Benutzer einfach zu verstehen sind und
- gepflegt werden können.

Das bedeutet, dass man bei der Erstellung der Work Products grundsätzlich keine spezielle Systematik einhalten muss, solange strukturiert vorgegangen wird. In der Praxis haben sich einige Möglichkeiten der Erstellung bewährt, die einerseits das Arbeiten erleichtern und andererseits auch die Informationen auf eine strukturierte Art und Weise miteinander verknüpfen. Einige dieser Möglichkeiten werden nun kurz beschrieben. An dieser Stelle soll auch erwähnt werden, dass die genannten Möglichkeiten auf unterschiedliche Weise kombiniert werden können, um auf die Voraussetzungen in einem Unternehmen gezielt eingehen zu können.

## 4.1 Anforderungsschablonen

Wie bereits erwähnt ist die korrekte Spezifikation von Anforderungen ein wichtiges Thema der Funktionalen Sicherheit. Nur wenn bereits am Anfang Anforderungen in ausreichendem Umfang festgelegt werden, können die späteren Phasen des Safety Lifecycle und vor allem die Ableitung von Anforderungen auf den nächsten Abstraktionsebenen in der geforderten Qualität erfolgen. Während für die Formulierung von funktionalen oder technischen Sicherheitsanforderungen die natürliche Sprache oft besser geeignet ist, wird vor allem von Sicherheitsanforderungen auf Hard- und Softwareebene gefordert, dass diese durch eine semi-formale oder formale Notation spezifiziert werden (ISO 26262-8, 2011, S. 17f).

Eine Möglichkeit, wie in der Praxis Anforderungen in der frühen Entwicklungsphase systematisch formuliert werden können, ist die Zuhilfenahme von Anforderungsschablonen. Anforderungsschablonen können als Bauplan gesehen werden, der die Struktur eines Anforderungssatzes festlegt (Rupp, 2014, S. 218). In Anlehnung an Chris Rupp zeigt Abbildung 14, aus welchen Teilen eine solche Schablone bestehen kann.

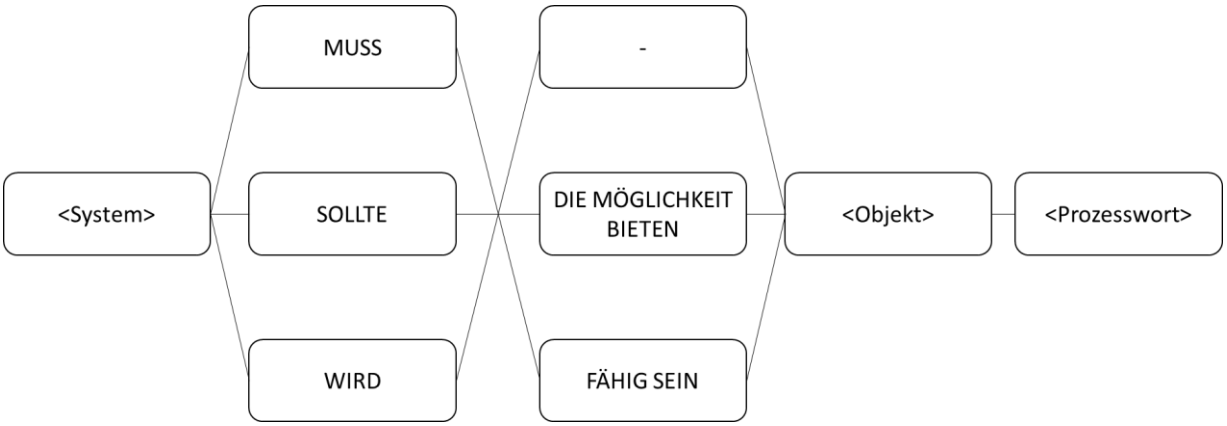


Abbildung 14: Anforderungsschablone

Die Teile aus denen eine Anforderungsschablone besteht, können je nach Bedarf ergänzt und angepasst werden. Die Formulierung einer kundenerlebbaren Funktion in der Item Definition kann dadurch zum Beispiel folgendermaßen lauten:

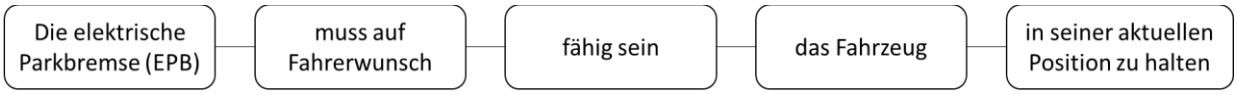


Abbildung 15: Beispiel Anforderungsschablone

Durch so eine Systematik ist es einerseits möglich, konsequent die geforderte „message-sequence-chain“ einzuhalten und andererseits stellt dies die Basis dafür dar, die Anforderungen auf den nächsten Ebenen weiter spezifizieren zu können. Unter Verwendung von Anforderungsschablonen gelingt es relativ einfach, die Qualität der formulierten Anforderungen zu steigern und die Anforderungen unabhängig vom Entwickler auf dieselbe Art und Weise zu beschreiben.

## 4.2 Grafische Funktionsbeschreibung

Je nach Branche und Komplexität eines Items werden in der Praxis unterschiedliche Methoden angewendet, um eine Funktion zu beschreiben und die funktionalen Zusammenhänge visuell darzustellen. Einige Möglichkeiten der grafischen Funktionsbeschreibung in unterschiedlichen Anwendungsbereichen sind:

- Funktionsdiagramm
- Flowchart
- Functional flow block diagram (FFBD)
- Unified Modeling Language (UML)
- Business Process Model and Notation (BPMN)

In Anlehnung an die Darstellung von Prozessmodellen ist bei einer möglichen grafischen Darstellung der kundenerlebbaren Funktionen eines Items die Schnittstelle zu anderen Items durch die entsprechende Itemgrenze eindeutig festgelegt. Um eine Itemfunktion zu ermöglichen, sind üblicherweise einzelne Teilfunktionen erforderlich. Diese Teilfunktionen werden durch einzelne Funktionsblöcke beschrieben, denen eine konkrete Eingangs- und Ausgangsinformation zugeordnet werden kann. Die einzelnen Teilfunktionen sollten dabei aus Gründen der Einheitlichkeit nach Möglichkeit mit einem Haupt- und Zeitwort beschrieben werden. An dem vorherigen Beispiel der elektrischen Parkbremse soll in Abbildung 16 vereinfacht gezeigt werden, wie eine entsprechende Funktionsbeschreibung grafisch dargestellt werden kann.

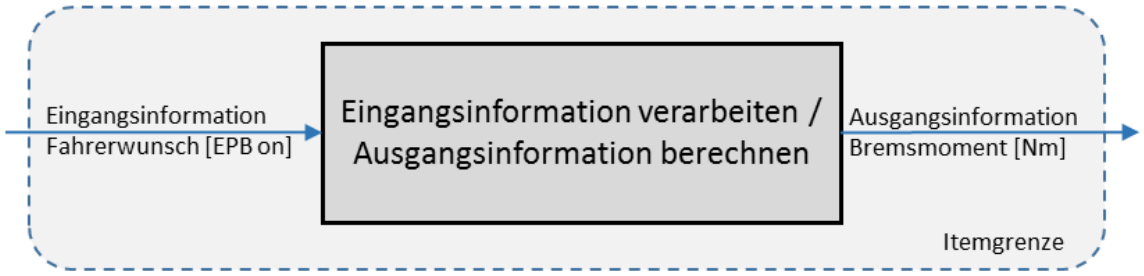


Abbildung 16: Beispiel Funktionsbeschreibung

## 4.3 Goal Structuring Notation

In einem Safety Case der auf reinem Text basiert gelingt es oft nicht, den Zusammenhang von Anforderung, Argument und Nachweis ausreichend übersichtlich darzustellen. Die Goal Structuring Notation (GSN) ist eine grafische Darstellungsart die oft in sicherheitskritischen Branchen angewendet wird, um die Struktur, Schlüssigkeit und Übersichtlichkeit von Sicherheitsargumenten, wie sie in einem Safety Case vorkommen, zu verbessern (Kelly & Weaver, 2004, S. 1). Die Elemente die dazu in der GSN verwendet werden sind in Abbildung 17 dargestellt.

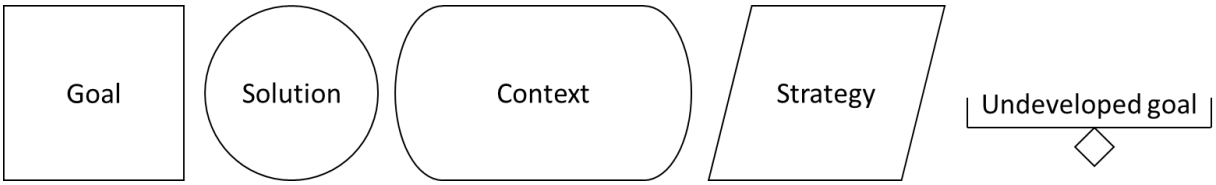


Abbildung 17: Elemente der Goal Structuring Notation

Wenn diese Elemente in einem Netzwerk miteinander verknüpft werden, spricht man auch von einer „goal structure“. Zweck dieser Verknüpfung ist es darzustellen, wie ein Ziel (Goal) sukzessive in Sub-Ziele heruntergebrochen werden kann, bis die Erreichung des Ziels schlussendlich mit einem Beleg (Solution) nachgewiesen werden kann. (Kelly & Weaver, 2004, S. 3)

Die GSN kann entweder manuell mit einem herkömmlichen Textverarbeitungsprogramm angewendet werden, oder automatisiert in einem Anforderungsmanagement-Tool. Es gibt unterschiedliche Ansätze wie die GSN noch erweitert oder in sogenannten „Patterns“ zusammengefasst werden kann (Macher, Sporer, & Kreiner, 2015, S. 2), um die Anwendung in Safety Cases noch weiter zu erleichtern.

## 4.4 Integrierte Toolketten

Integrierte Toolketten unterstützen dabei die Work Products, die während unterschiedlicher Entwicklungsschritte erstellt wurden, auf einfachstem Weg miteinander zu verknüpfen und so fehlerfrei Daten zu übertragen. Die Nachverfolgbarkeit und Konsistenz der Anforderungen ist gerade in der Funktionalen Sicherheit ein wichtiges Thema. Die Verknüpfung der Artefakte in integrierten Toolketten ermöglicht es, dass die Anforderungen die auf allen Abstraktionsebenen

erstellt werden, auch bidirektional nachverfolgt werden können. Die Toolintegration stellt dabei einen entscheidenden Faktor bei der Steigerung von Effizienz und Qualität im Entwicklungsprozess dar (Armengaud, Griessnig, & Mader, 2012, S. 351).

Ohne zu sehr ins Detail zu gehen gibt es in der Praxis unterschiedliche Modellbasierte Sprachen (UML, SysML, Autosar etc.) welche die Erstellung solcher integrierter Toolketten ermöglichen. Allerdings ist auch zu bemerken, dass solche Tools gerade von Anwendern mit geringem Wissen auf dem Gebiet der Softwareentwicklung, manchmal auch sehr schwierig anzuwenden sind. Es gibt unterschiedliche Ansätze, wie die Anwendung weiter vereinfacht werden kann (Sporer & Brenner, 2016, S. 3)

# 5. Erhebung der Ausgangssituation

Am Beginn des praktischen Teils der Arbeit steht die Erhebung der Ausgangssituation der Funktionalen Sicherheit bei Magna Steyr. Diese Analyse wird einerseits anhand der bereits bestehenden Strukturen in der Entwicklung und andererseits durch Befragung von einigen Fachbereichsvertretern aus dem Kernteam der Funktionalen Sicherheit durchgeführt.

## 5.1 Magna Steyr Development System

Der allgemeine Entwicklungsprozess wird intern durch das „Magna Steyr Development System“, kurz MSDS, dargestellt. MSDS stellt ein Framework dar, das für alle Bereiche der Fahrzeugentwicklung gültig ist. Es unterteilt den Entwicklungsprozess in einzelne Phasen, wobei am Ende jeder Phase ein Meilenstein steht, der den laufenden Projektfortschritt dokumentiert und überschritten werden muss, damit die nächste Phase im Projekt begonnen werden kann. Zu jedem Meilenstein gibt es Checklisten, die genau regeln, welche Arbeitsergebnisse, zu welchem Zeitpunkt vom jeweiligen Verantwortlichen erstellt werden müssen. Dadurch, dass MSDS von allen beteiligten Fachbereichen in der Produktentwicklung angewendet wird, ist somit eine zeitliche Abstimmung der notwendigen Arbeitsschritte während den einzelnen Phasen eines Entwicklungsprojektes gewährleistet.

MDSD ist grundsätzlich in zwei Phasen aufgeteilt. Die erste Phase bezeichnet die Konzeptentwicklung und die zweite Phase die Serienentwicklung. Diese Phasengliederung und die jeweiligen Meilensteine sind ausschnittsweise in Abbildung 18 dargestellt.

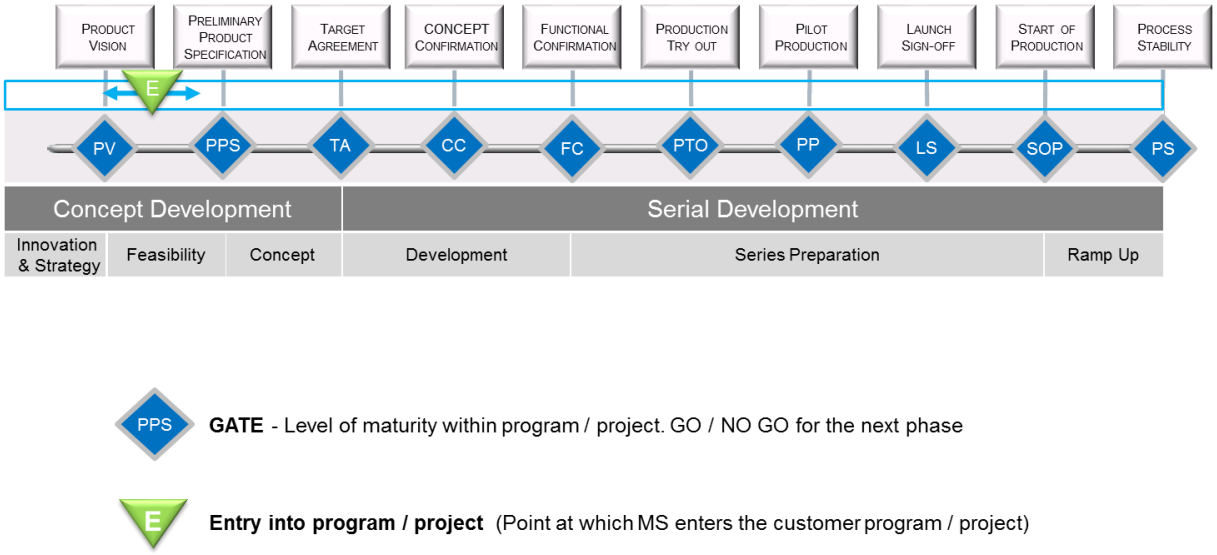


Abbildung 18: Phasengliederung und Meilensteine nach MSDS

Die Konzeptentwicklung unterteilt sich wiederum in die Subphasen „Innovation & Strategy“, „Feasibility“ und „Concept“. Die Serienentwicklung gliedert sich in „Development“, „Series Preparation“ und „Ramp Up“. In weiterer Folge soll nur mehr die Phase der Konzeptentwicklung betrachtet werden.

Ziel der Innovations- und Strategiephase ist es, eine Innovation im Bereich der Fahrzeugtechnik grob zu beschreiben und eine Strategie zu formulieren, wie diese Innovation in bestehende oder neue zu erschließende Märkte eingeführt werden könnte. Danach wird diese Innovation hinsichtlich der prinzipiellen Machbarkeit überprüft und eine vorläufige Produktbeschreibung erstellt. Wenn die Innovation erfolgversprechend ist, beginnt die Phase, in der ein vorläufiges Konzept zur Umsetzung der Innovation ausgearbeitet wird. Wie bereits erwähnt, steht am Ende jeder Phase ein Meilenstein. Die Meilensteine während der Konzeptentwicklung sind „Product Vision“, „Preliminary Product Specification“ und „Target Agreement“, mit den jeweils dazugehörenden Checklisten und „Deliverables“.

Die Organisationsstruktur in einem Projekt beschreibt, wie und aus welchen Mitgliedern sich das Projektteam zusammensetzt und welche Hierarchien innerhalb des Projektes bestehen. Die Rollenbeschreibungen legen fest, welche Aufgaben und Verantwortungen den einzelnen Projektmitgliedern zukommen.

Nachdem der allgemeine Entwicklungsprozess nun kurz beschrieben wurde, wird in weiterer Folge genauer auf den spezifischen Prozess der Funktionalen Sicherheit und die spezifischen Rollen der Funktionalen Sicherheit eingegangen.

## 5.2 Safety Lifecycle bis SOP

Der „Safety Lifecycle bis SOP“ beschreibt den internen Prozess in Bezug auf die Funktionale Sicherheit gemäß den Anforderungen der ISO 26262. In ihm sind einerseits die geforderten Sicherheitsaktivitäten aus dem Safety Lifecycle der ISO 26262 abgebildet und außerdem firmenspezifische Aktivitäten integriert, die im Zusammenhang mit der Funktionalen Sicherheit stehen. Abbildung 19 zeigt überblicksweise, wie einige Work Products aus dem Safety Lifecycle bis SOP zeitlich zu den einzelnen Phasen und Meilensteinen aus dem Entwicklungsprozess nach MSDS zugeordnet werden können.

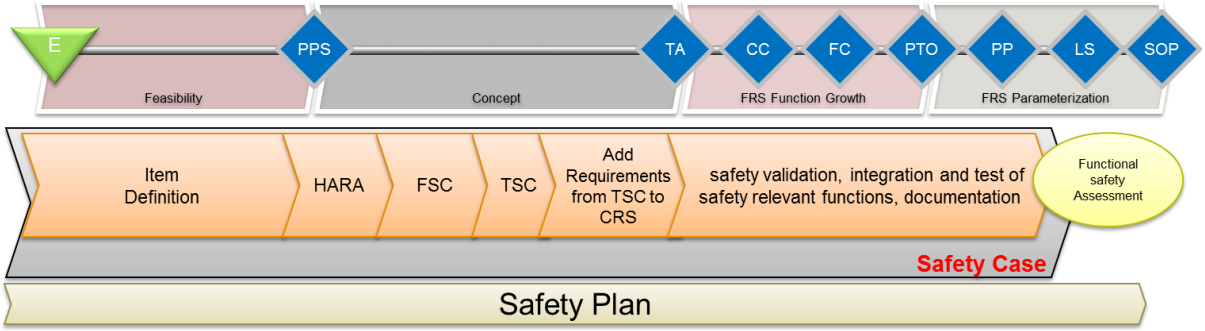


Abbildung 19: Safety Lifecycle bis SOP

## 5.3 Rollen der Funktionalen Sicherheit

An dieser Stelle wird darauf hingewiesen, dass es vor allem in umfangreichen Gesamtfahrzeugprojekten eine Vielzahl von Rollen der Funktionalen Sicherheit gibt, die Aufgaben während aller Phasen des Produktlebenszyklus übernehmen. Da der Fokus der vorliegenden Arbeit aber auf der Konzeptphase der Entwicklung liegt, wird auch nur auf die während dieser Phase wesentlichen Rollen der Funktionalen Sicherheit Bezug genommen.

### Engineering Responsible Functional Safety Manager

Um alle Anforderungen der Funktionalen Sicherheit an die Fahrzeugentwicklung erfüllen zu können ist es in großen Organisationen unabdingbar, einen zentralen

Ansprechpartner zu haben der hinreichende Kenntnis über die einzelnen Inhalte der Norm aufweist. Diese Rolle wird intern durch den Engineering Responsible Functional Safety Manager (ER-FSM) wahrgenommen. Ihm obliegt die Planung, Koordinierung und Dokumentation aller sicherheitsrelevanten Aktivitäten im Rahmen der Entwicklung von sicherheitsrelevanten Systemen. Die wesentlichen Aufgaben des ER-FSM sind:

- Leitung des FUSI-Teams
- Ansprechpartner zum Kunden
- Abstimmung der DIA mit dem Kunden
- Einfordern von Unterstützungsaktivitäten in Bezug auf die FUSI
- Erstellung und Verwaltung des Safety Plans
- Planung von Reviews, Audits und Assessments in Bezug auf die FUSI
- Berichterstattung über den Fortschritt der FUSI im Projekt
- Mitarbeit und Hilfeleistung bei der Erstellung der Work Products

**Engineering Responsible Functional Safety Item**

Der Itemverantwortliche, intern auch als Engineering Responsible Functional Safety Item (ER-FSI) bezeichnet, ist die Person die für die Entwicklung eines Items aus Sicht der Funktionalen Sicherheit hauptverantwortlich ist. Er erstellt die Item Definition, arbeitet an der Gefahren- und Risikoanalyse mit, erstellt die Sicherheitskonzepte und ist der Ansprechpartner für den ER-FSM.

Die Aufgaben des ER-FSI umfassen:

- Verantwortlichkeit für die sicherheitsorientierte Entwicklung
- Erstellung der Item Definition
- Analyse ob Item eine Modifikation ist oder nicht
- Durchführen der Einflussanalyse im Fall einer Modifikation
- Erstellung des Funktionalen Sicherheitskonzeptes
- Erstellung des Technischen Sicherheitskonzeptes
- Durchführung der Verifikationsplanung in Bezug auf die FUSI
- Planung von Itemintegration und Testing

## 5.4 Befragung und Situationsanalyse

Durch die Befragung einiger Fachbereichsvertreter aus dem Kernteam der Funktionalen Sicherheit wurde versucht, weitere Sichtweisen aus den involvieren Fachbereichen zu gewinnen. Insgesamt wurden daher vier Fachbereichsvertreter im Rahmen eines Einzelgespräches zu unterschiedlichen Aspekten der Funktionalen Sicherheit befragt. Zum Zweck einer einheitlichen Gesprächsführung wurde im Vorfeld der Gespräche ein Leitfaden mit konkreten Fragestellungen erstellt. Dieser Leitfaden umfasst folgende Fragen:

- Inwiefern betrifft Sie die Thematik der Funktionalen Sicherheit?
- Wie oft und in welcher Form sind Sie mit Themen der Funktionalen Sicherheit im Arbeitsalltag konfrontiert?
- Welche Aufgaben/Verantwortungen haben Sie in Ihrer Position?
- Hat sich durch Einführung der ISO 26262 im Vergleich zur früheren Arbeitsweise (IEC 61508 Standard) etwas verändert? Wenn ja, was hat sich verändert?
- Hindert/Unterstützt Sie die ISO 26262 im Vergleich zur früheren Arbeitsweise?
- Wie sehen Sie die aktuelle Situation der Funktionalen Sicherheit bei Magna Steyr?
- Welche Stärken/Schwächen sehen Sie?
- Wo steht Ihrer Meinung nach Magna Steyr in Bezug auf die Funktionale Sicherheit im Vergleich mit OEMs, Kunden, Zulieferern etc.?
- Welche Chancen/Risiken sehen Sie?
- Welche Problemfelder sehen Sie bei der Umsetzung der Funktionalen Sicherheit?
- Welche Fehlerquellen bzw. Ursachen für Fehler sehen Sie?
- Was hindert Sie bei der effizienten Umsetzung?
- Welche negativen Entwicklungen ergeben sich aus den Fehlern?
- Welche Lösungsansätze und Verbesserungsvorschläge fallen Ihnen im Vergleich zur aktuellen Situation ein?
- Was fehlt, um die Situation zu verbessern?
- Was muss/müsste sich ändern?

Die Erkenntnisse aus den Gesprächen wurden in Form einer SWOT-Analyse zusammengefasst, im Rahmen der ersten Zwischenpräsentation der Masterarbeit den Betreuern und Fachbereichsvertretern intern vorgestellt und gemeinsam diskutiert. An dieser Stelle wird angemerkt, dass diese SWOT-Analyse aus Gründen der Geheimhaltung nicht in der Masterarbeit abgebildet wird.

# 6. Erstellung der Templates

In diesem Kapitel werden nun die Templates zu den Work Products vorgestellt, die im Zuge dieser Masterarbeit erstellt wurden. Zuerst werden die Gründe für die Auswahl erläutert, danach einige Grundlagen und Gemeinsamkeiten beschrieben. In Folge wird auf die konkreten Inhalte und den Aufbau der einzelnen Templates näher eingegangen. Die vollständigen Templates sind im Anhang zu finden.

## 6.1 Auswahl

Die Basis für die Auswahl der zu erstellenden Templates stellt der interne Safety Lifecycle bis SOP dar. Nachdem der Fokus dieser Arbeit auf den Review-pflichtigen Work Products aus der Konzeptphase der Fahrzeugentwicklung liegt, wurden Work Products die zeitlich nach dem MSDS Meilenstein TA anfallen auch nicht berücksichtigt. Relevante Work Products während der Konzeptphase sind die „Item Definition“, das „Functional Safety Concept“ und das „Technical Safety Concept“. Da diese Dokumente auch in direktem Zusammenhang stehen, wurde entschieden für diese Work Products auch Templates zu erstellen. Wie in der Einleitung erwähnt war die Integration der Funktionsentwicklung in die Templates ein wichtiges Thema und daher wurden diese Templates auch um die Konzeptentwicklung auf funktionaler und technischer Ebene erweitert. Teilweise sind in der Konzeptphase schon intern freigegebene Vorlagen vorhanden. Dies betrifft beispielsweise die Gefahren- und Risikoanalyse, die aus diesem Grund in der vorliegenden Arbeit auch nur als Schnittstelle zwischen den erstellten Vorlagen betrachtet wurde.

Der interne Prozess der Funktionalen Sicherheit sieht vor, dass der „Safety Plan“, der „Safety Case“ sowie die Work Products „Software tool criteria evaluation report“ und „Software tool qualification report“ ebenfalls während der Konzeptphase angelegt werden müssen. Aus diesem Grund sind für diese Work Products ebenfalls Templates erstellt worden. Um eine Möglichkeit zu schaffen, intern selbst ein Review der Work Products durchführen zu können wurde außerdem vereinbart, Templates für jeweils ein allgemeines Confirmation- und ein Verification-Review zu erstellen.

Die konkrete Auswahl der zu erstellenden Templates dieser Arbeit umfasst dementsprechend:

- Item Definition
- Functional Concept / Functional Safety Concept
- Technical Concept / Technical Safety Concept
- Safety Plan
- Safety Case
- Confidence in the use of software tools
- Confirmation-Review
- Verification-Review

Auf die Grundlagen und Gemeinsamkeiten der Templates wird im nächsten Abschnitt genauer eingegangen.

## 6.2 Grundlagen

An dieser Stelle wird auch noch einmal darauf hingewiesen, dass es nicht Ziel war, das optimale Programm zur Erstellung der Templates zu finden, sondern man sich im Team darauf geeinigt hat, für die Erstellung der Templates auf das Tabellenkalkulationsprogramm Microsoft Excel zurückzugreifen. Die Gründe, die dafür gesprochen haben waren unter anderen, dass die entsprechenden Programm-Lizenzen allgemein im Unternehmen verfügbar sind. Außerdem sind die Mitarbeiter den Umgang mit Excel aus der täglichen Entwicklungsarbeit gewohnt und können die Templates selbstständig an die jeweiligen Bedürfnisse im Projekt anpassen. Des Weiteren können einfach fortlaufende Nummern an die „Requirements“ vergeben werden. Damit die Templates auch in internationalen Projekten verwendet werden können, sind die Templates in englischer Sprache verfasst und zur besseren Orientierung durchgehend mit Beispielen befüllt. Sonstige Gemeinsamkeiten der Templates sind nachfolgend zusammengefasst.

### 6.2.1 Aufbau

Aus Gründen der Übersicht und Nachverfolgbarkeit wird bei der Gliederung der Worksheets in den Templates eine grundsätzliche Struktur und Farbgebung allgemein beibehalten. Dies kommt dem Anwender insofern zu Gute, als dass die Umstellung von Template zu Template dadurch so gering wie möglich gehalten werden kann. Hinzu kommt, dass gewisse Inhalte einfacher übertragen werden können, falls es notwendig sein sollte. Folgender Aufbau wird daher für alle Templates angewendet, die jeweilige Befüllung unterscheidet sich aber naturgemäß je nach Work Product:

- „Hints“: Hinweisseite, als Hilfestellung zum richtigen Ausfüllen des Templates
- „Purpose of this document“: Seite, die den Sinn und Zweck des jeweiligen Dokumentes in Anlehnung an die ISO 26262 beschreibt
- „Coversheet“: Deckblatt mit Titel des Dokumentes, Name des Projektes, Bezeichnung des Items, Überblick über die verantwortlichen Rollen, Signaturmöglichkeit etc.
- „1_Formal“: Festlegung von Titel, Autor, Rollenverteilung, Statusvergabe
- „2_References“: Auflistung aller Referenzen des Dokumentes
- „3_Change_History“: Beschreibung der Änderungshistorie des Dokumentes
- „4_Abbreviations“: Liste mit allen Abkürzungen die im Dokument verwendet werden und der dazugehörigen Erläuterung

Alle weiteren Worksheets und Inhalte sind spezifisch und auf das jeweilige Work Product angepasst. Auf die Details wird in den nächsten Abschnitten genauer eingegangen.

### 6.2.2 Status der Dokumente

Die Freigabe von Dokumenten und die Vergabe eines dazugehörigen Dokumentenstatus spielen in der Praxis eine wichtige Rolle. Speziell dann, wenn nachgelagerte Dokumente auf zuvor festgelegte Inhalte zurückgreifen und stark davon abhängig sind. Daher ist es wichtig einen Status an ein Dokument zu vergeben, der Auskunft darüber gibt, ob ein Dokument für die weiteren Schritte freigegeben ist. Außerdem ist es auch wichtig klar festzulegen, welcher Status welche Bedeutung für die weitere Verwendung hat.

In den Templates können aus diesem Grund für jedes Dokument, je nach Fortschritt in der späteren Bearbeitung, folgende Status vergeben werden:

- „Template (empty)“: das Template wurde erstellt und ist mit Beispielen befüllt
- „Working“: das Template wird in einem Projekt zur Erstellung eines Work Products genutzt und gerade bearbeitet
- „Reviewed“: das Dokument ist überprüft worden
- „Released“: das Dokument wurde von den Verantwortlichen freigegeben

Verantwortlich für diese Statusvergabe ist grundsätzlich der ER-FSI, es sei denn es wurde etwas anderes vereinbart. Für die Statusvergabe von übergreifenden Dokumenten wie beispielsweise dem Safety Plan, ist der ER-FSM zuständig. An dieser Stelle wird auch darauf hingewiesen, dass die aufgezählten Status nur für diese Masterarbeit festgelegt wurden und keinen firmenintern definierten Dokumentenstatus entsprechen.

### 6.2.3 Status der Requirements

Ähnliches gilt auch für die Status von Requirements. Dies betrifft vor allem die sicherheitsrelevanten „Safety Requirements“. Aus diesem Grund wird für Requirements, die im Zuge des funktionalen und technischen Sicherheitskonzeptes angelegt werden, ebenfalls ein Status vergeben. Diese Notwendigkeit ergibt sich daraus, dass gewisse Requirements zuerst mit dem Kunden beziehungsweise dem Lieferanten abgestimmt werden müssen, bevor diese fixiert und für die weitere Entwicklung herangezogen werden können. Folgende Status können in den Templates an die Requirements vergeben werden:

- „Draft“: das Requirement wurde vorläufig erstellt
- „Internal reviewed“: das Requirement wurde intern überprüft
- „OEM reviewed“: das Requirement wurde durch den Kunden überprüft
- „Aligned with Supplier“: das Requirement wurde mit dem Lieferanten abgestimmt
- „Approved“: das Requirement wurde für die Weitergabe bestätigt
- „Dismissed“: das Requirement wurde verworfen und entfällt

Die Statusvergabe obliegt grundsätzlich wieder dem ER-FSI. Außerdem gilt hier ebenfalls wieder, dass diese Status nicht den firmenintern definierten entsprechen, sondern nur für die Masterarbeit festgelegt wurden.

### 6.2.4 Vercodung von Requirements

Ein weiterer wichtiger Aspekt ist die Nachverfolgbarkeit der Requirements. Dies wird in der Praxis oft auch als „Traceability“ bezeichnet. Um die Traceability gewährleisten zu können ist es notwendig, die einzelnen Requirements in den Templates eindeutig identifizieren zu können. Nachdem der entsprechende Code in den Templates manuell eingegeben werden muss und nicht automatisch vom System hinterlegt wird, wurde bei der Art der Vercodung bewusst darauf verzichtet, eine zu komplexe Systematik zu verwenden.

| Code | I | XXX | YYY | ZZZZZ |
|---|---|---|---|---|
| Beschreibung | Buchstabe I zur Itemzuordnung | 3 stellige Nummer - Itemnummer | 3 Buchstaben - Code für Dokument | 5 stellige Nummer - Nummerierung des Requirements |

Abbildung 20: Systematik der Vercodung von Requirements

Wie in Abbildung 20 ersichtlich, handelt es sich bei der gewählten Systematik um einen alphanumerischen Code, der sich aus folgenden Teilen zusammensetzt:

- I → stellt Bezug zu einem Item her
- XXX →3 stellige Nummer, schafft Zuordnung zum Item
- YYY →3 Buchstaben, Code für Zuordnung zum Dokument
- ZZZZZ → 5 stellige fortlaufende Nummer, zur Identifizierung des Requirements

Die einzelnen Teile werden jeweils durch einen Bindestrich getrennt. Abbildung 21 zeigt ein Beispiel, wie die Vercodung eines Requirements in einem Template aussieht.

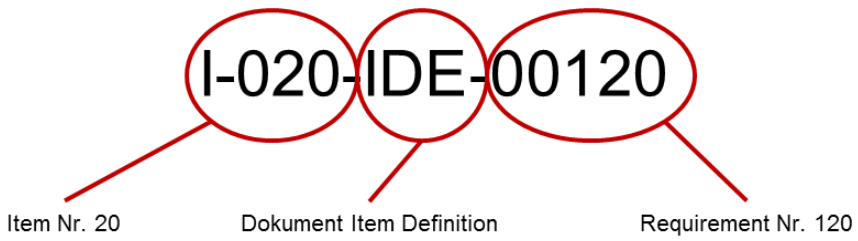


Abbildung 21: Beispielvercodung eines Requirements

In den Templates ist ein Bereich vorgesehen, in dem der Code manuell durch den ER-FSI eingetragen werden muss. Dieser Bereich ist so formatiert, dass der Anwender nur mehr den letzten Teil des Codes, die fortlaufende Requirement Nummer, selbst eingeben muss. Nach dieser Eingabe erscheint der vollständige Code automatisch.

Die gewählte Variante der Vercodung liefert alle wesentlichen Informationen auf den ersten Blick und stellt einen Kompromiss aus Komplexität, Informationsgehalt und Anwendbarkeit dar.

### 6.2.5 Attribute von funktionalen Requirements

Wie bereits kurz erwähnt, wird beim funktionalen und technischen Sicherheitskonzept, auch zwischen funktionalen und technischen Requirements unterschieden. Diesbezüglich unterscheiden sich natürlich auch die Attribute.

Ein funktionales Requirement besteht aus mehreren Attributen. Diese Attribute und damit die Informationen, die bezüglich des Requirements vorliegen, nehmen je nach Entwicklungsfortschritt immer mehr zu. Für die Templates wurden folgende Attribute festgelegt:

- „Traceability“: Zuordnung, wo das Requirement seinen Ursprung hat
- „Requirement ID“: eindeutige Identifikation des Requirements (siehe Abschnitt 6.2.4)
- „Functional Description“: Vollständige Beschreibung des Requirements
- „Allocation“: Zuordnung des Requirements zu einem Element der vorläufigen funktionalen Architektur
- „ASIL“: ASIL-Klassifizierung in Bezug auf das Gesamtsystem auf welches das Requirement allokiert ist
- „Status“: Status des jeweiligen Requirements (siehe Abschnitt 6.2.3)

Eine Übersicht und Beispiele für die Attribute von funktionalen Requirements sind in Abbildung 22 ersichtlich.

| Attribute | Traceability | Requirement ID | Functional Description | Allocation | ASIL | Status |
|---|---|---|---|---|---|---|
| **Description** | Links the requirement to a source. | In order to identify each requirement, a unique requirement ID has to be assigned. | Complete, unambiguous and clear functional description of the requirement. | Describes where the requirement is allocated. | Inherited ASIL level, if ASIL decomposition is performed give the original ASIL in brackets i.e. A (B). | Attribute to describe the current status of the requirement. |
| **Example** | I-XXX-IDE-ZZZZZ | I-XXX-ABC-ZZZZZ | FM-001 shall provide light modes [on, off, auto] according to the driver request | FM-001 | QM, A, B, C, D | Draft<br>Internal reviewed<br>OEM reviewed<br>Aligned with supplier<br>Approved<br>Dismissed |

Abbildung 22: Attribute der funktionalen Requirements

Wenn bei dem ASIL-Attribut QM eingetragen ist handelt es sich bei dem Requirement um ein rein funktionales. Sobald ein ASIL A oder höher eingetragen ist, handelt es sich um ein funktionales Safety Requirement.

### 6.2.6 Attribute von technischen Requirements

Wenn man die funktionale Ebene in Richtung der technischen verlässt, ist es nachvollziehbar, dass sich die Attribute der technischen Requirements von den funktionalen unterscheiden. Auf dieser Ebene geht es um die technische Realisierung der funktionalen Requirements. Diesbezüglich werden beispielsweise die Verifikation und ähnliches immer wichtiger. Dementsprechend umfassen die technischen Requirements folgende Attribute:

- „Traceability“: Zuordnung, wo das Requirement seinen Ursprung hat
- „Requirement ID“: eindeutige Identifikation des Requirements
- „Technical Description“: Technische Beschreibung des Requirements
- „Allocation to component“: Zuordnung des Requirements zu einer Komponente der vorläufigen technischen Architektur
- „ASIL“: ASIL-Klassifizierung in Bezug auf das Gesamtsystem auf welches das Requirement allokiert ist
- „Target Value“: Beschreibt einen Zielwert des Items
- „Comment“: Kommentarfeld für etwaige Anmerkungen
- „Status“: Status des jeweiligen Requirements

Die Attribute der technischen Requirements sind in Abbildung 23 dargestellt.

| Attribute | Traceability | Requirement ID | Technical Description | Allocation to component | ASIL | Target Value | Comment | Status |
|---|---|---|---|---|---|---|---|---|
| **Description** | Links the requirement to a source. | In order to identify each requirement, a unique requirement ID has to be assigned. | Complete, unambiguous and clear technical description of the requirement. | Describes where the requirement is allocated. | Inherited ASIL level, if ASIL decomposition is performed give the original ASIL in brackets i.e. A (B). | Describes a target value of the requirement in terms of e.g. FTTI, FIT | Possibility to make a comment concerning the requirement. | Attribute to describe the current status of the requirement. |
| **Example** | I-XXX-IDE-ZZZZZ | I-XXX-ABC-ZZZZZ | Light switch shall provide light modes [on, off, auto] according to the driver request | Light switch | QM, A, B, C, D | 10 FIT | None | Draft<br>Internal reviewed<br>OEM reviewed<br>Aligned with supplier<br>Approved<br>Dismissed |

Abbildung 23: Attribute der technischen Requirements

Analog zu den funktionalen Requirements handelt es sich bei einem ASIL QM um ein rein technisches Requirement und ab einem ASIL A um ein technisches Safety Requirement.

In den nächsten Abschnitten werden die einzelnen Templates beschrieben.

## 6.3 Item Definition

Die Item Definition ist ein Dokument, das unmittelbar vom ER-FSI verwaltet wird. Wie bereits erwähnt, dient die Item Definition grundsätzlich dazu, die kundenerlebbaren Funktionen auf Fahrzeugebene zu beschreiben. Diese Funktionen werden auch als Itemfunktion bezeichnet. Je nach Komplexität und dem angestrebten Detaillierungsgrad des Items, können diese Itemfunktionen noch in Unterfunktionen zerlegt werden. Es sollen außerdem ausreichend Informationen bereitgestellt werden, damit die weiteren Schritte des Functional Safety Lifecycle möglichst reibungsfrei durchgeführt werden können. In der Item Definition werden daher folgende Informationen festgehalten:

- Projekttitel
- Identifizierung des Items (Name und Nummer)
- Verantwortliche Personen (Autor, Projektleiter, Itemverantwortlicher)
- Versionsverwaltung (Version, Datum, Status, Änderungshistorie)
- Eingangsdokumente
- Beschreibung der kundenerlebbaren Funktion

- Zerlegung der Itemfunktionen in Unterfunktionen, falls notwendig
- Rechtliche Anforderungen in Bezug auf das Item (Gesetze, Regularien, Standards)
- Schnittstellen zu anderen Items
- Randbedingungen (Einsatzbereich, kritische Betriebszustände)
- Vorläufige Architektur, falls verfügbar
- Potenziell gefährliche Situationen, die relevant für die Gefahren- und Risikoanalyse sind

Abbildung 24 zeigt ausschnittsweise, wie die Eingabe der notwendigen Informationen erfolgt. Diese Informationen werden automatisch auf das Titelblatt sowie auf die Kopfzeile jedes Tabellenblattes übertragen.

| **Specification of cover sheet and header** | | |
|---|---|---|
| Document title | <Document_title> | |
| Project title | <Project_title> | |
| Identification of the Item | <Item_name> | <Item_number> |
| Status of the document | Template (empty) | |
| Current version and date | V0.1 | <dd.mm.yy> |

Abbildung 24: Festlegung von Titelblatt und Kopfzeile

In Abbildung 25 ist zu sehen, wie die verantwortlichen Rollen einer Person und der dazugehörigen Abteilung zugeordnet werden. Diese Informationen werden ebenfalls auf dem Titelblatt abgebildet.

| **Team members** | | |
|---|---|---|
| Role | Name | Department |
| Author of the document | <Author_name> | <Dept.> |
| Project Manager Engineering | <PM-E_name> | <Dept.> |
| Engineering Responsible Functional Safety Item | <ER-FSI_name> | <Dept.> |
| Technical Area Head of the Item Responsible | <TAH_name> | <Dept.> |

Abbildung 25: Festlegung der verantwortlichen Rollen

Ausgehend von den Anforderungen die ein OEM an ein Fahrzeug und somit an den Zulieferer stellt, gibt es unterschiedliche Dokumente, die als Eingangsdokumente vorliegen. Aus diesen gesammelten Informationen soll hervorgehen, welche Funktionen in einem Fahrzeug später verfügbar sein sollen.

Solche Dokumente umfassen zum Beispiel:

- Fahrzeug-Steckbrief
- Liste von Fahrzeugmerkmalen
- Anforderungsdefinitionen, Anforderungsschablonen
- Lastenheft
- Liste mit der Itemverantwortung

Aufgrund dieser Informationen wird zuerst festgelegt, in welchen Fachbereich die Verantwortung des Items fällt. Auf dieser Basis wird die Item Definition dann vom ER-FSI und seinem Entwicklungsteam erstellt. Der „Scope“ eines Item beschreibt, was das Item grundsätzlich für eine Funktion im Fahrzeug erfüllt und in welchem Anwendungsbereich es eingesetzt wird. Dies ist in Abbildung 26 beispielhaft dargestellt.

| **Scope of the item** |
| --- |
| *Give a short description of the item's scope.* |
| *e.g. Name: Electrical Parking Brake (EPB)*<br>*The item prevents the unintended movement of the vehicle during parking.* |

Abbildung 26: Möglicher Scope eines Items

Im nächsten Schritt werden aus dem Scope des Items die kundenerlebbaren Funktionen abgeleitet und an diese eine Identifikationsnummer vergeben (siehe Abschnitt 6.2.4). Diese Identifikationsnummer wird in weiterer Folge zur Funktionszuordnung herangezogen.

Neben den kundenerlebbaren Funktionen gibt es aber auch nicht-funktionale Anforderungen, die in der Item Definition festgelegt werden sollen. Diese nicht-funktionalen Anforderungen beschreiben unter anderem, in welcher Qualität und Güte eine kundenerlebbare Funktion ausgeführt werden soll. In welcher Zeit eine Funktion verfügbar sein soll, wäre beispielsweise eine nicht-funktionale Anforderung. Diese Informationen werden wiederum als Eingangsgrößen für die Gefahren- und Risikoanalyse herangezogen. Es ist also notwendig, sich schon am Beginn der Entwicklung über potenziell risikobehaftete Einsatzszenarien des Items Gedanken zu machen.

Die kundenerlebbaren Funktionen werden, falls es notwendig sein sollte, in Systemfunktionen zerlegt. Dies ist vor allem bei komplexeren Items und Funktionalitäten der Fall. Die Systemfunktionen beschreiben dann einzelne Teilfunktionen die innerhalb des Items ausgeführt werden. Diese sind dann allerdings nicht mehr direkt kundenerlebbare Funktionen. Um nicht den Überblick zu verlieren wird die Funktion auch grafisch beschrieben. Durch solche Beschreibungen werden Funktionen und die ausgetauschten Informationen grafisch abgebildet. Ein Beispiel, wie eine entsprechende Funktionsbeschreibung in den Templates durchgeführt wird, liefert Abbildung 27.

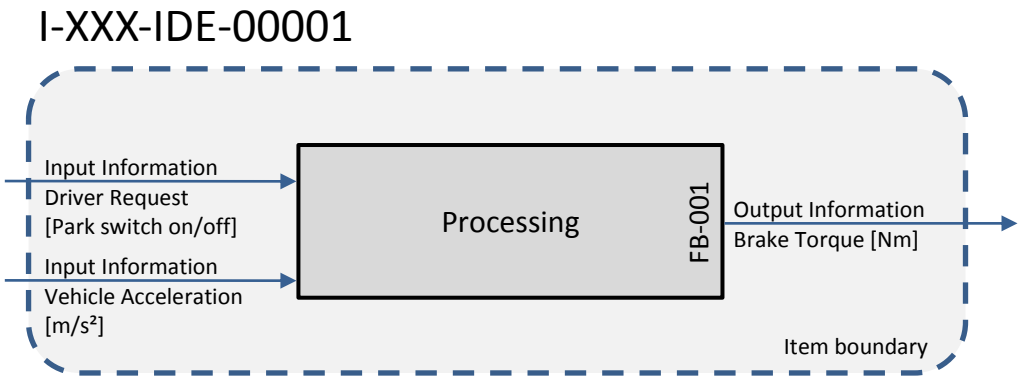


Abbildung 27: Grafische Funktionsbeschreibung

Die strichlierte Linie markiert dabei die Grenze zwischen den Elementen, die innerhalb des Items liegen und der außerhalb liegenden Umgebung. Innerhalb des Items gibt es mindestens eine Kette der Informationsübertragung, dies wird im englischen auch als „message-sequence-chain“ bezeichnet. Diese Kette besteht immer aus den Teilen „Input – Processing – Output“. Dabei wird eine Input-Information als Eingangsgröße über die Itemgrenze transportiert, in einem Funktionsblock verarbeitet und eine Output-Information als Ausgangsgröße wieder aus dem Item an die Umgebung übermittelt. Dieser Informationsaustausch umfasst immer eine Richtung und die jeweilige Information sollte in Bezug auf die transportierte Größe oder Einheit ebenfalls festgelegt werden. In der oberen Abbildung ist die grafische Funktionsbeschreibung einer elektrischen Parkbremse vereinfacht dargestellt. Die Funktion besteht dabei aus einem Funktionsblock mit den Eingangsgrößen „Driver Request“ und „Vehicle Acceleration“. Der Driver Request kann die Werte „Park switch on“ und „Park switch off“ annehmen und die Vehicle Acceleration wird in [m/s²] angegeben. Der Funktionsblock „FB-001“ verarbeitet diese Informationen und gibt schließlich das Signal „Brake Torque“ in [Nm] wieder aus.

Anhand dieser grafischen Funktionsbeschreibung wird eine erste Funktionsarchitektur erstellt, die dann in weiterer Folge, zuerst auf der funktionalen und dann auf der technischen Ebene, immer weiter spezifiziert wird. Wenn in der Item Definition alle notwendigen Informationen festgelegt wurden, wird anhand dieser Informationen die Gefahren- und Risikoanalyse durchgeführt. Diese Methode wird in Kapitel 3.2.3 beschrieben.

## 6.4 Functional Concept / Functional Safety Concept

Das funktionale Sicherheitskonzept wird, wie auch die Item Definition, vom ER-FSI erstellt. In diesem Work Product wird nun das Ziel verfolgt, bestimmte Sicherheitsmechanismen in das Item zu integrieren, um die Risiken im Fehlerfall minimieren zu können. Dabei wird von der vorläufigen Funktionsarchitektur der Item Definition und den Sicherheitszielen inklusive des dazugehörenden ASILs aus der Gefahren- und Risikoanalyse ausgegangen. Auf der Basis des durch die GuR erweiterten Wissensstandes wird zuerst das funktionale Konzept im Vergleich zu dem Konzept aus der Item Definition weiter verfeinert. Das bedeutet, dass die gesamte funktionale Architektur des Items in Funktionsblöcke und Funktionsmodule eingeteilt wird. Zwischen diesen Elementen findet der bereits erwähnte Informationsaustausch statt, der ebenfalls in der funktionalen Architektur abgebildet wird. Jeder Funktionsblock und jedes zusammengefasste Funktionsmodul wird nun in tabellarischer Form beschrieben. Ein Beispiel für die Beschreibung eines Funktionsblocks ist in Abbildung 28 dargestellt und gilt analog auch für Funktionsmodule.

| **Description of functional blocks** | | | | |
|---|---|---|---|---|
| *How is the item function built up? What function blocks are involved? The definitions of the function blocks in the columns "Input", "Processing", "Output" (= message sequence chain) shall be equivalent to the function architecture above.* | | | | |
| Block Nr. | Function block name | Input | Processing | Output |
| FB-001 | Define light mode | Driver request | Interpret the driver request as “light mode” information | Provide the selected light mode [*on, off, auto*] |

Abbildung 28: Beschreibung eines funktionalen Blocks

Aus diesen Elementen der funktionalen Architektur leiten sich wiederum funktionale Requirements ab, die in weiterer Folge anhand der vorher festgelegten Attribute beschrieben werden (siehe Abschnitt 6.2.5). Die funktionalen Requirements betreffen alle Elemente, die im Zuge der GuR mit dem ASIL QM eingestuft worden sind. Die

folgende Abbildung zeigt die Beschreibung eines funktionalen Requirements anhand eines Beispiels.

| **Functional requirements** | | | | | |
|---|---|---|---|---|---|
| *In the next step, functional requirements shall be described and allocated to each element of the functional architecture from above.* | | | | | |
| Traceability | Requirement ID | Description | Allocation | ASIL | Status |
| I-XXX-IDE-00001 | I-XXX-FSC-00001 | FB-001 shall provide Light mode [on, off, auto] information based on driver request. | FB-101 | QM | Draft |

Abbildung 29: Beschreibung eines funktionalen Requirements

Wenn das funktionale Konzept soweit fertiggestellt wurde, werden, falls es notwendig ist, alle sicherheitsrelevanten Safety Goals ab ASIL A verfeinert. Dies hat insofern praktische Relevanz, als dass mit der Festlegung der Architektur und dem zunehmenden Wissensstand in Bezug auf das gesamte Item, manche Safety Goals an die veränderten Bedingungen angepasst werden müssen.

Nun kommt der wesentlichste Teil, die Ausarbeitung des funktionalen Sicherheitskonzeptes zu jedem Safety Goal und die daraus resultierende Ableitung von funktionalen Safety Requirements. Dies ist eine sehr anspruchsvolle Tätigkeit, weil bei dieser Konzepterstellung eine Vielzahl von Informationen berücksichtigt werden müssen (funktionale Architektur, Fehlerbäume, Fehlertoleranzzeiten,…). Die Norm empfiehlt an dieser Stelle außerdem, mehrere Umsetzungsvarianten zu beschreiben. Diese Varianten sollen dann gegenübergestellt werden und die Begründung, warum welche Variante schlussendlich ausgewählt wurde, muss ebenfalls vorhanden sein. In weiterer Folge werden die Sicherheitsmechanismen beschrieben, die durch dieses Sicherheitskonzept realisiert werden. Dies beinhält ebenfalls wieder eine grafische Darstellung der Architektur, bei dem die beteiligten Elemente (Funktionsblöcke und Funktionsmodule) herausgehoben werden. Wenn es möglich ist, werden ähnliche Sicherheitsmechanismen zusammengefasst und die funktionalen Safety Requirements konsolidiert. Wenn das Functional Safety Concept fertiggestellt wurde, muss es in einem Verification-Review auf seine Vollständigkeit überprüft werden.

Die konsolidierten Safety Requirements und die konsolidierte funktionale Architektur dienen in weiterer Folge als Eingangsgrößen für die Erstellung des technischen Sicherheitskonzeptes.

## 6.5 Technical Concept / Technical Safety Concept

Das technische Konzept, beziehungsweise das technische Sicherheitskonzept, stellt die Überleitung von der funktionalen Architektur hin zur jeweiligen technischen Realisierung dar. Dementsprechend kommt es auch zu einer Überleitung der konsolidierten funktionalen Requirements hin zu den technischen Requirements beziehungsweise von den funktionalen Safety Requirements zu den technischen Safety Requirements. Abbildung 30 zeigt ausschnittsweise, wie von den funktionalen auf die technischen Requirements übergeleitet wird.

| **Functional Requirements (FR) / Functional Safety Requirements (FSR) out of consolidation** | | | | | | **Technical Requirements (TR) / Technical Safety Requirements (TSR)** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Traceability | Requirement ID | Functional Description | Allocation | ASIL | Status | Traceability | Requirement ID | Technical Description | Allocation to component | ASIL | Target Value | Comment | Status |
| I-XXX-IDE-00001 | *Illumination of the front of the car due to driver request* | | | | | I-XXX-IDE-00001 | *Illumination of the front of the car due to driver request* | | | | | | |

Abbildung 30: Überleitung der Requirements

Innerhalb dieser Elemente werden nun die Anteile an einem geforderten Zielwert, zum Beispiel einer Fehlertoleranzzeit die ein Element aufweisen darf, aufgeteilt. In diesem Zusammenhang spricht man auch vom sogenannten „Budgeting“. Ein Beispiel wie hier vorgegangen wird, zeigt Abbildung 31.

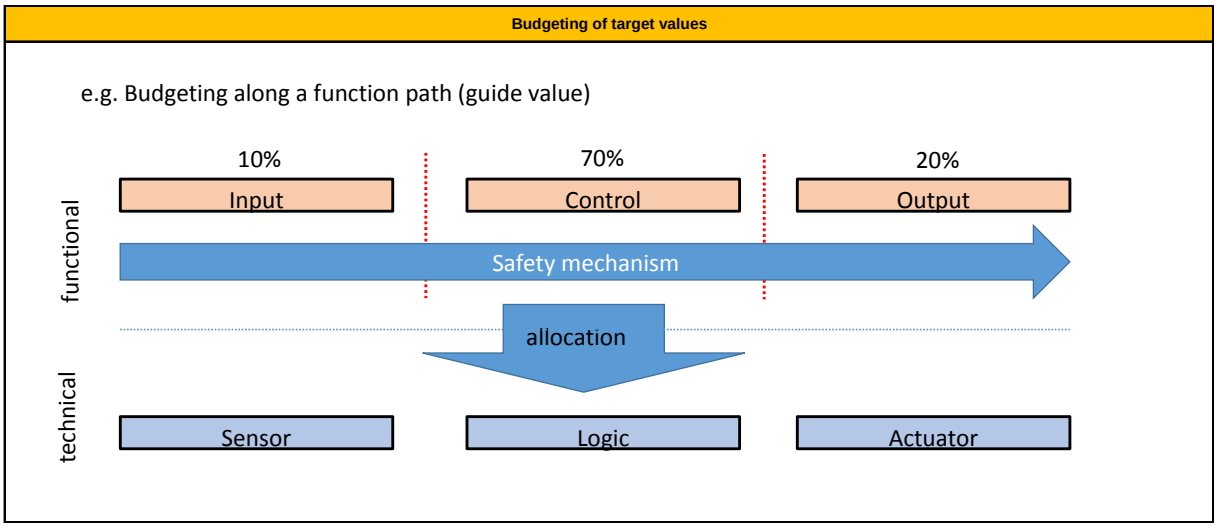


Abbildung 31: Aufteilung eines Zielwertes

Nach Abschluss des technischen Sicherheitskonzeptes wird gefordert, dass die Spezifikation der technischen Safety Requirements in einem Verification-Review auf die Vollständigkeit überprüft wird.

## 6.6 Safety Plan

Die Ausgangsbasis für den Safety Plan liefert der Safety Lifecycle bis SOP. Wie bereits erwähnt, sind im Safety Lifecycle bis SOP der grundsätzliche interne Prozess und die internen Aktivitäten der Funktionalen Sicherheit abgebildet. Außerdem findet man hier eine zeitliche Zuordnung, welche Work Products von welchen Rollen zu welchen Meilensteinen erstellt werden müssen. Der Safety Plan wird vom ER-FSM angelegt und verwaltet. Für die Planung von sicherheitsrelevanten Aktivitäten wird der Safety Lifecycle folgendermaßen erweitert:

**Übersicht zu den einzelnen Prozessschritten**

- Benennung der verantwortlichen Personen (OEM, Magna Steyr, Lieferant)
- Anpassung des vorgesehenen Meilensteins
- Dauer des zeitlichen Ablaufs (Geplanter Start, geplantes Ende)

**Übersicht der notwendigen Bestätigungsmaßnahmen**

- Höchste ASIL-Klassifikation innerhalb des Arbeitsproduktes
- Durchführungsverantwortung der Bestätigungsmaßnahme
- Dauer des zeitlichen Ablaufs (Geplanter Start, geplantes Ende)

**Sonstiges**

- Intern vorhandene Ressourcen zur Abarbeitung
- Kommentarfeld
- Datum des Kommentars

Abbildung 32 zeigt ausschnittsweise, wie die Planungen im Safety Plan Template grundsätzlich durchzuführen sind.

| Functional Safety Lifecycle | Overview of process specific process steps | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| | Responsibility | | | Tracking | | | | Final document / work product | |
| Work products | Responsible [OEM/MSE/ supplier] | Responsible [Name] | Responsible [Dept./Company] | Comment on progress of activity | Implemented Start Date | Implemented End Date | Status | Document ID | Link to document |
| 5.5.1 Organization-specific rules and processes for functional safety | MSE | Hr. Fusi | Fusihausen | Specific rules for fusa are already released and available | - | - | working | - | - |

Abbildung 32: Ausschnitt aus dem Safety Plan

In dem erstellten Template sind außerdem Bereiche für die Planung und Verfolgung der Confirmation- und Verification-Reviews integriert. Zusätzlich ist eine grafische Übersicht vorgesehen, die auf einen Blick Auskunft über die Vergabe und den Fortschritt aller durchzuführenden Aktivitäten und der zu erstellenden Work Products gibt. In einem Projekt muss der fertige Safety Plan in Form eines Confirmation-Reviews überprüft werden, ob er den Anforderungen der ISO 26262 entspricht.

## 6.7 Safety Case

Wie bereits erwähnt, liefert der Safety Case den Nachweis, dass ein Produkt den Anforderungen hinsichtlich der Funktionalen Sicherheit entspricht. Die Anforderungen werden dabei durch eine Argumentation mit dem Nachweis der Erfüllung, dem erstellten Work Product, verknüpft. Bei der gewählten Variante wurde bewusst gegen Methoden wie die GSN oder ähnliches entschieden, da man den Aufwand für die Erstellung des Safety Case so gering wie möglich halten möchte. Da allerdings auch kein Tool zur Verfügung steht, über das auf die Work Products und die dazugehörige Argumentation zugegriffen werden kann, muss für den Safety Case ein eigenes Dokument manuell angelegt werden. In Abbildung 33 ist ausschnittsweise dargestellt, wie der Safety Case in diesem Fall aufgebaut ist.

| Requirement | | Argumentation | Evidence | | |
|---|---|---|---|---|---|
| Part | Objective | Argumentation for achievement | Work Product (Filename) | Work Product (Link) | Status |
| | | | | | |
| 2 | Management of functional safety | | | | |
| 2-5 | Overall Safety Mangement | | | | |
| 2-6 | Safety management during the concept phase and the product development | | | | |
| 2-7 | Safety management after the item´s release for production | | | | |
| | | | | | |
| 3 | Concept phase | | | | |
| 4 | Product development at the system level | | | | |
| 5 | Product development at the hardware level | | | | |
| 6 | Product development at the software level | | | | |
| 7 | Production and operation | | | | |
| 8 | Supporting processes | | | | |
| | | | | | |

Abbildung 33: Ausschnitt aus dem Safety Case

Die Anforderungen des Safety Case ergeben sich aus der ISO 26262 und sind im Template in der Spalte „Requirements“ eingetragen. Es ist vorgesehen, dass zu jedem „Objective“ eine entsprechende Argumentation geliefert wird, dass die Anforderungen in ausreichendem Maße erfüllt werden. Diese Argumentation geht grundsätzlich aus dem dazugehörigen Work Product hervor und soll in Form einer kurzen Beschreibung in der Spalte „Argumentation for achievement“ zusammengefasst werden. Um abschließend auch den jeweiligen Nachweis anzuführen, wird im Abschnitt „Evidence“

der Name des Work Products mit der dazugehörigen Verlinkung eingetragen. Da der Safety Case ein Dokument ist, das während eines Projektes fortlaufend erstellt wird, ist außerdem ein Statusfeld integriert, wo der Dokumentenstatus (siehe 6.2.2) des Work Products eingetragen werden kann. Dies erleichtert die Übersicht, welche Nachweise gerade in Bearbeitung sind beziehungsweises welche Nachweise vielleicht sogar schon fertiggestellt wurden.

Wie eine entsprechende Argumentation in einem Safety Case durchgeführt werden kann, soll nun bespielhaft anhand des „Evidence of competence“ der involvierten Projektmitglieder beschrieben werden. Ein Argument für diesen Kompetenznachweis wäre zum Beispiel, dass alle beteiligten Projektmitglieder Schulungen zur Funktionalen Sicherheit besucht haben und Prüfungszertifikate vorlegen können. Diese Nachweise würden dann als Work Product eingetragen werden. Eine weitere denkbare Variante wäre, dass die Projektmitglieder bereits langjährige Erfahrung auf dem Gebiet der Funktionalen Sicherheit haben und zusammen bereits mehrere Projekte erfolgreich abgeschlossen wurden.

Wenn der Safety Case fertiggestellt wurde, muss er in einem Confirmation-Review auf seine Vollständigkeit hin überprüft werden.

## 6.8 Confidence in the use of software tools

Das Template „Confidence in the use of software tools“ umfasst die normativ geforderten Work Products „Software tool criteria evaluation report“ und „Software tool qualification report“. Dabei geht es darum, die im Lebenszyklus angewendeten Software-Tools zu identifizieren, zu klassifizieren und dem Einfluss des SW-Tools entsprechend auch zu qualifizieren. Dieser Ablauf ist überblicksweise in Abbildung 34 dargestellt.

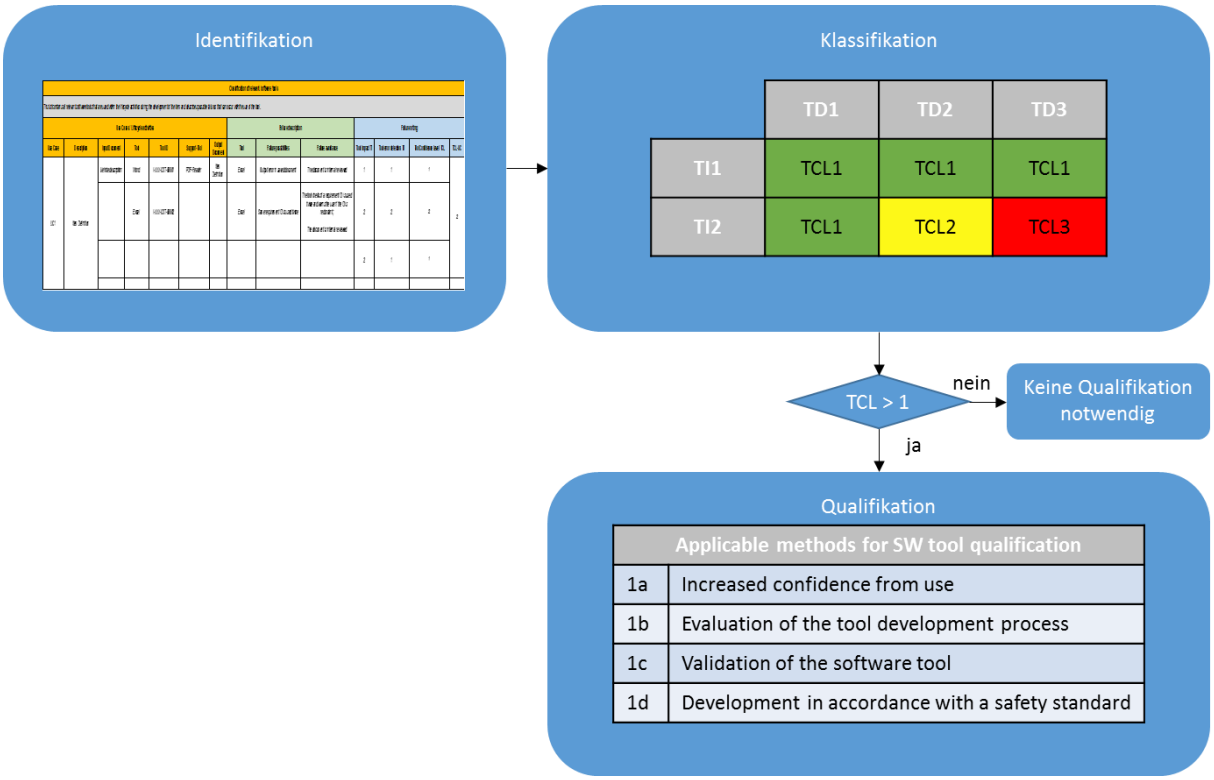


Abbildung 34: Identifikation, Klassifikation und Qualifikation von SW-Tools

In einem ersten Schritt werden dabei alle während eines Use-Case verwendeten Software-Tools identifiziert. Im nächsten Schritt werden mögliche auftretende Fehler beschrieben und diese Fehler je nach ihrer Auswirkung bewertet. Die Bewertungsklassen, die dabei eine Rolle spielen, sind der „Tool impact TI“ und die „Tool error detection TD“. Aus der Kombination dieser Werte ergibt sich das „Tool confidence level TCL“. Die höchste TCL-Bewertung eines Software-Tools über alle Use-Cases wird dann herangezogen um zu ermitteln, ob eine Tool-Qualifikation notwendig ist oder nicht. Die ISO 26262 listet dabei vier Methoden um die Qualifikation eines Software-Tools durchzuführen:

- Increased confidence from use
- Evaluation of the tool development process
- Validation of the software tool
- Development in accordance with a safety standard

Je nachdem welcher TCL-Wert ermittelt wurde, desto aufwändiger ist die anzuwendende Methode zur Qualifikation.

## 6.9 Confirmation-Review

Wie bereits in Kapitel 3.1.4.1 beschrieben, dient das Confirmation-Review der Überprüfung, ob ein Work Product grundsätzlich den Anforderungen der ISO 26262 entspricht. Das erstellte Template ist so aufgebaut, dass es in ausgefüllter Form den „Confirmation-Review Report“ darstellt. Einen groben Überblick, welche Prozessschritte ein Review beinhaltet, zeigt Abbildung 35.

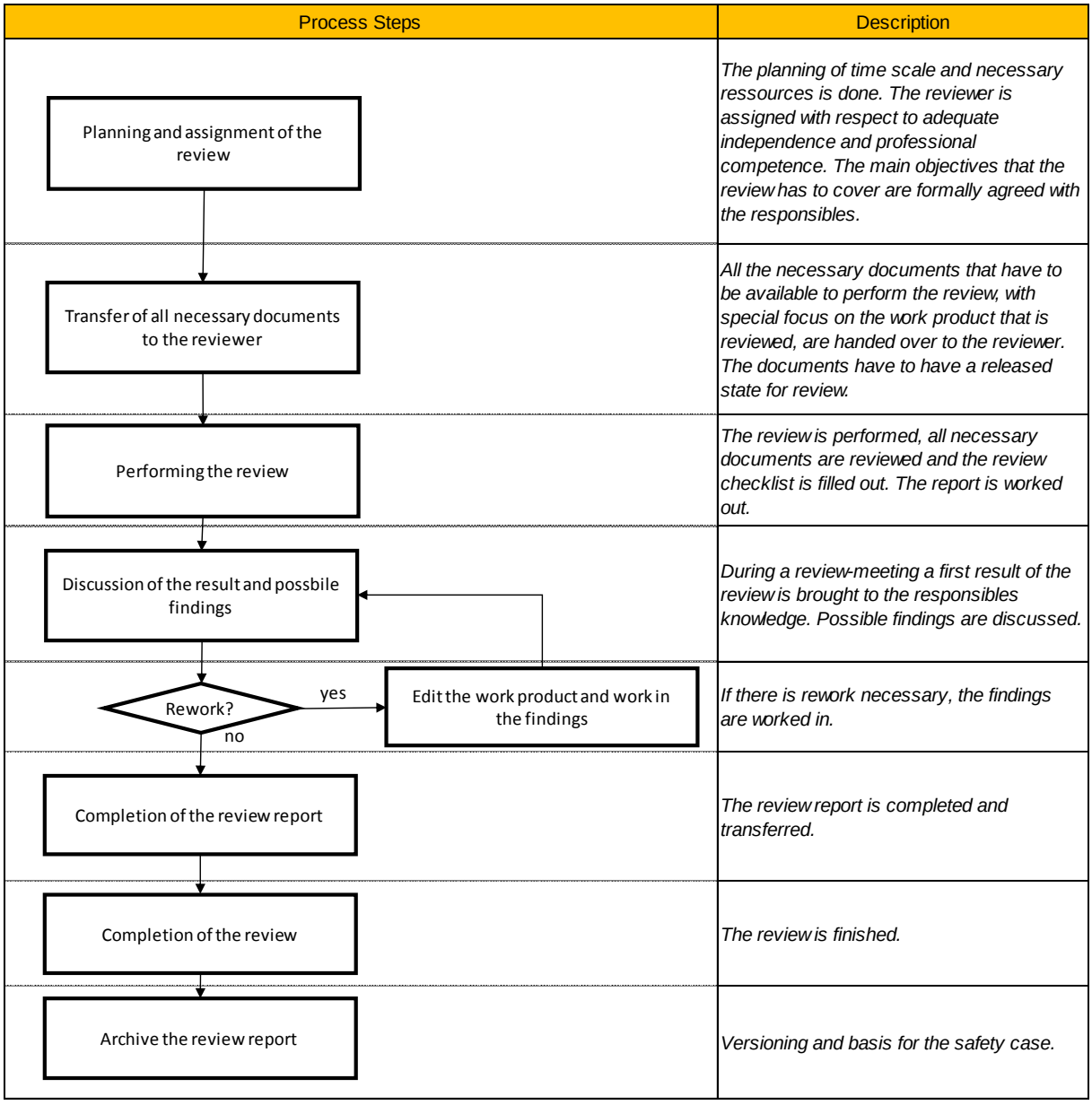


Abbildung 35: Prozessschritte eines Reviews

Bevor ein Review durchgeführt wird, kommt es zuerst zu einer Planung hinsichtlich des zeitlichen Ablaufs und der notwendigen Ressourcen. Dann werden die Ziele des

jeweiligen Reviews abgestimmt und festgehalten. Dies ist ausschnittsweise in Abbildung 36 dargestellt.

| **Objectives of this Confirmation Review** |
| --- |
| *The objectives and contents of this confirmation review should be described below.* |
| *e.g. Objective is to perform the required confirmation review of the hazard analysis and risk assessment in accordance with ISO 26262. Therefore this confirmation review checks:*<br>*- compliance with ISO 26262*<br>*- compliance with internal regulations* |

Abbildung 36: Mögliche Ziele eines Confirmation-Reviews

In weiterer Folge wird der Reviewer entsprechend der geforderten Unabhängigkeit und Qualifikation mit der Durchführung des Reviews beauftragt. Es kann sich dabei je nach Komplexität und Umfang auch um mehrere Personen handeln. Anschließend werden das zu überprüfende Work Product und alle zusätzlich notwendigen Dokumente an den Reviewer übergeben.

Nun wird das eigentliche Review durchgeführt. Zu diesem Zweck wird die Review-Checklist Punkt für Punkt abgearbeitet. Diesbezüglich ist die Checkliste in drei Bereiche unterteilt. Im Bereich „General“ werden allgemeine Punkte abgefragt, die ein Dokument gemäß internen und normativ geforderten Anforderungen erfüllen muss. Der Bereich „Specific requirements of ISO 26262“ ist dafür vorgesehen, dass er um Fragestellungen hinsichtlich spezifischer Inhalte eines Work Products ergänzt werden kann. Abschließend wird unter „Conclusive“ überprüft, ob der Review-Report vollständig ist.

Es ist vorgesehen, dass zu jeder Fragestellung eine Beurteilung und ein dazu gehöriger Status vergeben werden. Je nachdem ob es im vorliegenden Work Product bezüglich der Fragestellung eine Abweichung gibt, wird ein anderer Status vergeben. Eine Beschreibung der möglichen Status liefert Abbildung 37. Falls es keine Abweichung gibt, wird „no deviation“ eingetragen. Falls es eine Abweichung gibt, diese jedoch nicht zwangsläufig zu einem nicht-Bestehen des Reviews führt, handelt es sich um eine „minor deviation“. Wenn die Abweichung so schwerwiegend ist, dass das Review dadurch nicht bestanden wird, muss eine „major deviation“ festgestellt werden. Für den Fall, dass ein Punkt noch Unklarheiten umfasst, wird „to be clarified“ eingetragen.

| | | |
|---|---|---|
| Status description | no deviation | *There is no deviation concerning the requirement.* |
| | minor deviation | *There is a minor deviation concerning the requirement, rework on formal aspects necessary.* |
| | major deviation | *There is a major deviation concerning the requirement, rework is necessary in order to pass the review.* |
| | to be clarified | *The requirement has to be clarified.* |

Abbildung 37: Beschreibung zur Statusvergabe

Anhand der Abarbeitung aller Fragestellungen aus der Checkliste beurteilt der Reviewer, ob das Work Product das Confirmation-Review bestanden hat oder nicht. Dabei kann es vorkommen, dass nicht immer alle Fragen eindeutig beantwortet werden können. Aus diesem Grund ist diese Einschätzung teilweise sehr subjektiv und stark von der Qualifikation und Erfahrung des Reviewers abhängig. In jedem Fall muss das Ergebnis des Reviews durch ein Statement begründet werden. In diesem Statement sollten sowohl positive Aspekte, als auch mögliche Abweichungen genauer beschrieben werden.

Wenn vom Reviewer innerhalb des Work Products Abweichungen oder Lücken festgestellt wurden, ist eine Überarbeitung durch den ER-FSI und das Entwicklungsteam vorgesehen. In diesem Fall wird das Work Product überarbeitet und anschließend dem Reviewer zur neuerlichen Überprüfung vorgelegt. Für den Fall, dass keine Überarbeitung mehr notwendig ist, beschreibt der Reviewer in einer Zusammenfassung der Ergebnisse, dass das Review bestanden wurde. Dies ist ausschnittsweise in Abbildung 38 dargestellt.

| **Confirmation Review Summary** | |
|---|---|
| *According to the evaluation of the confirmation review checklist and based on the referenced documents, the reviewer assigns following state to the confirmed document:* | |
| X | Confirmation Review **passed**, state of document is accepted |
| | Confirmation Review **passed**, document rework on formal aspects is necessary |
| | Confirmation Review **not passed**, rework of content is necessary |

Abbildung 38: Ergebnis des Confirmation-Reviews

Abschließend wird der Review-Report fertiggestellt und an den ER-FSI übermittelt. Das Review ist dementsprechend abgeschlossen und der Review-Report wird von den verantwortlichen Personen signiert und vom ER-FSI archiviert.

An dieser Stelle soll noch einmal festgehalten werden, dass es beim Confirmation-Review eher um die Überprüfung der prozessmäßig korrekten Erstellung geht, als um die Vollständigkeit der Ergebnisse eines Work Products. Da, wie in Abbildung 5 ersichtlich, viele verschiedene Work Products einem Confirmation-Review unterzogen

werden müssen, liefert das erstellte Template einen allgemeinen Leitfaden hinsichtlich der Durchführung eines Reviews. Es kann in weiterer Folge um spezifische Fragestellungen (z.B. GuR, Safety Plan etc.) ergänzt werden, damit es zur Durchführung eines spezifischen Reviews herangezogen werden kann.

## 6.10 Verification-Review

Nachdem laut Norm im Vergleich zur „Confirmation“ teilweise andere Work Products einem „Verification-Review“ unterzogen werden müssen (siehe Abbildung 6) ist es sinnvoll, für beide Reviews auch unterschiedliche Templates zu erzeugen. Hinzu kommt, dass das Verification-Review den Zweck hat, zu überprüfen, ob ein Work Product den technischen oder projektspezifischen Anforderungen entspricht und ob inhaltlich alles vollständig ausgeführt wurde. Zusätzlich geht es darum die Durchgängigkeit und Vollständigkeit im Vergleich zu vorgelagerten Dokumenten zu überprüfen. Das bedeutet, dass zum Beispiel im Zuge des Verification-Reviews einer GuR auch überprüft wird, ob die getroffenen Annahmen mit denen aus der Item Definition übereinstimmen und sinnvoll sind. Die Ziele des Reviews sollten in jedem Fall zusätzlich noch einmal vereinbart werden. Dies ist beispielhaft in Abbildung 39 dargestellt.

| **Objectives of this Verification Review** |
| --- |
| *The objectives and contents of this verification review should be described below.* |
| *e.g. Objective is to perform the required verification review of the hazard analysis and risk assessment in accordance with ISO 26262.*<br>*Therefore this verification review checks:*<br>*- compliance with the item definition*<br>*- completeness with regard to situations and hazards*<br>*- completeness and coverage of the hazardous events*<br>*- consistency of the assigned ASILs with the corresponding hazardous events* |

Abbildung 39: Mögliche Ziele eines Verification-Reviews

Nachdem sich die beiden Reviews sonst allerdings nur bei den zu überprüfenden Work Products und den Fragestellungen der Checkliste unterscheiden, ist das „Verification-Review Template“ grundsätzlich gleich aufgebaut, wie das Confirmation-Review Template. Dementsprechend finden sich hier die bereits zuvor beschriebenen Abbildungen, nur mit anderer Überschrift, wieder. Die Fragestellungen der Checklist in dem Template orientieren sich an den in Teil 8 der Norm formulierten Fragestellungen in Bezug auf die Verifikation (ISO 26262-8, 2011, S. 24).

# 7. Anforderungen der Funktionalen Sicherheit

In diesem Kapitel sollen nun abschließend einige Anforderungen der Funktionalen Sicherheit zusammengefasst werden, die an die betroffenen Basisprozesse der Entwicklung gestellt werden, damit die Funktionale Sicherheit auch effizient umgesetzt werden kann.

## 7.1 Funktionsorientierte Entwicklung

Aus historischen Gründen ist die bauteilorientierte Entwicklung bei Fahrzeugherstellern nach wie vor sehr weit verbreitet. Diese Sichtweise war lange Zeit auch ausreichend, um die Kundenbedürfnisse erfüllen zu können. Aktuelle Entwicklungen in der Automobilindustrie können mit dieser Bauteilorientierung allerdings nichtmehr realisiert werden, da sie vielfach auf Funktionen beruhen, die oft auf mehrere Systeme verteilt sind. Die lösungsneutrale, funktionsorientierte Entwicklung ist daher vor allem am Anfang eines Entwicklungsprozesses ein wichtiger Faktor, um auf die konkreten Kundenbedürfnisse eingehen zu können und innovative Lösungen zu ermöglichen. Daraus ergeben sich weitere Vorteile wie zum Beispiel die Skalierbarkeit oder Übertragbarkeit von bereits ausgearbeiteten Systemen (Kaiser, Augustin, & Baumann, 2013, S. 7).

Wenn ein funktionsorientierter Entwicklungsprozess etabliert ist und gelebt wird, erleichtert dies wiederum die Durchführung von Aktivitäten der Funktionalen Sicherheit. Ein weiterer Aspekt ist, dass die ISO 26262 darauf basiert, dass die Systeme zuerst ausreichend funktional beschrieben werden. Daher ist die funktionsorientierte Entwicklung eine wichtige Voraussetzung, um die Anforderungen der Funktionalen Sicherheit erfüllen zu können.

## 7.2 Anforderungsmanagement

Neben der funktionsorientierten Denkweise spielt auch die korrekte Formulierung, Erfassung und Verwaltung von Anforderungen eine wichtige Rolle. Dies kann unter dem Begriff Anforderungsmanagement zusammengefasst werden. Seine Ursprünge hat das Anforderungsmanagement in der Softwareentwicklung. Wenn man sich aber wieder das V-Modell der Automobilindustrie vor Augen hält wird deutlich, dass es auf allen Abstraktionsebenen der Fahrzeugentwicklung Anforderungen gibt.

Aus den Kundenbedürfnissen auf oberster Ebene werden Anforderungen auf Fahrzeugebene abgeleitet und daraus ergeben sich wiederum Anforderungen die an die eingebauten Systeme und Komponenten gestellt werden. Daher ist es auch nachvollziehbar, dass die Anzahl der abgeleiteten Anforderungen mit zunehmendem Detaillierungsgrad der Entwicklung exponentiell zunimmt. Diese Anzahl liegt, noch ohne Berücksichtigung der Funktionalen Sicherheit, für aktuelle Straßenfahrzeuge schnell im oberen fünfstelligen Bereich. Ein weiterer Aspekt ist, dass diese Anforderungen auch miteinander verknüpft werden müssen, um die notwendige Nachverfolgbarkeit gewährleisten zu können.

Dieser Aufwand ist manuell fast nicht zu bewältigen und dementsprechend wichtig ist die Verwendung eines durchgängigen Anforderungsmanagementsystems, welches ein effizientes und vor allem fehlerfreies Arbeiten ermöglicht. Wenn diese Voraussetzung geschaffen ist, stellt die Integration von zusätzlichen sicherheitsrelevanten Anforderungen der Funktionalen Sicherheit kein großes Problem mehr dar. Dadurch können auch die Forderungen der ISO 26262 hinsichtlich der (formalen) Notation und vollständigen, atomaren Beschreibung und Traceability der Anforderungen relativ einfach erfüllt werden.

## 7.3 Konfigurationsmanagement

Das Vorgehensmodell des Functional Safety Lifecycle darf nicht als strikte Aneinanderreihung einzelner Teilschritte gesehen werden. Wie es in den meisten technischen Bereichen üblich ist, stellt das Modell einen iterativen Prozess dar, bei dem nachträgliche Adaptierung und Ergänzungen von zuvor getroffenen Annahmen unabdingbar sind. Aus diesem Grund bildet das Konfigurationsmanagement eine weitere wichtige Voraussetzung dafür, dass speziell bei verteilten Entwicklungen Klarheit darüber herrscht, welche Dokumente gerade den aktuellen Stand abbilden. Wichtig ist auch, dass die Dokumente zu jeder Zeit reproduziert werden können und dass die Änderungsstände der unterschiedlichen Versionen abrufbar sind. Daher sind das Versions- und das Änderungsmanagement ebenfalls Themen, die in diesem Zusammenhang relevant sind. Diese Aspekte können teilweise auch durch ein Anforderungsmanagementsystem abgedeckt werden.

## 7.4 Verifikation- und Validierungsplanung

Die Verifikation und Validierung spielt vor allem auf der rechten Seite des V-Modells, also bei der Integration von Systemen, eine wichtige Rolle. Die Voraussetzung für eine zuverlässige Verifikation ist die vollständige Systemspezifikation auf den definierten Abstraktionsebenen. (Wilhelm, Ebel, & Weitzel, 2015, S. 97). Ziel der Verifikation ist es, die Input/Output-Relation in den korrespondierenden Elementen des Produktes nachzuweisen (Wilhelm, Ebel, & Weitzel, 2015, S. 97). In diesem Zusammenhang muss vor allem anforderungsbasiert getestet werden um zu überprüfen, ob die Implementierung auch mit den Anforderungen übereinstimmt. Gemäß dem V-Modell stellt die Validierung eine Überprüfung auf oberster Ebene dar, ob das fertig entwickelte Produkt auch den Kundenanforderungen entspricht. Diese Überprüfungen werden aber auch für nicht-sicherheitsrelevante Produkte durchgeführt und sind daher allgemein in der Entwicklung ein wichtiges Thema. Dementsprechend sollte die Verifikation und Validierung in Bezug auf die Funktionale Sicherheit als ein Teil einer übergeordneten Verifikations- und Validierungsplanung gesehen werden, um dieses Thema zusammengefasst abdecken zu können.

## 7.5 Sicherheitskultur

Der Begriff Sicherheitskultur beschreibt wie in einem Unternehmen speziell mit der Entwicklung von sicherheitsrelevanten Produkten umgegangen wird. Aspekte, die in diesem Zusammenhang genannt werden müssen, sind die Führungskultur, das Sicherheitsbewusstsein, die Organisation und die Eskalationswege (Schnellbach, 2015, S. 15). Wenn in einem Unternehmen beispielsweise die Entwicklung von sicheren Produkten oberste Priorität hat und wirtschaftliche Aspekte eine eher untergeordnete Rolle spielen, dann spricht man von einer „guten“ Sicherheitskultur. In Teil 2 der ISO 26262 sind einige Punkte zusammengefasst, die auf eine gute oder schlechte Sicherheitskultur im Unternehmen schließen lassen. Um als Sicherheitsverantwortlicher seine Aufgaben korrekt erfüllen zu können, ist das Vorhandensein einer guten Sicherheitskultur im Unternehmen eine Grundvoraussetzung.

## 7.6 Erfahrung

Durch das interdisziplinäre Vorgehen und die vielen involvierten Teilbereiche bei der Entwicklung, ist die Erfahrung eine der wichtigsten Anforderungen der Funktionalen Sicherheit. Hinzu kommt, dass die ISO 26262 noch relativ neu ist und aus diesem Grund oft Anhaltspunkte und Erfahrungswerte fehlen, um gewisse Auswirkungen ausreichend abschätzen zu können. Diese Erfahrung und Kompetenz muss jedes Unternehmen für sich selbst aufbauen und kann hauptsächlich nur durch Projekte gewonnen werden, da Schulungen in diesem Zusammenhang nur begrenzt dazu geeignet sind, Wissen nachhaltig zu vermitteln.

# 8. Zusammenfassung

Im Zuge dieser Arbeit wurden einige Templates zu Work Products aus der Konzeptphase der Funktionalen Sicherheit erstellt, die sowohl die Anforderungen der ISO 26262 erfüllen, als auch den firmeninternen Anforderungen gerecht werden, die in der Einleitung beschrieben wurden.

Während der Literaturrecherche hat sich herausgestellt, dass es zwar einige theoretische Ansätze zur Erstellung von Work Products der Funktionalen Sicherheit gibt, jedoch praktische Beispiele in vielen Bereichen oft nicht verfügbar sind. Dies betrifft vor allem den, in einem Entwicklungsprojekt notwendigen Umfang und Detaillierungsgrad. Eine große Herausforderung für Unternehmen ist es also, die Anforderungen der Norm geeignet zu interpretieren und für das eigene Umfeld handhabbar zu machen, beziehungsweise unter Berücksichtigung der internen Gegebenheiten effizient umzusetzen (Dold & Trapp, 2007, S. 5). Insofern müssen Unternehmen hauptsächlich eigene Erfahrungen sammeln, um wirklich herauszufinden, welche Vorgehensweise zweckmäßig ist. Im Verlauf der Erstellung der Templates wurde deutlich, dass die Qualität der Templates erst durch die praktische Anwendung verbessert werden konnte. Ein wichtiger Teil der Arbeit war auch, dass die Erfahrungen die bisher in diversen Projekten gemacht wurden, unmittelbaren Einfluss auf die erstellten Templates hatten. Insofern war der direkte Kontakt und Austausch mit den Fachbereichsvertretern aus dem Kernteam ein wichtiger Aspekt der den Aufbau der Templates stark geprägt hat. Außerdem hat sich gezeigt, dass trotz vorhandener Ausfüllhilfen und einer Befüllung mit Beispielen, viele Fragen erst durch die gemeinsame Ausarbeitung beantwortet werden konnten.

Die konsequente Anwendung der Funktionalen Sicherheit verursacht vor allem am Beginn eines Entwicklungsprozesses einen Mehraufwand, der allerdings durch die bessere Qualität und andere Einsparungen zumindest wieder ausgeglichen werden kann (Armengaud, Griessnig, & Mader, 2012, S. 5). Ein weiterer Vorteil der sich ergibt, wenn einzelne Komponenten entsprechend den Anforderungen der ISO 26262 entwickelt werden ist, dass sozusagen als Nebeneffekt oft eine bessere Qualität und Zuverlässigkeit der Bauteile erreicht werden kann (Schnellbach, 2015, S. 18).

Zusammenfassend kann gesagt werden, dass die ISO 26262 von den OEMs und Zulieferern die Umsetzung einer höheren Systematik und eine gestiegene Formalität was die Arbeitsergebnisse betrifft einfordert. Bei durchgängiger Anwendung kann diese systematische Vorgehensweise allerdings auch unabhängig von der Funktionalen Sicherheit Verbesserungen bringen und den Entwicklungsprozess optimieren. In diesem Zusammenhang soll erwähnt werden, dass die auf Excel basierenden Templates gerade als Einstieg in die Thematik, beziehungsweise bei der Ausarbeitung von einfacheren Systemen, durchaus brauchbar sind. Jedoch soll nicht unerwähnt bleiben, dass im Hinblick auf die Entwicklung und Produktion von komplexeren Systemen die Templates recht bald an ihre Grenzen stoßen. Die Realisierung eines Gesamtfahrzeugprojektes wird ohne durchgehende Toolunterstützung nicht gelingen. Diesbezüglich gibt es am Markt einige Produkte, welche zwar in der Anschaffung unmittelbar hohe Kosten verursachen, jedoch kann man davon ausgehen, dass diese Kosten durch eine effizientere Entwicklung im Verlauf eines Projektes wieder kompensiert werden können.

# 9. Ausblick

Die Zahl der Verletzten Verkehrsteilnehmer sinkt von Jahr zu Jahr. Dies ist, neben vielen anderen Entwicklungen, vor allem auch auf die konsequente Anwendung der ISO 26262 im Bereich der Fahrzeugentwicklung zurückzuführen. Immer mehr Rückrufaktionen namhafter Hersteller im Automobilbereich zeigen allerdings, dass trotz der Anwendung der Norm, nach wie vor viele potentiell fehlerhafte Produkte in Umlauf gebracht werden. Die Tatsache, dass eben kein System fehlerfrei ist, rechtfertigt allerdings nicht, dass diese Fehler gerade bei sicherheitsrelevanten Systemen auftreten. Unterstützt von aktuellen Trends in Richtung Elektromobilität und integrierter Fahrzeugsicherheit werden Fahrzeugfunktionen außerdem immer umfangreicher. Warum in diesem Zusammenhang die Funktionale Sicherheit in Zukunft ebenfalls immer wichtiger wird, soll in Anlehnung an Adam Schnellbach noch einmal zusammengefasst werden (Schnellbach, 2015, S. 8):

- Zunehmende Anzahl der E/E-Komponenten im Auto
- Zunehmende Komplexität der Systeme
- Zunehmende Kritikalität der implementierten Funktionen

Dementsprechend ist es von hoher Wichtigkeit, dass vor allem sicherheitsrelevante Systeme mit größter Sorgfalt und dem Stand der Technik entsprechend entwickelt werden. Was die Mobilität der Zukunft betrifft, stehen wir vor einem Umbruch. Autonome Fahrzeuge und ähnliche Entwicklungen werden hoffentlich dazu beitragen, das Leben der Menschen zu erleichtern und helfen, den Straßenverkehr noch sicherer zu machen. Bevor diese Innovationen allerdings wirklich auf den Markt gebracht werden können, müssen noch viele Fragen beantwortet werden, die im Speziellen auch die Funktionale Sicherheit betreffen.

# Literaturverzeichnis


Armengaud, E., Griessnig, G., & Mader, R. (Oktober 2012). Innovative Ansätze für funktionale Sicherheit im Hybrid-Antriebsstrang. *ATZelektronik Volume 7*, S. 348–353.

Danzer, W. (2016). *Qualitätsmanagement in der Produkt- und Prozessentwicklung.* München: Carl Hanser Verlag.

Dietrich, B. (November 2010). Entwicklungsabläufe effizient steuern: Funktionsorientierte Entwicklung versus bauteilorientierte Entwicklung. *Hanser Automotive*, S. 82-84.

Dold, A., & Trapp, M. (2007). Herausforderungen und Erfahrungen eines OEM bei der Gestaltung sicherheitsgerechter Prozesse. *INFORMATIK 2007 Informatik trifft Logistik Band 2 Beiträge der 37. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 24. - 27. September 2007*, (S. 536-540). Bremen.

ISO 26262-1. (2011). *Road vehicles — Functional safety — Part 1: Vocabulary.* Genf: Internationale Organisation für Normung.

ISO 26262-10. (2011). *Road vehicles — Functional safety — Part 10: Guideline on ISO 26262.* Genf: Internationale Organisation für Normung.

ISO 26262-2. (2011). *Road vehicles — Functional safety — Part 2: Management of functional safety.* Genf: Internationale Organisation für Normung.

ISO 26262-3. (2011). *Road vehicles — Functional safety — Part 3: Concept phase.* Genf: Internationale Organisation für Normung.

ISO 26262-8. (2011). *Road vehicles — Functional safety — Part 8: Supporting processes.* Genf: Internationale Organisation für Normung.

Kaiser, B., Augustin, B., & Baumann, C. (Oktober 2013). Von der Komponenten- zur Funktionsorientierten Entwicklung in der Funktionalen Sicherheit. *Konferenz: Elektronik im Fahrzeug*, (S. 1-13). Baden-Baden.

Kelly, T., & Weaver, R. (2004). The Goal Structuring Notation – A Safety Argument Notation. *Department of Computer Science and Department of Management Studies*, 1-6.

Macher, G., Sporer, H., & Kreiner, C. (May 2015). Automotive Safety Case Pattern. *International Conference Proceedings Series (ICPS). jn 2, 3*, S. 1-18.

Ross, H.-L. (2014). *Funktionale Sicherheit im Automobil.* München: Hanser.

Rupp, C. (2014). *Requirementsengineering und -management.* München: Hanser.

Schmidt, M., Rau, M., Helmig, E., & Bauer, B. (August 2011). Funktionale Sicherheit – Umgang mit Unabhängigkeit, rechtlichen Rahmenbedingungen und Haftungsfragen. *SGS TÜV Saar*, S. 1-10.

Schnellbach, A. (18. November 2015). Funktionale Sicherheit im Automobil - Erfahrungen und Zukunftsperspektiven. *ÖVK-Vortrag TU Graz*, S. 1-34.

Sporer, H., & Brenner, E. (March 2016). An Automotive E/E System Domain-Specific Modelling Approach with Various Tool Support. *APPLIED COMPUTING REVIEW VOL. 16*, S. 1-10.

Stirgwolt, P. (28-31. January 2013). Effective management of functional safety for ISO 26262 standard. *Reliability and Maintainability Symposium (RAMS), 2013 Proceedings - Annual*, S. 1-6.

Wilhelm, U., Ebel, S., & Weitzel, A. (2015). Funktionale Sicherheit und ISO 26262. In H. Winner, S. Hakuli, F. Lotz, & C. Singer, *Handbuch Fahrerassistenzsysteme* (S. 85-102). Wiesbaden: Springer.

# Anhang

Der Anhang, der die erstellten Templates vollständig umfasst, wird aus Gründen der Geheimhaltung nur dem Magna Steyr Engineering Center zur Verfügung gestellt. Aus diesem Grund ist auch jede Vorführung, Vervielfältigung oder sonstige Verwendung ohne Genehmigung von Magna Steyr ausnahmslos verboten.