STUTTGARTER BEITRÄGE ZUR PRODUKTIONSFORSCHUNG

CHRISTOPH MAIER

Integriertes Modell zur Entwicklung von funktional sicheren Produkten in der Automobilbranche

Universität Stuttgart

Fraunhofer IPA

STUTTGARTER BEITRÄGE ZUR PRODUKTIONSFORSCHUNG BAND 23

Herausgeber:
Univ.-Prof. Dr.-Ing. Thomas Bauernhansl
Univ.-Prof. Dr.-Ing. Dr. h.c. mult. Alexander Verl
Univ.-Prof. a. D. Dr.-Ing. Prof. E.h. Dr.-Ing. E.h. Dr. h.c. mult. Engelbert Westkämper

Christoph Maier

Integriertes Modell zur Entwicklung von funktional sicheren Produkten in der Automobilbranche

FRAUNHOFER VERLAG

Kontaktadresse:
Fraunhofer-Institut für Produktionstechnik und Automatisierung IPA, Stuttgart
Nobelstraße 12, 70569 Stuttgart
Telefon 0711 970-00, Telefax 0711 970-1399
info@ipa.fraunhofer.de, www.ipa.fraunhofer.de

STUTTGARTER BEITRÄGE ZUR PRODUKTIONSFORSCHUNG

Herausgeber:
Univ.-Prof. Dr.-Ing. Thomas Bauernhansl
Univ.-Prof. Dr.-Ing. Dr. h.c. mult. Alexander Verl
Univ.-Prof. a. D. Dr.-Ing. Prof. E.h. Dr.-Ing. E.h. Dr. h.c. mult. Engelbert Westkämper

Fraunhofer-Institut für Produktionstechnik und Automatisierung IPA, Stuttgart
Institut für Industrielle Fertigung und Fabrikbetrieb (IFF) der Universität Stuttgart
Institut für Steuerungstechnik der Werkzeugmaschinen und Fertigungseinrichtungen (ISW)
der Universität Stuttgart

Titelbild: ©shutterstock.com

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.
ISSN: 2195-2892
ISBN (Print): 978-3-8396-0644-5

D 93

Zugl.: Stuttgart, Univ., Diss., 2013

Druck: Mediendienstleistungen des Fraunhofer-Informationszentrum Raum und Bau IRB, Stuttgart
Für den Druck des Buches wurde chlor- und säurefreies Papier verwendet.

Fraunhofer-Informationszentrum Raum und Bau IRB
Postfach 80 04 69, 70504 Stuttgart
Nobelstraße 12, 70569 Stuttgart
Telefon 0711 970-2500
Telefax 0711 970-2508
E-Mail verlag@fraunhofer.de
URL http://verlag.fraunhofer.de

GELEITWORT DER HERAUSGEBER

Produktionswissenschaftliche Forschungsfragen entstehen in der Regel im Anwendungszusammenhang, die Produktionsforschung ist also weitgehend erfahrungsbasiert. Der wissenschaftliche Anspruch der „Stuttgarter Beiträge zur Produktionsforschung" liegt unter anderem darin, Dissertation für Dissertation ein übergreifendes ganzheitliches Theoriegebäude der Produktion zu erstellen.

Die Herausgeber dieser Dissertations-Reihe leiten gemeinsam das Fraunhofer-Institut für Produktionstechnik und Automatisierung IPA und jeweils ein Institut der Fakultät für Konstruktions-, Produktions- und Fahrzeugtechnik an der Universität Stuttgart.

Die von ihnen betreuten Dissertationen sind der marktorientierten Nachhaltigkeit verpflichtet, ihr Ansatz ist systemisch und interdisziplinär. Die Autoren bearbeiten anspruchsvolle Forschungsfragen im Spannungsfeld zwischen theoretischen Grundlagen und industrieller Anwendung.

Die „Stuttgarter Beiträge zur Produktionsforschung" ersetzt die Reihen „IPA-IAO Forschung und Praxis" (Hrsg. H.J. Warnecke / H.-J. Bullinger / E. Westkämper / D. Spath) bzw. ISW Forschung und Praxis (Hrsg. G. Stute / G. Pritschow / A. Verl). In den vergangenen Jahrzehnten sind darin über 800 Dissertationen erschienen.

Der Strukturwandel in den Industrien unseres Landes muss auch in der Forschung in einen globalen Zusammenhang gestellt werden. Der reine Fokus auf Erkenntnisgewinn ist zu eindimensional. Die „Stuttgarter Beiträge zur Produktionsforschung" zielen also darauf ab, mittelfristig Lösungen für den Markt anzubieten. Daher konzentrieren sich die Stuttgarter produktionstechnischen Institute auf das Thema ganzheitliche Produktion in den Kernindustrien Deutschlands. Die leitende Forschungsfrage der Arbeiten ist: Wie können wir nachhaltig mit einem hohen Wertschöpfungsanteil in Deutschland für einen globalen Markt produzieren?

Wir wünschen den Autoren, dass ihre „Stuttgarter Beiträge zur Produktionsforschung" in der breiten Fachwelt als substanziell wahrgenommen werden und so die Produktionsforschung weltweit voranbringen.

Alexander Verl Thomas Bauernhansl Engelbert Westkämper

Integriertes Modell zur Entwicklung von funktional sicheren Produkten in der Automobilbranche

Von der Fakultät Konstruktions-, Produktions- und Fahrzeugtechnik

der Universität Stuttgart

zur Erlangung der Würde eines Doktors-Ingenieurs (Dr.-Ing.)

genehmigte Abhandlung

Vorgelegt von

Christoph Maier

aus Stuttgart

Hauptberichter:	Univ.-Prof. a.D. Dr.-Ing. Prof. E. h. Dr.-Ing. E. h. Dr. h. c. mult. Engelbert Westkämper
Mitberichter:	Univ.-Prof. Dr.-Ing. Bernd Bertsche

Tag der mündlichen Prüfung: 11. November 2013

Institut für Industrielle Fertigung und Fabrikbetrieb der Universität Stuttgart

2013

Vorwort des Autors

Die hier vorgelegte Arbeit ist während meiner Anstellung als wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Produktionstechnik und Automatisierung IPA in Stuttgart in der Abteilung Nachhaltige Produktion und Qualität entstanden. Zum erfolgreichen Abschluss dieser Arbeit hat eine Vielzahl von Menschen beigetragen, die mir persönlich und fachlich unterstützend zur Seite standen.

Besonders möchte ich mich bei Herrn Professor Dr.-Ing. Prof. E. h. Dr.-Ing. E. h. Dr. h. c. mult. Engelbert Westkämper, ehemaliger Institutsleiter des Fraunhofer-Institutes für Produktionstechnik und Automatisierung IPA, sowie Herrn Professor Dr.-Ing. Bernd Bertsche, Institutsleiter des Instituts für Maschinenelemente, für ihre Unterstützung, Förderung und Betreuung meiner Arbeit bedanken.

Ein weiterer Dank gebührt meinen Kolleginnen und Kollegen am Fraunhofer IPA, die durch ihre Hilfsbereitschaft und fachliche Diskussionen zur Vollendung der Arbeit beigetragen haben. Im Besonderen möchte ich Herrn Dr.-Ing. Alexander Schloske für seine hervorragende fachliche, methodische und menschliche Betreuung und Unterstützung sowie Förderung Dank aussprechen.

Bedanken möchte ich mich zudem bei den Hiwis und Studenten aus unserer Abteilung.

Nicht zuletzt möchte ich mich bei meiner Frau Bianca, meinen Eltern, meinen beiden Geschwistern und meinen Freunden für ihre uneingeschränkte Unterstützung und ihr Nachsehen in vielerlei Hinsichten in den vergangenen Jahren bedanken. Ohne euch wäre ich wohl nie so weit gekommen!

Stuttgart, den 15. November 2013

Christoph Maier

Kurzinhalt

Die neuen Anforderungen und Erwartungen der Kunden sowie der Norm ISO 26262 setzen die in der Automobil-Branche produzierenden Unternehmen verstärkt unter Druck, schnell und flexibel innovative und zugleich funktional sichere Produkte zu entwickeln. Dabei fordert die Norm die Erkennung von zufälligen elektrischen und elektronischen Fehlern und den anschließenden Übergang in einen sicheren Zustand. Ziel ist es, die Gefährdung der Insassen und anderer Verkehrsteilnehmer durch technische Fehler auf ein Minimum zu reduzieren.

Um diesen Anforderungen gerecht werden zu können, ist es notwendig, zu Beginn das Produkt und dessen Funktionen nachvollziehbar in das **A**utomotive **S**afety **I**ntegrity **L**evel (kurz ASIL) einzugruppieren. Zusätzlich ist eine abteilungs- und unternehmensübergreifende Interaktion mit den beteiligten Lieferanten aufzubauen, um Schnittstellen, Daten und Funktionen aufeinander abzustimmen. Dabei definiert das ASIL die Anforderungen an die Sicherheit.

Die erarbeitete Methodik greift deshalb drei Grundprobleme bei der Entwicklung mechatronischer Produkte im Kontext der ISO 26262 auf. Diese sind die zielmarktorientierte Festlegung des ASIL, das lieferantenübergreifende Handling von Schnittstellen sowie die durchgängige Umsetzung und Dokumentation von Requirements. Hierzu werden in der Arbeit die Einflussfaktoren auf das ASIL untersucht und in der Folge eine zielmarktabhängige Definition der Faktoren ermöglicht. Im weiteren Verlauf wurde dann auf Basis der **G**efahren- **u**nd **R**isikoanalyse (kurz GuR), erstellt mithilfe der **F**ehler**m**öglichkeits- und **E**influss**a**nalyse (kurz FMEA), eine IT-Architektur entwickelt und implementiert. Mit dieser werden die vorhandenen Daten der GuR in ein erweitertes Datenmodell überführt. Damit ist es möglich, Daten und Informationen lieferantenübergreifend zu nutzen. Das neue, modulare Modell beinhaltet alle wichtigen Informationen und Zusammenhänge sowie die Möglichkeit zur Dokumentation der Requirement-Umsetzung.

Die Vorgehensweise und das Modell wurden im Rahmen eines Forschungsprojekts im Bereich E-Mobility erprobt und validiert. Diese Validierung hat gezeigt, dass durch die Zentralisierung und Transparenz der Daten die Produktentwicklung stark beschleunigt, sowie die Fehlerzahl gesenkt und damit die Sicherheit erhöht werden konnte.

Short summary

The new demands and expectations of customers and the standard ISO 26262 forces companies in the automotive sector to fast and flexibly develop innovative, yet functional safe products. The standard postulates the requirement to detect random electrical and electronical faults in the products. If such a fault is detected, the product must be brought into a safe state to prevent damage to the passengers and other traffic participants.

To fulfill these requirements, it is necessary to define a transparent and traceable **A**utomotive **S**afety **I**ntegrity **L**evel (ASIL) classification at the beginning of the product development process, as well as to establish an exchange process for interfaces, data and functions across department and corporate boundaries. The ASIL defines the requirements for the functional safety.

The methodology developed has the goal to support and solve three of the main issues regarding the development of mechatronic products in context of ISO 26262. Those issues are the definition of an ASIL based on the target market, the handling of interface data across the complete development chain as well as to ensure a traceable and continuous implementation and documentation of requirements. This work analyzes the factors influencing the ASIL, which in consequence allows the definition of those factors with respect to the specific target market. In the further course of the work, an IT architecture based on the hazard and risk analysis (created with the **F**ailure **M**ode and **E**ffects **A**nalysis; abbr. FMEA) was developed and implemented. This IT concept transforms the FMEA data into a new, extended data model, which is capable of handling data across company boundaries. This enhanced and easily extendable data model can contain all relevant and important information and relationships, as well as the possibility to document the realization of requirements.

The approach and the model were validated within a research project in the field of e-mobility. The validation process has shown that the centralization and transparency of the data leads to an accelerated product development and to a reduced number of faults, which itself leads to higher level of safety.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Formelverzeichnis

Abkürzungsverzeichnis

A

AIS ..... Abbreviated Injury Scale
ASIL ..... Automotive Safety Integrity Level

B

BMS ..... Batterie-Management-System
bspw. ..... Beispielsweise
bzw. ..... Beziehungsweise

C

CAN ..... Controller Area Network
CARE ..... Computer Aided Requirements Engineering
CMMI ..... Capability Maturity Model Integration
CSS ..... Cascading Style Sheets

D

d. h. ..... das heißt
DC ..... Diagnostic Coverage
DIN ..... Deutsches Institut für Normung
DOM ..... Document Object Model

E

E/E ..... elektrisch, elektronisch
E/E/PE ..... elektrisch, elektronisch und programmierbar elektronisch
ECU ..... Electronic Control Unit
EN ..... Europäische Norm

F

FMEA ..... Fehlermöglichkeits- und Einflussanalyse
FSR ..... Fehlerbasierte System-Reaktionsanalyse

G

ggf. ..... Gegebenenfalls

H

HTML ..... Hypertext Markup Language

HV ..... High Voltage

I

IEC ..... International Electrotechnical Commission

J

JS ..... JavaScript

L

LFM ..... Latent-Fault Metric

LIN ..... Local Interconnect Network

M

MOST ..... Media Oriented Systems Transport

MS ..... Microsoft

O

OEM ..... Original Equipment Manufacturer

P

PC ..... Personal Computer

PDF ..... Portable Document Format

PEP ..... Produktentstehungsprozess

PKW ..... Personenkraftwagen

PMHF ..... Probabilistic Metric for random Hardware Failures

Q

QM ..... Quality Management

R

RE ..... Requirement Engineering
RE&M ..... Requirement Engineering & Management
RM ..... Requirement Management

S

SIL ..... Safety Integrity Level
SPFM ..... Single-Point-Fault Metric

U

u. U. ..... unter Umständen
UK ..... Unfallkategorie

V

VDA ..... Verband der Automobilindustrie
vgl. ..... Vergleiche

X

XML ..... Extensible Markup Language

Z

z. B. ..... zum Beispiel

1 Ausgangssituation

Die Realisierung komplexer Funktionen von mechatronischen Systemen schreitet unaufhaltsam voran. Sie sind aus unserem Alltag nicht mehr wegzudenken und werden in Zukunft stark zunehmen. Die Mechatronik beschäftigt sich dabei interdisziplinär mit dem Zusammenwirken mechanischer, elektronischer und informationstechnischer Elemente und Module in mechatronischen Systemen. [Czichos, H. 2008]

So soll es nach den Vorstellungen des Entwicklungschefs eines schwäbischen Automobilbauers künftig möglich sein, sich per mechatronischem Fahrerassistenzsystem (Autopilot) über Nacht in den Urlaub nach Italien fahren zu lassen. Sie drücken „Brenner“ und legen sich schlafen. [Weingartner, M. 2012]

Allein bis zum Jahr 2018 wird, wie Abbildung 1 zeigt, mit 244 Millionen ein nahezu verzehnfachter Absatz von Fahrerassistenzsystemen im Vergleich zu 2009 prognostiziert. [Focus Medialine 2008]

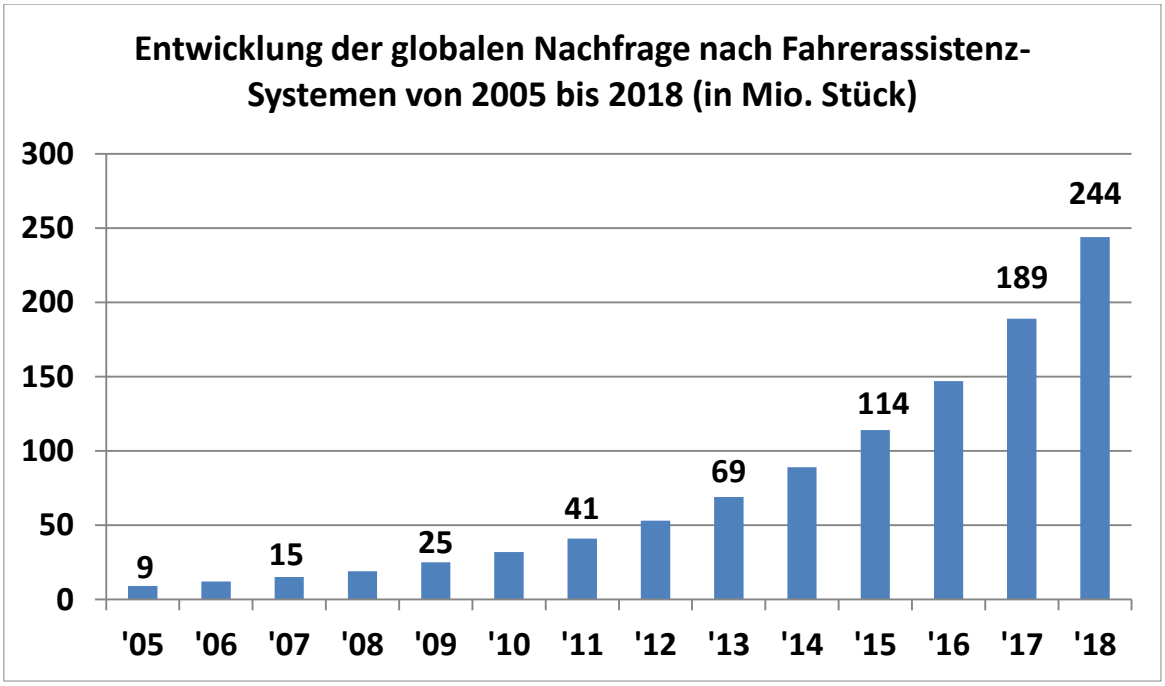


Abbildung 1 – Prognose der globalen Nachfrage von Fahrerassistenzsystemen bis 2018 [Focus Medialine 2008]

Allerdings erfordern mechatronische Systeme neue Ansätze in der Qualitätssicherung. Es ist dabei vor allem zu gewährleisten, dass durch Fehlfunktionen in den Systemen keine Gefahren für Menschen und an der Umwelt verursacht werden. [Westkämper, E.; Verl, A. 2008] Im Vordergrund steht dabei die Fähigkeit des elektrischen, elektronischen bzw. elektronisch programmierbaren Systems (E/E/PE-System), bei zufälligen und/oder systematischen Ausfällen mit Gefahr bringender Wirkung in einen sicheren Zustand überzugehen und dort zu verbleiben. Dieses Verhalten wird als „Funktionale Sicherheit“ bezeichnet. [Schloske, A. 2011b]

Der Trend zu Assistenz-, Regelungs- und Steuerungssystemen ist ungebrochen. In der Automobilbranche ist dies besonders in der Verkaufshistorie von Aktuatoren, Sensoren sowie Steuergeräten (**E**lectronic **C**ontrol **U**nit, kurz ECU) deutlich zu erkennen. Allein in den Jahren 2001 bis 2010 hat sich die Anzahl der abgesetzten Einheiten nahezu verdoppelt, wie Abbildung 2 zeigt. [Frost & Sullivan 2003]

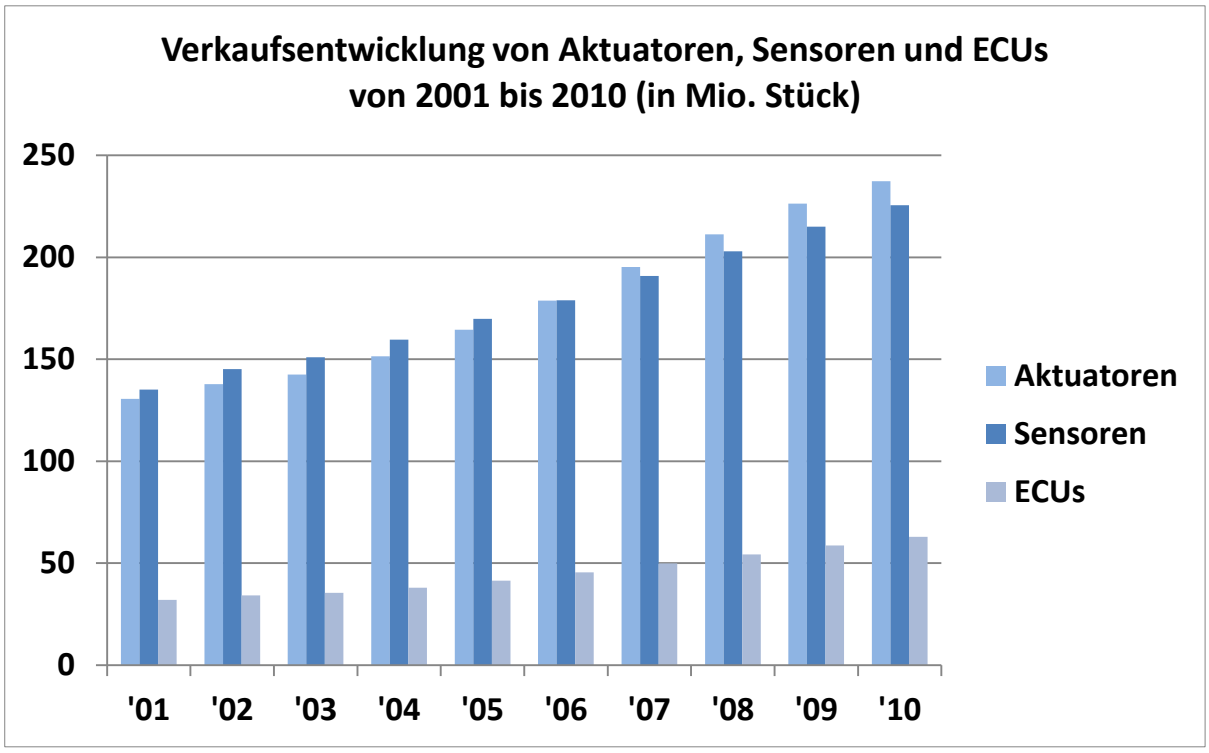


Abbildung 2 – Verkaufsentwicklung von Aktuatoren, Sensoren und ECUs von 2001 bis 2010 [Frost & Sullivan 2003]

Das Ziel der funktionalen Sicherheit ist es, die potenziellen Restrisiken auf ein unvermeidbares Maß zu reduzieren. Dabei müssen politisch vorgegebene, gesellschaftlich akzeptierte sowie gesetzliche und technisch mögliche Rahmenbedingungen beachtet werden.

Der Ursprung der funktionalen Sicherheit wird auf den Chemieunfall vom 10. Juli 1976 nahe Seveso (Italien) zurückgeführt. Der Überdruck im Reaktorkessel öffnete ein Sicherheitsventil, wodurch giftige, dioxinhaltige Gase in die Umwelt gelangten und ganze Landstriche für Jahrzehnte verseucht wurden. Dieses Unglück löste Normungsbestrebungen aus. Als Resultat ging die internationale Norm (IEC 61508) zur Entwicklung von sicheren elektrischen, elektronischen und programmierbar elektronischen Systemen (E/E/PE) hervor.

Auf Basis dieser Mutternorm IEC 61508, als Normenreihe DIN EN 61508 ratifiziert und übernommen im Juli 2001 [DKE 2002], entstanden nach und nach weitere Normen für spezifische Branchen, wie sie in Abbildung 3 dargestellt sind. [Schlummer, M. H. 2012]

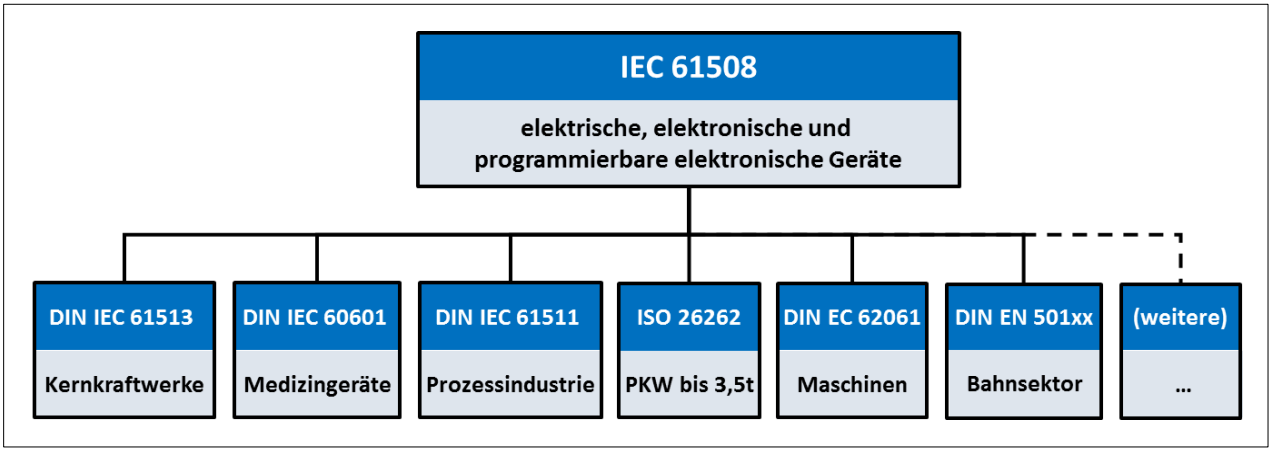


Abbildung 3 – Mutternorm IEC 61508 und Beispiele für abgeleitete Normen

Im Gegensatz zum Anlagenbau werden in der Automobilindustrie sehr hohe Stückzahlen produziert. Um unter anderem diesem Unterschied gerecht zu werden, wurde nach langjähriger Entwicklung am 29. Juni 2011, die an die Automotive-Bedürfnisse angepasste ISO 26262 mit der Bezeichnung „Road vehicles — Functional safety“ als „International Standard under publication“ im ISO-Komitee eingereicht und am 15. November 2011 in der finalen Version veröffentlicht.

Mit der Prozessnorm ISO 26262 versucht die Automobilindustrie der Sicherheit bei steigender Komplexität im Automobil sowie der erhöhten Nachfrage nach Fahrerassistenz-

Systemen gerecht zu werden. Durch diese Norm soll die Einhaltung, Durchführung und Dokumentation aller Entwicklungstätigkeiten, die für die funktionale Sicherheit bedeutend sind, gewährleistet werden. [ISO 26262-2 2011-11-15] Dabei legt die ISO 26262 Anforderungen an die Entwicklung mechatronischer Systeme hinsichtlich ihrer möglichen Fehler und Ausfälle fest. [ISO 26262-5 2011-11-15]

Der sich erhöhenden Komplexität mit der zunehmenden Kombination von einer Vielzahl unterschiedlicher Aktuatoren, Sensoren und Steuergeräten muss bei der Entwicklung Rechnung getragen werden. Hinzu kommen die Ansprüche an die geforderten Funktionalitäten. In diesem Zusammenhang soll die ISO 26262 mit ihren Entwicklungsrichtlinien und Anforderungen die Entwicklung der Systeme unterstützen. So waren bereits im Jahr 2008 in den Oberklassefahrzeugen zwischen 80 und 90 Steuergeräte sowie bis zu 150 Sensoren verbaut. [Richter, H. 2009], [Reif, K. 2011]

Abbildung 4 zeigt einige der integrierten Sensoren eines modernen Kraftfahrzeugs.

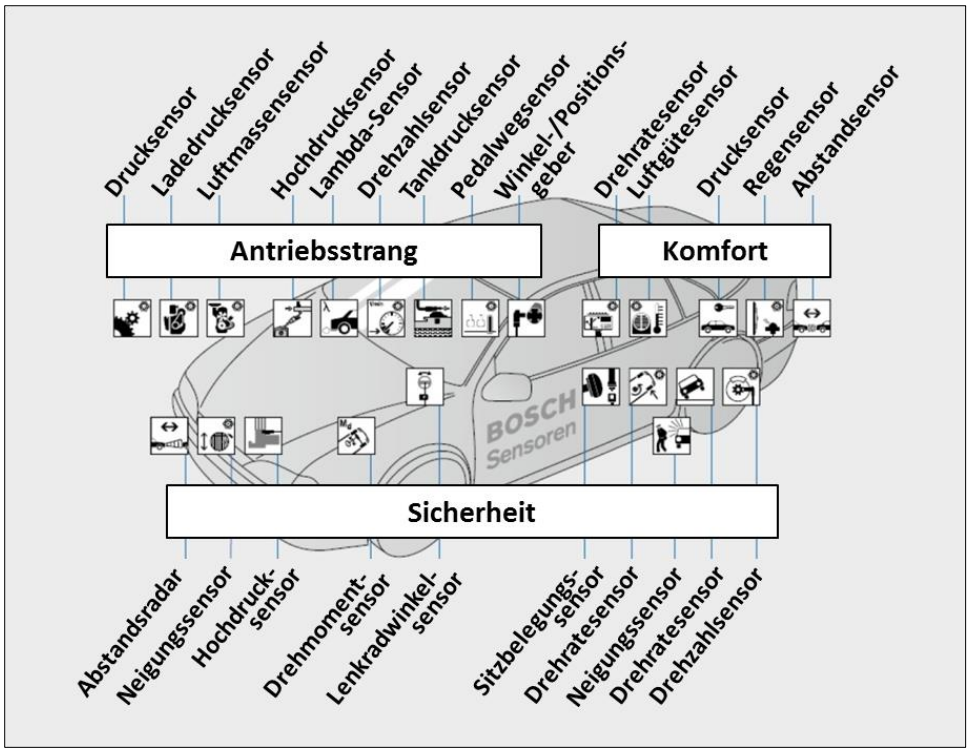


Abbildung 4 – Sensorübersicht eines KFZs [Reif, K. 2011] - modifizierte Darstellung

Während schon der Einsatz der zahlreichen ECUs eine Herausforderung darstellt, wird durch die zunehmend unternehmensübergreifende Zusammenarbeit und Produktentwicklung diese Entwicklungssituation weiter erschwert. Daher ist innerhalb der Entwicklung eine enge Koordination und Abstimmung notwendig.

In Abbildung 5 sind die Hersteller bzw. Zulieferer von ausgewählten Komponenten des im Jahr 2012 erschienen AUDI A3 (interne Typenbezeichnung 8V) aufgeführt. Daran ist zu erkennen, dass sehr viele Entwicklungspartner gemeinsam an Fahrzeugkomponenten arbeiten. [Pander, J. 2012]

Abbildung 5 – Wer liefert was? AUDI A3 (interne Typenbezeichnung 8V) [Pander, J. 2012] - modifizierte Darstellung

Wie wichtig und notwendig die Implementierung einer systematischen und risikominimierten Produktentwicklung ist, zeigen die nachfolgenden zwei Beispiele:

Renault musste im Jahr 2012 ca. 695.000 Fahrzeuge des Modells Scénic, siehe Abbildung 6, aufgrund eines Safety-Problems zurückrufen. Bei diesem Fahrzeug bestand die Gefahr, dass durch einen Fehler die elektromechanische Parkbremse spontan aktiviert, sprich angezogen wurde, obwohl der Fahrer sie nicht bediente. [Hoberg, F. 2010]

Abbildung 6 – Renault Scénic

Ein weiterer großer Automobilhersteller, Toyota, musste bereits 2010 ca. 373.000 Autos in die Werkstätten rufen. Das Lenkradschloss konnte sich durch einen Fehler während der Fahrt selbsttätig schließen und einrasten. Eine Lenkfähigkeit des Fahrzeugs war damit nicht mehr gegeben. [Baumann, U. 2010]

Wie Abbildung 7 zeigt, ist die Elektrik heutiger Fahrzeuge die Pannenursache Nummer 1. [ADAC e. V. 2012] Für sicherheitsrelevante mechatronische Systeme ist daher eine besondere Sorgfalt während der Entwicklung erforderlich.

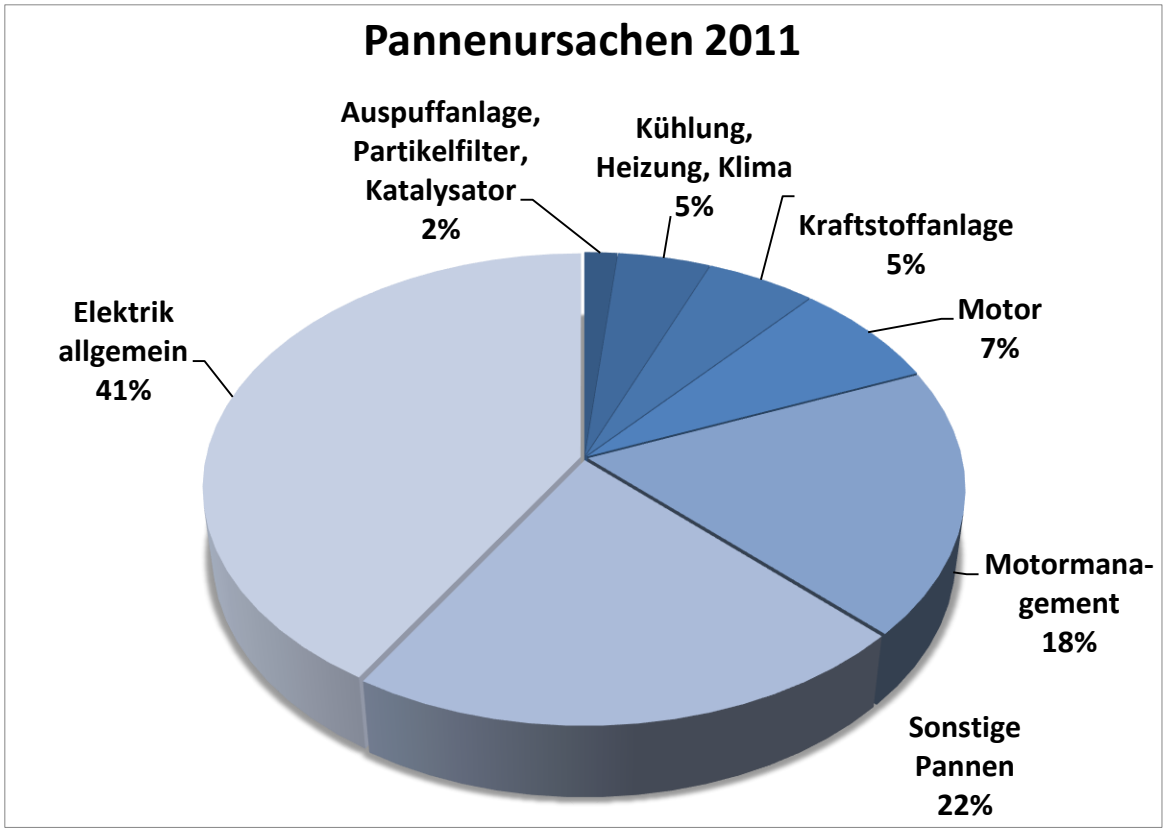


Abbildung 7 – Pannenursachen 2011 [ADAC e. V. 2012]

1.1 Problemstellung

Die Probleme bei der Entwicklung funktional sicherer Produkte sind vielfältig. Sie fangen in einigen Fällen bereits im ersten Gespräch des Unternehmens mit einem potenziellen Kunden (Automobilhersteller bzw. übergelagerter Zulieferer – nicht Endkunde) an. Auch nach Auftragserteilung ziehen sich verschiedene Probleme durch den gesamten Entwicklungsprozess des Produkts bis hin zur Serienfertigung und der Nutzungsphase. [Maier, C.; Schloske, A., et al. 2013] Die Mitarbeiter in den verschiedenen Unternehmensbereichen (Einkauf, Marketing, Verkauf, Entwicklung und Produktion) sind meist nicht für das Thema „Funktionale Sicherheit“ und dessen Einfluss bzw. Auswirkungen auf den Entwicklungsumfang und –aufwand sensibilisiert. Das Marketing bzw. der Verkauf sichert dem Kunden häufig die Erfüllung der Anforderungen aus der ISO 26262 zu, ohne die Anforderungen und die Konsequenzen für die Entwicklung solcher Systeme tatsächlich zu kennen. [Maier, C.; Schloske, A., et al. 2013] Im folgenden Entwicklungsverlauf muss dann mit knappen Ressourcen ein Produkt entwickelt werden, dessen Anforderungen und Entwicklungsaufwand merklich höher sind als bei einem konventionellen Produkt. [Schloske, A. 2011b] Dabei kommt auch die Tatsache zum Tragen, dass bereits bei der Entwicklung die Kosten für das Produkt maßgeblich beeinflusst werden. Das bedeutet, dass nachträgliche Änderungen den Produktpreis in die Höhe treiben und dass selbst bei Anwendung rationellster Fertigungstechniken, nur ein begrenzter Spielraum für die Reduzierung der Kosten besteht. [Westkämper, E. 2006]

Das Produkt muss nach der Entwicklung nicht nur allen Anforderungen seitens der Norm gerecht werden, sondern ebenso nach dem neuesten Stand der Wissenschaft und Technik konzipiert und ausgelegt sein, um beispielsweise etwaige Produkthaftungsansprüche abzuwenden. [OLG Jena 2009]

Vor dem Entwicklungsbeginn wird eine Risikoanalyse samt Sicherheitszielen für das zu entwickelnde System/Produkt benötigt. Die dort definierten Sicherheitsziele werden entweder vom Kunden vorgegeben oder selbst ermittelt. Für diese Ziele müssen in der Folge die **A**utomotive **S**afety **I**ntegrity **L**evel (kurz ASIL – siehe Seite 19) festgelegt und zugeordnet werden. Die notwendigen ASIL-Klassen werden der Norm entsprechend, anhand von drei Faktoren ermittelt. Jeder der drei Faktoren selbst besitzt verschiedene Abstufungen,

mit denen das ASIL beeinflusst werden kann. [ISO 26262-3 2011-11-15] Die ISO 26262 gibt hierzu Beispiele zur Einordnung der drei Bewertungsfaktoren an. Allerdings betrachtet die Norm bei den Einordnungsbeispielen nicht die Länder- oder Regionsspezifika. [ISO 26262-3 2011-11-15] Das kann dazu führen, dass Entwickler Länder- und Regionsspezifika annehmen, die aus ihrer persönlichen und subjektiven Sicht plausibel sind, jedoch bei objektiver Betrachtung von Dritten inkonsistent sein können.

Ein weiteres Problem tritt ein, wenn verschiedene Lieferanten einzelne Komponenten für ein Gesamtsystem/-produkt beisteuern, wie es in Abbildung 8 dargestellt ist.

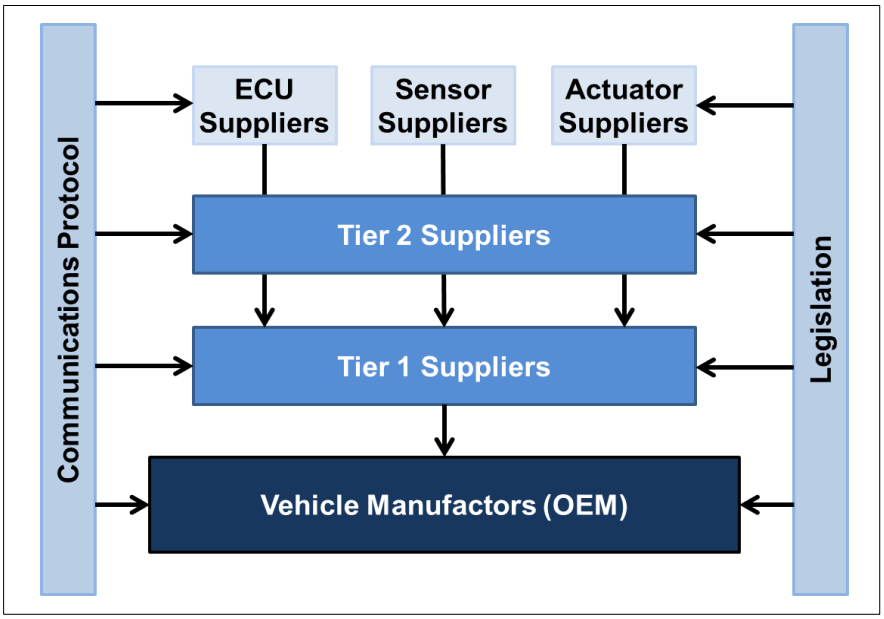


Abbildung 8 – Verteilte Entwicklung mechatronischer Systeme [Frost & Sullivan 2003]

Den Entwicklern fehlt hierbei der Blick auf das Gesamtsystem, dessen Schnittstellen sowie das Verhalten der anderen Teilsysteme bei Aktionen ihres Systems. Daher ist die Abstimmung untereinander eine wichtige Entwicklungsgrundlage. Selbst ein nach der ISO 26262 entwickeltes (Teil-) System kann durch fehlerhaft ausgelegte Schnittstellen beeinträchtigt und in seiner Funktion gestört werden. Im Extremfall entsteht durch eine mangelhafte Schnittstellendefinition und –rechtevergabe eine gefährdende Situation für Insassen und andere Verkehrsteilnehmer. [ISO 26262-8 2011-11-15]

Nicht zuletzt stellt bei der Entwicklung des Systems der Kunde selbst (Automobilhersteller oder höher gelagerte Zulieferer – nicht der Endkunde) häufig ein Problem dar. Er ist sich oft aufgrund der Komplexität sowie den Abhängigkeiten von weiteren Teilsystemen zu Beginn der Entwicklung nicht über alle notwendigen Funktionen, Anforderungen und Schnittstellen zu anderen Systemen im Klaren und passt diese daher über den Projektzeitraum weiter an (dynamisches Lastenheft). Diese „Change Requests“, zu Deutsch „Änderungsanforderungen“, müssen umgesetzt und dokumentiert werden. Sie führen häufig zu geänderten internen Anforderungen und damit zu erhöhten Kosten, was zu Projektverzögerungen oder -abbrüchen führen kann (siehe Abbildung 9).

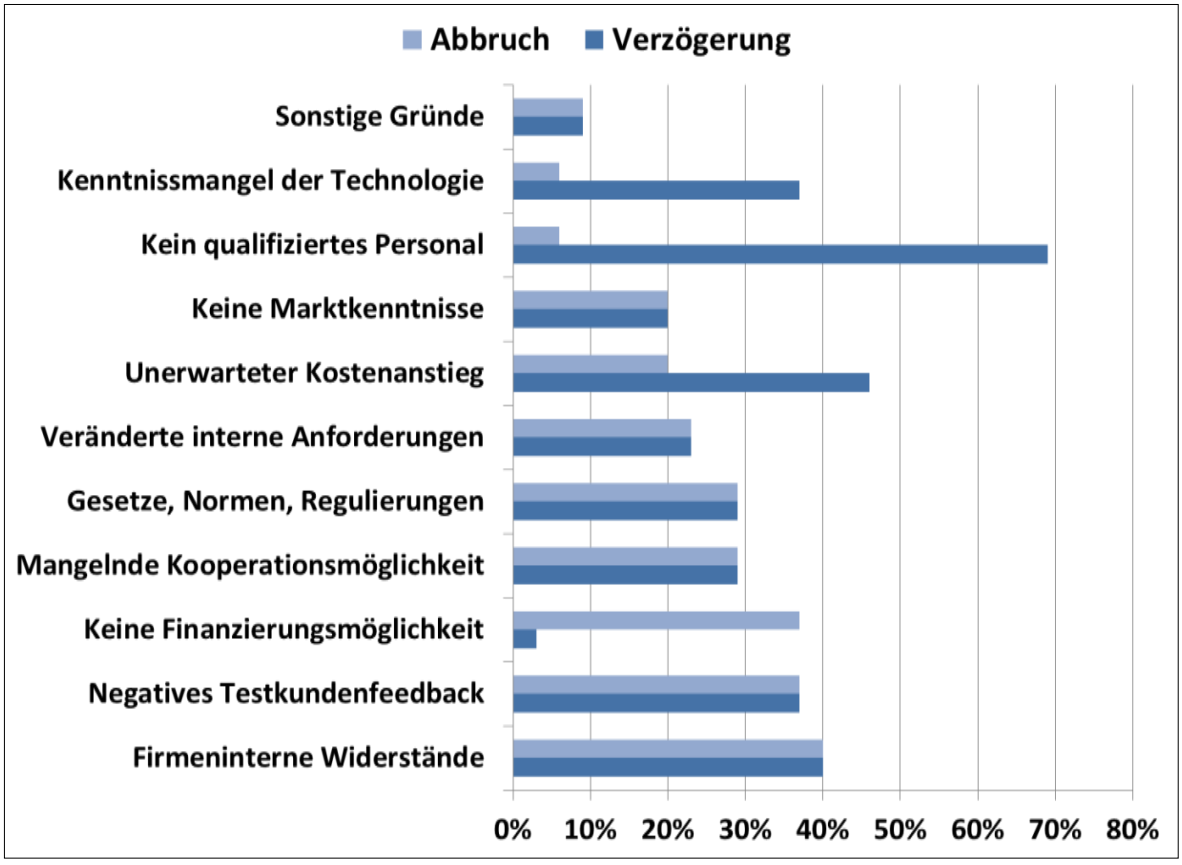


Abbildung 9 – Gründe für Projektverzögerungen und -abbrüche in der Automobilindustrie (Januar 2005 KPMG) - modifizierte Darstellung

Selbst wenn das Produkt schließlich entwickelt, produziert und vertrieben wird, können weitere Probleme entstehen. Zum Beispiel kann durch die Abkündigung eines elektroni-

schen Bauteils oder beim Wechsel auf ein kostengünstigeres, alternatives Bauteil, das erarbeitete Sicherheitskonzept und dessen Sicherheitsintegrität in der Funktion beeinträchtigt werden.

Zuletzt müssen die im Projekt gefällten Entscheidungen, die Entwicklungsarbeit, die Tests sowie sonstige Unterlagen und Dokumente übersichtlich, nachvollziehbar und revisionssicher abgelegt werden. [ISO 26262-8 2011-11-15] Im Fall eines Produkthaftungsprozesses stellen diese Dokumente eine Rückversicherung dar und ermöglichen vor Gericht nachzuweisen, dass systematisch und nach dem Stand der Wissenschaft und Technik gearbeitet wurde.

In der nachfolgenden Zusammenfassung zeigt sich, dass die Entwicklung von funktional sicheren Produkten und Systemen durch eine Vielzahl von Problemen sowie Aufgaben behindert und erschwert werden kann [Maier, C.; Schloske, A., et al. 2013]:

- Keine Sensibilisierung der Mitarbeiter zum Thema „Funktionale Sicherheit“
- ASIL-Klassifizierung länder- und regionsabhängig und damit uneinheitlich, unübersichtlich und nicht nachvollziehbar
- Schnittstelleninformationen nicht oder nur unzureichend vorhanden
- Keine Betrachtung des Produkts über den gesamten Lebenszyklus
- Keine klare Definition der Kundenanforderungen/-spezifikation (dynamisches Lastenheft)
- Hoher Dokumentationsaufwand zur durchgängigen Darstellung der Entscheidungen notwendig

1.2 Zielsetzung und Lösungsansatz

Aus den oben genannten Anforderungen und Defiziten leitet sich die Zielsetzung der vorliegenden Arbeit ab. Es sollen Methoden und Ansätze entwickelt werden, die die verantwortlichen Personen in die Lage versetzen, funktional sichere Produkte bzw. Systeme unter Beachtung der relevanten Rahmenbedingungen nachvollziehbar zu entwickeln und zur Marktreife zu bringen.

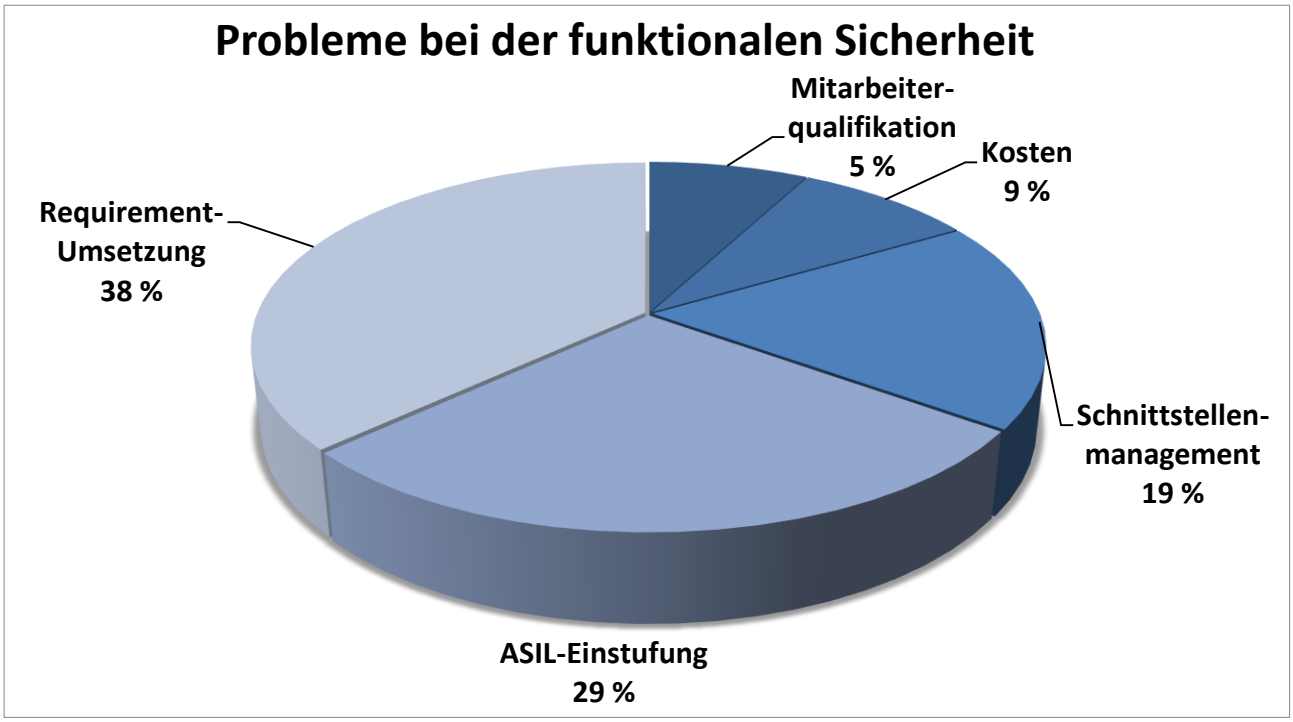


Abbildung 10 – Probleme bei der Entwicklung funktional sicherer Systeme [Maier, C.; Schloske, A., et al. 2013]

Hierbei sollen fokussiert für die folgenden drei Aufgabenstellungen Lösungen erarbeitet werden, die die Hauptprobleme, wie in Abbildung 10 gezeigt, bei der Entwicklung darstellen:

- Konzeption einer nachvollziehbaren ASIL-Einstufung unter Betrachtung von Länder- und Regionsspezifika, um im Produkthaftungsfall die Entscheidung für die ASIL-Klassifizierung sicher zu machen.
- Die Beschreibung eines Ansatzes zur Abstimmung der Systemschnittstellen zwischen Kunde und Entwickler. Des Weiteren sollen die Schnittstellen zu den ande-

ren Systemen im KFZ betrachtet werden, um Störungen und Fehlfunktionen zu verhindern.

- Die Entwicklung einer Herangehensweise zur systematischen und durchgängigen Umsetzung sowie Dokumentation der Anforderungen (z. B. Testing, Maßnahmentracking) unter Berücksichtigung der Norm-Anforderungen.

Ziel muss es sein, ein vereinheitlichtes und systematisches Vorgehen für die Entwicklung von funktional sicheren Produkten hinsichtlich deren gesamten Lebenszykluses im Unternehmen zu implementieren und zu verankern (siehe Abbildung 11). Zusätzlich müssen die Schnittstellen zum Kunden als auch zu anderen Teilsystemen im Automobil standardisiert werden.

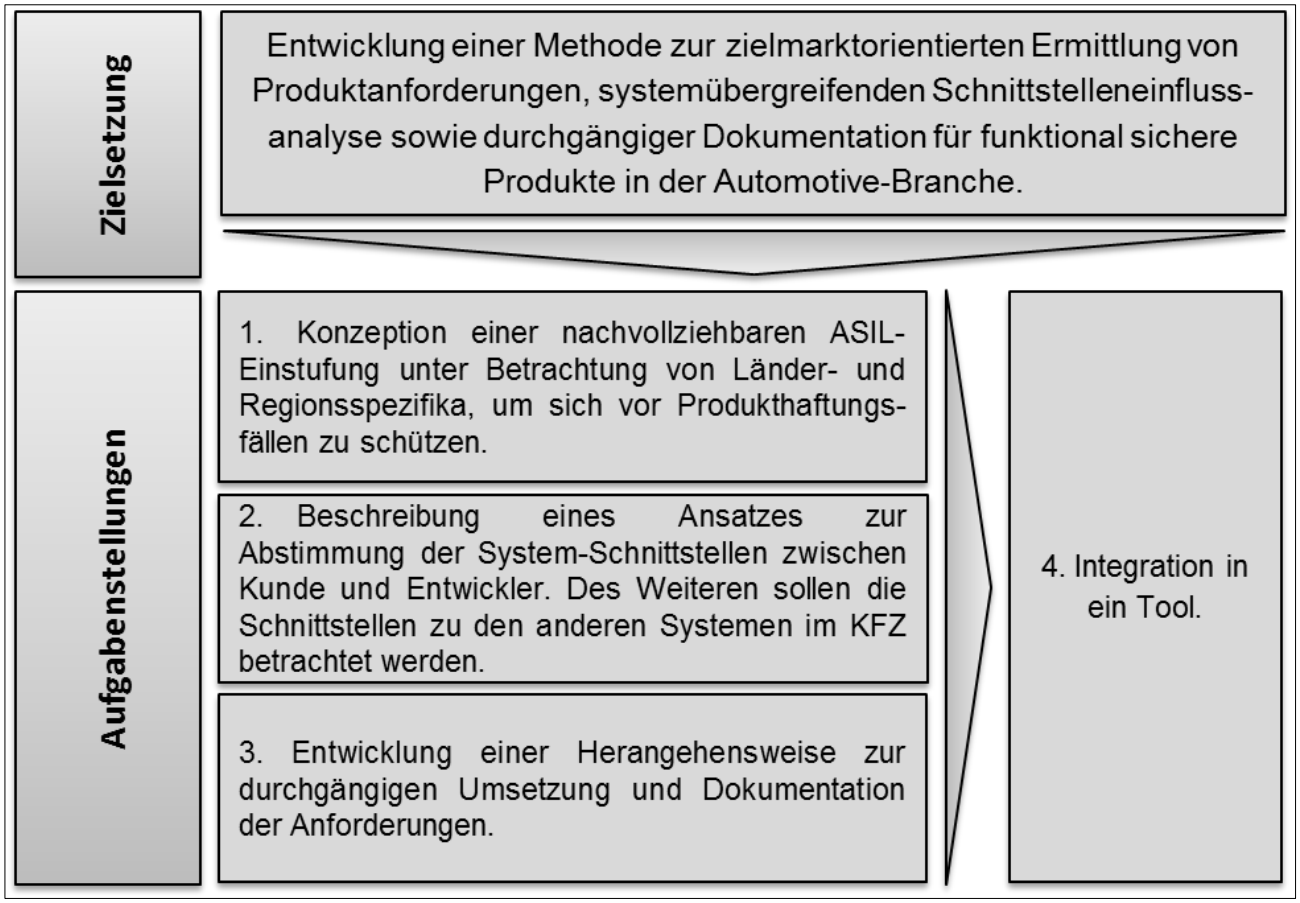


Abbildung 11 – Zielsetzung sowie Aufgabenstellung

1.3 Aufgabenstellung

Die in dieser Arbeit formulierten Aufgabenstellungen sollen in sechs Kapiteln, wie Abbildung 12 zeigt, bearbeitet werden.

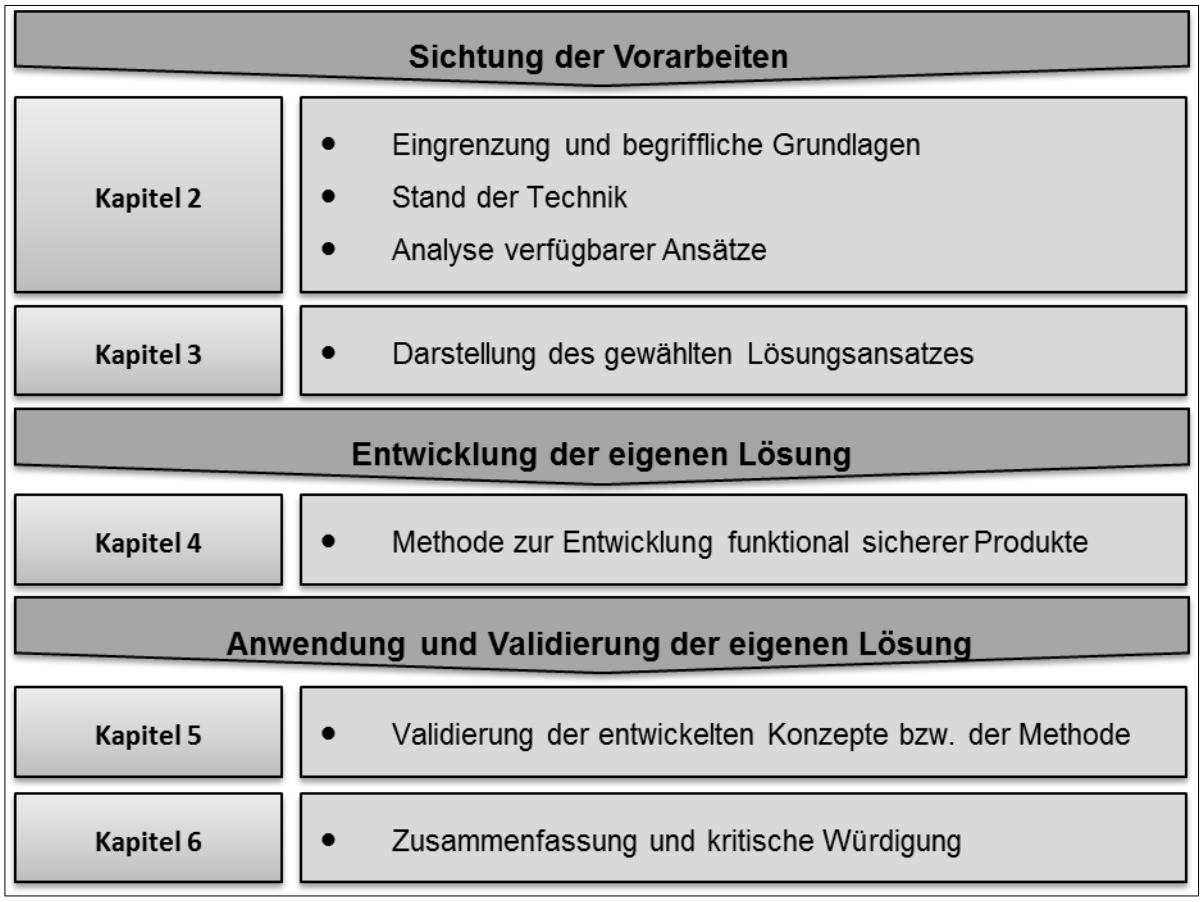


Abbildung 12 – Vorgehen innerhalb der Arbeit

Nachdem in ***Kapitel 1*** die Ausgangssituation und Problemstellung beschrieben und die Zielsetzung formuliert wurde, sollen in ***Kapitel 2*** die wichtigen Begriffe erklärt sowie definiert werden. Darüber hinaus soll in diesem Kapitel die Eingrenzung des Untersuchungsbereichs stattfinden. Zum Schluss sollen dort die bisher verfügbaren Ansätze und Methoden zur Entwicklung funktional sicherer Produkte gesichtet und hinsichtlich der gestellten Zielsetzung analysiert werden.

In ***Kapitel 3*** soll der gewählte Lösungsansatz für die in Kapitel 1 beschriebenen Probleme entwickelt werden.

Mit ***Kapitel 4*** wird die Erarbeitung der eigenen Methode zur systematischen Ermittlung und Umsetzung von Produkt- bzw. Systemanforderungen für funktional sichere Produkte im Automotive-Bereich dargelegt und beschrieben.

Die Validierung und Absicherung der entwickelten Methode soll in ***Kapitel 5*** unter Zuhilfenahme eines Forschungsprojekts stattfinden.

Im letzten ***Kapitel 6*** soll die Arbeit mit einer Zusammenfassung und Würdigung der Ergebnisse abgeschlossen werden. Dabei sollen ggf. im Rahmen der Arbeit aufgeworfene Fragestellungen formuliert werden.

2 Stand der Technik

In ***Abschnitt 2.1*** sollen zu Beginn die grundlegenden Begriffe im Kontext der „Funktionalen Sicherheit“ definiert sowie das Konzept der „Funktionalen Sicherheit“ erläutert werden. Auf dem darauf basierenden, einheitlichen Verständnis wird anschließend in ***Abschnitt 2.2*** der *Stand der Technik* hinsichtlich existierender Methoden und Vorgehensweisen dargelegt. Zusätzlich dazu sollen die vorhandenen Ansätze analysiert, gewürdigt und bewertet werden.

Abschließend soll in ***Abschnitt 2.3*** ein Fazit aus dem Stand der Technik bezogen auf die Problemstellung und Zielsetzung gezogen werden.

2.1 Begrifflichkeiten im Kontext der „Funktionalen Sicherheit“

Um eine fehlerhafte Interpretation der englischen Norm zu verhindern und ein einheitliches Verständnis für die Bedeutung der einzelnen Worte und Begriffe im Kontext der Funktionalen Sicherheit zu schaffen, werden im weiteren Verlauf relevante Begriffe definiert, erläutert und abgegrenzt.

2.1.1 Begriffserläuterung „Sicherheit

Dem Duden zufolge ist unter „**Sicherheit**“ ein

> *„Zustand des Sicherseins“,* das *„Geschütztsein vor Gefahr oder Schaden“*
> bzw. das *„höchstmögliche Freisein von Gefährdungen“*

zu verstehen. [Bibliographisches Institut GmbH 2013]

Die DIN EN 45020 [DIN EN 45020 2007-03] definiert Sicherheit weiter als

> *„Sicherheit ist die Freiheit von unvertretbaren Schadensrisiken“.*

Im Gegensatz zum Deutschen wird in der englischen Sprache der Begriff *„Sicherheit“* jedoch in zwei Begriffe unterteilt. Zum einen wird *„Sicherheit“* in *„Safety“* und zum anderen in *„Security“* unterteilt. [VDI 3780 2000-09]

Dabei wird ***Safety*** in der ISO 26262 [ISO 26262-1 2011-11-15] wie folgt definiert:

> *„absence of unreasonable risk“*

Übersetzt bedeutet das etwa “Abwesenheit unzumutbarer Risiken“.

Unreasonable risk definiert die Norm [ISO 26262-1 2011-11-15] weiter als

> *„judged to be unacceptable in a certain context according to valid societal moral concepts”*

was wie folgt verstanden werden kann: “Risiken, die in einem bestimmten Kontext in Bezug auf die gesellschaftlichen Moralvorstellungen als nicht tolerierbar angesehen werden“. Dabei geht es hier um die Gefährdung bzw. das Risiko für Menschen, das durch Fehlfunktionen einer Komponente bzw. eines Systems entsteht. [Spath, D. 2013]

Der Begriff „**Security**“ wird in der Norm selbst nicht definiert.

„Oxford Dictionaries“ [Oxford University Press 2010] umschreibt es folgendermaßen:

> *“the state of being free from danger or threat”*

„Wiktionary“ [Wikimedia 2013] präzisiert die Definition „Security**“** weiter:

> *„the condition of not being threatened, especially physically, psychologically, emotionally, or financially”*

Es geht hierbei insbesondere um den Zustand, keiner körperlichen, psychischen, emotionalen sowie finanziellen Bedrohung ausgesetzt zu sein. Des Weiteren wird der Begriff auch im Bereich von IT-Systemen (sowohl Software wie auch Hardware) eingesetzt, wobei es in diesem Kontext um den Schutz elektronischer Geräte bzw. Steuerungen (bspw. Computer, Tablets, Smartphones oder auch Industrieanlagen [Rieger, F. 2010], [Lischka, K.; Matthias, K. 2011]) vor Angriffen geht. Darunter ist der Schutz vor Manipulationen bzw. Bedrohungen durch Dritte zu verstehen.

2.1.2 Begriffserläuterung „Funktionale Sicherheit“

„**Funktionale Sicherheit**“, im Englischen „functional safety“, definiert die ISO 26262 [ISO 26262-1 2011-11-15] als

> *“absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems”*.

Auf Deutsch kann dies mit der Bedeutung „Abwesenheit unzumutbarer Risiken infolge Gefährdungen, hervorgerufen durch Fehlfunktionen von E/E-Systemen” (E/E steht für **E**lektrisch/**E**lektronisch) gleichgesetzt werden.

Allgemein definiert werden kann sie damit, dass eine Komponente bzw. ein System seine sicherheitsgerichtete Aufgabe entsprechend des abzudeckenden Risikos korrekt zu erfüllen hat. [Börcsök, J. 2011]

Weitergehend konkretisiert wird die Definition der „Funktionalen Sicherheit“ unter anderem folgendermaßen:

> *„Funktionale Sicherheit ist die Fähigkeit eines elektrischen oder elektronischen Systems (E/E-System) beim Auftreten*
>
> • *systematischer Ausfälle (z. B. fehlerhafte Systemauslegung)*
>
> • *zufälliger Ausfälle (z. B. Alterung von Bauteilen)*
>
> *mit gefahrbringender Wirkung, einen sicheren Zustand einzunehmen bzw. im sicheren Zustand zu bleiben.“* [Schloske, A. 2011b]

Durch den Titel der Norm (Road vehicles — Functional safety) und diese beiden Definitionen wird der zu betrachtende Fokus der ISO 26262 klar auf den Aspekt „Safety“ gelegt. „Security“ wird in der Norm, trotz steigender Notwendigkeit (wie in Abschnitt 2.1.1 dargestellt), nicht betrachtet. [Schmidt, M.; Rau, M., et al. 2011]

2.1.3 Begriffserläuterung „Stand der Technik“

Der Begriff **„Stand der Technik“** stellt eine Technikklausel dar und beschreibt die technischen Möglichkeiten und Fähigkeiten, die zu einem definierten Zeitpunkt verfügbar sind. Die verfügbaren technischen Möglichkeiten basieren auf den gesicherten Erkenntnissen von Wissenschaft und Technik unter dem Aspekt der wirtschaftlichen Umsetzbarkeit. Diese Generalklausel wird dabei stellvertretend für den tatsächlichen technologischen Stand in Rechtsnormen und Verträgen eingesetzt. Damit soll verhindert werden, dass der beschriebene technologische Stand bei jeder Änderung angepasst werden muss.

Die DIN EN 45020:2006 (*Normung und damit zusammenhängende Tätigkeiten - Allgemeine Begriffe (ISO/IEC Guide 2:2004))* legt den Begriff wie folgt fest [DIN EN 45020 2007-03]:

> *„Stand der Technik: entwickeltes Stadium der technischen Möglichkeiten zu einem bestimmten Zeitpunkt, soweit Produkte, Prozesse und Dienstleistungen betroffen sind, basierend auf entsprechenden gesicherten Erkenntnissen von Wissenschaft, Technik und Erfahrung“*

Im europäischen Patentübereinkommen (EPÜ) heißt es im Art. 54 Absatz 2 weiter:

> *„(2) Den Stand der Technik bildet alles, was vor dem Anmeldetag der europäischen Patentanmeldung der Öffentlichkeit durch schriftliche oder mündliche Beschreibung, durch Benutzung oder in sonstiger Weise zugänglich gemacht worden ist.“* [Europäisches Patentamt 2010]

2.1.4 Begriffserläuterung „Stand der Wissenschaft und Technik“

Im Gegensatz zum „**Stand der Technik“** (siehe Abschnitt 2.1.3) wird unter der höchsten Technikklausel, dem „**Stand der Wissenschaft und Technik“**, der aktuelle Forschungsstand in einem Fachgebiet dargestellt.

Im Kontext der funktionalen Sicherheit ist, laut einem Gerichtsurteil vom Juni 2009, der Begriff der **„Stand der Wissenschaft und Technik“** nicht mit der *„Branchenüblichkeit“* gleichzusetzen. [OLG Jena 2009] Das bedeutet für ein System, dass es nicht ausreichend

ist, den bereits bekannten und vom Mitbewerber genutzten Stand der Technik einzusetzen, sondern auch nach einer serienreifen, sicherheitstechnisch überlegenen Alternativkonstruktion bzw. –lösung Ausschau zu halten.

Sogenannte „Reißbrettlösungen“ oder noch in der Erprobung befindliche Lösungen müssen nicht betrachtet oder eingesetzt werden. [OLG Jena 2009]

2.1.5 Begriffserläuterung „Automotive Safety Integrity Level”

Das in der ISO 26262 definierte **„Automotive Safety Integrity Level“** (ASIL) ist eine spezifische Anlehnung an das in der Mutternorm DIN EN 61508 definierte **„Safety Integrity Level“** (kurz SIL).

Die DIN EN 61508 klassifiziert das **„Safety Integrity Level“** in vier Stufen, SIL 1 bis SIL 4. Dabei stellt SIL 1 die niedrigsten und SIL 4 die höchsten Sicherheitsanforderungen an das Produkt. [DIN EN 61508-5 2001-12]
Das Sicherheitslevel wird, wie Abbildung 13 zeigt, anhand von vier Kriterien ermittelt:

- **C:** Risikoparameter der **Auswirkung** – unterteilt in *vier Stufen* (engl. consequence)
- **F:** Risikoparameter der **Häufigkeit und Aufenthaltsdauer** – unterteilt in *zwei Stufen* (engl. frequency and exposure time)
- **P:** Risikoparameter der **Möglichkeit**, den **gefährlichen Vorfall** zu **vermeiden** – unterteilt in *zwei Stufen* (engl. possibility of avoiding hazard)

Schadensausmaß C	Aufenthaltsdauer F	Gefahrenabwendung P	W1	W2	W3
C1	F1	P1	-	-	-
		P2	-	-	-
	F2	P1	-	-	-
		P2	-	-	-
C2	F1	P1	-	-	1
		P2	-	1	1
	F2	P1	1	1	2
		P2	1	2	3
C3	F1	P1	2	3	3
		P2	2	3	3
	F2	P1	3	3	4
		P2	3	3	4
C4	F1	P1	3	4	4
		P2	3	4	4
	F2	P1	3	4	4
		P2	3	4	4

Abbildung 13 – SIL-Graph nach DIN EN 61508

- **W: Wahrscheinlichkeit** des **unerwünschten Ereignisses** – unterteilt in *drei Stufen* (engl. demand rate assuming no protection)

Das **„Automotive Safety Integrity Level“** übernimmt diese Klassifizierung leicht verändert. Es wird zwischen ASIL A, B, C und ASIL D unterschieden, wobei ASIL A die niedrigsten und ASIL D die höchsten Anforderungen an die Produktsicherheit stellt.
Das Klassifikationsergebnis „QM“ (**Q**uality **M**anagement) hingegen bedeutet, dass die Anforderungen an dieSicherheit durch die in der Automobilbranche etablierten und vorgeschriebenen Normen, Richtlinien und Prozesse abgedeckt werden können. Sofern diese Anforderungen erfüllt werden, ist quasi kein Mehraufwand zu erwarten.

Die ASIL-Klassifizierung wird, wie Abbildung 14 darstellt, anhand von drei Bewertungskriterien durchgeführt: [ISO 26262-3 2011-11-15]

- **S:** Risikoparameter „**Severity“ (Schwere)** – unterteilt in *vier Stufen*
- **E:** Risikoparameter „**Exposure“** (**Häufigkeit** des **Ausgesetztseins)** – unterteilt in *fünf Stufen*
- **C:** Risikoparamter „**Controllability**“ (**Möglichkeit**, den **gefährlichen Vorfall** zu **beherrschen)** – unterteilt in *4 Stufen*

Severity S	Exposure E	Controllability C: C0	C1	C2	C3
S0	E0 – E4	QM	QM	QM	QM
S1	E0	QM	QM	QM	QM
	E1	QM	QM	QM	QM
	E2	QM	QM	QM	QM
	E3	QM	QM	QM	A
	E4	QM	QM	A	B
S2	E0	QM	QM	QM	QM
	E1	QM	QM	QM	QM
	E2	QM	QM	QM	A
	E3	QM	QM	A	B
	E4	QM	A	B	C
S3	E0	QM	QM	QM	QM
	E1	QM	QM	QM	A
	E2	QM	QM	A	B
	E3	QM	A	B	C
	E4	QM	B	C	D

Abbildung 14 – ASIL-Graph nach ISO 26262

Mögliche Zusammenhänge zwischen der ASIL-Einstufung und der notwendigen Risikoreduzierung sind in Abbildung 15 dargestellt:

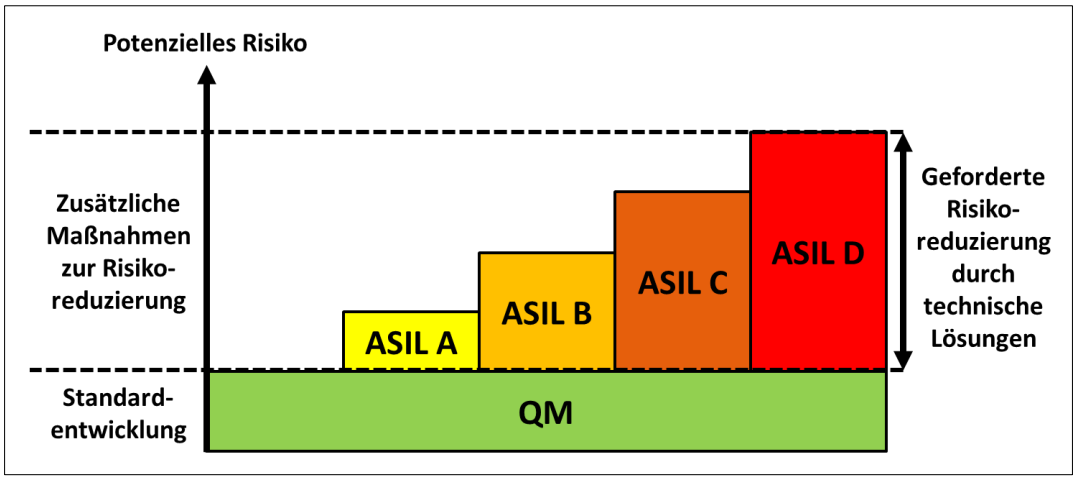


Abbildung 15 – Zusammenhang ASIL und Risikoreduzierung [Dold, A. 2008]

2.1.6 Begriffserläuterung der Entwicklungskenngrößen

Aus den drei Parametern (S, E und C) ergibt sich das ASIL, mit welchem aus der Norm die quantitativen und qualitativen Entwicklungsvorgaben an das zu entwickelnde System abgeleitet werden. Zusätzlich dazu definiert die Norm weitere organisatorische sowie prozessuale Voraussetzungen und Vorgehensweisen die im Projekt eingehalten werden müssen. Darunter fallen beispielsweise die Integration und Unabhängigkeit des Safety Managers, die Unternehmenskultur hinsichtlich Sicherheit, die Notwendigkeit von QM-Systemen sowie die Qualifizierung der eingesetzten Software. [ISO 26262-2 2011-11-15], [ISO 26262-8 2011-11-15]

Unter diese Entwicklungsvorgaben fallen einige elementare und wichtige „Hardware-Fehlerklassen“, die durch fehlerbehaftete Elektronikkomponenten auftreten können: [ISO 26262-5 2011-11-15]

- λ_{SPF}**:** Quantitative Aussage über die Anzahl von „**S**ingle-**P**oint **F**aults“, also Abweichungen (im englischsprachigen ISO 26262-Kontext: „fault“), die durch

keinen Sicherheitsmechanismus abgedeckt sind und sofort zur Verletzung eines oder mehrere Sicherheitsziele bzw. zur direkten Gefährdung von Menschen führen.

- $\boldsymbol{\lambda_{RF}}$**:** Quantitative Aussage über die Anzahl von „**R**esidual **F**aults“. Darunter werden die Teile einer Abweichung verstanden, die nicht durch einen Sicherheits-mechanismus abgedeckt werden und welche zur Verletzung eines oder mehrere Sicherheitsziele führen.

- $\boldsymbol{\lambda_{MPF}}$**:** Quantitative Aussage über die Anzahl von „**M**ultiple-**P**oint **F**aults“. Hierbei führt eine einzelne Abweichung in Kombination mit einer oder mehreren anderen unabhängigen Abweichungen zu einer kritischen, gefahrbringenden Situationen und zur Verletzung des Sicherheitsziels.
  Diese Hardware-Fehlerklasse weist weitere Unterteilungen auf. Dabei geht es um die Entdeckbarkeit dieser Abweichungen selbst:

  - $\boldsymbol{\lambda_{MPF,perceived}}$**:** Die Abweichung wird im Auto durch den Fahrer bzw. die Insassen wahrgenommen und erkannt.

  - $\boldsymbol{\lambda_{MPF,detected}}$**:** Diese Abweichung wird durch eine Diagnosefunktion im System detektiert.

  - $\boldsymbol{\lambda_{MPF,latent}}$**:** Diese Abweichung wird weder durch den Fahrer bzw. die Insassen noch durch das System entdeckt.

- $\boldsymbol{\lambda_{S}}$**:** Quantitative Aussage über die Anzahl von „**S**afe faults“, also Abweichungen, die zu keinen sicherheitskritischen Fehlern führen. Darunter können bspw. Funktionsausfälle bzw. Fehlfunktionen, die zu Komforteinschränkungen führen, subsummiert werden. Die Verletzung von Sicherheitszielen ist bei diesen Abweichungen ausgeschlossen.

- $\boldsymbol{\lambda_{SR,HW}}$**:** Quantitative Aussage über die Anzahl an „**S**afety **R**elated **H**ard**W**are“-Element-Faults. Darunter fallen alle Abweichungen, unabhängig von ihrem Gefahrenpotential, die an Bauelementen auftreten können, die an sicherheitsrelevanten Funktionen beteiligt sind. Diese Gesamtanzahl setzt sich wie dargestellt zusammen:

$$\boldsymbol{\lambda_{SR,HW}} = \lambda_{SPF} + \lambda_{RF} + \lambda_{MPF} + \lambda_S$$

Formel 1 – Berechnung der SR,HW-Element-Faults [ISO 26262-5 2011-11-15]

Unter Einsatz dieser oben genannten Fehlerklassen können unter anderem folgende wichtige Kenngrößen und Hardware-Metriken während der Entwicklung bestimmt werden:

- **S**ingle-**P**oint-**F**ault **M**etric (kurz SPFM)
  Die SPFM-Berechnung wird folgendermaßen durchgeführt:

$$\boldsymbol{SPFM} = 1 - \frac{\sum_{SR,HW}(\lambda_{SPF} + \lambda_{RF})}{\sum_{SR,HW}\lambda} = \frac{\sum_{SR,HW}(\lambda_{MPF} + \lambda_S)}{\sum_{SR,HW}\lambda}$$

Formel 2 – Berechnung der Single-Point-Fault Metric [ISO 26262-5 2011-11-15]

In Tabelle 1 werden die jeweilig einzuhaltenden SPFM-Grenzwerte der verschiedenen ASIL dargestellt:

	ASIL B	**ASIL C**	**ASIL D**
SPFM	≥90%	≥97	≥99

Tabelle 1 – Grenzwerte der einzelnen ASIL hinsichtlich SPFM [ISO 26262-5 2011-11-15]

Je höher die Metrik, desto weniger Gefahrenpotenzial durch „Single-Point Faults“ besteht. Für ASIL A gibt es keine SPFM-Vorgabe.

- **L**atent-**F**ault **M**etric (kurz LFM)
  Die LFM wird wie folgt berechnet:

$$\boldsymbol{LFM} = 1 - \frac{\sum_{SR,HW}\left(\lambda_{MPF,latent}\right)}{\sum_{SR,HW}(\lambda - \lambda_{SPF} - \lambda_{RF})} = \frac{\sum_{SR,HW}\left(\lambda_{MPF,perceived\ or\ detected} + \lambda_S\right)}{\sum_{SR,HW}(\lambda - \lambda_{SPF} - \lambda_{RF})}$$

Formel 3 – Berechnung der Latent-Fault Metric [ISO 26262-5 2011-11-15]

In Tabelle 2 werden die jeweilig einzuhaltenden LFM-Grenzwerte der jeweiligen ASIL dargestellt:

	ASIL B	**ASIL C**	**ASIL D**
LFM	≥60%	≥80	≥90

Tabelle 2 – Grenzwerte der einzelnen ASIL bezüglich LFM [ISO 26262-5 2011-11-15]

Je höher die Metrik, desto weniger Gefahrenpotenzial durch „Latent-Point Faults“ besteht. Ebenso wie bei der SPFM gibt es für ASIL A keine LFM-Vorgabe.

- **P**robabilistic **M**etric for random **H**ardware **F**ailures (kurz PMHF)
  Die PMHF legt die quantitativ einzuhaltenen Grenzenwerte für zufällig auftretende Hardware-Fehler fest, deren Auswirkung zur Verletzung eines Sicherheitsziels führt. Die Berechnung der PMHF wird folgendermaßen durchgeführt:

$$\boldsymbol{PMHF} = \lambda_{SPF} + \lambda_{RF} + \lambda_{LMPF}$$

Formel 4 – Berechnung der Probabilistic Metric for random Hardware Failures [Schloske, A. 2011b]

Tabelle 3 gibt die jeweiligen Grenzwerte an, wobei es für ASIL B nur eine Empfehlung, aber keine Vorgabe gibt:

	(ASIL B)	**ASIL C**	**ASIL D**
PMHF	($<10^{-7}$ h^{-1})	$<10^{-7}$ h^{-1}	$<10^{-8}$ h^{-1}

Tabelle 3 – Grenzwerte der einzelnen ASIL bezüglich PMHF [ISO 26262-5 2011-11-15]

- **D**iagnostic **C**overage (kurz DC)
  Der DC, zu Deutsch „Diagnosedeckungsgrad“, gibt den prozentualen Anteil der Hardware-Fehler an, die durch Sicherheits- und Diagnosefunktionen entdeckt und beherrscht werden. Das bedeutet, dass die Höhe des DCs die Auftretenshäufigkeit eines gefährlichen Zustands reduzieren kann. Dabei gilt, je höher der Diagnosedeckungsgrad ist, desto weniger gefahrbringende Situationen können entstehen. [ISO 26262-1 2011-11-15]
  Zu beachten ist, dass es zwei verschiedene DCs gibt, die sich ihrerseits auf einzelne Fehlerarten auswirken:
  - DC für „Residual Faults“
  - DC für „Latent Multiple-Point Faults“

Um nun ein ISO 26262-konformes Produkt zu entwickeln, müssen unter anderem die oben genannten Kenngrößen und Metriken erfüllt und eingehalten werden.

2.1.7 Begriffserläuterung „Produkthaftung“

Unter **„Produkthaftung“** wird die Haftung des Herstellers oder Inverkehrbringers (z. B. Importeur) für Schäden verstanden, die infolge von Fehlern eines Produkts entstehen bzw. entstanden sind.

Dem *Produkthaftungsgesetz* (kurz *ProdHaftG*) zufolge sind alle Parteien im Falle eines Unfalls regresspflichtig, die einen Grundstoff, ein Teilprodukt oder das Endprodukt hergestellt haben. Als Hersteller eines Produkts gilt auch derjenige, der nur seinen Namen, seine Marke oder ein anderes unterscheidungskräftiges Kennzeichen (z. B. Emblem) an dem Produkt anbringt. [Bundesministerium der Justiz 1989]

Die Haftung regelt das *ProdHaftG* in § 1, Absatz 1 [Bundesministerium der Justiz 1989]:

> ***§ 1 Haftung***
>
> *(1) Wird durch den Fehler eines Produkts jemand getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache beschädigt, so ist der*

> *Hersteller des Produkts verpflichtet, dem Geschädigten den daraus entstehenden Schaden zu ersetzen. Im Falle der Sachbeschädigung gilt dies nur, wenn eine andere Sache als das fehlerhafte Produkt beschädigt wird und diese andere Sache ihrer Art nach gewöhnlich für den privaten Ge- oder Verbrauch bestimmt und hierzu von dem Geschädigten hauptsächlich verwendet worden ist.*

Des Weiteren regelt das *Produkthaftungsgesetz* in § 1, Absatz 2 den Haftungsausschluss:

> *(2) Die Ersatzpflicht des Herstellers ist ausgeschlossen, wenn*
>
> *1. er das Produkt nicht in den Verkehr gebracht hat,*
>
> *2. nach den Umständen davon auszugehen ist, daß das Produkt den Fehler, der den Schaden verursacht hat, noch nicht hatte, als der Hersteller es in den Verkehr brachte,*
>
> *3. er das Produkt weder für den Verkauf oder eine andere Form des Vertriebs mit wirtschaftlichem Zweck hergestellt noch im Rahmen seiner beruflichen Tätigkeit hergestellt oder vertrieben hat,*
>
> *4. der Fehler darauf beruht, daß das Produkt in dem Zeitpunkt, in dem der Hersteller es in den Verkehr brachte, dazu zwingenden Rechtsvorschriften entsprochen hat, oder*
>
> *5. der Fehler nach dem Stand der Wissenschaft und Technik in dem Zeitpunkt, in dem der Hersteller das Produkt in den Verkehr brachte, nicht erkannt werden konnte. [Bundesministerium der Justiz 1989]*

Besonders relevant für die Entlastung des Herstellers hinsichtlich der funktionalen Sicherheit ist der in § 1, Absatz 2 genannte Punkt 5, der auf den Stand von Wissenschaft und Technik (siehe Abschnitt 2.1.4) verweist, ohne diesen weiter zu definieren.

2.2 Vorhandene Vorgehensweisen und Ansätze

Nachdem in Abschnitt 2.1 die Begrifflichkeiten im Kontext der funktionalen Sicherheit (nach ISO 26262) erläutert wurden, werden im Folgenden die existierenden Vorgehensweisen und Ansätze zu den in Abschnitten 1.2 und 1.3 definierten Problemstellungen und daraus abgeleiteten Aufgabenstellungen

- ASIL-Ermittlung
- Schnittstellendefinition und -betrachtung
- durchgängigen Umsetzung und Dokumentation der Anforderungen

dargestellt, gewürdigt und kritisch bewertet.

2.2.1 ASIL-Klassifizierung

Die ASIL-Einstufung ist bei der Entwicklung funktional sicherer Systeme und Komponenten ein elementarer und grundlegender Schritt, der im Idealfall den Start der Entwicklungstätigkeiten einleitet. Basierend auf diesem Einstufungsergebnis werden die weiteren Entwicklungsanforderungen und -maßnahmen durch die Norm festgelegt und für die Entwicklungsumfänge und das Entwicklungsvorgehen abgeleitet. Daher ist eine angemessene, einheitliche und nachvollziehbare ASIL-Klassifizierung von besonderer Wichtigkeit, damit es später zu keinen produktspezifischen Rückrufen wie auch juristischen Produkthaftungsproblemen kommen kann.

2.2.1.1 Grundsätzliche Probleme der ASIL-Einstufung

Die Schwierigkeit bei der ASIL-Einstufung liegt darin, weder eine zu niedrige noch eine zu hohe Klassifizierung zu ermitteln.

Zum einen kann eine zu niedrige, unterhalb der Mitbewerber eingeordnete, ASIL-Stufe dazu führen, dass im Produkthaftungsfall dem Hersteller mit der niedrigeren Einstufung (in diesem Beispiel „QM“) des Systems Kosteneinsparung vorgeworfen wird. Dies wird in Abbildung 16 auf der folgenden Seite dargestellt. [Kriso, S. 2011]

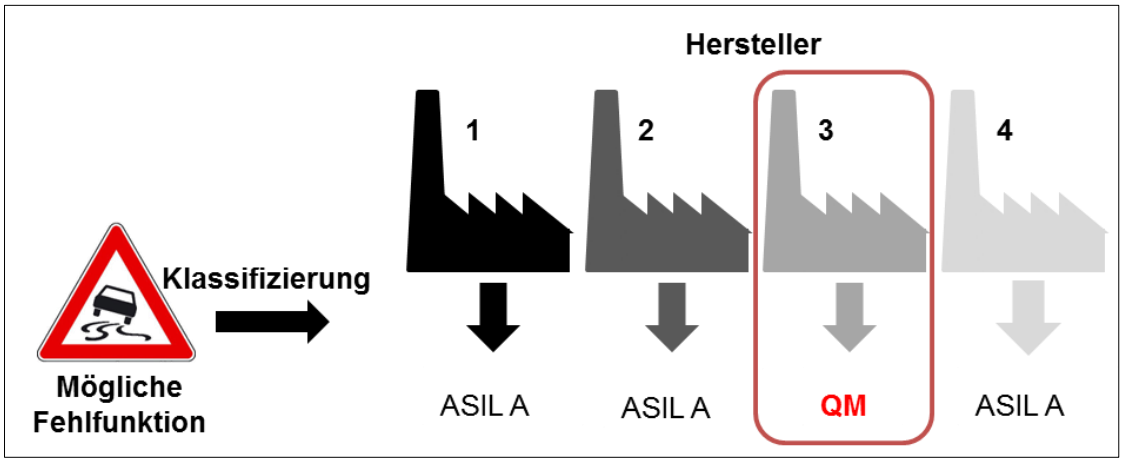


Abbildung 16 – Probleme einer zu niedrigen ASIL-Klassifizierung [Kriso, S. 2011]

Zum anderen kann eine zu hohe (hier ASIL B bzw. nach der Adaption ASIL C), über den Mitbewerbern eingeordnete Klassifizierung dazu führen, dass die Kosten für die Entwicklung des entsprechenden Systems zu hoch sind oder sich ein mechatronisches System über die Zeit zu einem ASIL D-System aufschaukelt. Denn ein System, das nach einem höheren ASIL entwickelt wurde, suggeriert zumindest auf dem Papier mehr Sicherheit für den Endkunden und stellt damit ein Differenzierungsmerkmal gegenüber den restlichen Mitbewerbern dar. Zusätzlich definiert ein verbessertes System theoretisch auch den Stand der (Wissenschaft und) Technik. [Kriso, S. 2011]

Abbildung 17 auf der folgenden Seite zeigt das oben beschriebene Aufschaukeln der Klassifikation. Hersteller 1 und 2 haben ihr Produkt auf ASIL B angehoben, um sich an das Niveau von Hersteller 3 anzugleichen. Hersteller 4 hat sein System jedoch direkt auf ASIL C adaptiert, sodass dieses nun theoretisch den Stand von Wissenschaft und Technik definiert und Hersteller 1, 2 und 3 nachziehen müssten.

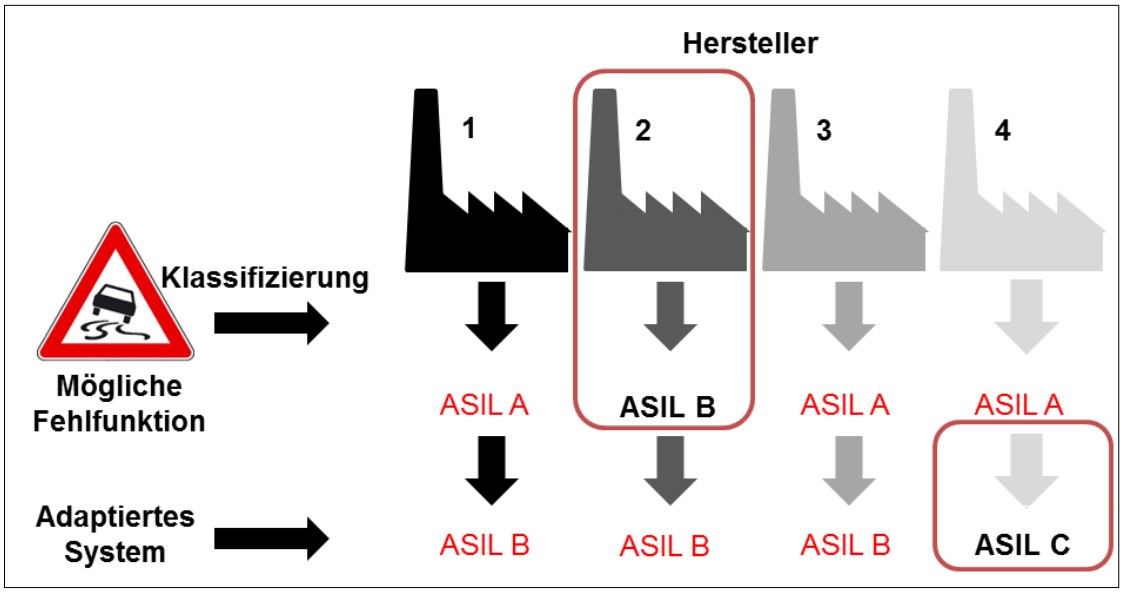


Abbildung 17 – Probleme einer zu hohen ASIL-Klassifizierung [Kriso, S. 2011]7

Um eine geeignete Klassifikation zu erreichen, gibt es verschiedene Ansätze. Dazu gehört die Klassifikation anhand der ISO 26262 sowie der Risikopoker. [ISO 26262-3 2011-11-15], [Ständer, T. 2012] Diese beiden Ansätze werden im Weiteren vorgestellt sowie deren Stärken und Schwächen dargelegt.

2.2.1.2 ASIL-Klassifizierung nach Vorgabe durch die ISO 26262

Die ASIL-Klassifizierung wird, wie in Abschnitt 2.1.5 bereits beschrieben, durch die Festlegung von drei Faktoren bestimmt. Laut ISO 26262 sind dies:

- Severity
- Exposure
- Controllability

Um das Ergebnis einer ASIL-Klassifizierung abzusichern und juristisch belastbar zu gestalten, werden nachfolgend die einzelnen Faktoren hinsichtlich ihrer Unabhängigkeit und Einflussgrößen untersucht.

Bewertung des Faktors „Severity“

Die „**Severity**“ teilt sich in vier Verletzungskategorien ein:

- **S0: keine Verletzungsgefahr**
- **S1: geringe** und **mäßige Verletzungen**
- **S2: ernste** und **möglicherweise tödliche Verletzungen**
- **S3: schwere** und **wahrscheinlich tödliche Verletzungen**

Die Norm schlägt vor, zur Bestimmung der Verletzungsgefahr die auf der amerikanischen Unfallforschung basierende „Abbreviated Injury Scale“ (kurz AIS) zu verwenden. [ISO 26262-3 2011-11-15]

Alternativ dazu können die aus der deutschen Unfallforschung stammenden „Unfallkategorien“ (kurz UK) genutzt werden. Bei der UK-Einstufung wird ein Unfall in sechs Stufen unterteilt, wobei die Stufen eins (höchste Verletzung) bis drei (niedrigste Verletzung) für Personenschäden und vier bis sechs für Sachschäden genutzt werden.

Die Bewertung des Faktors „Severity“ ist durch die Norm unter Verwendung der AIS bzw. UK eindeutig definiert. Weltweit betrachtet gibt es bei diesem Bewertungsfaktor quasi keine Einflussgrößen (bspw. regionale bzw. länderspezifische Eigenheiten) bei der Bewertung einer Unfallfolge, da die menschliche Physiologie weltweit weitestgehend als einheitlich angenommen werden kann. [Eveleth, P. B.; Tanner, J. M. 1976] Praktisch bedeutet das, dass es für die Insassen (Fahrzeugführer und potenzielle Mitfahrer) und anderen Verkehrsteilnehmer keinen Unterschied hinsichtlich der Verletzungen bzw. des Verletzungspotenzials macht, ob man in Stuttgart oder in New York bzw. in Deutschland oder in den USA „gegen einen Baum fahren“ oder mit einem vergleichbaren Objekt auf der Fahrbahn kollidieren. Beide Verletzungspotenziale und Unfallfolgen werden für alle Unfallbeteiligten identisch sein.

Für die Praxis ergibt sich daraus, dass der Faktor „Severity“ bei der zielmarktorientierten Ermittlung von Produktanforderungen als statisch betrachtet werden kann, da er in allen Zielmärkten gleich ist.

Bewertung des Faktors „Exposure“

Der Faktor „**Exposure**“ separiert sich in *fünf* Stufen, *praktisch* werden jedoch *nur vier* genutzt:

- **E0** - **unwahrscheinlich** (engl. infeasible, unusual)**:** Situation tritt für die meisten Fahrer **nie ein** (Unfall eines Fahrzeugs mit einem auf der Straße/Autobahn landenden Flugzeug)
- **E1** - **selten:** Situation tritt für die meisten Fahrer **seltener als einmal pro Jahr** auf
- **E2** - **gelegentlich:** Situation tritt für die meisten Fahrer **wenige Male pro Jahr** auf bzw. **weniger als in 1 %** der **durchschnittlichen Betriebsdauer**
- **E3** - **ziemlich oft:** Situation tritt für Durchschnittsfahrer **einmal im Monat oder öfter** auf bzw. **zwischen 1 % und 10 %** der **durchschnittlichen Betriebsdauer**
- **E4** - **oft:** Situation, die bei nahezu jeder Fahrt auftritt bzw. **bei mehr als 10 %** der **durchschnittlichen Betriebsdauer**

Die Norm gibt zur Orientierung und als Hilfestellung eine Vielzahl verschiedener Fahrsituationen vor, die im Lauf einer Fahrt auftreten können. [ISO 26262-3 2011-11-15]

In der nachstehenden Tabelle 4 werden exemplarisch einige Norm-Exposure-Beispiele aufgeführt:

E1	E2	E3	E4
Verlorene Ladung auf der Fahrbahn	Schnee und Eis auf der Fahrbahn	Nasse Fahrbahn	Bremsen
Bergab fahren mit ausgeschaltetem Motor	Fahren mit Anhänger	Fahren im Tunnel	Spurwechsel
Abgeschleppt werden	Parkendes Fahrzeug mit schlafender Person	Stopp & Go Verkehr	Einparken

Tabelle 4 – Exposure-Beispiele aus der ISO 26262 [ISO 26262-3 2011-11-15]

Die Bewertung der Exposure anhand der vorgegebenen Beispiele ergibt auf den ersten Blick ein valides Bewertungsergebnis. Bei tiefer gehender Analyse gibt es jedoch Interpretationsspielraum, der das resultierende ASIL-Ergebnis stark infrage stellen kann.

Betrachtet man beispielsweise den Fall „**Schnee und Eis auf der Fahrbahn**“ mit der **Bewertung E2** anhand von **Eistagen** (Tage bei denen die Höchsttemperatur unter 0 °C liegt) genauer, so ergeben sich bereits erste Unterschiede.

In München gibt es *im vieljährigen Mittel 38,8 Eistage*. Legt man ein Jahr mit 365,25 Tagen (0,25 Tage, da der Schalttag bereits in die einzelnen Jahre mit eingerechnet wurde) zugrunde, so ergibt sich ein Verhältnis von Eistagen zum Gesamtjahr von 10,62 %. Betrachtet man die Normauslegung, so ergibt sich für die Exposure eine Klassifizierung von 4 (E4).

Betrachtet man hingegen Köln, so ergibt sich aus dem vieljährigen Mittel von 7,9 Eistagen ein Verhältnis von 2,16 %, was ein E3 ergibt.

Für die ASIL-Klassifizierung hat diese unterschiedliche E-Bewertung folgende Auswirkungen bei einer exemplarischen Bewertung von **S2** und **C2** (siehe Abbildung 18):

- bei **E2** ergibt sich **QM (Normvorschlag)**
- bei **E3** ergibt sich **ASIL A (Köln)**
- bei **E4** ergibt sich **ASIL B (München)**

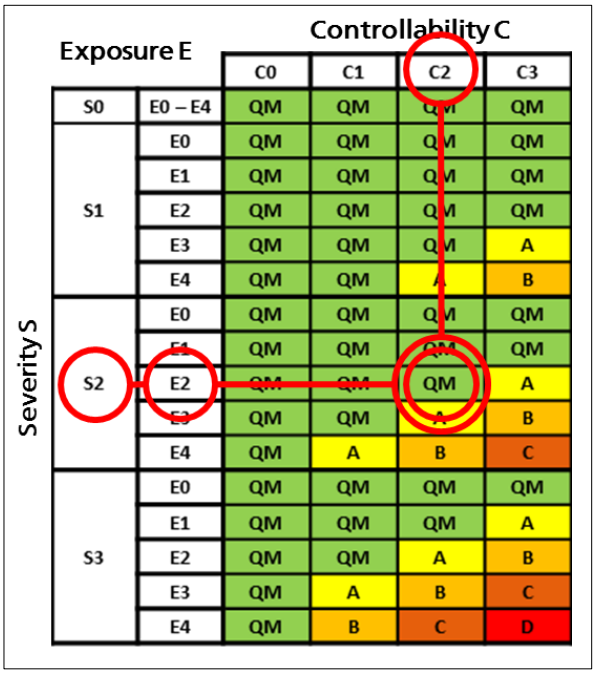


Abbildung 18 – Beispielhafte Ermittlung des ASIL

Geht man von einer regionalen zu einer länderübergreifenden Betrachtung über, so können sich die Auswirkungen unterschiedlicher E-Bewertungen noch deutlicher in den Entwicklungsvorgaben niederschlagen.

Betrachtet man die Hauptstadt Norwegens, Oslo, so ergeben sich hier im vieljährigen Mittel 46 Eistage. In der italienischen Hauptstadt Rom hingegen gibt es im Mittel keine Eistage. Dort hat es im Jahr 2012 seit 27 Jahren das erste Mal wieder geschneit. [Kleinjung, T. 2012], [Kreiner, P. 2012]

Betrachtet man hier erneut die Exposure E, so zeichnet sich ein weiter differenziertes Ergebnis ab. Für Oslo gibt es bei „Schnee und Eis auf der Fahrbahn“ ein E4 und für Rom ein E0. [CelsiusPro 2013]

Stellt man nun alle Bewertungen sowie den daraus resultierenden ASIL gegenüber, so ergibt sich folgendes Bild:

- bei **E0** ergibt sich **QM (Rom)**
- bei **E2** ergibt sich **QM (Normvorschlag)**
- bei **E3** ergibt sich **ASIL A (Köln)**
- bei **E4** ergibt sich **ASIL B (München, Oslo)**

Unter den definierten Bedingungen ergibt sich hier maximal ein ASIL B.

Bei entsprechend kritischer Bewertung der Unfallschwere, **S3** anstelle von S2, und der Beherrschbarkeit, **C3** anstatt C2, kann sich ein noch stärker differenziertes Bild ergeben:

- bei **E0** ergibt sich **QM (Rom)**
- bei **E2** ergibt sich **ASIL B (Normvorschlag)**
- bei **E3** ergibt sich **ASIL C (Köln)**
- bei **E4** ergibt sich **ASIL D (München, Oslo)**

In diesem Fall ergibt sich ein maximaler ASIL-Wert von D.

Alle selbst ermittelten Exposure-Bewertungen unterscheiden sich von der Norm-Vorgabe bzw. dem Norm-Vorschlag E2. Daraus wird deutlich, dass der Faktor „Exposure“ einen hohen Einfluss auf die Ermittlung von Produktanforderungen hat.

Bewertung des Faktors „Controllability“

Der dritte und letzte Teilaspekt zur Bestimmung des ASIL ist die Möglichkeit bzw. Fähigkeit zur Beherrschung der Fehlersituation oder des Fehlers durch den Fahrer.

Die Norm bezeichnet dies als „**Controllability**“ und legt für diese Bewertung einen fiktiven, durchschnittlichen Fahrer zugrunde. Darunter ist der nicht müde oder sonst beeinträchtigte Fahrer mit durchschnittlicher Fahrpraxis und durchschnittlichem Alter gemeint, der die Verkehrsregeln beherrscht, Rücksicht auf andere Verkehrsteilnehmer nimmt und zudem im Besitz einer gültigen Fahrerlaubnis ist. [ISO 26262-3 2011-11-15]

Die Beherrschbarkeit eines Zustands wird in vier Stufen unterteilt:

- **C0:** Situation ist für **jeden Fahrer beherrschbar** (engl. controllable in general)
- **C1: mehr als 99 %** aller **Fahrer bzw. Verkehrsteilnehmer** sind üblicherweise in der Lage, die Situation zu **beherrschen** und dadurch einen **Schaden zu vermeiden**
- **C2: mehr als 90 %** aller **Fahrer bzw. Verkehrsteilnehmer** sind üblicherweise in der Lage, die Situation zu **beherrschen** und dadurch einen **Schaden zu vermeiden**
- **C3: weniger als 90 %** aller **Fahrer bzw. Verkehrsteilnehmer** sind üblicherweise bzw. kaum in der Lage, die Situation zu **beherrschen** und dadurch einen **Schaden zu vermeiden**

Die Norm gibt einige Beispiele zur Orientierung für die Bestimmung der Beherrschbarkeit. [ISO 26262-3 2011-11-15] Weltweit betrachtet gibt es bei diesem Bewertungsfaktor keine bis wenige Einflussgrößen (bspw. regionale bzw. länderspezifische Eigenheiten), die dazu führen, dass in einer Region, einem Land oder einer Stadt die Fahrfähigkeiten besser oder schlechter sind als in einem anderen. Praktisch bedeutet das, dass Fahrer in Stuttgart gleich gut bzw. schlecht mit Fahrsituationen umgehen können, wie Fahrer in New York. Beide Beherrschungspotenziale sind quasi identisch. [Özkan, T.; Lajunen, T., et al. 2006], [World Health Organization 2011]

Für den Fall, dass die Beherrschbarkeit einer Fahrsituation nicht eindeutig bestimmbar ist, können Probanden zur Ermittlung des Werts sowie zur Validierung eingesetzt werden. Dazu werden die unwissenden Probanden den zu bewertenden Situationen in der Realität ausgesetzt, in dem durch die gezielte Einbringung von Fehlern von außen (eng. „fault injection“) die kritischen Situationen erzeugt und deren Beherrschbarkeit bewertet wird.

Kritische Würdigung des Normansatzes zur ASIL-Ermittlung

Die Ermittlung des ASIL anhand der vorgegebenen Normstruktur bietet eine erste grobe Orientierung anhand eines leicht verständlichen Vorgehens.

Vorteil der Normklassifizierung ist, dass bei strikter Einhaltung der Bewertungskriterien ein region- und länderübergreifend gleicher ASIL entsteht. Allerdings wird es im Produkthaftungsfall problematisch, diesen zu verteidigen und aufrechtzuerhalten. Da die Norm nur einen Mindeststandard bzw. ein Beispiel vorgibt, ist es nicht zwangsläufig zielführend, sich im juristischen Streit darauf zu berufen. [ISO 26262-3 2011-11-15]

Eine juristisch belastbare Bewertung lässt sich aus der Norm nur für Situationen ermitteln, deren Häufigkeit des Ausgesetztseins unabhängig von variablen Faktoren, wie zum Beispiel geografischen Eigenheiten, ist.

Die mangelnde Nachvollziehbarkeit und fehlende Transparenz schränkt die Anwendung der Norm weiter ein. Das Ergebnis unter Anwendung der Normvorgehensweise ist bekannt, jedoch fehlen die Annahmen und Voraussetzung für die jeweiligen C, S und E-Bewertungen. Dies kann sich im Haftungsfall negativ auswirken.

2.2.1.3 ASIL-Klassifizierung durch den „Risikopoker“

Der Risikopoker setzt auf der ASIL-Klassifizierung der Norm auf. Im Gegensatz zu dieser zielt der Risikopoker darauf ab, die Bildung einer gruppenkonformen, subjektiven Exposure-Bewertung auf Basis subjektiver E-Einzelbewertungen zu erreichen. Dazu werden im ersten Schritt die Parameter Severity und Controllability wie beim Vorgehen nach der Norm zur Bestimmung der Teilklassifizierung ermittelt.

Im Gegensatz dazu erfolgt die E-Wert-Bestimmung in einer abgewandelten Form. Alle beteiligten Personen erhalten hierbei die Möglichkeit, eine verdeckte Exposure-Bewertung zu einer vorher definierten Situation abzugeben. Nachdem alle Personen eine subjektive Bewertung abgegeben haben, werden alle Bewertungen offengelegt. Anschließend werden diese Bewertungen ausgewertet.

Bei einzelnen, gravierenden Abweichungen nach oben (in Richtung E-4) müssen die Abweichler ihre E-Bewertung erklären und begründen. Dabei sollen sie ihre subjektive Situation bzw. ihr Szenario, das zu der höheren E-Bewertung geführt hat, weiter erläutern und für alle anderen Bewertungsteilnehmer nachvollziehbar machen. Im Anschluss daran wird die gleiche Situation erneut verdeckt bewertet, offengelegt und diskutiert. Auf Basis dieser

Einzelbewertungen wird eine gruppenkonforme E-Bewertung unter Verwendung des Medians gebildet. [Ständer, T. 2012]

Kritische Würdigung des Risikopoker-Ansatzes zur ASIL-Ermittlung

Die Ermittlung des ASILs durch den Risikopoker ermöglicht es, alle Projektbeteiligten gleichermaßen in den Bewertungsprozess einzubinden. Meinungsführer werden hierdurch abgeschwächt.

Durch die Abgabe einer eigenen subjektiven Bewertung sowie der anschließenden Vorstellung des entsprechenden Szenarios kann der eigene Standpunkt gut verdeutlicht werden. Zudem verstehen die anderen Projektbeteiligten die Beweggründe und die damit angelegten Bewertungsgrundlagen.

Neben den aufgeführten Vorteilen weist diese Vorgehensweise allerdings auch einige Mängel und Nachteile auf:

- Das Entstehen der Endbewertung ist objektiv nicht nachvollziehbar und daher im Produkthaftungsfall juristisch nicht vertretbar.
- Aus vielen einzelnen, subjektiven Bewertungen entsteht eine subjektive Gruppenbewertung, die nicht durch Fakten belegt ist.
- Durch die Mittelung mithilfe des Medians werden nicht alle Bewertungen betrachtet und die Szenarien einzelner Projektbeteiligter sind nicht in das Endergebnis integriert.

2.2.1.4 Ziel bei der ASIL-Bewertung

Ziel dieser Arbeit soll es sein, eine wissenschaftlich begründbare und fundierte Methode zur objektiven Bewertung des Parameters „Exposure“ zu entwickeln.

Die Methode soll sich dabei auf Daten der einzelnen Länder stützen, die eine objektive Bewertung sowie eine Zusammenfassung in Regionen ermöglicht. Das ASIL, genau genommen die Exposure-Bewertung, muss schnell, fundiert, transparent und nachvollziehbar ermittelbar sein.

2.2.2 Ermittlung und Analyse von systemübergreifenden Schnittstellen

Ein weiteres Problem bei der Entwicklung funktional sicherer Produkte ist die Beherrschung der Schnittstellen (wie in Kapitel 1 dargestellt). Aufgrund der steigenden Komplexität sowie der hohen Anzahl unterschiedlicher Teile- und Systemlieferanten wird es immer wichtiger, die verschiedenen Schnittstellen im Automobil zu koordinieren und abzustimmen. Allein bis zum Jahr 2015 wird ein Anstieg der Zuliefererenteile in der Automobilentwicklung und –produktion auf 80 % erwartet. [Siebenlist, J. 2004] Abbildung 5 in Kapitel 1 hat bereits die Vielfalt der an einer „Baugruppe“ mitwirkenden Unternehmen gezeigt.

Insbesondere die elektromechanischen Substitute der rein mechanischen Baugruppen und Systeme erfordern dabei eine besondere Betrachtung im Kontext der „Funktionalen Sicherheit“, um die Anzahl sicherheitskritischer Situationen zu reduzieren bzw. deren Auftreten gänzlich auszuschließen.

2.2.2.1 Grundsätzliche Probleme bei der Schnittstellenauslegung

Bei der „Funktionalen Sicherheit“ interagiert eine Vielzahl unterschiedlicher Systeme miteinander. [Löw, P.; Pabst, R., et al. 2010] Diese müssen aufeinander abgestimmt sein.

Allerdings arbeiten bzw. kommunizieren die verschiedenen Zulieferer, deren Systeme aufeinander angewiesen sind, oftmals nicht im wünschenswerten und notwendigen Umfang miteinander.

Dafür gibt es aus Sicht des Autors mehrere Gründe:

- keine direkte Kommunikation zwischen den verschiedenen Entwicklungspartnern
- Angst vor Informations- und Know-how-Verlust
- Kein Bedarf seitens der verschiedenen Entwicklungspartnern
- Kein Bewusstsein für die Notwendigkeit eines Informationsaustauschs
- Entwicklungspartner sehen OEM bzw. übergeordneten Lieferanten verantwortlich für Kommunikation und Koordination der Schnittstellen
- Keine kompatiblen IT-Systeme

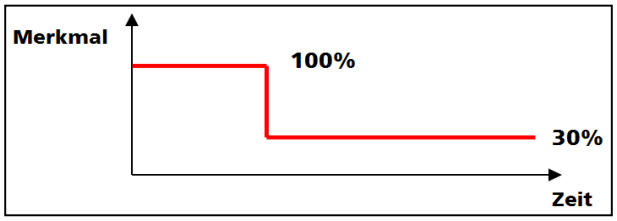
Federführend und verantwortlich für die Koordination der relevanten Schnittstellen der einzelnen Teilsysteme ist der OEM oder der vorgelagerte Lieferant. Nur jene haben einen

Einblick und Überblick über alle Schnittstellen/Informationen. [Löw, P.; Pabst, R., et al. 2010]

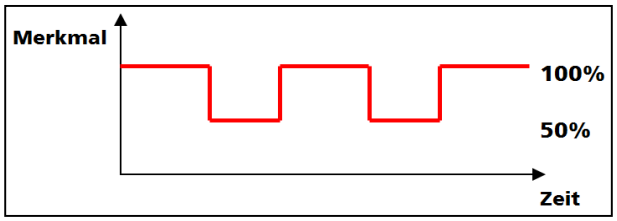
Bei dieser Koordinationsarbeit geht es jedoch um mehr als nur darum, dass jeder Entwicklungspartner die richtigen Parameter zur Datenübertragung einhält. Dies wird üblicherweise über die Standardisierung der im Automobil typischen Bussysteme (z. B. CAN, FlexRay, MOST, LIN) und Protokolle erreicht und sichergestellt.
Wichtig ist die Festlegung, wie ein System mit fehlenden, fehlerhaften oder unerwarteten Signalen/Informationen umzugehen hat und wie vertrauenswürdig bzw. sicher diese vor Manipulation durch andere Teilsysteme sind.

Dabei können unter anderem folgende sechs Fehler einbezogen werden (in Anlehnung an von Regius 2008):

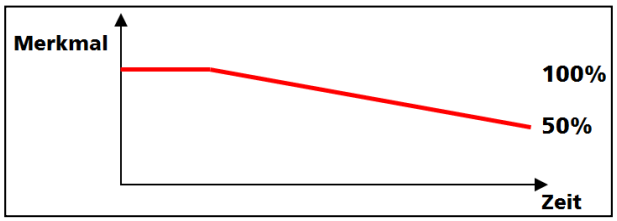
1. Das Signal reduziert sich plötzlich:



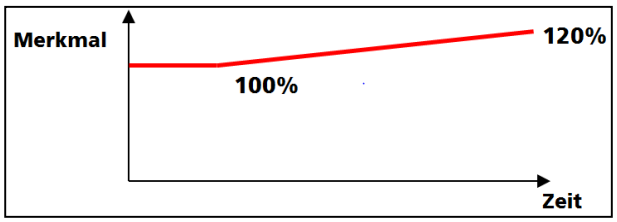
2. Das Signal alterniert unerwartet:



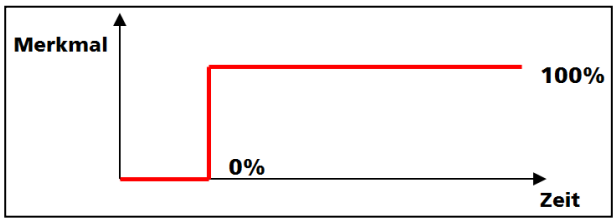
3. Das Signal nimmt langsam über die Zeit ab:



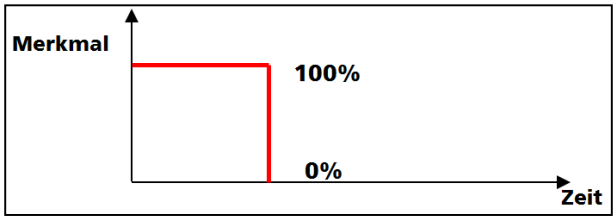
4. Das Signal nimmt langsam über die Zeit zu:



5. Ein Signal liegt ungewollt an:



6. Ein Signal ist unerwartet nicht mehr vorhanden:



Betrachtet werden müssen auch solche Situationen, in denen Eingangssignale eines Teilsystems, gewollt oder ungewollt, von einem anderen System manipuliert werden.

Anhand eines Beispiels soll dieses Problem verdeutlicht werden:
Nebenaggregate (z. B. Pumpen zur Umwälzung von Kühlwasser und Öl, Unterstützung der Lenkung oder des Klimakompressors) werden heute aus verschiedenen Gründen elektrifiziert. Ein Grund ist das Potenzial zur Reduktion des Kraftstoffverbrauchs. Nicht benötigte Aggregate werden abgeschaltet oder entsprechend der aktuell benötigten Leistung geregelt. [Winner, H.; Hakuli, S., et al. 2009] Das Klimaaggregat kann im Zuge der Leistungsregulierung gewisse Anforderungen an das Motormanagement-System stellen, um im Stand genügend Leistung zur Kühlung des Fahrzeuginnenraums zu erhalten. Dazu hebt das Motorsteuergerät die Leerlaufdrehzahl an. Die elektromechanische Parkbremse hat eine Komfortfunktion mit der Bezeichnung „Auto Hold“ (vergleichbar mit der „Hill Hold“-Funktion). Diese Funktion ermöglicht es dem Fahrer, das Fahrzeug z. B. an einer roten Ampel temporär festzusetzen. Beim Gasgeben löst das Bremssystem die Bremse automatisch und ermöglicht so ein zügiges und ruckfreies Anfahren.

Jedes der Teilsysteme funktioniert für sich gesehen fehlerfrei. Allerdings kann es in Kombination mit anderen Teilsystemen zu einem gefahrbringenden Fehler kommen.

Steigt der Fahrer bei hohen Temperaturen im Sommer z. B. kurz aus seinem Fahrzeug aus, um seine Garage zu öffnen, so kann durch die geöffnete Autotür eine große Menge warmer Umgebungsluft ins Autoinnere strömen. Die Klimaanlage kann das Fahrzeuginnere nicht mehr auf die voreingestellte Temperatur kühlen, da der kontinuierliche Zustrom

warmer Umgebungsluft das Klimaaggregat schnell an sein aktuell definiertes Limit der Leistungsaufnahme bringt. Das Klimagerät kann daraufhin mehr Leistung vom Motormanagementgerät anfordern, um die erforderliche Kühlleistung bereitzustellen. Das Motormanagement erhöht infolgedessen die Leerlaufdrehzahl. Diese Drehzahl wird dann von der EPB ausgelesen, erkennt u. U. einen Wegfahrwunsch des Fahrers und öffnet die Bremsen. An einer ebenen Straße wird das Auto stehen bleiben und der Fahrer bemerkt nichts von der potenziellen Gefährdung. Ist die Straße dagegen leicht abschüssig, so kann das Fahrzeug offenbar „ohne Grund“ davonrollen. Diese Situation stellt sowohl für den Fahrer, mögliche Insassen wie auch für andere Verkehrsteilnehmer einen gefahrbringenden Zustand dar.

2.2.2.2 Schnittstellenbetrachtung anhand einer FMEA

Ein Ansatz zur Untersuchung von Schnittstellen ist die Fehlermöglichkeits- und Einflussanalyse (FMEA).

Bei dieser Methode handelt es sich um einen Ansatz zur Fehlerermittlung und Darstellung der daraus resultierenden Risiken, Problemen und Gefahren. Dabei wird zwischen verschiedenen FMEA-Arten unterschieden. Die wichtigsten drei sind folgende:

- Produkt-FMEA, Konstruktions-FMEA (K-FMEA)

  Die Produkt-FMEA bzw. Konstruktions-FMEA betrachtet die geforderten Funktionen von Produkten und Systemen bis auf die Auslegung der Eigenschaften und Merkmale.

  Dabei werden die möglichen Abweichungen betrachtet und die Maßnahmen zur Sicherstellung der Forderungen definiert. [Verband der Automobilindustrie e. V. 1996]

- Prozess-FMEA (P-FMEA)

  Die Prozess-FMEA betrachtet alle Abläufe zur Herstellung von Produkten und Systemen bis zu den Anforderungen an die Prozesseinflussfaktoren.

  Dabei werden die möglichen Abweichungen betrachtet und die Maßnahmen zur Sicherstellung der Abläufe und der Produktmerkmale definiert. [Verband der Automobilindustrie e. V. 1996]

- System-FMEA (S-FMEA)

  Die System-FMEA betrachtet das Zusammenspiel von verschiedenen Teilsystemen in einem übergeordneten Systemverbund bzw. das Zusammenwirken mehrerer Komponenten in einem komplexen System. Das Ziel ist die Identifikation potenzieller Schwachstellen. Dabei stehen insbesondere die vorhandenen Schnittstellen im Vordergrund, bei denen durch das Zusammenwirken der einzelnen Komponenten oder die Interaktion des eigenen Systems mit der Umgebung Fehler entstehen können. Die Betrachtung beinhaltet zufällige und systematische Fehler während des Betriebes. [Verband der Automobilindustrie e. V. 1996], [Bertsche, B.; Lechner, G. 2004]

Die Anwendung der einzelnen FMEA-Arten orientiert sich hierbei an dem **P**rodukt**e**ntstehungs**p**rozess, kurz PEP. Abbildung 19 auf der folgenden Seite zeigt den Einsatz der verschiedenen FMEAs anhand einer beispielhaften Getriebeentwicklung:

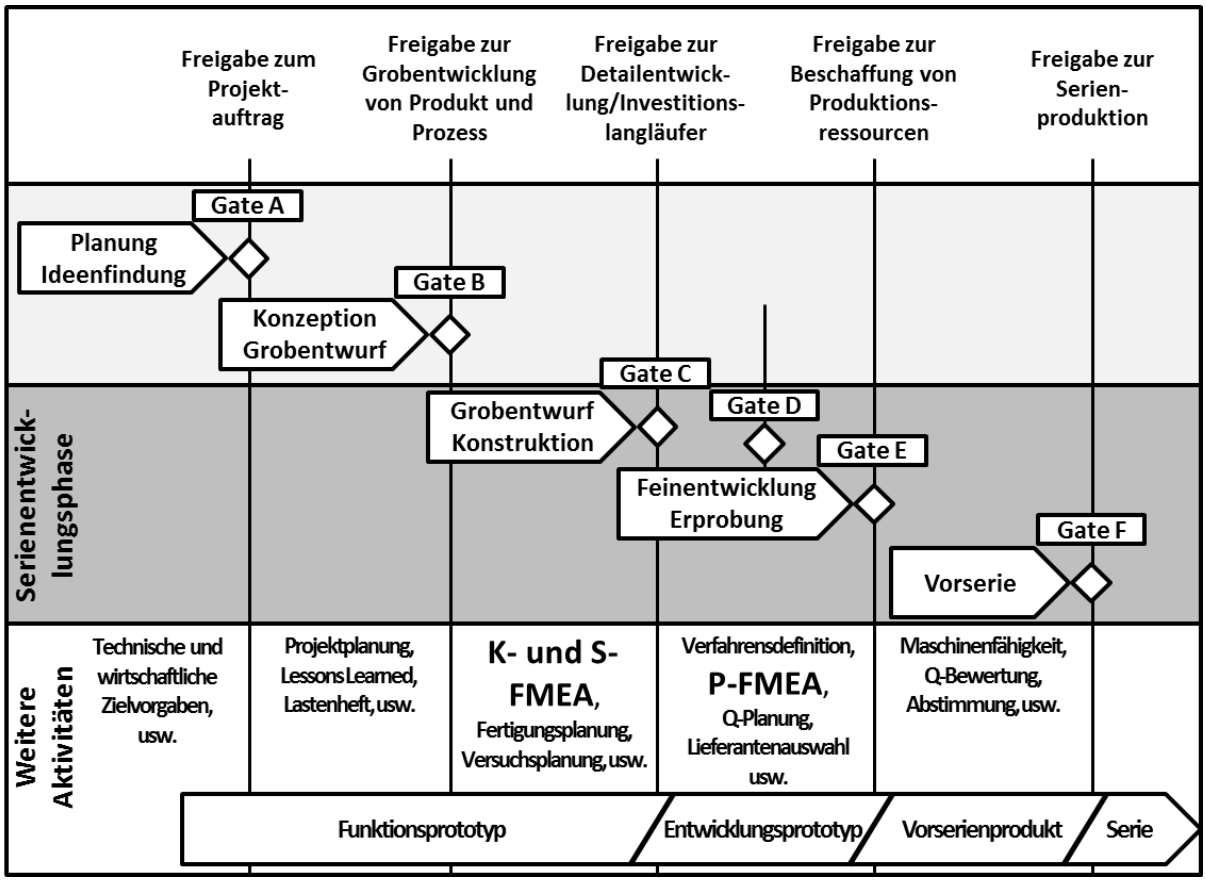


Abbildung 19 – FMEA-Arten im PEP [Lechner, G.; Naunheimer, H., et al. 2007] - modifizierte Darstellung

Von den existierenden FMEA-Arten eignet sich besonders die System-FMEA für mechatronische Produkte und deren Schnittstellen.

Bei der System-FMEA werden die Schnittstellen eines Produkts betrachtet. Dazu werden alle Inputs und Outputs eines Systems analysiert und mit hypothetischen Fehlern belegt. Hierzu wird nur die Frage gestellt, welche potenziellen Fehler bei In- und Outputs auftreten können. Warum die Fehler auftreten, ist an dieser Stelle nicht von Interesse. Anschließend werden die Auswirkungen der möglichen Fehler betrachtet. Basierend auf diesen Ergebnissen werden Optimierungsmöglichkeiten gesucht.

In Abbildung 20 ist ein Auszug einer System-FMEA dargestellt, der unter Verwendung der in der Automobile-Branche weitverbreiteten Software „APIS IQ-RM“ entstanden ist.

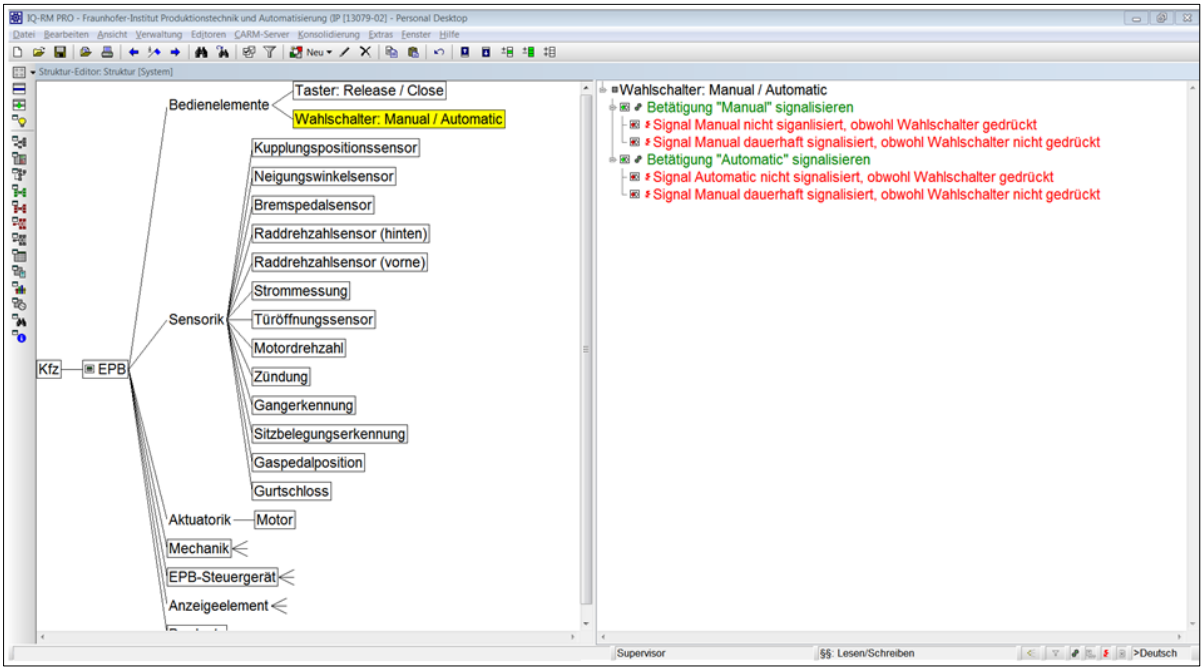
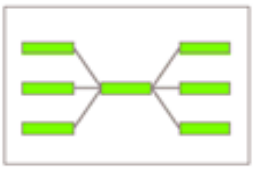


Abbildung 20 – System-FMEA in APIS IQ-RM Pro

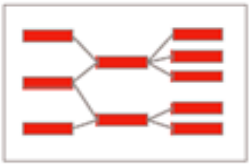
Die FMEA wird im Idealfall in fünf Schritten nach der VDA-Vorgehensweise aus dem VDA-Band 4, Kapitel 3 aufgebaut. [Verband der Automobilindustrie e. V. 1996]

1. **System-Strukturierung:**
   - Welche Input-Schnittstellen gibt es?
   - Welche Output-Schnittstellen gibt es?

2. **Funktions-Analyse**
   - Welche Informationen/Daten/Signale werden an den Inputs erwartet?
   - Welche Informationen/Daten/Signale müssen ausgegeben werden (Outputs)?



3. **Fehler-Analyse**



- Welche Fehler kann es bei den Inputs geben?
- Welche Fehler kann es bei den Outputs geben?

4. **Maßnahmenanalyse und Bewertung**

- Erarbeitung von Maßnahmen, um die Inputs zu überprüfen, damit sie bei fehlerhaften/fehlenden Signalen in den sicheren Zustand übergehen und darin verbleiben (Fehlererkennung und –reaktion).
- Erarbeitung von Maßnahmen, um sicherzustellen, dass die Outputs korrekt ausgegeben werden.
- Durchführung von Tests, um die Wirksamkeit von Maßnahmen sicherzustellen und die Anforderungen seitens der ISO 26262 zu erfüllen (Testing).

5. **Optimierung der Maßnahmen (sofern notwendig)**

- Weitere Verbesserung und Optimierung der Fehlererkennung und Fehlerreaktion bei nicht spezifizierten Input-Signalen.
- Weitere Verbesserung und Optimierung zur Sicherstellung der Output-Signale.

Die FMEA ist eine, auch außerhalb der Automobil-Branche, stark verbreitete, akzeptierte und bewährte Methode. [Schloske, A. 2011a] Sie ermöglicht es, ein System mit überschau- und vertretbarem Aufwand detailliert zu analysieren, Schwachstellen aufzudecken und Handlungsanweisungen zur Optimierung abzuleiten. Durch das systematische Vorgehen wird zudem sichergestellt, dass keine Schnittstellen übersehen werden. [Enger-Wiechers, E. 2008]

Kritische Würdigung der Schnittstellenbetrachtung anhand einer System-FMEA

Die FMEA ermöglicht es, ein System unter Betrachtung verschiedener Aspekte systematisch und konsequent zu untersuchen. Die Stärke der System-FMEA ist die detaillierte Be-

trachtung der Inputs und Outputs (Schnittstellen) eines Produkts im Rahmen der definierten Systemgrenzen.
Wichtig ist, die Grenzen und Nachteile dieser Schnittstellenbetrachtung zu kennen, auch wenn diese nicht zwangsläufig der FMEA zuzuordnen sind. Mit der FMEA werden nur Schnittstellen analysiert, die innerhalb des zu betrachtenden Systems liegen sowie an dieses angrenzen. Die zulässigen Veränderungen von Input-Signalen durch Steuergeräte Dritter und die daraus möglicherweise resultierende ungewollte Funktionsausführung werden nicht erfasst, da diese keinen Einblick auf Systeme außerhalb ihres Einflussbereichs haben.

2.2.3 Durchgängige Umsetzung und Dokumentation der Anforderungen

Nachdem die Entwicklungsanforderungen durch die ASIL-Determinierung festgelegt sind und die Entwicklungsarbeiten begonnen haben, ist es im weiteren Verlauf erforderlich, die vollständige und korrekte Umsetzung der Kunden- sowie Normanforderungen samt Dokumentation sicherzustellen. Aufgrund der Komplexität sowie der Vielzahl von Funktionen und Schnittstellen ist dies eine besondere Herausforderung und erfordert eine hohe Disziplin.

Fehler während der Entwicklung in Form von nicht oder fehlerhaft implementierten Funktionen bedeuten ein hohes Maß an Nacharbeit, verbunden mit hohen und unnötigen Kosten.

Abbildung 21 auf der folgenden Seite stellt den zeitlichen Verlauf der Fehlerentstehung sowie die Korrelation mit der Fehlerbeseitigung und den damit verbundenen, notwendigen Kosten („Rule of 10“ bzw. „1-10-100“-Regel) über den Produktlebenszyklus dar:

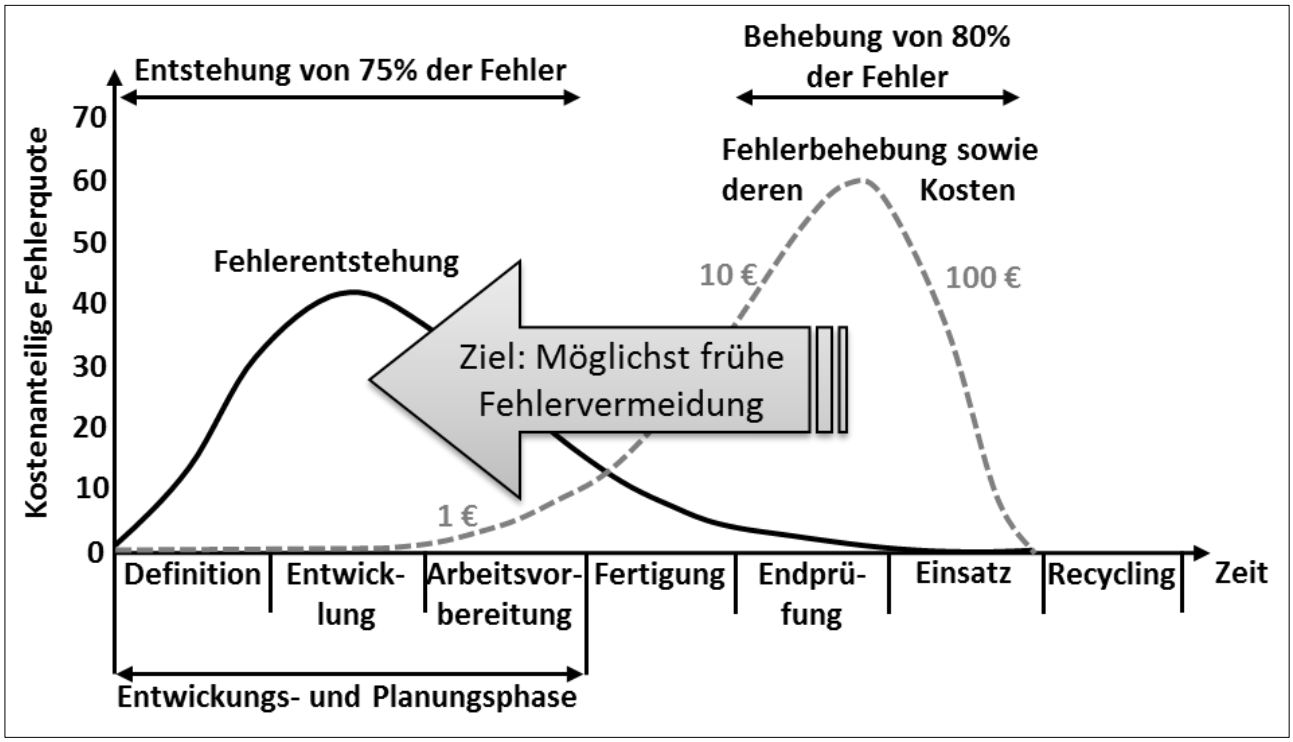


Abbildung 21 – Fehlerentstehung sowie Fehlerbehebung [DGQ 2008] - modifizierte Darstellung

Reifegradmodelle wie SPICE ISO/IED 15504 oder CMMI bewerten beispielsweise auf Basis praxisbewährten Vorgehensweisen die Reife einzelner Prozessschritte anhand definierter Kriterien. [Verband der Automobilindustrie e. V. 2010b] Insbesondere bei der Entwicklung sicherheitskritischer Systeme wird ein hohes Maß an Nach- bzw. Rückverfolgbarkeit (Traceability) über den gesamten Entwicklungsprozess verlangt. Ziel ist es hierbei, die verschiedenen Anforderungen von deren Entstehung/Ermittlung bis hin zur vollständigen Implementierung verfolgen zu können. [Chrissis, M. Beth; Konrad, M., et al. 2009]

Ähnliche Ansätze zur Durchgängigkeit verfolgt der VDA mit seiner „Besonderen Merkmal“-Strategie. [Verband der Automobilindustrie e. V. 2010a] Dabei geht es insbesondere um

- die Festlegung,
- die Herstellung
- sowie die Dokumentation der besonderen Merkmale.

Zusammengefasst gibt es drei Schritte, die durchgängig und nachvollziehbar behandelt werden müssen:

1. Erfassung der Anforderungen
2. Umsetzung der Anforderungen
3. Dokumentation der Umsetzung sowie deren Prüfung (Testing/Validierung)

2.2.3.1 Grundsätzliches Problem bei der Durchgängigkeit

Das grundsätzliche Problem und die besondere Aufgabe bestehen vor allem darin, den gesamten Entwicklungsprozess zu verfolgen und lückenlos zu dokumentieren. Dies bedeutet, dass alle in den frühen Phasen des Produktentstehungsprozesses ermittelten, wie auch die im Nachhinein geänderten, sowie die neu hinzugekommenen oder auch die weggefallenen Anforderungen nahtlos erfasst werden müssen. (vgl. Besondere Merkmale [Verband der Automobilindustrie e. V. 2010a])

Dies umfasst folgende Aufgaben:

- Implementierung der initialen Anforderungen
- Implementierung von Anforderungsänderungen (inkl. Wegfall)
- Implementierung nachträglicher, neuer (Kunden-)Anforderungen
- Gefährdungs- und Risikoanalyse (GuR) der Anforderung im Kontext der funktionalen Sicherheit (ISO 26262)
- Implementierung von neuen, abgeleiteten Anforderungen aus der GuR
- Dokumentation der Anforderungsumsetzung sowie der Testmaßnahmen

Allerdings gibt es zur Bewältigung der Anforderungen bzw. der Abänderungen kein einheitliches und durchgängiges Werkzeug. Stattdessen gibt es unterschiedliche Softwaretools, die in den verschiedenen Phasen genutzt werden können.

Requirement Engineering und Requirement Management (RE&M)

Das RE&M ist dafür verantwortlich, im Produktentstehungsprozess die Anforderungen sowie deren dazugehörigen Eigenschaften zu sammeln, zu analysieren und weiterzuentwickeln. Dabei wird unter einer Anforderung die Festlegung hinsichtlich zu erbringender Produkt- sowie Prozesseigenschaften bzw. Produkt- und Prozessleistungen verstanden. Zusätzlich fällt darunter auch die Leistung von Menschen an den beteiligten Prozessen, die Beschaffenheit von Produktmerkmalen sowie die Bedingungserfüllung hinsichtlich des RE&M. [Pohl, K.; Rupp, C. 2009] Nicht zuletzt muss das RE&M diese Anforderungen verfolgen und verwalten. Hierbei stellen die Anforderungen aus dem Lasten- bzw. Pflichtenheft die Grundlage für den späteren Entwurf des Produkts dar.

Fehler, die bereits in der Entstehungsphase entstehen, lassen sich meist nur unter hohem Einsatz von personellen und monetären Ressourcen korrigieren (siehe Abbildung 21). Im Extremfall führen diese Fehler zum Scheitern des Projekts, da die Mängel des RE&M häufig erst sehr spät im Produktentstehungsprozess bzw. bei der Kundenabnahme aufgedeckt werden. [Partsch, H. 2010]

Verschiedene Studien und Untersuchungen zeigen einen deutlichen Zusammenhang zwischen der Qualität der Anforderungen und dem Erfolg in der Produktentwicklung. [Kamata, M. I.; Tamai, T. 2007]

Im Rahmen der ISO 26262 ist es ferner wichtig, die Anforderungen in zwei Bereiche zu unterteilen:

1. **Externe Anforderungen**
   Anforderungen, die durch den Kunden (OEM) des Systems an dieses gestellt und eingefordert werden. Dazu gehören zum Beispiel:
   - Vorhandensein und korrekte Funktion der geforderten Funktionalitäten
   - Erfüllung der Anforderungen bzgl. der Robustheit des Produkts
   - Einhalten der Bauraumvorgaben
   - Einhalten der Gewichtsvorgaben

2. **Interne Anforderungen**

   Anforderungen, die sich aus den externen (OEM-) Anforderungen ableiten, selbst definiert sind oder im Rahmen der funktionalen Sicherheit notwendig sind:

   - Integration von Diagnose-Funktionen
   - Durchlaufen diverser Testing-Szenarien/-Strategien
   - Einhaltung der Vorgaben der funktionalen Sicherheit (ISO 26262)
   - Wahl der Materialien, um z. B. die Robustheit zu erfüllen
   - Auswahl geeigneter Fertigungsverfahren

Insbesondere bei mechatronischen Systemen sind die Anforderungen und Testing-Szenarien aus der funktionalen Sicherheit am Entwicklungsanfang nur sehr grob umrissen oder gänzlich unbekannt und ergeben sich erst aus der Gefahren- und Risikoanalyse. [Maier, C.; Schloske, A., et al. 2013]

Interne und externe Anforderungsdefinition

Im Gegensatz zu vielen anderen Branchen und Bereichen läuft die Produktentwicklung in der Automobil-Branche sehr verteilt und dezentralisiert ab (siehe Abbildung 5). Dieser Zustand ist in Abbildung 22 auf der folgenden Seite dargestellt. Zusätzlich ist dort eine mögliche Weiterentwicklung weg von der Wertschöpfungskette hin zum Wertschöpfungsnetz für die kommenden Jahre abgebildet.

Das führt dazu, dass durch den OEM die Grundanforderungen zentralisiert eingesteuert werden, diese sich anschließend von Stufe zu Stufe weiterverteilen und sich damit im Entwicklungsnetz vererben.

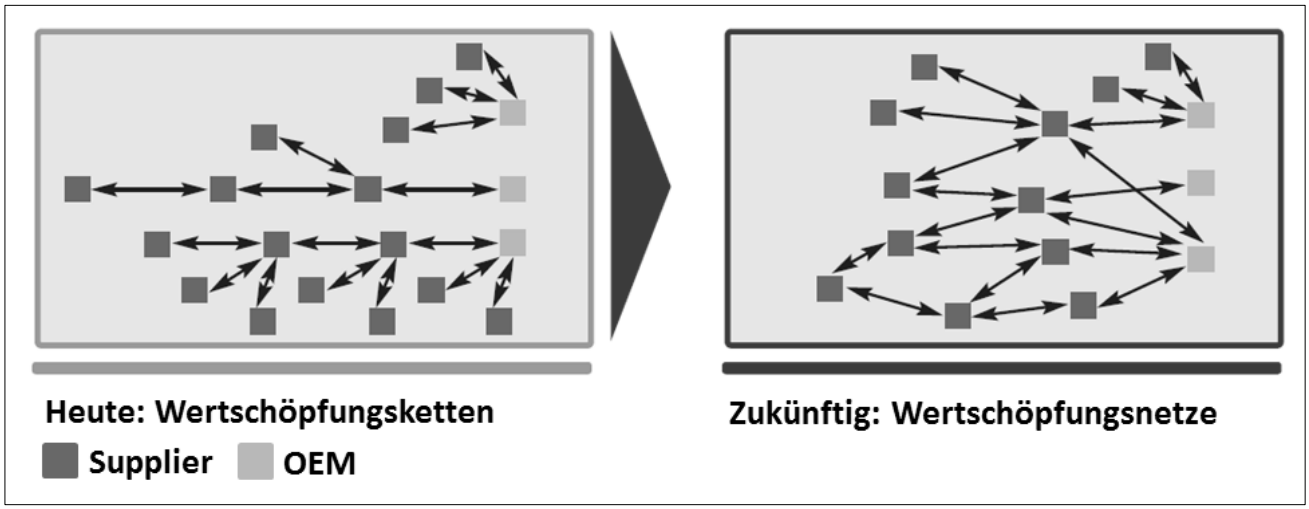


Abbildung 22 – Veränderungen des Wertschöpfungssystems [T-Systems Enterprise Services GmbH 2009]

Um nun die externen Komponenten- und Systemanforderungen im Lieferantengeflecht unter Berücksichtigung der verschiedenen Interessen realisieren zu können, müssen zu Beginn vom Kunden (meist OEM oder 1st Tier– nicht der Endkunde) die Anforderungen initial definiert werden. Dieser Vorgang wird durch die Nutzung entsprechender Software-Tools unterstützt. Zu diesen CARE-Tools (**C**omputer **A**ided **R**equirements **E**ngineering) gehören neben Microsoft Word und Excel unter anderem DOORS, RequisitePro, RTM Workshop, CaliberRM und IrqA. [Shahid, M.; Ibrahim, S., et al. 2011], [Partsch, H. 2010] Die Tools ermöglichen es, Anforderungen zu erfassen und zu verwalten. Anschließend können die definierten Anforderungen gezielt an Lieferanten und Partner kommuniziert werden. Zusätzlich können deren Anmerkungen und Rückfragen bzgl. einzelner Anforderungen entgegengenommen und verarbeitet werden. Der sich daraus ergebene Regelkreis präzisiert über die einzelnen Iterationsschleifen die (externen) Anforderungen, bis diese schließlich als final betrachtet werden können. Zu beachten ist, dass während des Entwicklungsprozesses jederzeit Anforderungen hinzukommen und/oder wegfallen können.

Die internen Anforderungen hingegen werden, so weit möglich, zu Beginn selbst vom Lieferanten bzw. Entwicklungspartner festgelegt. Viele der Funktionen und Anforderungen,

besonders zur Beherrschung kritischer und/oder gefährlicher Zustände, ergeben sich nur sukzessiv aus der Risikobetrachtung beispielsweise durch die FMEA.

Es sind aber nach Ansicht des Autors genau diese erarbeiteten, internen Anforderungen besonders kritisch, da sie im Falle einer fehlenden oder fehlerhaften Implementierung zur Gefährdung von Menschen führen können und im Vorfeld nicht bekannt sind.

Bereits an diesem Punkt wird im Allgemeinen in verschiedenen, voneinander unabhängigen Systemen gearbeitet (CARE- sowie FMEA-Tool). Allerdings fehlt noch die Dokumentation der Umsetzung wie auch das Testing inkl. der Ergebnisse, was zum Einsatz weiterer Tools führt.

Umsetzung von Anforderungen

Im Bereich der Funktionalen Sicherheit ist es unerlässlich, die internen und externen (Sicherheits-) Anforderungen hinsichtlich ihres Risiko- und Gefahrenpotenzials zu untersuchen. Dies kann durch die FMEA realisiert werden. [ISO 26262-3 2011-11-15]

Die Vorgehensweise der FMEA ermöglicht es, die Anforderungen hinsichtlich systematischer wie auch zufälliger Fehler zu untersuchen.

- *Systematische Fehler* sind Fehler, die aufgrund menschlichen Versagens in den verschiedenen Stadien des Lebenszyklus auftreten. Dazu zählen Spezifikationsfehler, Entwurfsfehler, Implementierungsfehler und Installations- oder Bedienungsfehler.

- *Zufällige Fehler* sind das Ergebnis der begrenzten Zuverlässigkeit von Hardwarebauteilen. [Löw, P.; Pabst, R., et al. 2010]

Zudem können in der FMEA weitere sicherheitsrelevante Anforderungen und Funktionen durch die Risikobetrachtung sowie entsprechende Testing-Szenarien abgeleitet werden.

Abbildung 23 zeigt beispielhaft die integrierte Darstellung von systematischen und zufälligen Fehlern.

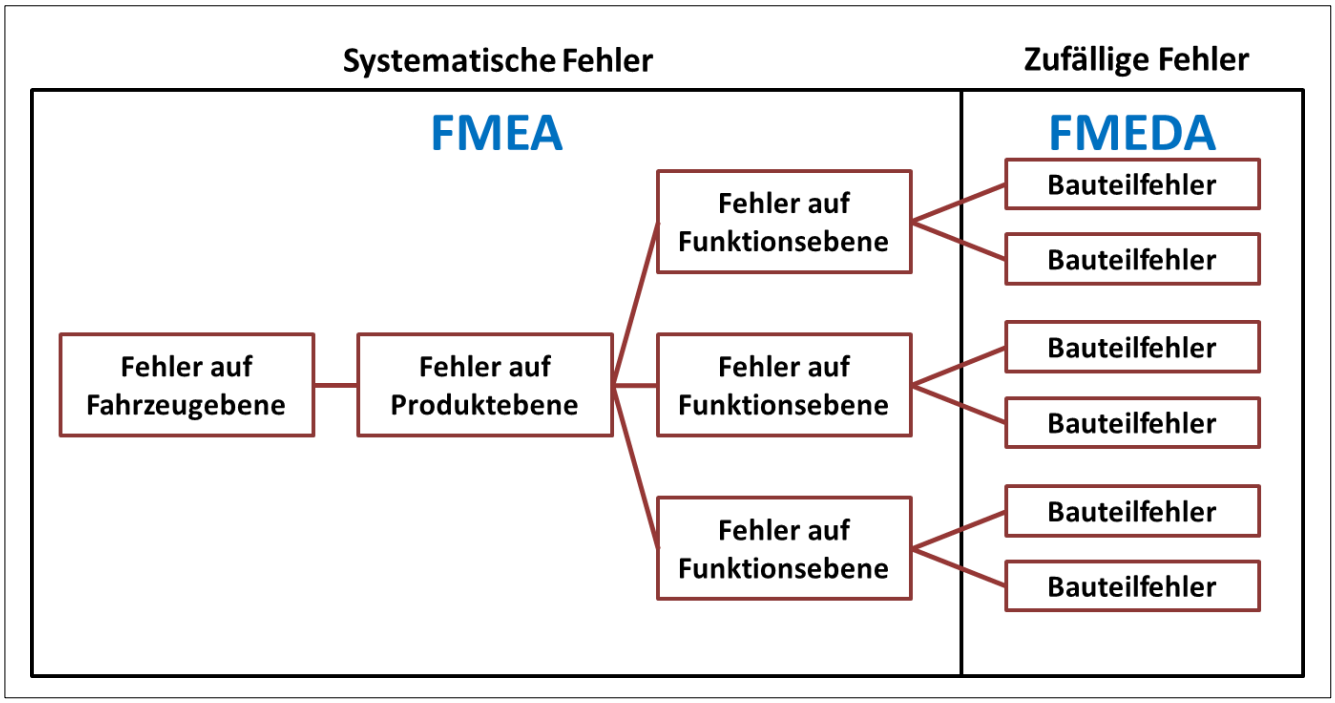


Abbildung 23 – Fehlerbetrachtung mit der FMEA im Kontext der Funktionalen Sicherheit [Schloske, A. 2012] - modifizierte Darstellung

Dabei wird bei der reinen Betrachtung zufälliger Fehler von der **F**ailure **M**ode, **E**ffects and **D**iagnostic **A**nalysis (kurz FMEDA) gesprochen. [Schloske, A. 2012]

Der Prozess zur Funktions-/Anforderungsumsetzung sowie der Risikoanalyse kann, wie in Abbildung 24 auf der folgenden Seite dargestellt, durchgeführt werden. Dabei werden nach der Gefahren- und Risikoanalyse die Anforderungen in Form von Komponenten und deren Funktionen in der FMEA verknüpft. In der Folge werden mögliche systematische sowie zufällige Probleme und Gefahren erarbeitet und durch das Fehlernetz dargestellt. Anschließend werden entsprechende Maßnahmen zur Vermeidung bzw. Entdeckung definiert. Dabei ergeben sich neue interne Anforderungen bezüglich der Diagnosefähigkeit, die sich ihrerseits auf die Erhöhung des Diagnosedeckungsgrads (Definition, siehe Seite 25) auswirken. Daraus resultieren wiederum interne Anforderungen an das Testing. Dieses muss dann sicherstellen, dass die Diagnosefunktionen, wie vorgesehen, die zufälligen Fehler erkennt und das System in einen sicheren Zustand überführt.

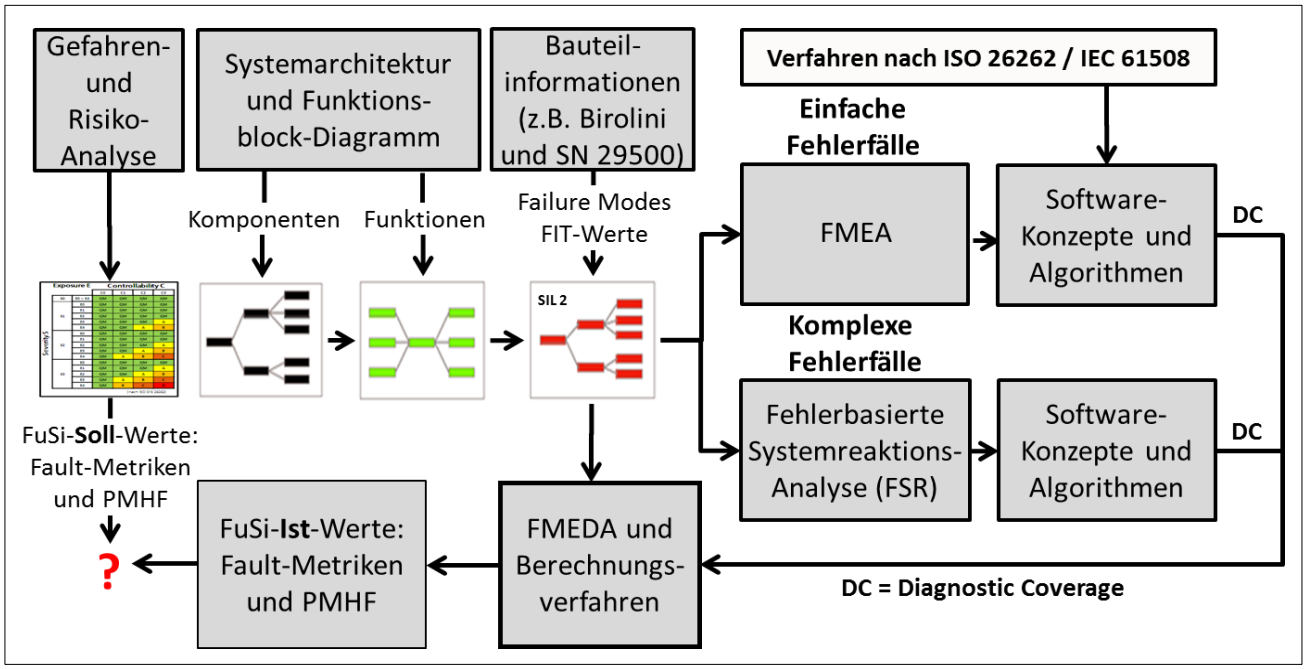


Abbildung 24 – Vorgehensmodell bei der ISO 26262 unter Verwendung der FMEA [Schloske, A. 2012]

Der dargestellte Gesamtprozess, d. h. alle resultierenden, internen Anforderungen sowie die Testings mit den Ergebnissen, müssen nachvollziehbar dokumentiert werden.

Dokumentation der Anforderungs- und Testing-Szenarien-Umsetzung

Die Dokumentation ist eine wichtige und nicht zu unterschätzende Forderung bei der Entwicklung funktional sicherer Systeme. Allein die ISO 26262 sieht mehr als 90 verschiedene „Work Products“ vor, von denen einige am Ende im „Safety Plan“ münden.

Der Safety Plan ist ein Dokument in Textform mit Anhängen, Tabellen und Verweisen auf Dritt-Dokumente zu spezifischen Entwicklungsaspekten. Mit diesem Safety Plan sollen organisatorische Rahmenbedingungen, Verantwortlichkeiten und die Entwicklungstätigkeiten festgehalten werden, um sicherzustellen, dass die Sicherheitsanforderungen erfüllt sind. Er ist ein Planungs- und Steuerungsinstrument und soll als Informationsdrehscheibe für alle Beteiligten sowie als Entlastungsdokument im Streitfall (Produkthaftung) dienen.

Der Safety Plan ist das zentrale Dokument für das Management der funktionalen Sicherheit. Allerdings enthält die Norm keine verbindlichen Kriterien für den Inhalt des Safety Plans, jedoch sind häufig die folgenden Inhalte vorhanden:

- *Strategie*: Wie wird grundsätzlich vorgegangen, um die funktionale Sicherheit zu erreichen?
- *Arbeitspakete*: Welche Arbeitspakete werden zur funktionalen Sicherheit ausgeführt?
- *Ergebnisse*: Welche Arbeitsprodukte werden zur funktionalen Sicherheit im Lauf des Projekts erzeugt?
- *Phasen und Meilensteine*: In welchen Phasen wird vorgegangen?
- W*esentliche Meilensteine: Welche* gibt es in dem Projekt und was ist darunter jeweils zu verstehen? Wie ist der Sicherheitslebenszyklus auf das Phasenmodell abgebildet?
- *Zeitplan*: Wie ist der Zeitplan?
- *Ressourcen*: Welche wesentlichen Ressourcen werden benötigt und sind geplant?
- *Rollen und Personenzuordnung*: Welche Rollen zur funktionalen Sicherheit existieren? Wie sind sie definiert und welche Personen nehmen diese Rollen ein?
- *Beurteilung der funktionalen Sicherheit*: Welche Beurteilungen der funktionalen Sicherheit sind geplant und von wem werden diese durchgeführt?
- *Normen und Standardprozesse*: Welche Normen und Standardprozesse sollen zur Anwendung kommen?
- *Projektspezifische Prozesse*: Welche projektspezifischen Regelungen werden getroffen? [Löw, P.; Pabst, R., et al. 2010]

Das Problem ist allerdings, dass eine durchgängige Dokumentation nur mit erheblichem Aufwand zu erreichen ist. Bei jeder Änderung einer Anforderung bzw. deren Umsetzung und dessen Testing muss dies „manuell“ nachgepflegt werden. Zudem existieren organisatorische Probleme, da es im Unternehmen verschiedene Bereiche und unterschiedliche Personen gibt, die für die einzelnen Tätigkeiten zuständig sind. Daraus resultieren unwei-

gerlich Fehler in der Umsetzung und Dokumentation, die ihrerseits zu Inkonsistenzen führen.

Kritische Würdigung der Anforderungsdurchgängigkeit

Prinzipiell gibt es für alle Teildisziplinen wie Anforderungsermittlung, -umsetzung und Dokumentation unterstützende Tools, Hilfsmittel und Vorlagen sowie normative Vorgaben. Allerdings wird damit nicht die gewünschte und von mehreren Seiten geforderte Durchgängigkeit sowie Transparenz geschaffen, da die vielen Tool- und Dokumenten-Schnittstellen oft zu Fehlern und Inkonsistenzen führen.

Konkret bedeutet dies, dass die Anforderungsdefinitionen nicht oder nicht ausreichend mit der Betrachtung, Umsetzung und Risikoanalyse in der FMEA verknüpft sind. Zusätzlich werden diese externen und internen Anforderungen ebenso wie die aus der FMEA resultierenden Anforderungen (in Form von Sicherheitsfunktionen, Vermeidungs-, Entdeckungsmaßnahmen sowie Tests) oft nicht weiter mit dem Safety Plan verknüpft.

Begründet werden kann diese Gesamtproblematik damit, dass die einzelnen Tools keine Schnittstellen untereinander haben und jeder Bereich, der an der Projektumsetzung beteiligt ist, ein anderes Werkzeug und Dokument als Basis einsetzt. Das liegt nicht zuletzt daran, dass die Entwicklungs- und Dokumentationswerkzeuge sowie die Arbeitsdokumente nicht für alle Personen im Unternehmen gleichermaßen zugänglich sind und deren Bedienung bzw. Strukturierung meist unklar ist.

Zusammengefasst sind folgende Hindernisse identifiziert:

- Unterschiedliche Softwaretools als Arbeitsbasis
- Keine (automatisiert nutzbare) Schnittstellen zwischen den Softwaretools
- Kein Zugriff auf Tools aus anderen Bereichen
- Fehlende Bedienungskenntnisse bei „fremden“ Tools

3 Lösungsansätze

In diesem Kapitel sollen die möglichen und gewählten Lösungsansätze kurz beschrieben werden. Dabei werden die folgenden, eingangs erarbeiteten und dargestellten Probleme behandelt:

1. Nachvollziehbare ASIL-Einstufung unter Betrachtung von Länder- und Regionsspezifika.
2. Beschreibung eines Ansatzes zur Abstimmung der System-Schnittstellen zwischen Kunde und Entwickler sowie anderen KFZ-Systemen.
3. Herangehensweise zur systematischen Umsetzung und Dokumentation von Anforderungen und Funktionen des Produkts/Systems.

3.1 Ansatz um eine nachvollziehbare ASIL-Klassifizierung zu gewährleisten

Wie bereits in Abschnitt 2.2.1.1 (Seite 30) beschrieben, ist der Faktor Severity aufgrund der weltweit vergleichbaren menschlichen Anatomie und der körperlichen Belastbarkeit quasi identisch.

Ebenso verhält es sich mit der Controllability (Seite 33). Hier können die Fahrfähigkeiten der Fahrzeugführer leicht ermittelt, verifiziert sowie weltweit gleichgesetzt werden. Diese beiden Punkte bilden die Grundstruktur der weiteren Modellierung.

Um nun eine eindeutige, belegbare und reproduzierbare ASIL-Klassifizierung zu ermöglichen, muss der verbleibende dynamische Faktor „Exposure“ betrachtet und ein Vorgehen zur Ermittlung und Bewertung erarbeitet werden.

Im Gegensatz zur Normvorgehensweise soll von einer globalen, einheitlichen Bewertung einzelner Ereignisse bzw. Fahrsituation abgesehen werden. Stattdessen sieht der gewählte Lösungsansatz eine dynamische, individuelle Bewertung von Fahrsituationen auf Basis des tatsächlichen Zielmarkts und der dort herrschenden Rahmenbedingungen vor.

Um dies zu ermöglichen, ist ein dreistufiger Ansatz gewählt worden:

1. Im ersten Schritt müssen die tatsächlichen Einsatzorte des zu entwickelnden Systems ermittelt werden. Dies kann zum Beispiel auf Basis der Fahrzeug-Exporte erfolgen.

Quelle: http://commons.wikimedia.org

2. Im nächsten Schritt der Vorgehensweise ist es notwendig, die tatsächlichen Rahmenbedingungen der Systeme bzw. KFZs in den jeweiligen Einsatzorten zu ermitteln. Dazu sollen öffentlich verfügbare Informationen genutzt werden, um eine Transparenz und Nachvollziehbarkeit zu gewährleisten.

Quelle: Fotolia.com

3. Im letzten Schritt wird der endgültige Exposure-Wert durch die Kopplung von Export-Anzahl und Rahmenbedingung ermittelt.

Durch diese Vorgehensweise soll sichergestellt werden, dass subjektive Einflüsse der „Entwickler“ relativiert und herausgefiltert werden. Ebenso wird durch die systematische, nachvollziehbare Bewertung der durch die Norm vorgegebene Exposure-Wert hinterfragt und validiert. Zuletzt fördert die objektive Betrachtung die Dokumentation sowie Transparenz der ASIL-Ermittlung. Die daraus resultierenden Grundlagendaten sollen anschließend in das IT-Konzept, das in Abschnitt 3.2 erarbeitet wird, integriert werden. Das Ziel dieser Integration ist eine durchgängige Grundlage für die ASIL-Klassifikation über die verschiedenen Entwicklungshierarchien zu gewährleisten.

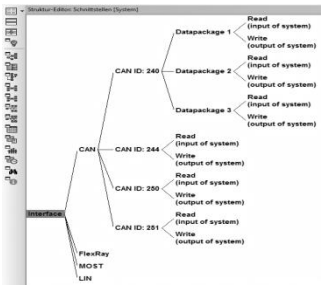
3.2 Ansatz, um die Ermittlung und Analyse von systemübergreifenden Schnittstellen sowie die durchgängige Anforderungsumsetzung und Dokumentation sicherzustellen

Für die beiden Teilprobleme „Ermittlung und Analyse von systemübergreifenden Schnittstellen“ (Abschnitt 2.2.2) sowie „Durchgängige Umsetzung und Dokumentation der Anforderungen“ (Abschnitt 2.2.3) soll ein gemeinsames IT-Konzept als Lösung dienen.

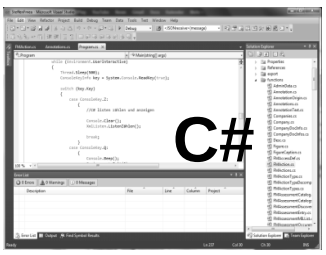
Um diese Lösung zu erreichen, soll die FMEA als zentraler Bestandteil genutzt werden. Diese wird dabei um einige grundlegende Aspekte erweitert:

- Zentralisierung der Datenbasis
- Überführung in ein erweiterbares Datenmodell
- Integration eines Zugriffs- und Rechtemanagements
- Globale Zugriffsmöglichkeiten
- Simultaneous Engineering
- Zentrales Maßnahmentracking
- Zentrale Dokumentenverwaltung
- Standardisierte Bereitstellung und Eingabe zwingend benötigter Schnittstelleninformationen

Um diese Anforderung erfüllen zu können, soll der bestehende FMEA-Ansatz im ersten Schritt durch die Remodellierung der FMEA-Daten um die neuen, zusätzlich notwendigen Objekteigenschaften und -attribute erweitert werden.



Im nächsten Schritt wird eine Client-Server-Architektur mit zentraler Datenhaltung zugrunde gelegt, in der rechtebasiert die Schnittstellen und Anforderungen sowie deren Details und Dokumentation darstellbar, editierbar sowie automatisiert auswertbar sind.



Mit der zentralen Datenhaltung und dem webbasierten Ansatz wird zudem die Möglichkeit eröffnet, die grundlegenden Schnittstellenzusammenhänge und -informationen einmalig zu erarbeiten und diese als Basis für die Kommunikation und Entwicklungsgrundlage aller Lieferanten bzw. Partner zu nutzen. Zusätzlich wird damit die Durchgängigkeit und Informationskonsistenz der Schnittstellen wie auch der Anforderungen sichergestellt, da alle auf den identischen Datenstamm zugreifen und mit diesem arbeiten können.

Bilder: Fotolia.com

Durch das zusätzlich implementierte Rechtemanagement werden die System- und Komponentenentwickler im Kontext der Schnittstellenumsetzung befähigt, ihre Inputs und Outputs der Schnittstellen selbst einzuarbeiten, einzusehen und manipulieren zu können.

Im Rahmen der Anforderungsumsetzung steuert das Rechtemanagement die Zugriffe auf die Maßnahmen sowie die Möglichkeit, daran Veränderungen vorzunehmen.

Bilder: Fotolia.com

Die integrierte Dokumentenverwaltung kann den Dokumentationsaufwand auf ein Minimum reduzieren, da auch hier wieder jeder Entwicklungspartner selbst die eigenen Schnittstellendokumente verwaltet.

Bei den Anforderungen können die unterschiedlichen, projektbeteiligten Mitarbeiter die Dokumente der Umsetzung wie auch die Ergebnisse der Tests selbst hinterlegen.

Quelle: Fotolia.com

Mit diesem Konzept werden unternehmensübergreifend alle mitwirkenden Mitarbeiter befähigt, gemeinsam an der Entwicklung eines Produkts zu arbeiten. Durch den integrierten Rechteansatz kann der unerwünschte Zugriff auf sensible Informationen verhindert werden. Nicht zuletzt ermöglicht die zentrale Datenhaltung sowie -verwaltung die Reduktion von Software-Tool-Schnittstellen und verringert damit die unerwünschten Dateninkonsistenzen.

4 Lösungsmodelle

Zu der in Kapitel 1 beschriebenen Entwicklung wurden im vorherigen Kapitel die einzelnen Lösungsansätze für die jeweiligen Probleme skizziert. In diesem Kapitel sollen nun diese Lösungsansätze sowie ihre Entstehung und Erarbeitung detailliert beschrieben werden.

4.1 ASIL-Klassifizierung

Um diese Anforderungen möglichst umfassend zu erfüllen, soll ein Ansatz zur Modellierung der Exposure gewählt werden, der öffentlich verfügbare, statistisch ermittelte Zahlen und Fakten zugrunde legt.

4.1.1 Ziel des neuen Ansatzes

Ziel des neuen Modells zur Klassifizierung des ASILs ist, die in der Norm vorgegebenen Exposure-Bewertungen für den jeweiligen Anwendungs- bzw. Entwicklungszweck präziser als bisher zu definieren. Dies soll zudem unter Berücksichtigung zweier Rahmenaspekte geschehen:

Zum einen ist dies die rechtliche *Seite*, die im Falle einer Klage bzw. eines Regressanspruchs, die für die Entwicklungsarbeit notwendige Einstufung des Produkts nach seinem Gefährdungspotenzial stichhaltig und nachvollziehbar begründen und verteidigen muss.

Zum anderen gibt es Anforderungen aus der Entwicklungsseite, die das neue Modell erfüllen muss, um eine verzögerungsfreie, angemessene Einstufung und damit spätere Entwicklung zu gewährleisten.

Um diesen Anforderungen gerecht zu werden, muss das Modell einige Basisanforderungen erfüllen. Darunter fallen:

- Neutralität
- Transparenz
- Objektivität
- Zeitlicher Aufwand
- Kosten

- Betrachtung von Einflussfaktoren
- Regional auswertbar

4.1.2 Modellierungsansatz

Die Idee hinter dem Modellierungsansatz sieht vor, die globalen Normvorgaben durch individualisierte Werte zu substituieren, um präzisere und begründbare Bewertungen zu erhalten.

Hierbei wird folgendermaßen vorgegangen:

1. Im ersten Schritt werden die für das Modell benötigten Informationen identifiziert und gruppiert.
2. Die Welt wird im zweiten Schritt in verschiedene, geografisch zusammenhängende Zonen eingeteilt.
3. Im dritten Schritt werden die benötigten Informationen gesammelt, strukturiert und statistisch ausgewertet bzw. aufbereitet.
4. Im letzten Schritt werden die ermittelten Informationen den geografischen Bereichen zugeordnet.

Für jeden dieser geografischen Bereiche sollen die verschiedenen Exposure-Bewertungen individuell erarbeitet werden.

4.1.2.1 Einteilung der Welt in verschiedene Zonen

Die Einteilung der Welt in verschiedene Zonen ermöglicht es, unkompliziert und schnell einen Überblick über die Rahmenbedingungen einzelner Bereiche der Welt zu erhalten, ohne die einzelnen Länder einer Region analysieren zu müssen.

Damit wird der Situation, dass Fahrzeuge bzw. Systeme nicht für einzelne Länder, sondern für ganze Zielmärkte/-regionen entwickelt werden, Rechnung getragen. Um die Welt in konkrete Zonen einzuteilen, wird die vorhandene kontinentale Einteilung als Grundlage genutzt. Auf Basis dieser Gruppierung wird im weiteren Verlauf der Modellentwicklung eine zusätzliche Unterteilung eingeführt. Dabei gibt es zwei Faktoren:

- Anzahl der Bevölkerung in der betrachteten Region
- Kontinent-Zugehörigkeit der Länder

Mithilfe dieser Kriterien entstehen in der Summe 10 Regionen/Zonen, die im weiteren Verlauf genutzt werden.

Sofern es, wie beispielsweise bei der Türkei, zu der Situation kommt, dass sich das Land über zwei Kontinente erstreckt, wird der Anteil der Landmassen am jeweiligen Kontinent als Faktor mit einbezogen. Das Land wird schließlich der Region, im Fall der Türkei also Nahost, zugeordnet, in der es die größere Landmasse besitzt.

Abbildung 25 zeigt die Zoneneinteilung anhand einer Weltkarte.

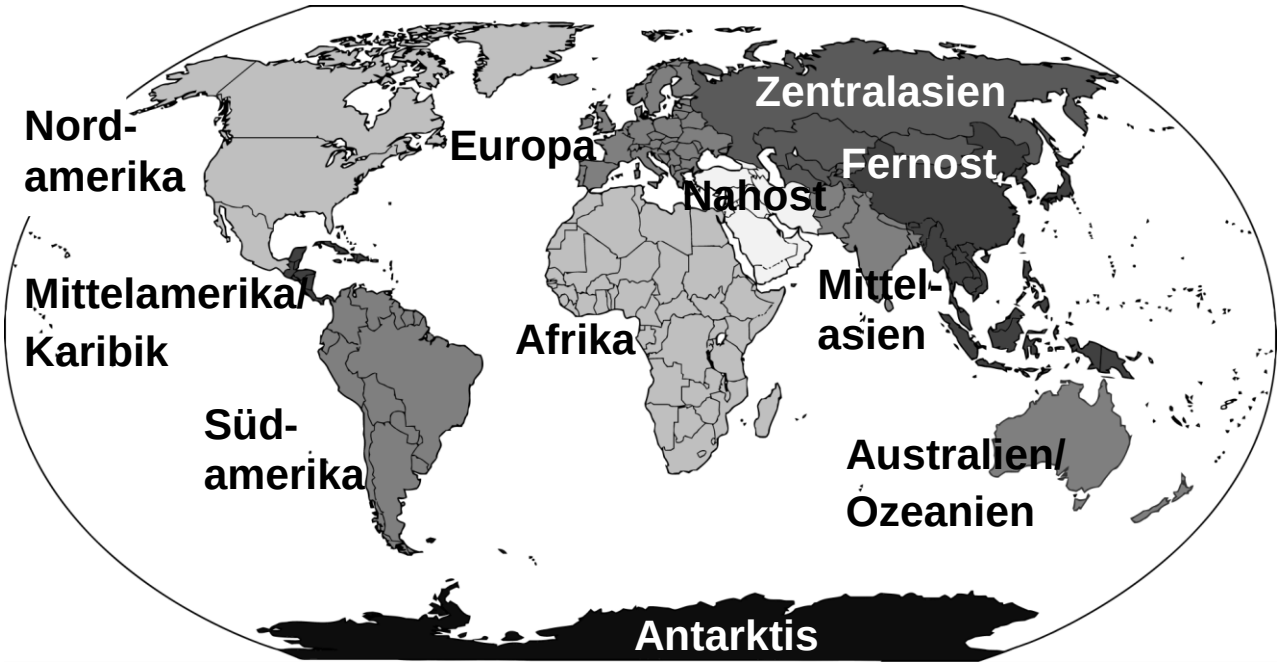


Abbildung 25 – Einteilung der Welt in Zonen - Bildquelle: http://commons.wikimedia.org

Das detaillierte Endergebnis der Einteilung ist in Tabelle 5 und Tabelle 6 auf den folgenden Seiten dargestellt. In den Tabellen sind die jeweiligen Ländername enthalten. Es ist zu beachten, dass nur Länder aufgeführt sind, von denen ausreichend statische auswertbare Zahlen vorliegen. Des Weiteren sind einige Länder bereits zu größeren Einheiten (z. B. Skandinavien) zusammengefasst.

Europa	Afrika	Fernost	Mittelameika/ Karibik	Südamerika
Deutschland	Nigeria	China	Guatemala	Brasilien
Frankreich	Äthiopien	Indonesien	Kuba	Kolumbien
Vereinigtes Königreich	Ägypten	Japan	Dominikanische Republik	Argentinien
Italien	Kongo	Philippinen	Haiti	Peru
Spanien	Südafrika	Vietnam	Honduras	Venezuela, Bol. Republik
Ukraine	Tansania, Vereinigte Republik	Thailand	El Salvador	Chile
Polen	Kenia	Myanmar	Nicaragua	Ecuador
Skandinavien	Sudan	Korea, Republik (Südkorea)	Costa Rica	Bolivien, Plurinat. Staat
Rumänien	Algerien	Malaysia	Puerto Rico	Paraguay
Niederlande	Uganda	Korea, Demokratische Volksrepublik	Panama	Uruguay
Portugal	Marokko	Kambodscha	Jamaika	
Griechenland	Ghana	Singapur	Trinidad-Tobago	
Belgien	Côte d'Ivoire	Taiwan		
Tschechische Republik	Mosambik			
Ungarn	Madagaskar			
Österreich	Kamerun			
Schweiz	Tunesien			

Tabelle 5 – Einteilung der Welt in Zonen inkl. Länderzuordnung - Teil 1

Nahost	Mittelasien	Zentralasien	Australien/ Ozeanien	Nordamerika
Türkei	Indien	Russische Föderation	Australien	Vereinigte Staaten
Iran	Pakistan	Kirgisistan	Neuseeland	Kanada
Irak	Bangladesch	Tadschikistan	Sonstige	Mexiko
Saudi-Arabien	Afghanistan	Turkmenistan		
Jemen	Nepal	Usbekistan		
Syrien/ Arabische Republik	Sri Lanka	Kasachstan		
Aserbaidschan				
Israel				
Jordanien				
Vereinigte Arabische Emirate				

Tabelle 6 – Einteilung der Welt in Zonen inkl. Länderzuordnung - Teil 2

4.1.2.2 Identifikation und Auswertung der Informationen

In dieser Phase werden die benötigten Informationen identifiziert, strukturiert und bewertet. Um ein nachvollziehbares und transparentes Ergebnis zu erzielen, werden nur öffentlich verfügbare Quellen und Statistiken genutzt.

Zu Beginn werden dafür die verschiedenen Exposure-Vorgaben aus der Norm hinsichtlich möglicher Cluster-Faktoren analysiert. Dabei lassen sich die benötigten Informationen in die folgenden vier Bereiche einteilen:

- Umwelt- und Gesellschaftsaspekte (z. B. Wetter, Geologie)
- Infrastrukturaspekte (z. B. Straßenbeschaffenheit, Tunnelkilometer)
- Fahrzeugzubehör (z. B. Anhänger, Dachboxen)
- Besondere Situationen (z. B. Ladung auf der Fahrbahn, Fahrzeug wird abgeschleppt)

Auf Basis dieser ersten Grobeinteilung werden exemplarisch für zwei der vier Cluster-Faktoren die benötigten Teildaten erarbeitet.

Umwelt- und Gesellschaftsaspekte

Grundsätzlich sind alle Umweltaspekte von Interesse, die es ermöglichen, Rückschlüsse auf die Exposure einzelner oder mehrerer Fahrzustände zu erhalten. Nach weiterer Analyse der Norm-Zustände ergeben sich folgende besonders relevante Einflüsse:

- Gesamt-Niederschlag im Jahr [in mm]
- Anzahl an Tagen mit Niederschlag
- Schneetage
- gemittelte Sonnenscheindauer [in h]
- Landfläche [in km^2]
- Küstenlinie [in km]
- Tiefster Punkt [in m]
- Höchster Punkt [in m]
- Höhendifferenz als Resultat aus dem tiefsten und höchsten Punkt [in m]

- Anzahl der 1500m Schartenhöhen/Prominenzen
- Anzahl der Einwohner
- Bevölkerung unter 14 Jahre

Nach Sammlung und Auswertung der Daten entstanden folgende Erkenntnisse, die auf der folgenden Seite in Tabelle 7 zusammengefasst sind:

	Afrika	Australien/ Ozeanien	Europa	Fernost	Mittelamerika/ Karibik
Landfläche [km²]	16.129.560	8.467.050	4.681.450	13.999.480	687.530
Bevölkerung	804.612.000	26.519.500	532.488.000	2.141.232.500	80.107.500
Bevölkerung unter 14 Jahre	309.842.783	8.448.194	82.449.911	450.381.455	25.161.607
Niederschlagsmenge [mm/a]	853	812	731	1.672	1.317
Niederschlagstage [d/a]	68	85	107	109	107
gemittelte Sonnenscheindauer [h/d]	7,54	7,07	5,26	6,17	7,38
Küstenlinie [km]	21.649	4.0894	51.668	154.068	14.486
Tiefster Punkt [m]	-133	-15	-7	-154	-46
Höchster Punkt [m]	5.895	3.754	4.807	8.850	4.211
Maximale Höhendifferenz [m]	6.028	3.769	4.814	9.004	4.257
Gemittelte Höhendifferenz [m]	3.104	2.999	2.474	3.594	2.821
Anz. der 1500m Schartenhöhen	84	54	98	347	31
	Mittelasien	**Nahost**	**Nordamerika**	**Südamerika**	**Zentralasien**
Landfläche [km²]	4.732.530	5.970.430	20.184.880	17.115.170	20.303.660
Bevölkerung	1.608.332.000	286.711.500	459.852.500	397.032.500	202.914.000
Bevölkerung unter 14 Jahre	498.293.484	83.986.776	100.719.220	104.957.182	39.165.954
Niederschlagsmenge [mm/a]	1.387	316	987	1.577	444
Niederschlagstage [d/a]	89	40	99	106	73
gemittelte Sonnenscheindauer [h/d]	7,40	7,22	6,21	6,10	5,71
Küstenlinie [km]	9.966	16.054	231.334	30.234	37.653
Tiefster Punkt [m]	70	-408	-86	-105	-132
Höchster Punkt [m]	8.850	5.671	6.194	6.960	7.495
Maximale Höhendifferenz [m]	8.780	6.079	6.280	7.065	7.627
Gemittelte Höhendifferenz [m]	6.161	3.430	5.983	4.851	5.803
Anz. der 1500m Schartenhöhen	91	91	296	209	121

Tabelle 7 – Umwelt- und Gesellschaftsaspekte (Stand 2012)

Infrastrukturaspekte

Um Aussagen über die Infrastruktur zu ermöglichen, werden mit Blick auf die Norm folgende Daten eruiert, anschließend erfasst und ausgewertet:

- Straßenkilometer gesamt
- Straßenkilometer geteert
- Autobahnkilometer
- Sonstige Straßenkilometer
- Tunnelkilometer
- PKW pro 1.000 Einwohner
- Verkaufte PKW in 2010
- Verkaufte Nutzfahrzeuge in 2010
- Gesamtzahl registrierter PKW
- Gesamtzahl registrierter Nutzfahrzeuge

Um eine leichtere Vergleichbarkeit der Infrastruktur zu ermöglichen, werden verschiedene Faktoren gebildet:

- **Teerfaktor [in %]**
  Der „Teerfaktor“ gibt prozentual an, in welchem Umfang das vorhandene Straßennetz geteert ist:

$$Teerfaktor = \frac{Straßenkilometer_{geteert}}{Straßenkilometer_{gesamt}} * 100\%$$

Formel 5 – Berechnung des Teerfaktors

- **Autobahnfaktor 1 [in m/km]**
  Der „Autobahnfaktor 1“ gibt das Verhältnis von der Anzahl an Autobahnmetern zu einem Straßenkilometer an:

$$Autobahnfaktor\ 1 = \frac{Autobahnkilometer * 1000\frac{m}{km}}{Straßenkilometer_{gesamt}}$$

Formel 6 – Berechnung des Autobahnfaktors 1

- **Autobahnfaktor 2 [in %]**
  Der „Autobahnfaktor 2“ gibt das prozentuale Verhältnis von Autobahnkilometer zum gesamten Straßennetz an:

$$Autobahnfaktor\ 2 = \frac{Autobahnkilometer}{Straßenkilometer_{gesamt}} * 100\%$$

Formel 7 – Berechnung des Autobahnfaktors 2

- **Tunnelfaktor**
  Der „Tunnelfaktor“ stellt das Verhältnis von Tunnelkilometer pro Straßenkilometer dar. Dabei gelten laut DIN 1076 künstliche Passagen, die unterhalb der Erd- oder Wasseroberfläche verlaufen als Tunnel. Dazu zählen auch oberirdisch verlaufende Einhausungen von Straßen ab einer Länge von 80 Metern. [DIN 1076:1999-11]
  Da der Quotient sehr klein ist, wird er zusätzlich mit dem Faktor 100.000 multipliziert, um die Lesbarkeit und Vergleichbarkeit zu erhöhen:

$$Tunnelfaktor = \frac{Tunnelkilometer}{Straßenkilometer_{gesamt}} * 100.000$$

Formel 8 – Berechnung des Tunnelfaktors

- **Faktor Straßenbelegung [in „Anzahl Fahrzeuge“ pro km]**
  Der Faktor „Straßenbelegung“ gibt an, wie viele Fahrzeuge (PKW und LKW) sich statistisch auf einem Straßenkilometer befinden, also quasi deren Häufigkeit pro Straßenkilometer:

$$Straßenbelegung = \frac{Gesamtzahl\ registrierter\ Fahrzeuge}{Straßenkilometer_{gesamt}}$$

Formel 9 – Berechnung der Straßenbelegung

- **Faktor Straßenbelegung PKW [in „Anzahl PKW“ pro km]**
  Der Faktor „Straßenbelegung PKW“ gibt an, wie viele PKW sich statistisch auf einem Straßenkilometer befinden, also deren Häufigkeit pro Straßenkilometer:

$$Straßenbelegung\ PKW = \frac{Gesamtzahl\ registrierter\ PKW}{Straßenkilometer_{gesamt}}$$

Formel 10 – Berechnung der Straßenbelegung PKW

Die daraus resultierten Ergebnisse sind auf den folgenden Seiten in Tabelle 8 und Tabelle 9 dargestellt:

	Afrika	Australien/ Ozeanien	Europa	Fernost	Mittelamerika/ Karibik
Straßenkilometer	1.569.185	940.148	5.695.759	6.292.186	208.173
Straßenkilometer geteert	368.369	61.879	5.311.946	4.647.837	92.841
Autobahnkilometer	2.012	172	110.449	78.602	1.511
Tunnelkilometer	0,000	58,755	4.529,712	2.303,088	0,000
PKW pro 1.000 Einwohner	29	408	433	97	111
Verkaufte PKW	529.992	637.687	12.984.025	20.740.527	88.535
Gesamtzahl registrierter PKW	14.470.233	14.868.873	232.266.683	97.944.723	737.000
Verkaufte Nutzfahrzeuge	211.846	478.222	1.704.027	6.227.106	21.724
Gesamtzahl registrierter Nutzfahrzeuge	7.001.566	3.582.537	35.892.551	39.289.858	607.500
Gesamtzahl registrierten Fahrzeuge	21.471.799	18.451.410	268.159.234	137.234.581	1.344.500
Teerfaktor [%]	23 %	7 %	93 %	74 %	45 %
Autobahnfaktor 1 [m/km]	1,2822	0,1829	19,3914	12,4920	7,2584
Autobahnfaktor 2 [%]	0,13 %	0,02 %	1,94 %	1,25 %	0,73 %
Tunnelfaktor	0,000	6,250	79,528	36,602	0,000
Faktor Straßenbelegung PKW [PKW/km]	9,2	15,8	40,8	15,6	3,5
Faktor Straßenbelegung [Fahrzeuge/km]	13,7	19,6	47,1	21,8	6,5

Tabelle 8 – Infrastrukturaspekte - Teil 1 (Stand 2010)

	Mittelasien	Nahost	Nordamerika	Südamerika	Zentralasien
Straßenkilometer	4.432.514	1.053.748	8.097.958	2.609.165	1.253.223
Straßenkilometer geteert	226.128	651.624	4.922.673	249.009	983.188
Autobahnkilometer	911	8.832	98.517	3.148	30.000
Tunnelkilometer	20,622	46,721	166,341	66,977	18,403
PKW pro 1.000 Einwohner	10	137	344	70	87
Verkaufte PKW	2.516.338	2.332.682	6.829.349	3.943.254	2.113.746
Gesamtzahl registrierter PKW	15.979.347	18.805.645	160.041.236	39.803.602	34.797.488
Verkaufte Nutzfahrzeuge	675.018	880.428	7.374.164	1.314.604	228.302
Gesamtzahl registrierter Nutzfahrzeuge	8.675.791	8.280.903	131.251.668	13.149.724	6.427.425
Gesamtzahl registrierten Fahrzeuge	24.655.138	27.086.548	291.292.904	52.953.326	41.224.913
Teerfaktor [%]	5 %	62 %	61 %	10 %	78 %
Autobahnfaktor 1 [m/km]	0,2055	8,3815	12,1657	1,2065	23,9383
Autobahnfaktor 2 [%]	0,02 %	0,84 %	1,22 %	0,12 %	2,39 %
Tunnelfaktor	0,465	4,434	2,054	2,567	1,468
Faktor Straßenbelegung PKW [PKW/km]	3,6	17,8	19,8	15,3	27,8
Faktor Straßenbelegung [Fahrzeuge/km]	5,6	25,7	36,0	20,3	32,9

Tabelle 9 – Infrastrukturaspekte - Teil 2 (Stand 2010)

Auf die entstandene Datengrundlage kann während des Produktentstehungsprozesses zugegriffen werden. Dazu wird zum frühestmöglichen Zeitpunkt der Zielmarkt (engl. target market) für das jeweilige Produkt bzw. System festgelegt. Durch diese Entscheidung werden die Rahmen- und Umweltbedingungen für die Entwicklung festgelegt.

Um nun das endgültige ASIL für das Produkt festlegen zu können, müssen alle für das Produkt relevanten Betriebszustände bzw. Fahrsituationen betrachtet und analysiert werden.

Um dies zu erreichen, wird, wie Abbildung 26 zeigt, auf Basis der Ergebnisse der FMEA das zu entwickelnde Produkt hinsichtlich möglicher Fehler auf „Produktebene“ (Komponente) sowie deren Auswirkungen auf das Gesamtfahrzeug (Fahrzeug) untersucht. Im Anschluss daran werden die Fehler auf Fahrzeugebene im Kontext aller relevanten Betriebs- bzw. Fahrsituationen weiter betrachtet. Dazu werden die Verletzungen der Sicherheitsziele mit den Gefährdungen für die Kunden bzw. anderen Verkehrsteilnehmer unter Beachtung der aktuellen Fahrsituation mithilfe von S, E und C bewertet.

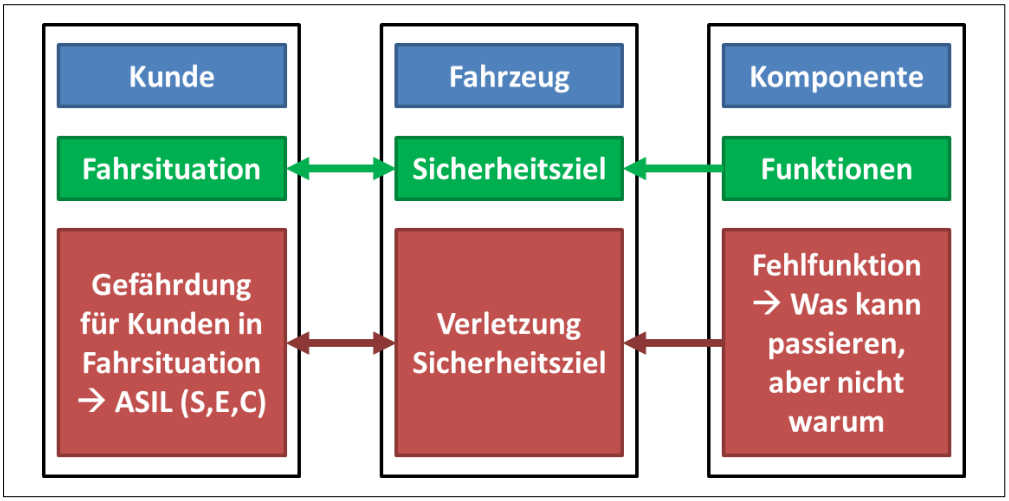


Abbildung 26 – Ermittlung des ASIL mit der System-FMEA

Bei der Festlegung des ASIL ist darauf zu achten, dass für jedes Sicherheitsziel ein separates ASIL definiert wird. Für das jeweilige Sicherheitsziel gilt dann das höchste ASIL, dass durch die Paarung von Sicherheitsziel und Fahrsituation entstanden ist.

Zusammengefasst läuft der Prozess wie in Abbildung 27 dargestellt ab:

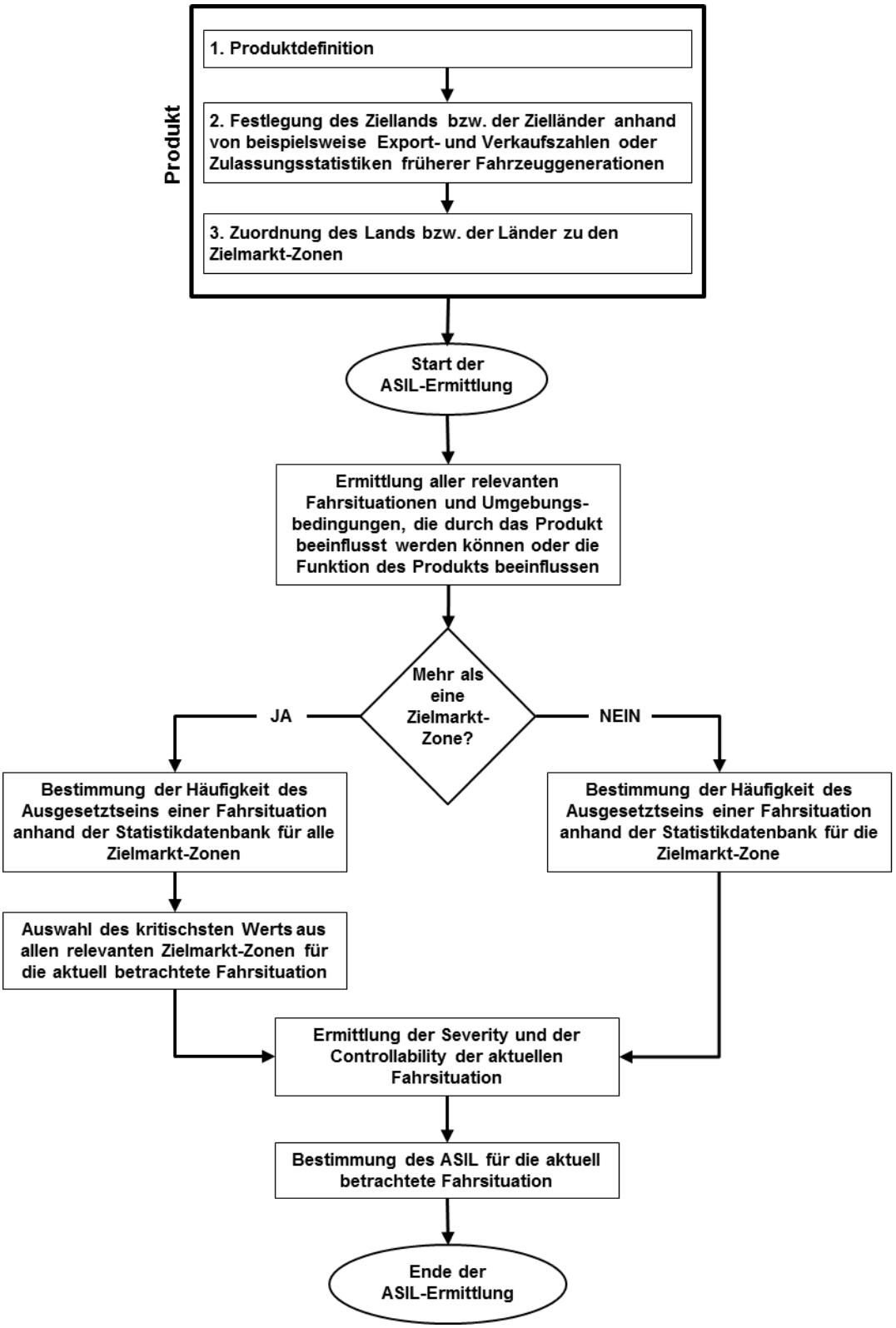


Abbildung 27 – Ermittlung eines Zielmarktabhängigen ASIL

4.2 Schnittstellenanalyse sowie Anforderungsdurchgängigkeit

Sowohl der Ansatz zur Schnittstellenanalyse als auch der Ansatz zur Anforderungsdurchgängigkeit werden auf Basis der FMEA realisiert. Die FMEA inkl. ihrer Denkweise bietet hierbei eine sehr gute Modellierung der Wirkzusammenhänge (Funktionsnetz und Fehlernetz) inkl. der Maßnahmen zur Vermeidung und Entdeckung von Fehlern während der Entwicklung. Daneben gibt es bereits verschiedene FMEA-Arten, die für den Entwicklungsprozess eingesetzt werden (siehe Abbildung 19 – Seite 42). Nicht zuletzt ist die FMEA im Automobilbereich eine vorgeschriebene, anerkannte und bewährte Methode.

Für die Realisierung der Schnittstellenzusammenhänge wie auch des Anforderungsmanagements ist es im ersten Schritt notwendig, ein erweitertes Datenmodell samt Framework (zu Deutsch „Programmiergerüst“) aufzubauen. Mit diesem Datenmodell und –framework ist es möglich, die Daten einer FMEA elektronisch weiter auszuwerten und zu verarbeiten. Zusätzlich dazu werden Schnittstellen geschaffen, um gezielt Daten zwischen mehreren Systemen austauschen zu können.

Der zentrale Gedanke ist, den Output einer FMEA weiter nutzbar zu machen und somit den Entwicklungsprozess für funktional sichere Produkte zu vereinfachen. Es ist nicht das Ziel, ein neues Tool zur Erstellung von FMEAs zu entwickeln.

Abbildung 28 auf der folgenden Seite zeigt den zentralen Gedanken der FMEA-Erstellung, dem Export der Daten als XML, der Datenremodellierung sowie der Weiterverarbeitung und Erweiterung des Datenmodells.

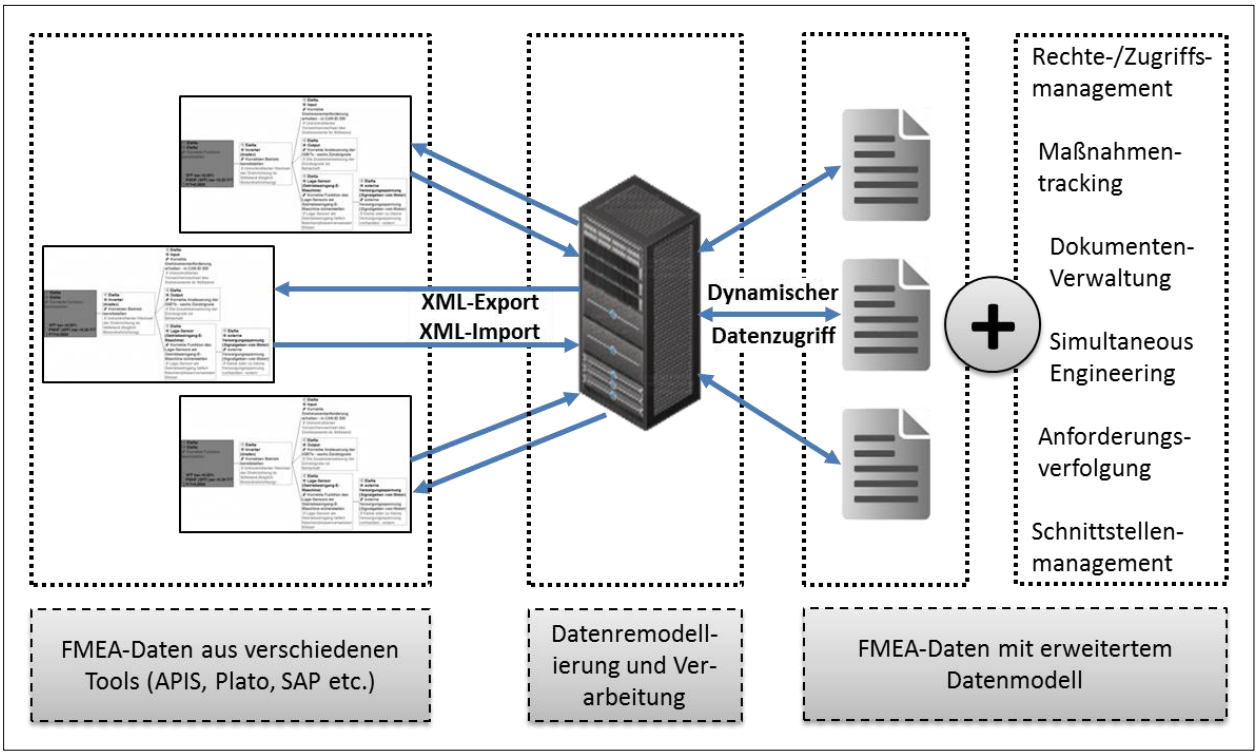


Abbildung 28 – Datenverarbeitung und -erweiterung

4.2.1 Architektur und Umsetzung des Ansatzes

Um die gestellten Anforderungen an die Schnittstellentransparenz und Anforderungsdurchgängigkeit (Erstellung, Betrachtung sowie Bearbeitung der Schnittstellen/Anforderungen) erfüllen zu können, wird in einem ersten Schritt eine entsprechende IT-Architektur zugrunde gelegt und implementiert. Dabei handelt es sich um eine Client-Server-Struktur, wie in Abbildung 29 auf der folgenden Seite beispielhaft gezeigt.

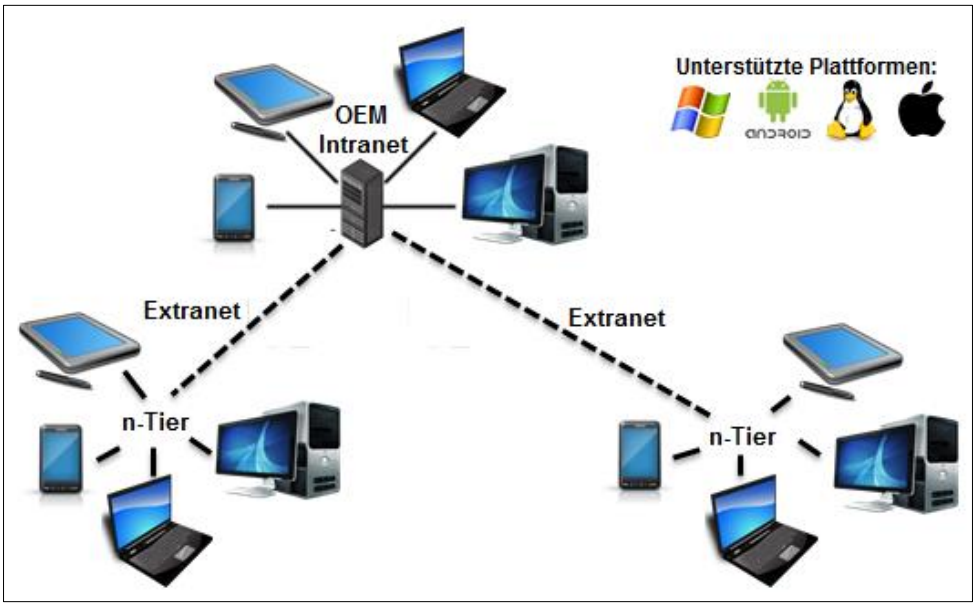


Abbildung 29 – Client-Server-Architektur - Bilder: Fotolia.com

Das bedeutet, dass es einen zentralen Datenspeicher sowie Rechenleistung gibt (Server), der die Datenverarbeitung sowie –bereitstellung übernimmt. Dies ist vergleichbar mit modernen Cloud-Anwendungen. Die einzelnen Rechner im Netzwerk können schließlich unabhängig von ihrem Aufenthalts- bzw. Standort auf die Daten zugreifen, diese anzeigen und manipulieren.

Mit dieser Architekturentscheidung wird gewährleistet, dass sowohl der OEM wie auch seine zahlreichen Entwicklungspartner und Lieferanten Zugriff auf relevante und aktuelle Ressourcen erhalten.

Ein weiterer großer Vorteil dieser Architektur ist die vereinfachte Datensicherung sowie die Möglichkeit einer zentralen Versionierung. Mit diesem Ansatz wird das Auftreten eines Datenverlusts, z. B. durch defekte Arbeitsrechner, verlorene oder gestohlene Datenträger sowie durch ausgeschiedene Mitarbeiter auf ein Minimum reduziert.

Um eine möglichst hohe Flexibilität und Plattformunabhängigkeit zu erreichen, wird ein webbasiertes Browser-Framework entwickelt. Damit wird es möglich, dass verschiedenste Geräteklassen (z. B. Desktop-PCs, Notebooks, Tablets, Smartphones) und Betriebssysteme/Plattformen (z. B. Windows, Linux, Android, Apple) auf die Daten zugreifen können.

Aus der browserbasierten Darstellung ergibt sich zusätzlich der große Vorteil, dass keine Software auf den Clients installiert und konfiguriert werden muss. Alle Aktionen können in einem Webbrowser ausgeführt werden. Außerdem werden dadurch Probleme, die aufgrund verschiedener Softwareversionen entstehen können, konzeptionell ausgeschlossen, da jeder Nutzer zu jeder Zeit die vom Server zentral bereitgestellte Version nutzt.

Nicht zuletzt wird durch den zentralisierten Ansatz ein lokales Updaten der Software nicht mehr notwendig sein. Software-Updates werden nur noch auf dem Server installiert und stehen damit sofort allen Nutzern zur Verfügung. Zugriffsprobleme auf Daten aufgrund veralteter Anwender-Software werden damit ausgeschlossen.

4.2.1.1 Serverapplikation

Die Serverapplikation wird in der modernen objekt-orientierten Programmiersprache „C#“ entwickelt, um zukünftigen Anforderungen und Entwicklungen möglichst einfach gerecht werden zu können.

Durch einen modularen Aufbau kann die Basis-Serverapplikation jederzeit und problemfrei an neue Bedürfnisse und Anforderungen angepasst sowie um Funktionen erweitert werden. Die Intergration aktueller und flexibler Schnittstellen (wie z. B. Websockets), ermöglicht zudem den standardisierten, komfortablen und leichten Austausch von Daten bei gleichzeitig niedrigem Ressourcenverbrauch (CPU, RAM und Datenübertragung).

4.2.1.2 Clientapplikation

Das clientseitige Interface wird mittels Hypertext Markup Language (HTML – Version 5), Cascading Style Sheets (CSS – Version 3), JavaScript sowie dem darauf basierenden Framework jQuery realisiert.

HTML

HTML ist eine textbasierte Sprache zur strukturierten Darstellung von Webseiten und Dokumenten. Darin können verschiedene Formate (bspw. Texte, Bilder, Links, Videos) eingebettet sein. Diese Sprache bildet das Grundgerüst

Quelle: commons.wikimedia.org

der Clientapplikation.

CSS

Quelle: wikipedia.org

Cascading **S**tyle **S**heets, kurz CSS, ist eine textbasierte „Gestaltungssprache“. Sie ermöglicht es, das Aussehen und die Darstellung von Webseiten sehr präzise festzulegen. Daher wird CSS in der Clientapplikation vorzugsweise zur Gestaltung und Positionierung von Texten, Grafiken sowie Schaltelementen eingesetzt.

JavaScript

JavaScript, kurz JS, ist eine textbasierte Skriptsprache, mit der der Programmcode direkt im Browser des Betrachters ausgeführt wird. Dies bedeutet, dass zum Ausführen des Codes auf dem Server keine Rechenleistung, außer der zur Übertragung des auszuführenden Codes, notwendig ist. In Kombination mit HTML und CSS lassen sich damit Anwendungen entwickeln, die sich im Verhalten und in der Bedienung nicht mehr von lokal installierten (nativen) Anwendungen unterscheiden. In der Clientapplikation übernimmt JS genau diese Aufgabe.

Quelle: wikipedia.org

jQuery

jQuery ist eine, durch Plug-Ins, erweiterbare Sammlung von JavaScript-Funktionen (Bibliothek) zur Implementierung von Navigations- und Steuerungselementen sowie Manipulation von Document Object Models (kurz DOM). Insbesondere die Dialoge sind in der Clientapplikation zum Einsatz gekommen.

Quelle: jquery.com

Mithilfe der Kombination dieser drei Standards sowie der Scriptsammlung „jQuery“ kann einerseits der Schnelllebigkeit der Technologien (z. B. Software, Schnittstellen) wie auch dem Wandel der IT-Infrastruktur (z. B. Tablets, Smartphones) Rechnung getragen werden.

Nicht zuletzt kann das entwickelte Client-Interface auf Basis dieser etablierten Technologien und Standards mit geringem Aufwand in eine „App“ überführt werden.

4.2.2 Remodellierung der FMEA-Daten

Nachdem im ersten Schritt die notwendigen Architekturgrundlagen geschaffen wurden, ist im zweiten Schritt eine Übernahme der vorhandenen FMEAs notwendig.

Bei dieser Remodellierung werden die Daten aus einem offenen und standardisierten Format (MSRFMEA-XML [Off, S. 2009]) in ein eigenes Datenmodell überführt und aufbereitet. Dies ist notwendig, da das MSRFMEA-XML nicht die notwendigen Eigenschaften und Fähigkeiten besitzt, die zur Schnittstellenbetrachtung sowie Anforderungsumsetzung benötigt werden.

In den Abbildungen 30 bis 32 (siehe folgende Seiten) sind Auszüge aus dem XML-Quellcode, der durch einen Export aus der Software „IQ-RM PRO“ (Version 6) erstellt wurde, dargestellt. Darin ist der Header der FMEA, eine Funktion samt Funktions- und Fehlerverknüpfung sowie ein Fehler zu sehen. Im Header der FMEA sind diverse Einstellungen und Dateiinformationen abgelegt.

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE MSRFMEA PUBLIC "-//MSR//DTD MSR FMEA
DTD:V2.1.2:LAI:IAI:XML:ML:MSRFMEA.DTD//EN" "MSRFMEA_2_1_2.ML.DTD">
<MSRFMEA>
   <SHORT-NAME>Filename.xml</SHORT-NAME>
   <ADMIN-DATA>
      <LANGUAGE>Deutsch</LANGUAGE>
      <USED-LANGUAGES>
         <L-10 L="DE">Deutsch</L-10>
      </USED-LANGUAGES>
      <COMPANY-DOC-INFOS>
         <COMPANY-DOC-INFO>
            <COMPANY-REF>Firmenname</COMPANY-REF>
            <SDGS>
               <SDG SI="DICTIONARY" GID="root">
                  <SDG SI="DICTIONARY" GID="documentSettings">
                     <SD SI="Symbol" GID="causesView">causesAll</SD>
                     [...]
                  </SDG>
                  <SDG SI="DICTIONARY" GID="exportInfo">
                     <SD SI="String" GID="databaseCreationVersion">6.0</SD>
                     [...]
                  </SDG>
               </SDG>
            </SDGS>
         </COMPANY-DOC-INFO>
      </COMPANY-DOC-INFOS>
   </ADMIN-DATA>
   [...]
</MSRFMEA>
```

Abbildung 30 – XML-Quellcode-Auszug – Basisdaten

Die Verknüpfung und Zuordnung von Funktionen, Fehlern sowie weiterer Eigenschaften erfolgt über eine eineindeutige Identifikationsnummer (ID) für jedes Element (Funktion, Fehler, Eigenschaften (siehe Abbildung 32)) innerhalb der FMEA sowie einer „ID-REF“, in der auf die ID referenziert wird (siehe Abbildung 31 auf der folgenden Seite).

```
<FM-FUNCTION ID="U5ACC797860B292" T="2012.11.06 08:38:35" ↵
F-ID-CLASS="FM-FUNCTION">
   <LONG-NAME>
      <L-4 L="DE">Funktion</L-4>
   </LONG-NAME>
   <SHORT-NAME SI="AUTONUMBER">1.a</SHORT-NAME>
   <FM-FUNCTION-TYPE-REF ID-REF="U5ACC79785048F4" F-ID-CLASS= ↵
   "FM-FUNCTION-TYPE">U5ACC79785048F4_Funktion</FM-FUNCTION-TYPE-REF>
   <FM-PREREQUISITES>
      <FM-FUNCTION-REF ID-REF="U5ACC798560097E" F-ID-CLASS= ↵
      "FM-FUNCTION">1.1.a</FM-FUNCTION-REF>
   </FM-PREREQUISITES>
   <FM-FAULT-REFS>
      <FM-FAULT-REF ID-REF="U5ACC799E100FE4" F-ID-CLASS= ↵
      "FM-FAULT">1.a.1</FM-FAULT-REF>
   </FM-FAULT-REFS>
</FM-FUNCTION>
```

Abbildung 31 – XML-Quellcode-Auszug - Funktion samt Funktions- und Fehlerverknüpfung

Für die Remodellierung wird bewusst das standardisierte XML-Format als Basis eingesetzt, um mit möglichst vielen FMEA-Tools kompatibel und zugleich unabhängig von einzelnen Herstellern zu sein. Dies hat den Vorteil, dass eine Änderung des proprietären Datenformats eines FMEA-Tools keinen Einfluss auf die, in dieser Arbeit entwickelte, Vorgehensweise hat.

```
<FM-FAULT-TYPES>
   <FM-FAULT-TYPE ID="U5ACC799E008C9E" T="2012.11.06 08:38:30" ↵
   F-ID-CLASS="FM-FAULT-TYPE">
     <LONG-NAME>
       <L-4 L="DE">Fehler</L-4>
     </LONG-NAME>
   </FM-FAULT-TYPE>
</FM-FAULT-TYPES>
```

Abbildung 32 – XML-Quellcode-Auszug – Fehler

Insbesondere jedoch wird durch den Einsatz von XML die Entwicklung eines softwareübergreifenden Konzepts ermöglicht.

Das bedeutet konkret, dass theoretisch jede FMEA-Software, die in das Format MSRFMEA-XML exportieren kann, zur Grundmodellierung der Schnittstellenzusammenhänge und ebenfalls zur Anforderungsverfolgung genutzt werden kann. Damit wird ein proprietäres, softwareabhängiges Vorgehen vermieden und die Integration in die Software-

infrastruktur/-landschaft der Komponenten-/Systementwickler vereinfacht und sichergestellt. Abbildung 33 zeigt die Hauptzusammenhänge innerhalb des Datenmodells und der Datenverarbeitung.

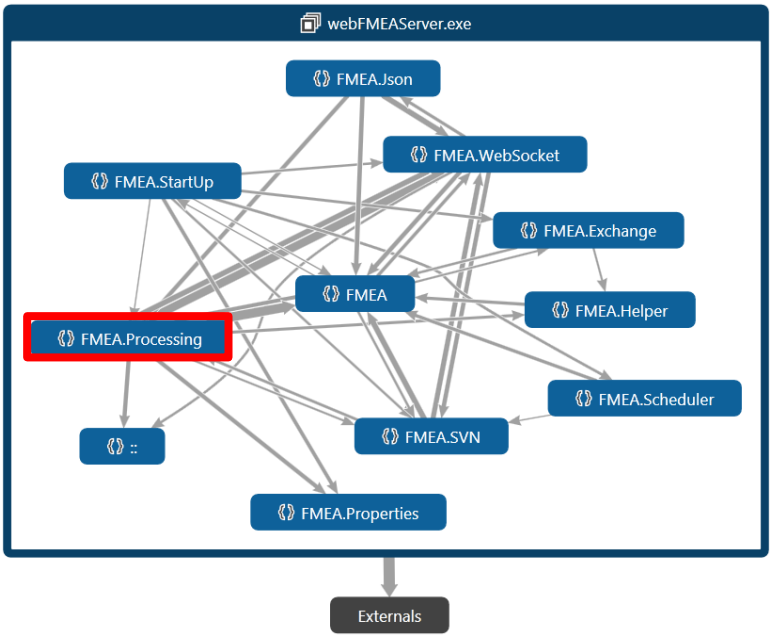


Abbildung 33 – Reduzierter Auszug aus dem Dependency Graph (in MS Visual Studios 2012)

In Abbildung 34 sind beispielhaft weiterführende Datenzusammenhänge von FMEA-Processing dargestellt.

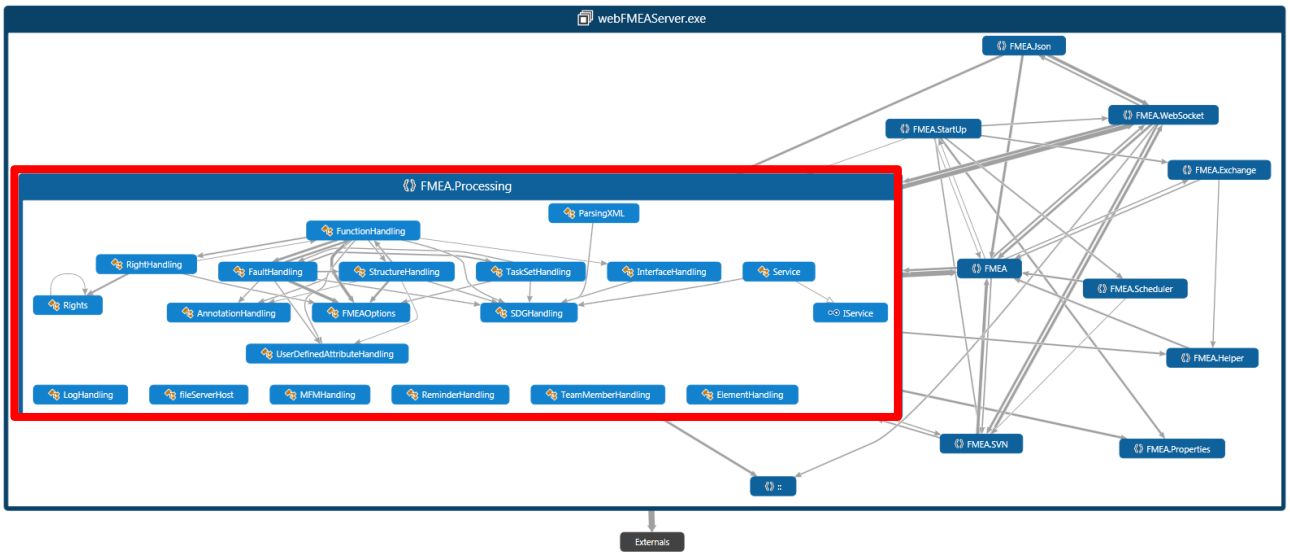


Abbildung 34 – Erweiterter Auszug aus dem Dependency Graph (in MS Visual Studios 2012)

Für jeden Daten- bzw. Informationstyp wurden Objekte angelegt, die Daten des XML-Files beinhalten. Die Objekte ihrerseits können untereinander in Verbindung gesetzt werden.

4.2.2.1 Erweiterung des Datenmodells

Um den definierten und geforderten Bedingungen gerecht zu werden, wird das neu geschaffene Datenmodell um mehrere Aspekte erweitert:

- Anforderungsdurchgängigkeit
- Rechte-/Zugriffsmanagement
- Dokumenten-Verwaltung
- Maßnahmentracking
- Schnittstellen-Informationen
- Simultaner Zugriff auf mehrere FMEAs
- Simultaneous Engineering

Dazu werden neue Objekte generiert und vorhandene, um neue Attribute und Eigenschaften erweitert. Diese Erweiterungen werden in den folgenden Abschnitten detailliert vorgestellt.

4.2.3 Anforderungsdurchgängigkeit

Neben der Remodellierung und Erweiterung der eigentlichen FMEA-Daten werden zusätzlich verschiedene Verarbeitungsschritte während des Imports implementiert. Damit soll erreicht werden, dass die Anforderungen durchgängig betrachtet werden können.

Ziel dieser zusätzlichen Prozesse ist es, den Menschen von fehlerträchtigen und wertschöpfungsfreien Tätigkeiten zu entlasten bzw. gänzlich zu entbinden.

Damit dies möglich ist, müssen während der FMEA-Erstellung maschinell auswertbare Informationskennzeichnungen (engl. Tag (Plural Tags)) eingearbeitet werden.

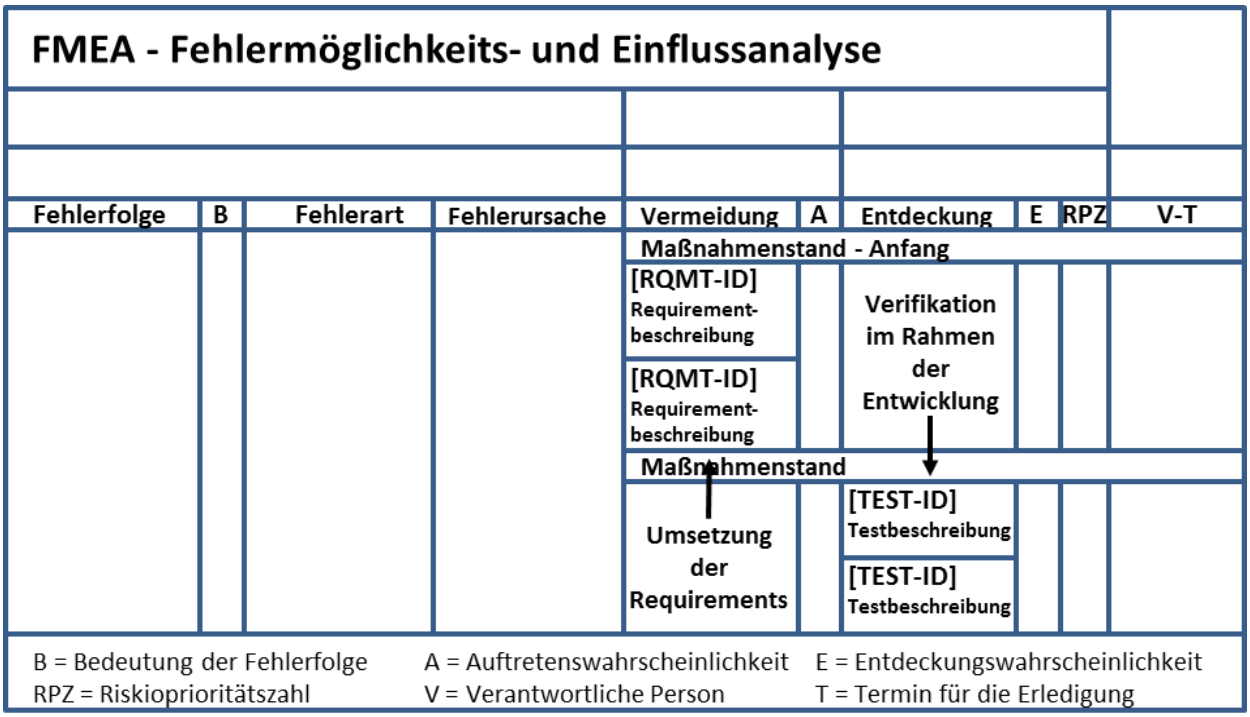


Abbildung 35 – Vereinfachtes FMEA-Formblatt mit Requirements [Schloske, A. 2012] - modifizierte Darstellung

In Abbildung 35 wird die Verwendung von Tags für Requirements, Verfahren, Tests und auch Verifikationsmaßnahmen innerhalb eines FMEA-Formblatts beispielhaft dargestellt.

4.2.3.1 Tagdefinition

Der Tag-Aufbau ist generisch gestaltet:

- [TAG-TYPE]

bzw.

- [TAG-TYPE:VALUE]

Dabei haben die einzelnen Elemente im Tag folgende Bedeutung:

- **TAG** steht hierbei für die verschiedenen Taggruppen:
  - RQMT steht für Requirement
  - TEST steht für Testing/Test
- „**-**“ dient als Trennzeichen zwischen TAG und TYPE

- **TYPE** steht für die Untertypen der jeweiligen Taggruppe:
  - EXT: steht für Extern
  - INT: steht für Intern
  - HW: steht für Hardware
  - SW: steht für Software
- „**:**“ dient als Trennzeichen zwischen TYPE und VALUE
- **VALUE** ist ein optionaler Parameter in Form einer Nummer. Mit dieser Nummer wird die eindeutige Identifikation sowie der Verweis auf andere Daten realisiert.

  Sofern VALUE nicht vorhanden ist, wird während der Remodellierungsphase eine noch nicht genutzte Nummer generiert und als VALUE gesetzt.

Mittels des Taggings können somit die Anforderungen aus dem Lasten-/Pflichtenheft in Form einer Requirement-ID mit der FMEA verknüpft werden. Dieser Tag wird dann einer Komponente bzw. einer Funktion vorangestellt und sieht wie folgt aus:

[RQMT-Ext:23]

„**RQMT**“ steht hierbei für Requirement und „**Ext**“ für „Extern“ (vom Kunden vorgegeben). Die Nummer „**23**“ dahinter kommt im Allgemeinen aus einem CARE-Tool (siehe Abschnitt 2.2.3.1, Seite 50).

Sofern sich aus der Gefahren- und Risikobetrachtung eine neue Anforderung ergibt, kann diese mit [RQMT-Int] markiert werden. Während des Remodellierungsvorgangs wird dieser Requirement-Tag dann automatisch erfasst und um eine ungenutzte Value (Nummer) ergänzt. Wenn für eine Funktion z. B. eine Änderung oder Erweiterung der Software erfolgen muss, kann diese „Vermeidungsmaßnahme“ mit [RQMT-SW] markiert werden. Eine mögliche Hardwaremodifikation wird entsprechend mit [RQMT-HW] bezeichnet. Bei neuen, zusätzlichen internen Test-Szenarien ist der Tag [TEST-INT]. Auch hier wird dann das neue Requirement bzw. der zusätzliche Test automatisch um eine eindeutige, fortlaufende Identifikationsnummer (Value) ergänzt.

Mithilfe des Tagging-Prinzips kann zudem überprüft werden, ob eine Anforderung hinsichtlich ihres Gefahrenpotenzials untersucht und entsprechende Tests durchgeführt wurden. In Abbildung 36 ist der gesamte Prozess der Requirement-Erstellung bis hin zur Umsetzung und Dokumentation dargestellt.

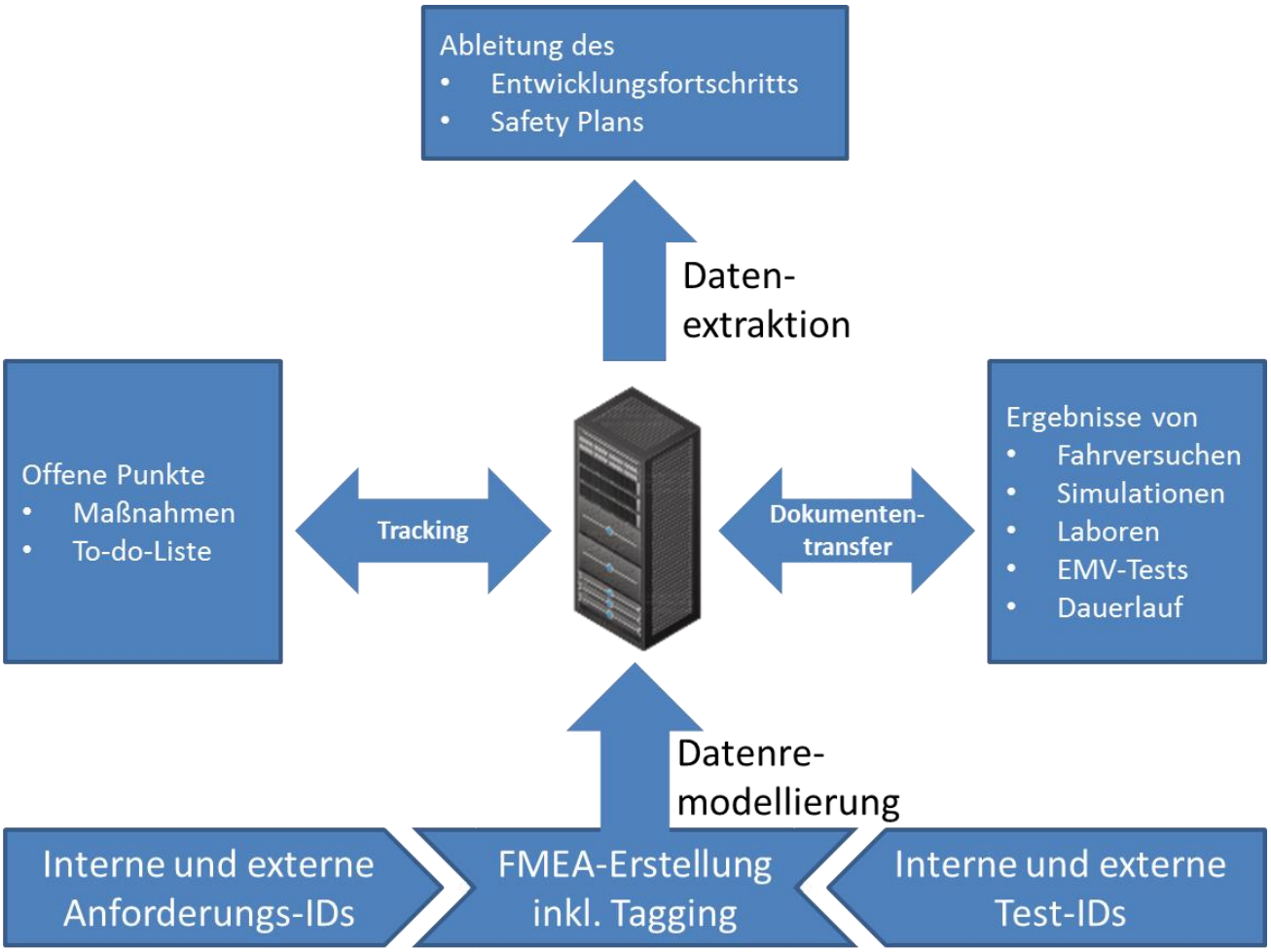


Abbildung 36 – Modell der Anforderungsdurchgängigkeit

4.2.4 Rechtemanagement

Da das „FMEA-Standard-Datenmodell“ (wie z. B. das vom FMEA-Software-Marktführer „APIS IQ“), wie auch das daraus abgeleitete, exportierbare XML-Format kein Rechtemanagement auf Struktur-, Funktions-, Fehler- sowie Maßnahmenebene beinhaltet, wird das neue Datenmodell an mehreren Stellen um entsprechende Möglichkeiten erweitert.

Dazu werden vier Rechteebenen eingeführt:

- Rechte auf Strukturebene
- Rechte auf Funktionsebene
- Rechte auf Fehlerebene
- Rechte auf Dokumentenebene

Die Rechtevergabe ist so aufgebaut, dass Rechte auf alle Elemente einer Ebene angewendet werden können (siehe Abbildung 37).

<table>
<tr><th colspan="4">Ebenen</th></tr>
<tr><th>Struktur</th><th>Funktionen</th><th>Fehler</th><th>Dokumentation</th></tr>
<tr><td rowspan="2">1. Struktur</td><td colspan="2" rowspan="2"></td><td>1. Dokument</td></tr>
<tr><td>n. Dokument</td></tr>
<tr><td rowspan="6"></td><td rowspan="2">1. Funktion</td><td colspan="2" rowspan="2"></td><td>1. Dokument</td></tr>
<tr><td>n. Dokument</td></tr>
<tr><td rowspan="2"></td><td rowspan="2">1. Fehler</td><td>1. Dokument</td></tr>
<tr><td>n. Dokument</td></tr>
<tr><td rowspan="2"></td><td rowspan="2">n. Fehler</td><td rowspan="2">n Dokumente</td></tr>
<tr><td></td></tr>
<tr><td colspan="3">n. Funktion</td></tr>
<tr><td colspan="4">n. Struktur</td></tr>
</table>

Abbildung 37 – Rechteebenen des Rechtemanagements

Damit wird sichergestellt, dass kein Informationsabfluss durch unberechtigte Datenzugriffe erfolgen kann. So können pro Benutzer (wobei es bei der Anzahl keine Beschränkung gibt) und pro Ebene lokale und/oder globale Rechte gesetzt werden.

Lokale Rechte beziehen sich immer auf das aktuell ausgewählte Element (Struktur, Funktion, Fehler oder Dokument) und globale Rechte zusätzlich noch auf seine hierarchisch untergeordneten Elemente (z. B. auf alle untergeordneten Strukturelemente des aktuellen Strukturelements). Die globalen Rechte werden also an die Unterebenen vererbt.

Tabelle 10 auf der folgenden Seite zeigt, welche Rechte vergeben werden können.

		Rechte		
		Lokal (nur aktuelles Element)	**Global eingeschränkt** (aktuelles und untergeordnete Elemente)	**Global uneingeschränkt** (aktuelles und untergeordnete Elemente)
FMEA-Elemente	Struktur	Lesen/Anzeigen **eigener** Einträge	Lesen/Anzeigen **eigener** Einträge	Lesen/Anzeigen **beliebiger** Einträge
	Funktion	Bearbeiten **eigener** Einträge Löschen **eigener** Einträge	Bearbeiten **eigener** Einträge Löschen **eigener** Einträge	Bearbeiten **beliebiger** Einträge Löschen **beliebiger** Einträge
	Fehler	Betrachtung **eigener** Dokumente Bearbeiten eigener Dokumente	Betrachtung **eigener** Dokumente Bearbeiten eigener Dokumente	Betrachtung **beliebiger** Dokumente Bearbeiten eigener Dokumente
	Dokumentation	Löschen **eigener** Dokumente	Löschen **eigener** Dokumente	Löschen **beliebiger** Dokumente
Administration		Verwalten von Funktionen, Rechten etc.		

Tabelle 10 – Möglichkeiten bei der Rechtevergabe

4.2.4.1 Dokumenten-Verwaltung

Die Dokumenten-Verwaltung wird in die Strukturen der bestehenden FMEA integriert. Das bedeutet, dass man zu jedem Systemelement, jeder Funktion, Fehlfunktion sowie zu jeder Maßnahme beliebig viele und unterschiedliche Dateien und Dateitypen revisionssicher ablegen und verankern kann. Dabei kann es sich beispielsweise um folgende Dateitypen handeln:

- Textdokumente
- Präsentationen
- Tabellen
- PDFs
- Videos
- Bilder

- Audiodateien
- Gepackte Archive (z. B. ZIP, 7z)
- Konstruktionsdateien
- Messergebnisse
- Simulationen

Um die geforderte Revisionssicherheit der Daten zu gewährleisten, d. h. jede Datenänderung nachvollziehbar zu machen und bei Bedarf eine vorherige Version wieder herstellen zu können, wird das System an eine freie, bekannte und bewährte Versionsverwaltungs-Software (Subversion, kurz SVN) angebunden. Damit wird zusätzlich die Änderungshistorie aller Dateien normgerecht sichergestellt.

4.2.5 Maßnahmentracking

Um die Aktualität und Durchgängigkeit in der Maßnahmenumsetzung zu garantieren, wird in der Architektur und dem Datenmodell ein zentrales Maßnahmentracking implementiert. Dieses zentrale Maßnahmentracking ermöglicht es, dass jede Person, die Maßnahmen aus der FMEA zugewiesen bekommen hat, diese selbstständig einsehen und bearbeiten kann. Medienbrüche und die damit verbundenen Inkonsistenzen während der Maßnahmenumsetzung werden durch diese Vorgehensweise vermieden. Sobald eine Maßnahme abgeändert wird, steht diese sofort allen zugriffsberechtigten Personen in der geänderten Version zur Verfügung. Des Weiteren kann mit dem Datenmodell und dem zentralen Server der Zugriff auf mehrere FMEAs und deren Maßnahmen realisiert werden. Das bedeutet, dass ein Entwickler gleichzeitig seine Maßnahmen von mehreren Projekten bzw. FMEAs auf einen Blick zur Verfügung hat. Nicht zuletzt können damit auch mehrere Personen gleichzeitig auf die Maßnahmenverfolgung zugreifen und somit schneller und effizienter die offenen Punkte abarbeiten.

4.2.6 Schnittstellenbetrachtung

Für die OEM übergreifende, durchgängige Schnittstellenbetrachtung dockt sich das neue Datenmodell ebenfalls an die bekannte und bewährte sowie in der Automobilbranche verwendete FMEA-Methode nach der VDA-Vorgehensweise (wie in Abschnitt 2.2.2.2 beschrieben) an und erweitert diese zugleich um eigene Elemente.

Dazu wird die System-FMEA nach folgendem Schema aufgebaut:

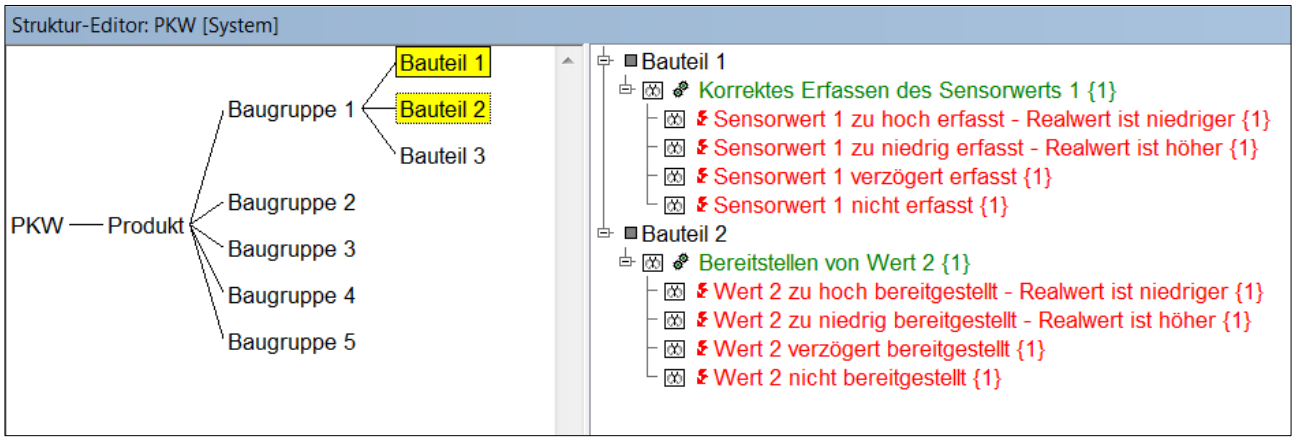


Abbildung 38 – Beispielstruktur zur Schnittstellenanalyse (in APIS IQ-RM)

Der System-FMEA-Strukturierungsgedanke sieht vor, die Inputs und Outputs des Systems zu betrachten. Dabei stellt sich grundsätzlich die Frage, welche Fehler auftreten können, nicht jedoch warum sie auftreten.

Jeder Komponenten- bzw. Systemlieferant erfasst dabei seine verwendeten und benötigten Schnittstellendaten, die im Anschluss auf den Server hochgeladen und dort weiter verarbeitet werden.

Integration der Schnittstellen-Informationen

Um später eine automatisierbare Auswertung der Schnittstellenzusammenhänge zu ermöglichen, müssen nun die Schnittstellen einheitlich in das System eingepflegt und detailliert spezifiziert werden. Diese Daten werden mit der entsprechenden „Funktion“ (in Abbildung 38) verknüpft und verankert.

Im ersten Schritt werden die Schnittstellen-Daten, wie beispielsweise ein Sensor oder eine Information, die über den CAN-Bus kommt, im System erstellt. Dabei werden unter anderem eine Bezeichnung, der Typ des Signals und Toleranzen eingetragen. Dieser Schritt wird einmalig für jede Schnittstelle durchgeführt.

Im zweiten Schritt legt jeder Komponenten-Lieferant Schnittstellenzugriffe fest. Dabei wählt er zuerst die Schnittstelle aus, auf die er zugreifen möchte. Zusätzlich definiert er dann noch die Art und Weise, wie auf die Daten zugegriffen wird (zum Beispiel Zugriffszeiten, Zugriffsart (Lesen/Schreiben)) definiert.

Um alle notwendigen Daten während der Datenerfassung einheitlich und vollständig zu erhalten, wird ein Template aus Eigenschaften, die an die Schnittstellen gestellt werden, aufgebaut.

Dieses Template wird zur Abfrage innerhalb einer vordefinierten Eingabemaske bzw. in einem Assistenten genutzt. Der Assistent orientiert sich dabei an dem in Abbildung 39 dargestellten Prozessablauf, der auf der nächsten Seite abgebildet ist:

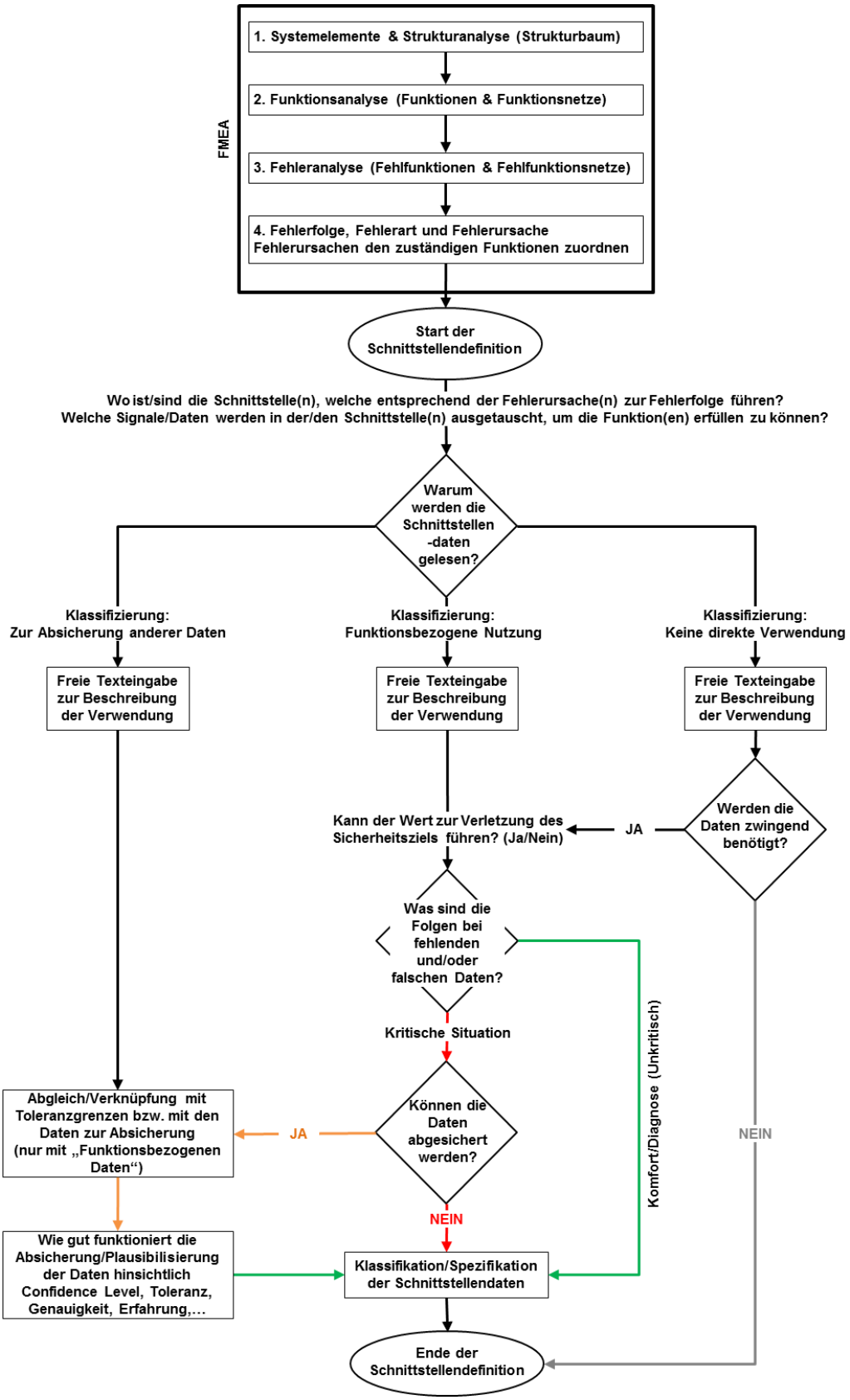


Abbildung 39 – Schnittstellendefinitionsprozess

Durch die Zusammenführung der verschiedenen FMEAs auf einem Server und die einheitliche Klassifikation der Schnittstellen können in der Folge beispielsweise unerwünschte Einflüsse zwischen einzelnen Komponenten durch unkoordinierte Lese- und Schreibzugriffe aufgedeckt werden. Zugleich können durch die Angabe von Plausibilisierungsmöglichkeiten die Wichtigkeit einzelner Signale erkannt und notwendige Maßnahmen zur Absicherung getroffen werden.

5 Validierung der Lösungen

Im vorliegenden Kapitel 5 wird die Anwendung der entwickelten Methode anhand eines Forschungsprojekts dargestellt, das die herstellerübergreifende Entwicklung eines Hybrid-Fahrzeug-Nachrüstsatzes zum Ziel hatte. Mit dieser Anwendung soll eine Methodenvalidierung realisiert werden.

Dazu wird die Validierung, wie in Abbildung 40 dargestellt, zweistufig ablaufen. In der ersten Stufe wird das IT-Konzept hinter der Methode untersucht und validiert. Im zweiten Schritt werden die ASIL-Einstufung, die Schnittstellenanalyse sowie die Anforderungsdurchgängigkeit unter Verwendung des IT-Konzepts bewertet.

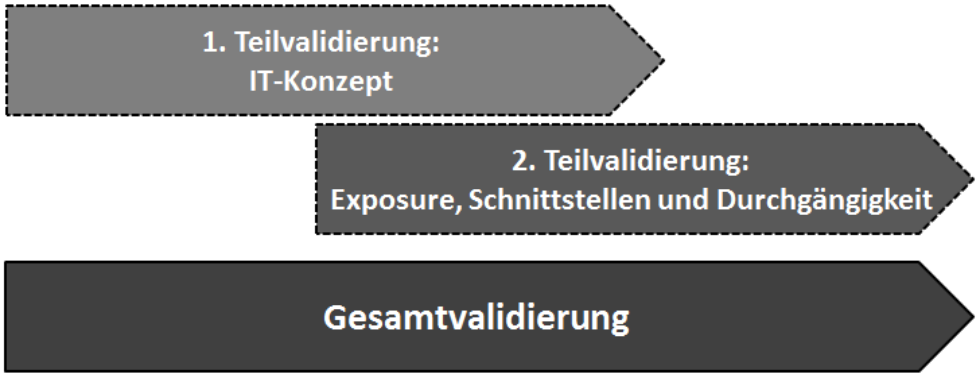


Abbildung 40 – Zweistufiges Validierungsvorgehen

Daraus ergibt sich eine vollständige Gesamtvalidierung. Hierzu werden in Abschnitt 5.1 der grundlegende Aufbau und die Entwicklung des Hybridantriebs erläutert. Daran wird ersichtlich, warum das Projekt nicht nur aufgrund der verteilten, unternehmensübergreifenden Entwicklung, sondern auch angesichts der komplexen Funktionszusammenhänge eine sehr gute Validierungsgrundlage bildet.

In Abschnitt 5.2 wird auf die Umsetzung des IT-Konzepts inkl. Remodellierung und dessen Stärken und Schwächen eingegangen. Im darauf folgenden Abschnitt 5.3 wird unter Zuhilfenahme des in Abschnitt 5.2 validierten IT-Konzepts die zielmarktorientierte ASIL-Ermittlung, die Schnittstellenbetrachtung wie auch die Anforderungsdurchgängigkeit betrachtet und gewürdigt.

Abschließend werden in Abschnitt 5.4 die Ergebnisse der Validierung kritisch bewertet sowie ein Ausblick hinsichtlich Verbesserungspotenzial und einer weiteren Entwicklung aufgezeigt.

5.1 Aufbau und Entwicklung des Hybridantriebs

Der Aufbau des Hybridantriebs besteht aus unterschiedlichen Komponenten und ist schematisch in Abbildung 41 dargestellt.

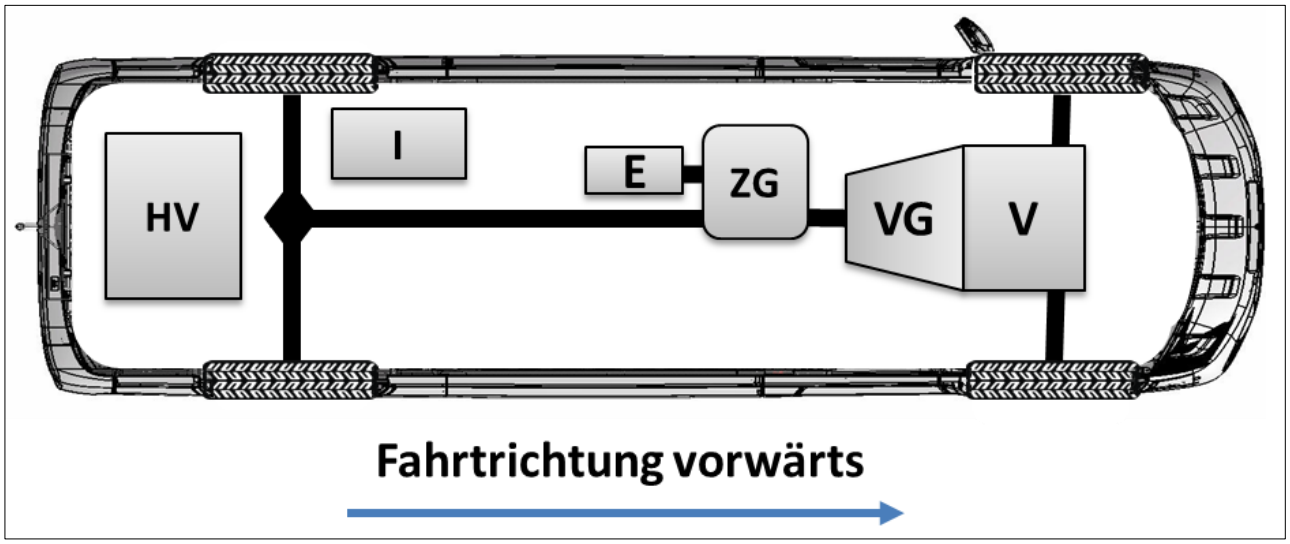


Abbildung 41 – Vereinfachter Aufbau des Hybrid-Fahrzeugs

Vereinfacht lassen sie die einzelnen Teile des Hybrid-Nachrüstsatzes in folgende Gruppen zusammenfassen:

- Antriebsstrang Verbrennungs-Motor (Motor (**V**) und Getriebe (**VG**))
- Antriebsstrang Elektro-Motor (Motor (**E**) und Inverter (**I**))
- Zwischengetriebe (**ZG**) für die Kopplung von V- und E-Motor
- Hochvolt-Bereich (Batterien, Batterie-Management-System, DC-DC-Wandler, Ladegerät, Isolationswächter, Schütze, Kabel), kurz **HV**
- Steuergerät/ECU (befindet sich im Fahrzeuginneren)
- Nebenaggregate (Vakuum-, Servo-, Öl-, Wasserpumpe)

Das **Zwischengetriebe (ZG)** hat die Aufgabe, die Verbindung der zwei Antriebe (**V** sowie **E**) mit dem zentralen Abtrieb zu koordinieren. Abhängig von der Getriebestellung ist damit das diesel- bzw. benzin-, elektrisch- oder hybrid-betriebene Fahren möglich. Die Antriebsleistung wird hierbei von einem klassischen **Verbrennungsmotor** wie auch einer **E-Maschine** erzeugt.

Der V-Motor und das Verbrenner-Getriebe werden unverändert übernommen und genutzt. Der E-Motor ist hingegen zusätzlich integriert worden und wird vom **Inverter** angesteuert und mit Leistung versorgt. Die dafür notwendige Leistung erhält der Inverter von **Batterien**, die durch das **Batterie-Management-System** (kurz BMS) gesteuert sowie überwacht werden. Mit dem BMS kann eine Tiefentladung bzw. Überladung, Überhitzung oder ein zu hoher Entladestrom erkannt werden und damit die Batterien vor Schäden oder einer thermischen Reaktion (Brand) schützen.

Der **Isolationswächter** ist für die Erkennung von Isolationsschäden im Hochvolt-Bereich zuständig. Er sorgt dafür, dass im Fehlerfall eine an der Karosserie anliegende Spannung erkannt wird und das System die Zentralschütze öffnet (Trennung der Batterien vom HV-Kreis).

Die zusätzlichen **Nebenaggregate** sorgen im E-Betrieb für die Lenkbarkeit sowie die Kühlung, Schmierung und Schaltbarkeit des Zwischengetriebes.

Alle Koordinations- und Steuerungsaufgaben übernimmt die zentrale **Electronic Control Unit** (ECU).

In der Summe werden die neuen Komponenten von drei unterschiedlichen Firmen entwickelt. Daneben werden die Zukaufkomponenten (wie z. B. die Nebenaggregate) von weiteren Entwicklungspartnern koordiniert. Durch die verteilte Entwicklung ist eine direkte Zusammenarbeit nur erschwert möglich (Abbildung 42 auf der nächsten Seite).

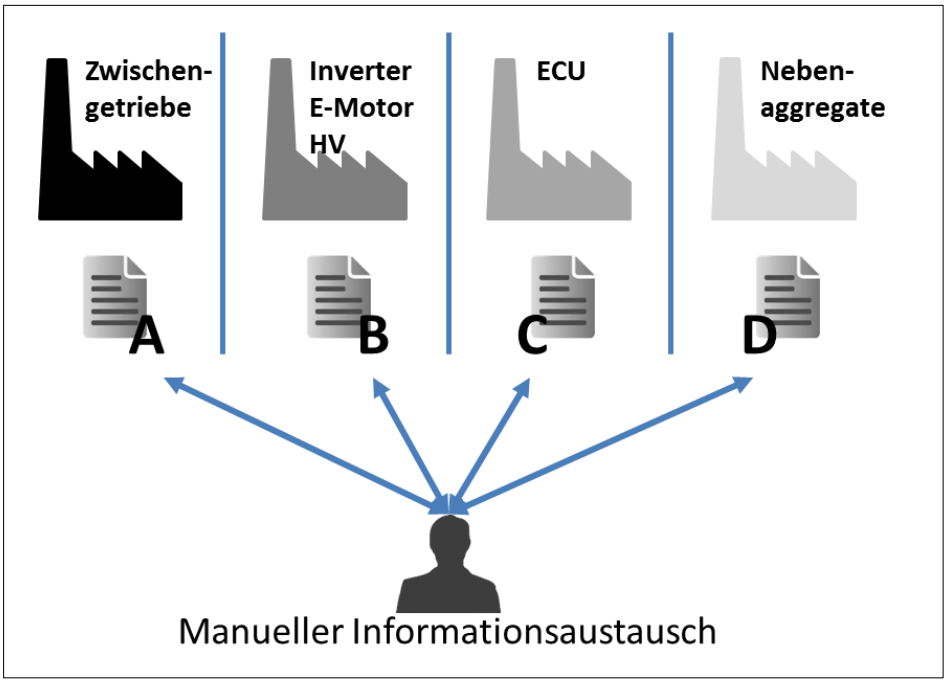


Abbildung 42 – Manueller Informationsaustausch

Durch die Hybridisierung bzw. die rein elektrische Fahrfähigkeit des Fahrzeugs ergeben sich neue Entwicklungsziele, die im rein verbrennungsmotorischen Betrieb nicht existierten.

Ein sehr wichtiger Entwicklungsaspekt ist die Fahrtrichtung. Im rein verbrennungsmotorischen Betrieb mit Schaltgetriebe muss sich der Entwickler um diese Funktion wenig Gedanken machen. Der Motor dreht sich immer in die gleiche Richtung und die Fahrtrichtung wird schlussendlich durch die Übersetzung, genauer die „Anzahl an Übersetzungsstufen", des Getriebes festgelegt bzw. vorgegeben. Im rein elektrischen Fahrbetrieb wird die Fahrtrichtung dagegen durch die im mechanischen Getriebe verbauten Sensoren vorgegeben. So ist ein Rückwärtsgangsensor dafür verantwortlich, dem Steuergerät den Rückwärtsfahr-Fahrerwunsch zu signalisieren. Im Falle eines Sensordefekts („dauerhaftes Senden eines Signals" bzw. „dauerhaft kein Signal" unabhängig vom tatsächlich eingelegten Gang) kann es dazu kommen, dass das Fahrzeug nicht in die Richtung fährt, die vom Fahrer durch den eingelegten Gang selektiert ist.

Ein weiteres Problem bei der Hybridisierung ist das Zusammenspiel der zwei Antriebe miteinander. So ist sicherzustellen, dass beide Motoren zu jeder Zeit ein vorzeichengleiches

Antriebsmoment bzgl. der Fahrtrichtung bereitstellen, da ansonsten das Getriebe beschädigt wird.

Beide Probleme können durch unterschiedliche Komponenten im Nachrüstsatz entstehen, da die einzelnen Funktionen nur durch ein korrektes Zusammenspiel aller relevanten Komponenten erreicht werden kann.

Anhand der zwei oben beispielhaft dargestellten Probleme sowie der Vielzahl der Komponenten und deren Zusammenspiel ist ersichtlich, wie komplex das Forschungsprojekt ist und wie systematisch sowie durchgängig die Entwicklung erfolgen muss.

5.2 Validierung IT-Konzept

In diesem Abschnitt werden die Stärken und Schwächen der IT-Konzeptumsetzung dargestellt. Abbildung 43 zeigt, wie das IT-Konzept ein übergreifendes Zusammenarbeiten der verschiedenen Hersteller ermöglicht.

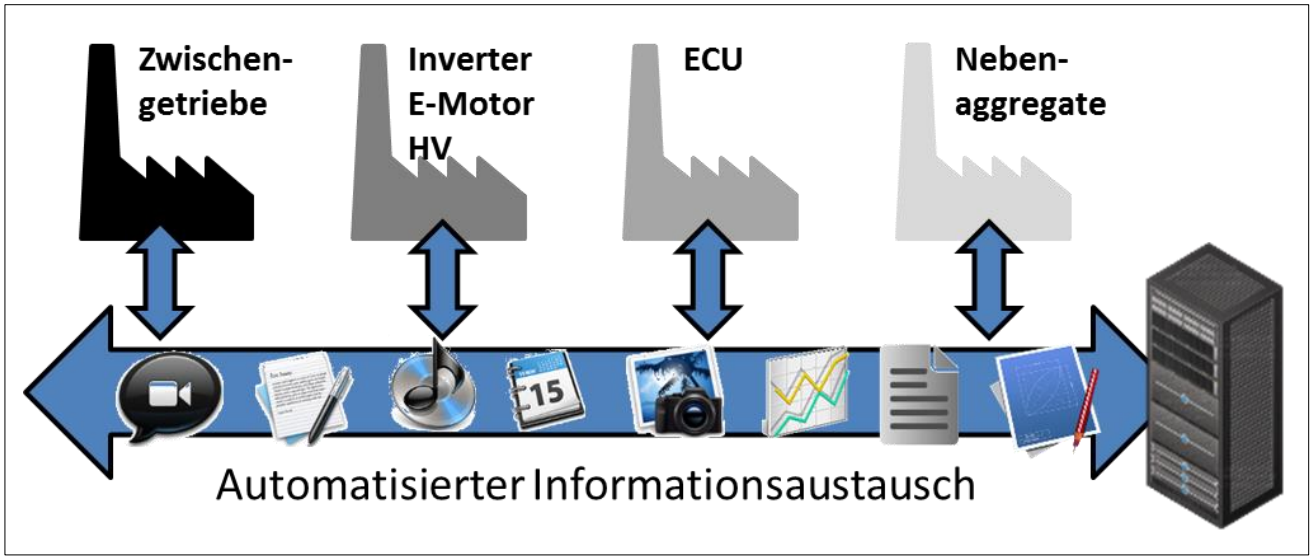


Abbildung 43 – Automatisierter Informationsaustausch

5.2.1 Serverimplementierung

Zuerst wird die zentrale Serversoftware betrachtet. Dazu muss zu Beginn die FMEA-Struktur aus einer FMEA-Software in das standardisierte XML-Format (MSRFMEA) expor-

tiert werden. Anschließend kann dieses in die Serversoftware importiert werden. Im Gegensatz zur herkömmlichen Nutzung ist damit die verteilte Betrachtung der erarbeiteten Zusammenhänge und Daten möglich. Besonders bewährt hat sich dieses Konzept in dem durchgeführten Forschungsprojekt, da hier die verteilte Abarbeitung der Maßnahmen über die Firmengrenzen hinweg wichtig und notwendig ist. Der größte Vorteil ist jedoch der Umstand, dass kein sequenzielles Arbeiten an der FMEA mehr erforderlich ist. Stattdessen kann parallel an der FMEA gearbeitet werden. Somit ist ein vollwertiges „Simultaneous“ bzw. „Concurrent Engineering“ möglich.

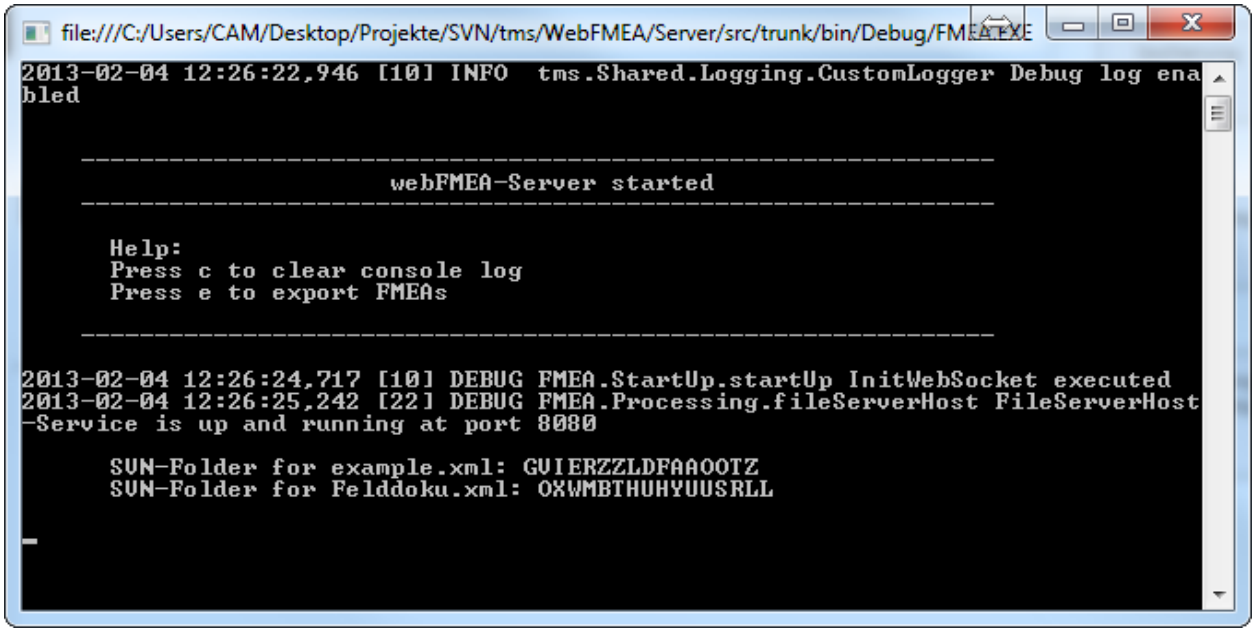


Abbildung 44 – Server-Software

Als größte Schwäche der Datenzentralisierung hat sich jedoch die Tatsache herausgestellt, dass aufgrund des Architekturansatzes eine konstante Verbindung zum Zentralserver vorhanden sein muss. Das bedeutet, dass bei fehlender Internetverbindung kein Zugriff auf die Daten möglich ist. Eine Offline-Verfügbarkeit, wie es von klassischen Dateisystemen bekannt ist, ist nicht vorhanden. Dies würde dem grundsätzlichen Daten-Konzept widersprechen und sich mit diesem nicht oder nur unter hoher Funktionseinbuße vereinen lassen.

5.2.2 Client

Die „Client-Software“ wurde in Anlehnung an die Software „IQ-RM PRO“ der APIS IT GmbH entwickelt. Damit soll der Umstieg erleichtert werden. Der generelle Zugriff auf den Server durch einen Browser hat in dem Projekt eine weitere Akzeptanzsteigerung zur Folge gehabt. Die Tatsache, dass quasi keine Software installiert werden musste (da standardmäßig ein Browser in den unterschiedlichen Betriebssystemen vorhanden ist) und praktisch von jedem Gerät aus auf die Daten zugegriffen werden konnte, hat die Arbeit weiter erleichtert.

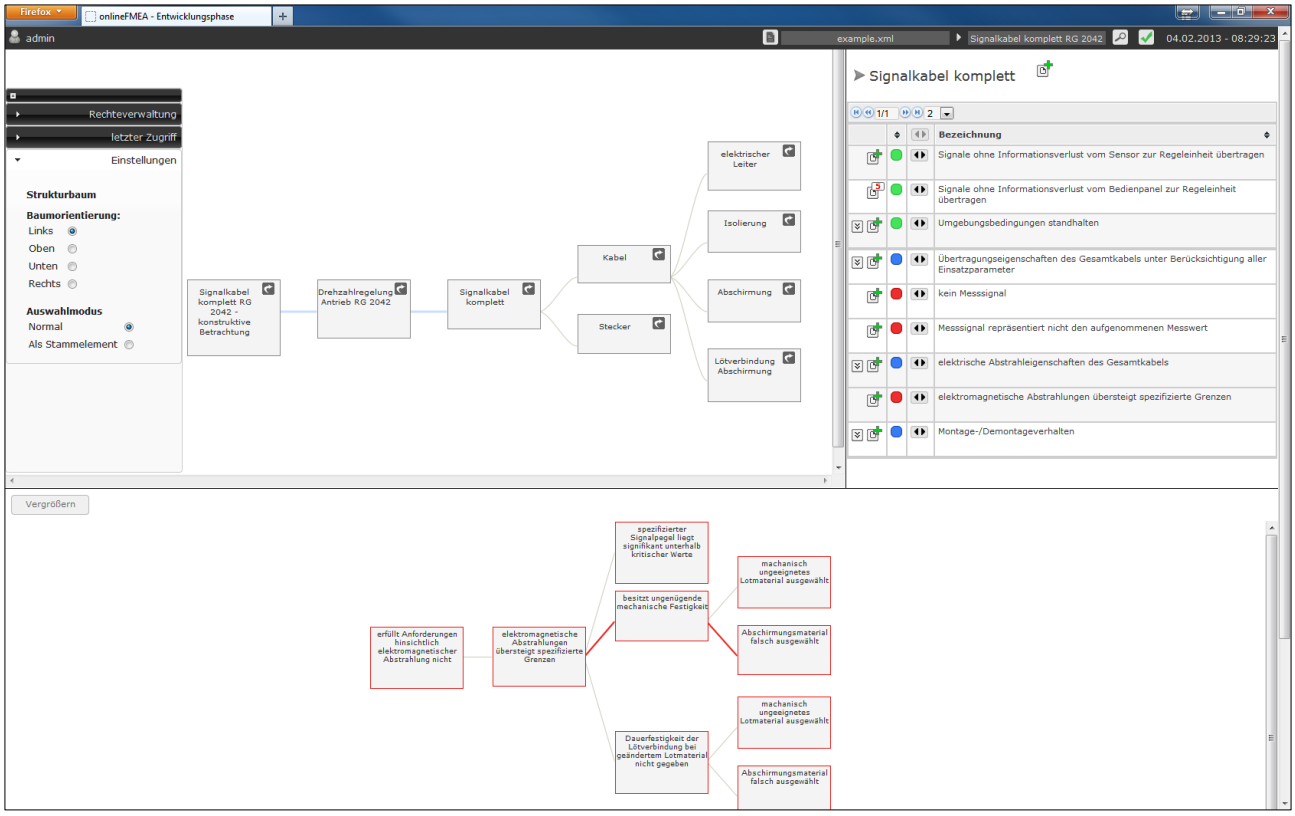


Abbildung 45 – webFMEA - Benutzeroberfläche im Mozilla Firefox 19.0

Als größter Nachteil und am meisten verbesserungswürdig wurde jedoch besonders der Zugriff von Tablets und Mobiltelefonen angesehen. Hier haben die zwei Faktoren, Bildschirmgröße sowie Auflösung des Displays, einen hohen Einfluss auf die Bedienbarkeit des Systems. Obwohl durch Zoomgesten der Bildschirminhalt mehr oder weniger beliebig

und stufenlos vergrößert und verkleinert werden kann, wird damit die Bedienbarkeit nicht verbessert. Ebenso ist die Bedienung der FMEA-Strukturen (Struktur-, Funktions- und Fehlerbaum) nur eingeschränkt möglich, da die Touchscreen-Bedienung nur eine eingeschränkte, zum Teil umständliche Bedienung zulässt. So ist eine komfortable Drag&Drop-Nutzung, wie es ein Rechner mit Maus bietet, nicht möglich. Diese Bedienung ist aber zur Navigation durch große Strukturen notwendig und sehr hilfreich. Zuletzt hat der reduzierte Funktionsumfang unnötigen Aufwand bereitet. Bei Änderungen an den Strukturen oder Funktionen bzw. Fehlfunktionen muss zuerst ein Export aus dem Zentralserver und anschließend nach der Bearbeitung ein Reimport durchgeführt werden. Da dies doch relativ häufig nötig war, ist die Implementierung von Basisbearbeitungsfunktion erforderlich.

5.2.3 Remodellierung der Daten

Der Remodellierungsprozess stellt die grundsätzliche Erweiterung der vorhandenen FMEA-Daten dar. In der Folge werden die Tag-Definition, die Rechteerweiterung sowie die Dokumentation betrachtet.

Tag-Definition

Die technische Integration der Tag-Definition (siehe Abbildung 46 auf der nächsten Seite) funktionierte während des Erstellungsprozesses der FMEA problemfrei. Dabei war sehr positiv zu bewerten, dass sich durch diese integrierte ID-Verwaltung die Fehler bei der Vergabe von IDs auf ein Minimum reduzieren ließen. Doppelte oder für gleiche Maßnahmen unterschiedlich vergebene IDs konnten damit vollständig eliminiert werden.

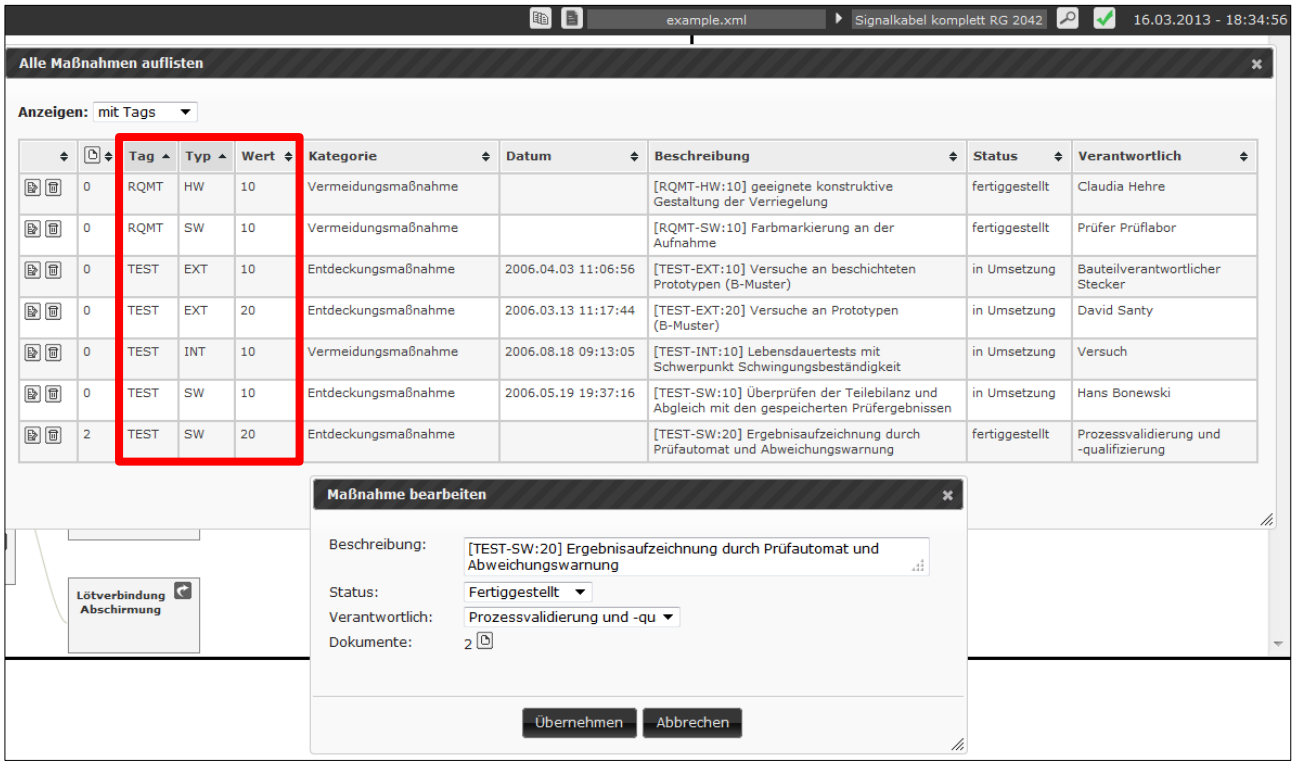


Abbildung 46 – webFMEA - Tag-Definition und Auswertung

Nachteilig zu bewerten waren die statisch definierten und vorgegebenen Tag-Klassen. Es hat sich während der Nutzung herauskristallisiert, dass die dynamische Integration neuer Tag-Kategorien/Klassen sinnvoll und für die Entwicklung hilfreich ist. Des Weiteren hat sich bei der Anwendung des Web-Interface die Anforderung ergeben, dass nicht nur während der Erstellung der FMEA in z. B. APIS IQ-RM, sondern auch in der späteren Betrachtung im Webinterface die Vergabe und Integration von Tags notwendig ist.

Rechtevergabe

Die Rechtevergabe ermöglicht die Bereitstellung von Informationen für einzelnen Benutzer, um den unerwünschten Zugriff auf möglicherweise sensible Daten zu unterbinden. Während der Nutzung hat das Rechtemanagement diese Aufgabe gut erfüllt.

Negativ sind die vielen vorhandenen Rechte sowie das Fehlen von Gruppenrechten aufgefallen. Oft ist einfach unklar, welches Recht tatsächlich notwendig ist und damit vergeben werden sollte. Die Erweiterung um eine gruppenbasierte Rechtevergabe wäre zudem sehr

wichtig. Damit können global verfügbare Gruppen angelegt werden (bei einer verteilten Entwicklung zum Beispiel für jede Firma eine Gruppe), in die die Personen eingeordnet werden, die dann die Rechte der Gruppe vererbt bekommen. Somit sind Mitarbeiter-Fluktuationen in der Projektbearbeitung schneller und fehlerfrei zu realisieren. Ebenso entfällt damit die zeitaufwendige und fehlerbehaftete Rechtevergabe für einen neu hinzukommenden Projektmitarbeiter. Stattdessen wird er nur noch der jeweiligen Gruppe zugeordnet und erhält damit direkt alle notwendigen Zugriffsmöglichkeiten. Ebenso muss bei einer Rechteänderung nur die Gruppe angepasst werden und nicht die Rechte der einzelnen Mitarbeiter.

Abbildung 47 – webFMEA - Knoten mit vollen Rechten

Abbildung 48 – webFMEA - Knoten mit eingeschränkten Rechten

Dokumentation

Durch die Integration einer strukturbasierten Dokumentenverwaltung hat sich der Dokumentationsaufwand im Forschungsprojekt stark reduziert. Jede Person, die für eine Maß-

nahme verantwortlich ist, kann selbst alle notwendigen Dokumente einpflegen und verwalten (siehe Abbildung 49).

Insbesondere für den Projektleiter stellt das eine wesentliche Entlastung dar, da die Dokumentenzusammenstellung bisher ein sehr zeitintensiver Prozess war.

Problematisch sind jedoch die Qualität der bereitgestellten Dokumente sowie deren Formate. Zum Teil wurde aus Gründen der Einfachheit eine Vielzahl von Dokumenten in ein Archiv gepackt (gezippt). Damit ist jedoch nicht mehr klar, welche Dokumente tatsächlich an ein Element, eine Funktion oder an einen Fehler angehängt sind. Zukünftig sollten daher keine Archive mehr hochgeladen werden können oder diese automatisiert entpackt werden. Die im Archiv enthaltenen Dateien könnten dann direkt an das jeweilige Element angehängt werden.

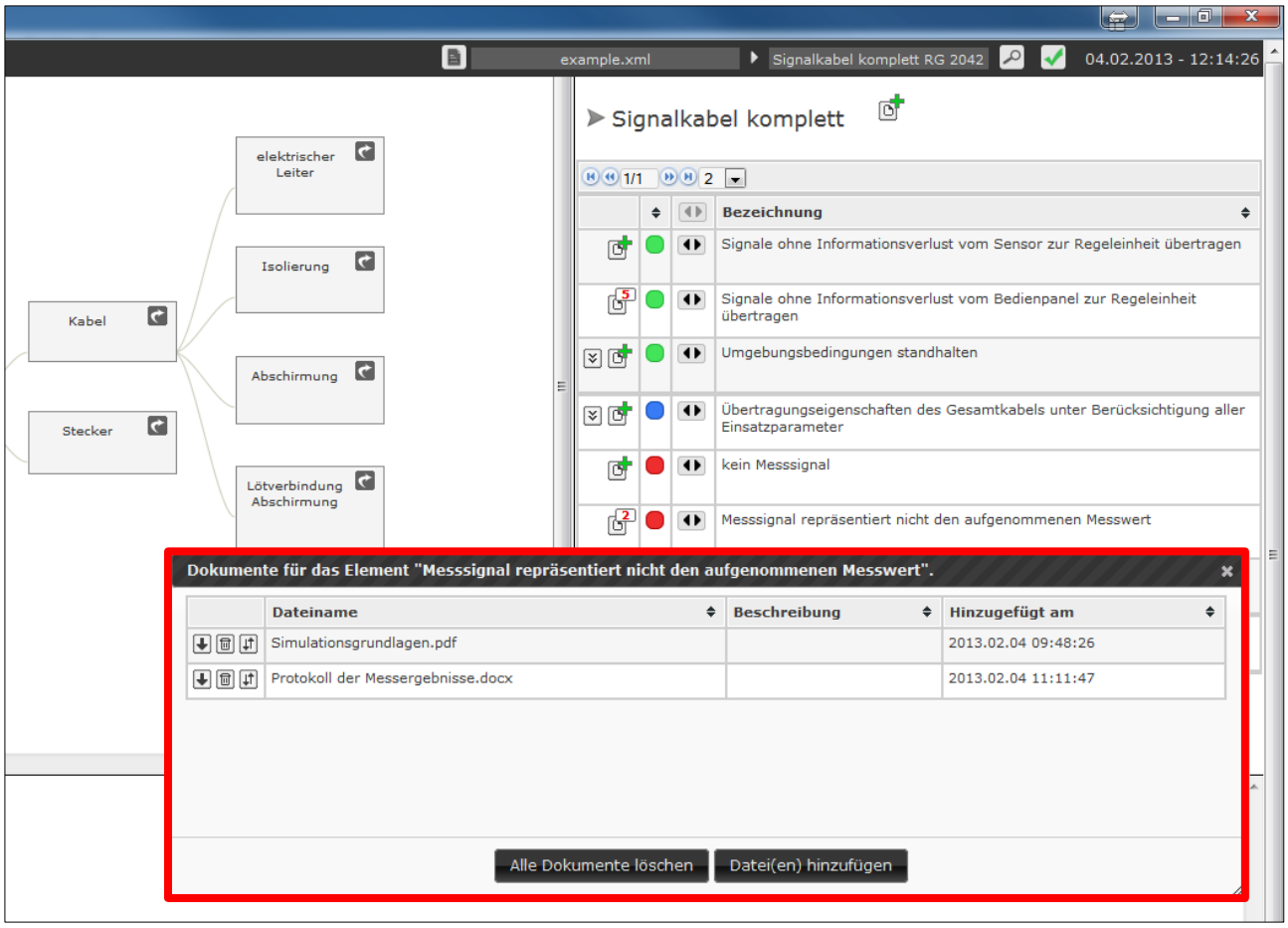


Abbildung 49 – webFMEA - Dokumentenhandling

Eine weitere Schwachstelle in der Dokumentenverwaltung war die Tatsache, dass die bereitgestellten Dateien nicht durchsucht werden können. Daher wäre zumindest die Möglichkeit der Dateinamensuche sehr hilfreich, um nicht alle Dateien per Hand durchsuchen zu müssen.

5.3 Validierung der Exposure-Ermittlung, Schnittstellenbetrachtung und Anforderungsdurchgängigkeit

In diesem Abschnitt sollen die Ergebnisse der Validierung zu den Ausgangsproblemen (siehe Kapitel 1 und 2) dargestellt werden.

5.3.1 Methode zur zielmarktorientierten Bestimmung des ASIL

Eine Entwicklungsschwierigkeit bestand zu Beginn des Projekts darin, dass die verschiedenen Hersteller unterschiedliche Sicherheitsziele und ASIL-Klassifikationen für ihr zu entwickelndes Produkt zugrunde gelegt haben. Im Kontext der ISO 26262 ist es jedoch erforderlich, dass alle an einer sicherheitskritischen Funktion beteiligten Komponenten in der Summe die Entwicklungsvorgaben einhalten. Daher war es im ersten Schritt notwendig, die einzelnen Hersteller miteinander zu synchronisieren.

Konkret bedeutet das, dass die ASIL-Einstufungen nivelliert und vereinheitlicht werden mussten. So gab es in den verschiedenen Komponenten Fehler, deren Auswirkungen die gleiche Folge hatten (bspw. Fahrt in die nicht vom Fahrer erwartete und angeforderte Fahrtrichtung). Trotz des gleichen „Top-Fehlers“ bzw. der gleichen Fehlerfolge waren von den Entwicklungspartnern unterschiedliche ASIL-Bewertungen als Entwicklungsgrundlage ermittelt und angenommen worden. Aus diesem Grund wurde die ASIL-Einstufung für alle relevanten und sicherheitskritischen Top-Fehler erneut vorgenommen, um ein unternehmensübergreifendes einheitliches und akzeptiertes Verständnis unter den Entwicklungspartner zu schaffen. Um dies zu erreichen, wurde zu Beginn die mögliche Folgenschwere der Fehlfunktion einer Funktion definiert. Diese Severity wurde unter Zuhilfenahme der amerikanischen „Abbreviated Injury Scale“ bzw. der deutschen „Unfallkategorien“ ermittelt. Im zweiten Schritt wurde die Beherrschbarkeit der Gefährdungssituation definiert. Dabei

konnte von den Erfahrungswerten, die mit einem früheren Prototyp gesammelt wurden, profitiert werden. Im letzten Schritt musste die Exposure der relevanten Fahrsituationen bestimmt werden. Die sehr subjektiven Einschätzungen konnten durch den Einsatz der statistikbasierten Bewertungen auf einen, von allen Partnern akzeptierten, Wert festgelegt werden. Ein positiver Nebeneffekt ist die Tatsache, dass durch die faktenbasierte Beurteilung die Nachvollziehbarkeit stark verbessert wurde und auch Personen die nicht direkt am Bewertungsprozess beteiligt waren die Hintergründe und Entscheidungsgrundlagen verstehen.

Als Nachteil hat sich der Initialaufwand zur Erstellung der Statistiken gezeigt. Um hier einen validen und belastbaren Wert zu erhalten, müssen vorab unterschiedlichste Daten gesammelt und ausgewertet werden. Des Weiteren müssen für die einzelnen Systeme und deren Funktionalitäten in einem Fahrzeug unterschiedliche Fahrsituationen bzw. Betriebszustände betrachtet werden. Dafür ist eine hohe Anzahl an Statistiken erforderlich, was einen hohen Initialaufwand darstellt.

5.3.2 Schnittstellenanalyse

Aufgrund der verteilten Entwicklung und der Vielzahl an Schnittstellen war es erforderlich, diese systematisch abzustimmen und zu entwickeln. Durch den integrierten FMEA-Ansatz und die verteilte Zugriffsmöglichkeit konnten im Forschungsprojekt diese Übergänge gut analysiert und betrachtet werden.

Dazu wurden in einem ersten Schritt alle Datenschnittstellen aufgenommen und aufbereitet. Anschließend war es Aufgabe der Projektpartner, die relevanten Daten einzupflegen. Besonders die Möglichkeit, direkt Plausibilisierungsmöglichkeiten für Signale festzulegen, hat bei der Entwicklung der ECU enorme Zeit- und Ressourcenvorteile zur Folge gehabt. So war es für den entsprechenden Entwicklungspartner ohne großen Aufwand und zusätzliche Rückfragen möglich, die Daten in seine Modelle zu integrieren und die Kombination mehrerer Datenquellen zu realisieren.

Als Negativpunkt wurde der hohe Aufwand zur Integration und Pflege der Daten angesehen. Insbesondere für die Entwicklungspartner, die nicht die ECU entwickelt haben, war

das Aufwand-Nutzen-Verhältnis nicht ausreichend hoch. Daher wurden trotz der verteilt organisierten Datendetaillierung und des hohen Nutzens für den ECU-Entwickler die Schnittstellendaten nur in geringem Umfang eingetragen. Hierbei zeigte sich, dass der Faktor Mensch die entscheidende Rolle spielt. Das darunterliegende Datenmodell und dessen Bearbeitungsmöglichkeiten können die Schnittstellenbetrachtung nur erleichtern, jedoch nicht erzwingen.

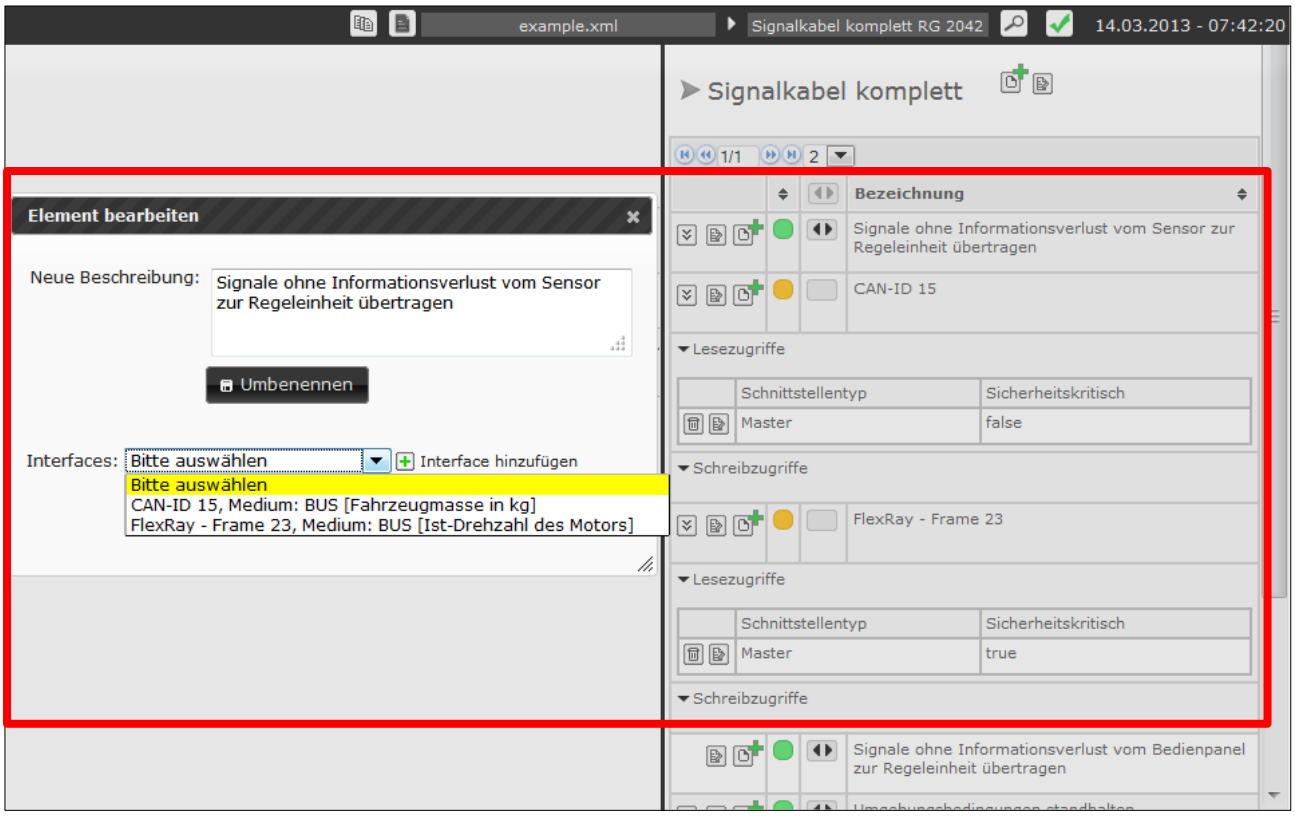


Abbildung 50 – webFMEA - Darstellung der Schnittstellenzugriffe

Im Kontext einer Serienfahrzeugentwicklung und nicht eines Forschungsprojekts sieht diese Situation anders aus. Hier hat der übergelagerte Lieferant bzw. der OEM (als Kunde des Herstellers) die Möglichkeiten, die Betrachtung, Integration und Pflege der Schnittstellendaten einzufordern und durchzusetzen.

5.3.3 Anforderungsdurchgängigkeit

Die Anforderungsdurchgängigkeit stellte bei dem Projekt die größte Herausforderung dar. Dies war nicht nur der verteilten Entwicklung geschuldet, sondern auch der Komplexität des eigentlichen Systems sowie der Vielzahl an externen Anforderungen und den daraus abgeleiteten internen Anforderungen und Testing-Maßnahmen.

Um diese Komplexitätsfaktoren zu beherrschen, wurden zu Beginn mit der System-FMEA die System-Architektur sowie mögliche Fehler analysiert. Darauf aufbauend wurden neue Anforderungen inkl. notwendiger Testmaßnahmen abgeleitet und in die FMEA als interne Funktionen integriert. Dabei wurde zur Absicherung der Nachverfolgbarkeit und Durchgängigkeit auf das Tagging-System gesetzt. Zusätzlich dazu wurden die relevanten Systemelemente, Funktionen und Fehlfunktionen mit Rechten sowie die Maßnahmen mit Verantwortlichkeiten versehen. Damit war es für die Entwicklungspartner möglich, ihre Maßnahmen abzuarbeiten, ihren eigenen Stand im Projekt abzuleiten und offene Punkte einzusehen.

Durch das integrierte Dokumentenmanagement konnte die Umsetzung direkt in der FMEA bei den Strukturelementen, Funktionen bzw. Fehlfunktionen verankert und damit auffindbar und nachvollziehbar gestaltet werden. Davon betroffen waren z. B. die Sicherheits- und Diagnosefunktionen wie auch das Testing. Ein Zusammenführen, wie es bei einem konventionellen Konzept üblich und notwendig ist, war hier nicht mehr erforderlich. Durch die automatische Verwaltung der Dokumente sowie deren Zuordnung verringerte sich die Fehlerrate gegenüber der manuellen Dokumentenverwaltung erheblich. Ein weiterer Nebeneffekt war die Transparenzsteigerung innerhalb eines Unternehmens, was allerdings unterschiedlich, d. h. nicht immer positiv aufgenommen wurde. Dadurch war es für andere Mitarbeiter oder Manager möglich, den tatsächlichen Projektfortschritt zu verfolgen und nicht auf aufbereitete Informationen Dritter angewiesen zu sein.

Alles in allem konnte durch die neue Vorgehensweise bzw. erweiterte Methode, die Ermittlung, Umsetzung wie auch die Dokumentation der Tätigkeiten stark verbessert und gesteigert werden.

5.3.4 Zusammenfassende Bewertung

Zusammengefasst ergibt sich folgendes Bild bei der Betrachtung der Situation vor und nach der Arbeit bezogen auf die Problemstellung bzw. Zielsetzung:

	Konventionell	**Neuer Ansatz**
Konzept zur nachvollziehbaren ASIL-Einstufung unter Beachtung von Länder- und Regionsspezifika		
Dokumentation des ASILs	Ja	Ja
Transparenz des ASILs	Schlecht	Sehr gut
Nachvollziehbarkeit des ASILs	Schlecht	Sehr gut
Zielmarktspezifischer ASIL	Nein	Ja
Aufwand	Niedrig	Initial hoch, danach niedrig

	Konventionell	**Neuer Ansatz**
Ansatz zur Abstimmung von System-Schnittstellen zwischen Kunde und Entwicklern		
Lieferantenübergreifende Betrachtung möglich	Eingeschränkt	Ja
Zentrale Bereitstellung von Schnittstellendaten	Eingeschränkt	Ja
Automatisierte Darstellung der Zusammenhänge	Nein	Ja
Aufwand	Hoch	Initial hoch, danach niedrig

	Konventionell	**Neuer Ansatz**
Herangehensweise zur systematischen und durchgängigen Umsetzung sowie Dokumentation der Anforderungen unter Normaspekten		
Durchgängige Dokumentation	Eingeschränkt	Ja
Zentrales übergreifendes Maßnahmentracking	Nicht möglich	Ja
Zugriffssteuerung auf FMEA-Daten	Eingeschränkt	Ja
Verknüpfung aller relevanten Daten	Eingeschränkt	Ja

6 Bewertung der Ergebnisse und Ausblick

In der vorliegenden Arbeit wurde eine neue Herangehensweise bzw. Methode basierend auf der Fehlermöglichkeits- und Einflussanalyse (kurz FMEA) entwickelt. Damit soll den geänderten, neuen und höheren Anforderungen, die bei der Entwicklung funktional sicherer, mechatronischer Produkte nach der ISO 26262 gefordert werden, Rechnung getragen werden.

Die im November 2011 veröffentlichte und von der IEC 61508 abgeleitete ISO 26262 steht für eine systematische Analyse und Entwicklung von sicherheitskritischen (mechatronischen) Produkten in serienproduzierten Automobilen bis 3,5 t.

Diese neue Norm hat das Ziel, kritische und gefahrbringende Situationen für die Insassen eines Fahrzeugs sowie die anderen Verkehrsteilnehmer auf ein technisch und gesellschaftlich akzeptiertes Restrisiko zu minimieren. Solche Situationen können aufgrund systematischer (z. B. Auslegungsfehler bei Bauteilen) oder zufälliger (z. B. ein driftender Widerstandswert, verursacht durch altersbedingte Bauteilabweichung) Fehler entstehen.

Um die Risikominimierung zu erreichen, müssen die unterschiedlichen Teile, Komponenten, Produkte und Systeme hinsichtlich ihrer Fehlerkritikalität sowie –auswirkung analysiert und abschließend bewertet werden. Es wird bei der Bewertung zwischen vier **A**utomotive **S**afety **I**ntegrity **L**evels (kurz ASIL) differenziert. ASIL A hat die geringste und ASIL D die höchste Kritikalität. Das ASIL selbst wird anhand von drei Faktoren ermittelt:

- Severity (S): Gibt die Folgenschwere einer Fehlfunktion an
- Exposure (E): Gibt die Häufigkeit des Ausgesetztseins einer bestimmten Fahrsituation an
- Controllability (C): Die Beherrschbarkeit C gibt an, wie gut ein durchschnittlicher Fahrer mit dem aufgetretenen Fehler umgehen und die Folgen davon beherrschen kann

Anhand des ermittelten ASIL werden die Entwicklungsanforderungen aus der Norm übernommen.

In Kapitel 1 wurden die Ausgangssituation und die Problemstellung erläutert. Dabei wurde besonders in der Ausgangssituation die Wichtigkeit der systematischen Entwicklung auf-

grund der Komplexitätssteigerung dargestellt. Der Grund dafür liegt in der stark steigenden Substitution rein mechanischer Systeme durch mechatronische Systeme.

Aus den Ergebnissen wurden drei zentrale Fragestellungen und Probleme identifiziert:

- Wie kann eine zielmarkt- und funktionsorientierte ASIL-Klassifikation realisiert werden? Konkret heißt das, dass diese weder zu hoch noch zu niedrig sein darf und die Grundlagen für die Ermittlung des ASILs nachvollziehbar und ggf. bei einem Produkthaftungsfall belastbar sein müssen.
- Wie können Schnittstellen zwischen den Systemen betrachtet werden, um Fehlfunktionen durch Schnittstelleneinflüsse und –fehler sowie fehlerhafte Kommunikationsspezifikationen bei einer verteilten Produktentwicklung (über mehrere Standorte und Firmen) zu verhindern?
- Wie kann eine Durchgängigkeit der Produktrequirements (Anforderungen) hinsichtlich der Ermittlung, der Umsetzung, der Risikobetrachtung, der Funktionsvalidierung (Testing) sowie der Dokumentation aller Aktivitäten (Auslegung, Implementierung und Validierung) erreicht werden?

In Kapitel 2 wurde der Stand der Technik hinsichtlich der oben genannten Probleme untersucht. Dabei wurden die verfügbaren Lösungen bzgl. ihrer Stärken und Schwächen analysiert. Basierend auf den Erkenntnissen aus Kapitel 2 sind in Kapitel 3 die Lösungsansätze vorgestellt worden. Es ergaben sich in Kapitel 3 für die einzelnen Teilprobleme individuelle Lösungen, die in der Gesamtheit in Kapitel 4 in eine integrierte IT-Methode bzw. eine Web-Applikation überführt wurden. Mit diesem Client-Server-Konzept wurde es unter anderem möglich, eine tatsächlich verteilte, durchgängige sowie betriebssystem- und geräteunabhängige Entwicklung zu realisieren. Einzig ein Netzwerkzugriff (Intra-/Internet) und ein Browser sind erforderlich.

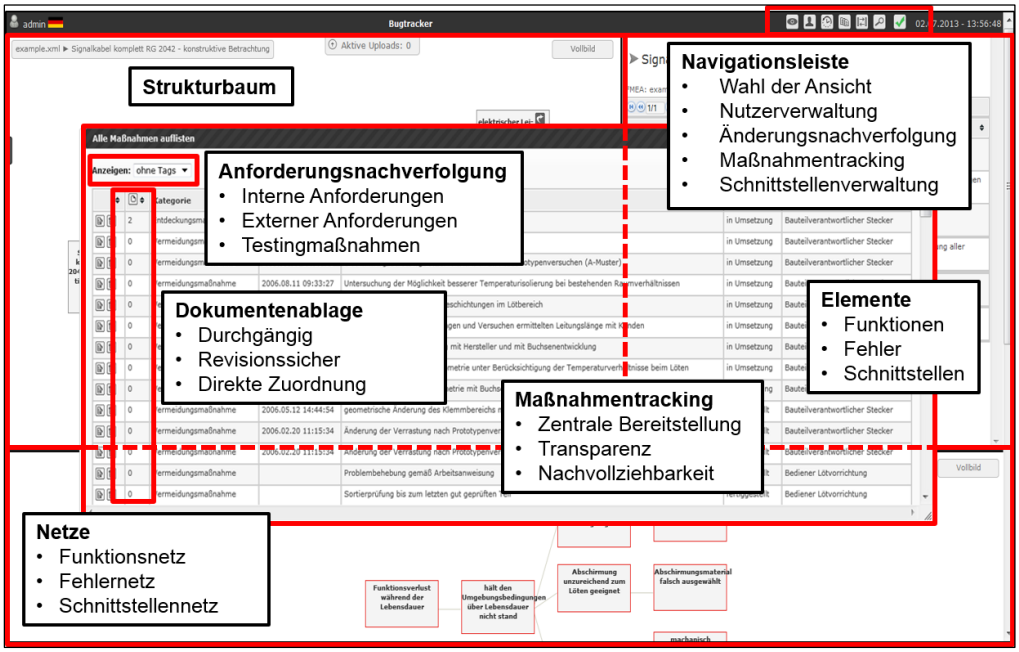


Abbildung 51 – webFMEA - Funktionsübersicht

Die Web-Applikation selbst baut auf Daten aus der Gefahren- und Risikoanalyse anhand der FMEA auf. Diese FMEA-Daten werden dazu in ein neues Datenmodell überführt. Die Datenremodellierung ermöglichte es, neue Objektinformationen und –attribute zu integrieren und damit die automatisierte Daten- und Dokumentenverarbeitung, das Handling (erweitertes User-Interface), die Zugriffsmöglichkeiten (Rechtemanagement) sowie die erweiterte Betrachtung von Schnittstellen zu integrieren. Des Weiteren wurden verschiedene andere Systeme angebunden, sodass eine integrierte, durchgängige Methode für die Entwicklung funktional sicherer Produkte entstand.

Um die zielmarktorientierte ASIL-Klassifikation zu ermöglichen, wurde ein statistisch basiertes Vorgehen entwickelt und umgesetzt. Dieses basiert auf der Tatsache, dass die menschliche Konstitution weltweit identisch bzw. zumindest sehr vergleichbar ist. Das bedeutet, dass bei einem Unfall, unabhängig vom Land (also dem Zielmarkt), die Folgen für den Menschen gleich sind. Somit muss der Severity-Faktor einmalig, unter Berücksichtigung der jeweiligen Fahrsituation festgelegt werden. Danach kann er weltweit als statisch angesehen werden. Bei der Controllability (Beherrschbarkeit einer Fehlersituation) sieht es genauso aus. Auch dieser Wert ist zielmarktunabhängig, da die Fahrfähigen weltweit als vergleichbar angenommen werden können. Als letzte Variable bleibt damit nur noch der

Exposure-Faktor (Häufigkeit des Ausgesetztseins einer Fahrsituation), um den ASIL zu beeinflussen. Um dort ein valides Ergebnis zu erhalten, wurde eine Datenbasis aufgebaut, mit der detaillierte Aussagen über einzelne Fahrsituationen in den jeweiligen Ländern bzw. Regionen getroffen werden können. Da die genutzten Daten öffentlich verfügbar, prüfbar sowie die statistische Auswertung nachvollziehbar sind, kann diese Vorgehensweise im Produkthaftungsfall sehr gut argumentiert werden. Nicht zuletzt werden damit subjektive Empfindungen und Erfahrungen der verschiedenen beteiligten Parteien und Personen reduziert oder komplett eliminiert.

Der gesamte Ansatz sowie die integriert durchgängige Methode auf Basis des IT-Konzepts hat sich während der Validierungsphase, siehe Kapitel 5, als sehr nützlich herausgestellt. Vor allem die Entwicklungstätigkeiten, Absprachen zwischen Entwicklungsparteien sowie die Umsetzung und Dokumentation wurden stark vereinfacht. Nicht zuletzt hat die Vereinfachung des Entwicklungsprozesses zu einer reduzierten Entwicklungszeit sowie zur Reduktion von Entwicklungsschleifen geführt, was sich positiv auf den Ressourcenbedarf ausgewirkt hat.

Bei einer kritischen Betrachtung der Methode während der Validierungsphase ergaben sich auf der anderen Seite Verbesserungspunkte. Neben Bedienungsproblemen auf Smartphones und Tablets, die durch die Überführung der reinen browserbasierten zu einer plattformspezifischen, browserbasierten Applikation relativ leicht überwindbar sind, fehlt noch die direkte Anbindung an Requirement-Tools wie zum Beispiel „Doors“.

An dieser Stelle wird die Durchgängigkeit noch durch einen Medienbruch gestört. Um am Ende zu prüfen, ob alle Requirements, der an der Entwicklung beteiligten Unternehmen, korrekt und vollständig integriert sind, ist noch ein manueller Abgleich notwendig. Diese Schwachstelle stellt einen wichtigen Anknüpfungspunkt für weitere Arbeiten dar.

Daneben muss die Methode auf mögliche Optimierungen untersucht werden, um die Anwendungsfreundlichkeit sowie Methoden- und Software-Transparenz und damit die Anwenderakzeptanz weiter zu steigern. Denn eine IT basierte Methode kann nur Funktionen bzw. Prozesse bereitstellen. Erst durch die Akzeptanz dieser durch den Menschen und die anschließende Nutzung kann ein tatsächlicher Mehrwert erbracht und die Idee dahinter weiter entwickelt werden.

7 Abstract

In this thesis, a new approach or rather a method based on the well-known Failure Mode an Effect Analysis (short FMEA) was developed. With it, the new, higher and changed requirements, which are needed for the development of function safe mechatronic products according to ISO 26262, should be treated. The Standard ISO 26262, which was published in November 2011 is derived from the IEC 61508, stands for systematically analysis and development of safety critical (mechatronics) products in serial produced cars up to 3.5t.

This new standard has the goal to reduce critical and dangerous situations for drivers, car passengers and other traffic participants to a technical and socially accepted residual risk. These critical situations can be triggered by either systematically (e.g. design faults) or random faults (e.g. resistor value drifts, because of age-related hardware element derivation). Therefore the different parts, components, products and systems must be considered regarding their failure criticality as well as effects and finally be rated. The rating differentiates between four Automotive Safety Integrity Levels (short ASIL). ASIL A has the lowest and ASIL D the highest criticality. The ASIL itself will be determined with the help of three parameters:

- Severity (S): Defines the extent of harm to one or more individuals that can occur in a potentially hazardous situation
- Exposure (E): Defines the occurrence of being in in a specific driving/operational situation
- Controllability (C): Defines the ability of an average driver to avoid a specified harm or damage through a timely reaction

Based on the ASIL result, the development requirements and restrictions will be derived from the standard.

In chapter 1, the initial situation as well as the problem statement will be explained. In this first part, the importance of the systematical development due to the increasing number of substitution of pure mechanical solutions with mechatronics systems and its resulting

complexity was outlined. With these results, three central questions and problems where identified:

- How is it possible, to get a target market and function orientated ASIL? This means, that the ASIL result is not allowed to be either too high or too low. In addition, the fundamentals for the determination of the ASIL must be comprehensible and well documented to be taken into account in case of a product liability lawsuit.
- How is it possible to analyze interfaces between different systems to identify malfunctions caused by interface interferences and failures as well as faulty implemented communication specifications during a distributed/shared development (over various locations and companies)?
- How is it possible to implement a continuous process for handling product requirements from the definition, realization, risk analysis, validation (testing) and documentation of all activities (design, implementation and validation)?

In chapter 2, the state of the art was considered, focusing on three above-named problems. Therefore, the available approaches and solutions were reviewed regarding their strengths and weaknesses. Based on the results of chapter 2, solution approaches were worked out in chapter 3. This resulted in three individual approaches, which were combined into one single integrated IT method respectively a web application. Using this client-server-architecture it is possible to realize a real distributed, continuous as well as operating system and device independent development of functional safe products. Only a network access (intra-/internet) and a web browser are required.

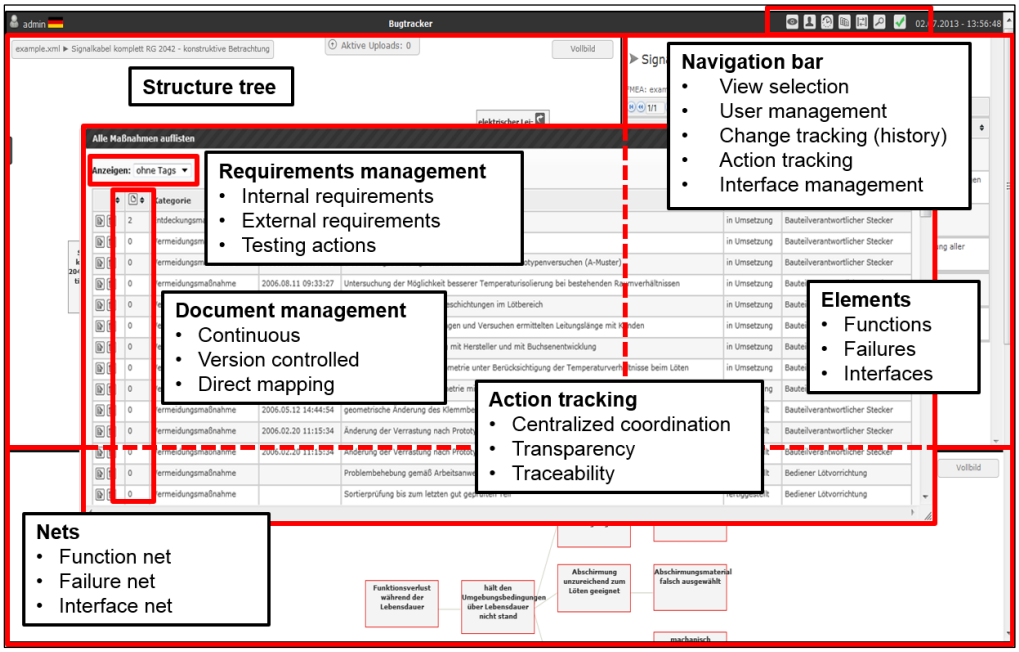


Abbildung 52 – webFMEA – Functional overview

The web application itself builds up on data coming from a hazard analysis and risk assessment. This data was transformed into a new data format. Using this transformation process, it is possible to add new object information and attributes to the existing FMEA data. With this additional information, an automated data and document processing as well as the handling (user interface), the access restrictions (right management) and the advanced analysis of interfaces between different parts of a system where included. On top of that, different other systems were included into the client-server-architecture. At the end, an integrated, continuous method for developing functional safe products was created.

To handle target market based ASIL classification, a statistics based approach was developed and implemented. This approach builds upon two facts. One fact, which was taken into account, is that the human constitution worldwide is identical or at least very comparable. This means, that the effects for humans, caused by an accident are independent of their location in the world. Consequently, the severity parameter can be considered as a constant and must be only defined once (for the considered driving situation). The same applies to the controllability of a failure caused situation. This parameter is also independent of its target market. At the end, there is only the exposure parameter left, which can influence the ASIL result. To get a valid result, a data base was built up, to allow for de-

tailed statements about driving situations in a country or region. Because of the fact, that the used statistical data are available for everybody, the results can be validated from others without being influenced. With this systematic argumentation, the results of the ASIL classification can be argued very well in case of product liability issues. Lastly, you are able to eliminate subjective feelings and experiences of the different involved persons or parties.

The complete approach as well as the integrated, continuous method based on the IT concept was validated with very good feedback. It supports the development process in different stages. The complete development activities, the arrangements between different development companies as well as the implementation and documentation were significantly improved. The simplified development process has led to a reduced development time and to a reduced number of development cycles, which positively influenced the need of resources.

During the validation process, some weak or negative points of the concept were discovered, which leaves some room for improvements in further works.

Besides some handling problems, especially with smart phones and tablets, which can be handled by developing dedicated apps for the different operation system platforms, there is a major gap in the requirement process. Currently there is no direct interface between the IT concept and requirement tools (like Doors).

At this place, the continuous traceability is broken. To check if every external requirement, specified by the customer (OEM or higher tier), is fulfilled, a manual comparison is required. This weakness offers an important link for future works.

In addition, the method must be examined for further optimization regarding its usability as well as method and software transparency to increase user acceptance. An IT based method can only offer functionality, but without acceptance by the human and its subsequent usage, no benefit and additional value can be generated. Therefore these aspects need to be examined in detail to improve the concept and its idea.

8 Literaturverzeichnis

[ADAC e. V. 2012] ADAC e. V., Infogramm - Die häufigsten Pannenursachen 2011. http://www.adac.de/sp/presse/Media/club/infogramm.aspx. (28.02.2013)

[Baumann, U. 2010] Baumann, Ulrich, 373.000 Avalon müssen in die Werkstätten - Toyota US-Rückruf - Lenkradschloss kann einrasten. 2010. http://www.auto-motor-und-sport.de/news/toyota-us-rueckruf-lenkradschloss-kann-einrasten-373-000-avalon-muessen-in-die-werkstaetten-1949318.html (28.02.2013)

[Bertsche, B.; Lechner, G. 2004] Bertsche, Bernd; Lechner, Gisbert, Zuverlässigkeit in Maschinenbau und Fahrzeugtechnik - Ermittlung von Bauteil- und System-Zuverlässigkeiten. 3. Aufl. Berlin: Springer, 2004

[Bibliographisches Institut GmbH 2013] Bibliographisches Institut GmbH, Sicherheit, die. http://www.duden.de/node/673347/revisions/1083449/view. 2013

[Börcsök, J. 2011] Börcsök, Josef, Funktionale Sicherheit - Grundzüge sicherheitstechnischer Systeme. 3. Aufl. Berlin: VDE Verlag, 2011

[CelsiusPro 2013] CelsiusPro, Oslo - Blindern - Periode: 1988-2008. http://www.celsiuspro.com/celsiusproapp/weatherStatistics.aspx?station_id=29. (28.02.2013)

[Chrissis, M. Beth; Konrad, M., et al. 2009] Chrissis, Mary Beth; Konrad, Mike; Shrum, Sandy, CMMI - Richtlinien für Prozess-Integration und Produkt-Verbesserung. 1. Aufl. München: Addison-Wesley, 2009

[Czichos, H. 2008] Czichos, Horst, Mechatronik - Grundlagen und Anwendungen technischer Systeme. 2., aktualisierte und erweitere Auflage. Wiesbaden: Vieweg + Teubner, 2008

[DGQ 2008] DGQ, FMEA - Fehlermöglichkeits- und Einflussanalyse - DGQ-Band 13-11. 4. Aufl. Berlin, Wien, Zürich: Beuth, 2008

[DIN 1076:1999-11] DIN 1076:1999-11: Ingenieurbauwerke im Zuge von Straßen und Wegen - Überwachung und Prüfung

[DIN EN 45020 2007-03] DIN EN 45020 2007-03: Normung und damit zusammenhängende Tätigkeiten - Allgemeine Begriffe (ISO/IEC Guide 2:2004)

[DIN EN 61508-5 2001-12] DIN EN 61508-5 2001-12: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/ programmierbarer elektronischer Systeme - Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level)

[DKE 2002] DKE, Funktionale Sicherheit speicherprogrammierbarer Steuerungen - IEC 61508 übernommen als DIN EN 61508 (VDE 0803). 2002. http://www.dke.de/de/DKE-Arbeit/Mitteilungen-

zurNormungsarbeit/2004/Seiten/Funktionale%20Sicherheit%20speicherprogrammierbarer%20Steuerungen.aspx. (28.02.2013)

[Dold, A. 2008] Dold, Axel: Implementation of Requirements From ISO 26262 in the Development of E/E Components and Systems – Challenges & Approach. Automotive Electronics and Electrical Systems Forum 2008, Stuttgart, 2008.

[Enger-Wiechers, E. 2008] Enger-Wiechers, Elke, FMEA sichert die Entwicklung ab. In: Der F&E Manager, (2008) Nr. 3, S. 16–19

[Europäisches Patentamt 2010] Europäisches Patentamt, Europäisches Patentübereinkommen - Übereinkommen über die Erteilung europäischer Patente (Europäisches Patentübereinkommen). 14. Aufl. München, 2010

[Eveleth, P. B.; Tanner, J. M. 1976] Eveleth, Phyllis B.; Tanner, J. M., Worldwide variation in human growth. Cambridge [Eng.], New York: Cambridge University Press, 1976

[Focus Medialine 2008] Focus Medialine (Hrsg.): Der Markt der Mobilität - Daten, Fakten, Trends. München: Focus Magazin Verlag, August 2008

[Frost & Sullivan 2003] Frost & Sullivan, The European Market for Mechatronics in Passenger Cars - B237-18. http://www.frost.com/prod/servlet/report-brochure.pag?id=B237-01-00-00-00

[Hoberg, F. 2010] Hoberg, Fabian, Renault ruft fast 700.000 Scénic in die Werkstatt - Rückruf. 2010. http://www.welt.de/motor/article8224499/Renault-ruft-fast-700-000-Scenic-in-die-Werkstatt.html. 28.02.2013)

[ISO 26262-1 2011-11-15] ISO 26262-1 2011-11-15: Road vehicles — Functional safety - Part 1: Vocabulary

[ISO 26262-2 2011-11-15] ISO 26262-2 2011-11-15: Road vehicles — Functional safety - Part 2: Management of functional safety

[ISO 26262-3 2011-11-15] ISO 26262-3 2011-11-15: Road vehicles — Functional safety - Part 3: Concept phase

[ISO 26262-5 2011-11-15] ISO 26262-5 2011-11-15: Road vehicles — Functional safety - Part 5: Product development at the hardware level

[ISO 26262-8 2011-11-15] ISO 26262-8 2011-11-15: Road vehicles — Functional safety - Part 8: Supporting processes

[Kamata, M. I.; Tamai, T. 2007] Kamata, Mayumi Itakura; Tamai, Tetsuo: How Does Requirements Quality Relate to Project Success or Failure? In: 15th IEEE International Requirements Engineering Conference. Los Alamitos, Calif: IEEE Computer Society, 2007, S. 69–87

[Kleinjung, T. 2012] Kleinjung, Tilmann, Italien: Kolosseum das erste Mal seit 27 Jahren in schneeweiß - Wunder und Chaos in Italien. 2012. http://www.tagesschau.de/ausland/italienwinter100.html. (20.10.2012)

[Kreiner, P. 2012] Kreiner, Paul, Die Römer hat es kalt erwischt - Winter in Europa. 2012. http://www.tagesspiegel.de/weltspiegel/winter-in-europa-die-roemer-hat-es-kalt-erwischt/6160844.html. (28.02.2013)

[Kriso, S. 2011] Kriso, Stefan: Nach der ISO 26262-Veröffentlichung: Offene Punkte und mögliche Lösungsansätze. In: 2. Osnabrücker Forum Funktionale Sicherheit - Erfahrungen in der Praxis, offene Punkte und Lösungen, 29.-30. November 2011, Osnabrück, 2011

[Lechner, G.; Naunheimer, H., et al. 2007] Lechner, Gisbert; Naunheimer, Harald; Bernd, Bertsche, Fahrzeuggetriebe - Grundlagen, Auswahl, Auslegung und Konstruktion. 2. Aufl. Berlin; Heidelberg: Springer, 2007

[Lischka, K.; Matthias, K. 2011] Lischka, Konrad; Matthias, Kremp, Risiko für Industrieanlagen - Neuer Stuxnet-Virus erschreckt Sicherheitsprofis. 2011 http://www.spiegel.de/netzwelt/web/0,1518,792640,00.html. (14.03.2013)

[Löw, P.; Pabst, R., et al. 2010] Löw, Peter; Pabst, Roland; Petry, Erwin, Funktionale Sicherheit in der Praxis - Anwendung von DIN EN 61508 und ISO/DIS 26262 bei der Entwicklung von Serienprodukten. 1. Aufl. Heidelberg: dpunkt-Verl, 2010

[Maier, C.; Schloske, A., et al. 2013] Maier, Christoph; Schloske, Alexander; Steffen, Bothe, Studie zur Funktionalen Sicherheit in der Automobilbranche (ISO 26262). 2013. http://www.ipa.fraun hofer.de/fileadmin/www.ipa.fhg.de/Publikationen/ Marktstudie ISO26262.pdf

[Off, S. 2009] Off, Sven, Element Attribute Documentation - MSRFMEA V2.2.0 (multi language). Stuttgart: Robert Bosch GmbH, 2009

[OLG Jena 2009] OLG Jena: Zur Haftung eines Fahrzeugherstellers für die Fehlauslösung von Airbags. VI ZR 107/08, 16.06.2009, S. 1–20. http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=Aktuell&Sort=12288&nr=48599&pos=20&anz=565&Blank=1.pdf

[Oxford University Press 2010] Oxford University Press, security. http://oxforddictionaries.com/definition/english/security. (07.03.2013)

[Özkan, T.; Lajunen, T., et al. 2006] Özkan, Türker; Lajunen, Timo; Chliaoutakis, Joannes El.; Parker, Dianne; Heikki, Summala, Cross-cultural differences in driving behaviours: A comparison of six countries. 2006. http://cyrus.tcdn.teicrete.gr/LinkClick.aspx?fileticket=hxndIaS6vts%3D&tabid=1089

[Pander, J. 2012] Pander, Jürgen, Der erste Serieneinsatz - Die große Reifeprüfung für den MQB - Wer liefert was? AUDI A3. In: Automobilwoche, (2012) Nr. 11, S. 17

[Partsch, H. 2010] Partsch, Helmuth, Requirements-Engineering systematisch - Modellbildung für softwaregestützte Systeme. 2. Aufl. Berlin, Heidelberg: Springer, 2010

[Pohl, K.; Rupp, C. 2009] Pohl, Klaus; Rupp, Chris, Basiswissen requirements engineering - Aus- und Weiterbildung zum Certified Professional for Requirements Engineering; Foundation-Level nach IREB-Standard. 1. Aufl. Heidelberg: Dpunkt-Verl., 2009

[ProdHaftG 1989] Bundesministerium der Justiz: Gesetz über die Haftung für fehlerhafte Produkte (Produkthaftungsgesetz - ProdHaftG), 15.12.1989, Fassung: Art. 9 Abs. 3 G vom 19. Juli 2002 (BGBl. I S. 2674, 2678 f.)

[Reif, K. 2011] Reif, Konrad (Hrsg.), Bosch-Autoelektrik und -Autoelektronik - Bordnetze, Sensoren und elektronische Systeme; mit 43 Tabellen. 6. Aufl. Wiesbaden: Vieweg + Teubner, 2011

[Richter, H. 2009] Richter, Harald: Elektronik und Datenkommunikation im Automobil, Clausthal, TU Clausthal, 2009, (IfI Technical Report Series IfI-09-05)

[Rieger, F. 2010] Rieger, Frank, Der digitale Erstschlag ist erfolgt - Trojaner „stuxnet“. 2010. http://www.faz.net/aktuell/feuilleton/debatten/digitales-denken/trojaner-stuxnet-der-digitale-erstschlag-ist-erfolgt-1578889.html. (28.02.2013)

[Schloske, A. 2011a] Schloske, Alexander: Studie zur Risikobewertung in der FMEA. In: 6. Osnabrücker FMEA Forum 2011, 29.-30. März 2011, Osnabrück, 2011

[Schloske, A. 2011b] Schloske, Alexander, Funktionale Sicherheit nach ISO/DIS 26262. Karlsruhe, 07. Februar 2011. http://www.qm-karlsruhe.de/programm/files/public/1292764246/DGQ_KA_Vortrag_-Schloske_beim_DGQRegionalkreis_20110207.pdf

[Schloske, A. 2012] Schloske, Alexander: Erfahrungsbericht aus einem FuSi-Projekt nach DIN EN 61508 im automotive Umfeld - Neue Herausforderungen – Erfolg versprechende Lösungsansätze. In: ISO 26262 - FUNKTIONALE SICHERHEIT - Neue Herausforderungen – Erfolg versprechende Lösungsansätze, 03.-04. Juli 2012, Stuttgart, 2012

[Schlummer, M. H. 2012] Schlummer, Marco Heinz, Beitrag zur Entwicklung einer alternativen Vorgehensweise für eine Proven-in-Use-Argumentation in der Automobilindustrie. 2012. http://nbn-resolving.de/urn/resolver.pl?urn=urn%3Anbn%3Ade%3Ahbz%3A468-20120405-124552-2

[Schmidt, M.; Rau, M., et al. 2011] Schmidt, Martin; Rau, Marcus; Helmig, Ekkehard; Bauer, Bernhard, Funktionale Sicherheit – Umgang mit Unabhängigkeit, rechtlichen Rahmenbedingungen und Haftungsfragen. 2011. http://www.sgs-tuev-saar.com/pdf/Fachartikel-ISO-26262-Jura-08-2011.pdf

[Shahid, M.; Ibrahim, S., et al. 2011] Shahid, Muhammad; Ibrahim, Suhaimi; Mahrin, Mohd Naz'ri, An Evaluation of Requirements Management and Traceability Tools. http://www.waset.org/journals/waset/v54/v54-117.pdf

[Siebenlist, J. 2004] Siebenlist, Jürgen, Bis 2015 steigt der Zulieferer-Anteil am Auto auf 80 % Produktion - Fraunhofer-Institute erwarten nur bei der Elektronik ein verstärktes OEM-Engagement. In: VDI Nachrichten 2004, 19.03.2004

[Spath, D. 2013] Spath, Dieter, Vorlesung: Grundzüge der Produktentwicklung I - Sicherheit. Universität Stuttgart - Institut für Arbeitswissenschaft und Technologiemanagement IAT. 2013

[Ständer, T. 2012] Ständer, Tobias: Systematische Ermittlung von Expositionszuständen - Ganzheitlicher Entwurf sicherheitsrelevanter Fahrzeugsysteme. In: TÜV SÜD (Hrsg.): safe.tech 2012 - Automobiltechnik, Bahntechnik und Automatisierung auf neuen Wegen, 13.-14. März 2012, München. München, 2012

[T-Systems Enterprise Services GmbH 2009] T-Systems Enterprise Services GmbH, Vernetzte Wertschöpfung. - Die Automobilbranche im

Wandel – von der produzierenden zur Dienstleistungsindustrie. 2009. http://www.automotiveit.eu/wp-content/uploads/2009/08/WhitePaper_Vernetzte-Wertschoepfung-ps.pdf

[VDI 3780 2000-09] VDI 3780 2000-09: Technikbewertung Begriffe und Grundlagen

[Verband der Automobilindustrie e. V. 1996] Verband der Automobilindustrie e. V., Qualitätsmanagement in der Automobilindustrie - Sicherung der Qualität vor Serieneinsatz. 1. Aufl. Frankfurt/Main: Verband der Automobilindustrie e. V., März 1996

[Verband der Automobilindustrie e. V. 2010a] Verband der Automobilindustrie e. V., Produktentstehung - Prozessbeschreibung Besondere Merkmale (BM). 1. Aufl. Berlin: Verband der Automobilindustrie e. V., 2010

[Verband der Automobilindustrie e. V. 2010b] Verband der Automobilindustrie e. V., Automotive SPICE Prozessassessmentmodell - Prozessbewertung gemäß Automotive SPICE in der Entwicklung von softwarebestimmten Systemen. 1. Aufl. Berlin: Verband der Automobilindustrie e. V., August 2010

[Weingartner, M. 2012] Weingartner, Maximilian, Das Automobil wird neu erfunden - Der Bordcomputer übernimmt die Macht im Cockpit: Er gibt Gas, bremst und überholt von ganz allein. In: Frankfurter Allgemeine Sonntagszeitung, 08.01.2012, (2012) Nr. 1, S. 27

[Westkämper, E. 2006] Westkämper, Engelbert, Einführung in die Organisation der Produktion. 1. Aufl. Berlin: Springer, 2006

[Westkämper, E.; Verl, A. 2008] Westkämper, Engelbert; Verl, Alexander, Sichere und zuverlässige mechatronische Produkte - Neue Herausforderungen - Erfolg versprechende Lösungsansätze: FpF - Verein zur Förderung produktionstechnischer Forschung, Stuttgart, 2008

[Wikimedia 2013] Wikimedia, security. http://en.wiktionary.org/wiki/security. (14.03.2013)

[Winner, H.; Hakuli, S., et al. 2009] Winner, Hermann; Hakuli, Stephan; Wolf, Gabriele, Handbuch Fahrerassistenzsysteme - Grundlagen, Komponenten und Systeme für aktive Sicherheit und Komfort. 1. Aufl. Wiesbaden: Vieweg+Teubner Verlag, 2009

[World Health Organization 2011] World Health Organization, Mobile Phone use - A growing problem of driver distraction, 2011

Die neuen Anforderungen und Erwartungen der Kunden sowie der Norm ISO 26262 setzen die in der Automobil-Branche produzierenden Unternehmen verstärkt unter Druck, schnell und flexibel innovative und zugleich funktional sichere Produkte zu entwickeln. Dabei fordert die Norm die Erkennung von zufälligen elektrischen und elektronischen Fehlern und den anschließenden Übergang in einen sicheren Zustand. Ziel ist es, die Gefährdung der Insassen und anderer Verkehrsteilnehmer durch technische Fehler auf ein Minimum zu reduzieren. Die erarbeitete Methodik greift deshalb drei Grundprobleme bei der Entwicklung mechatronischer Produkte im Kontext der ISO 26262 auf. Diese sind die zielmarktorientierte Festlegung des ASIL, das lieferantenübergreifende Handling von Schnittstellen sowie die durchgängige Umsetzung und Dokumentation von Requirements. Hierzu werden in der Arbeit die Einflussfaktoren auf das ASIL untersucht und in der Folge eine zielmarktabhängige Definition der Faktoren ermöglicht. Für die anderen oben genannten Probleme wurde ein integrierter IT-Ansatz basierend auf der Fehlermöglichkeits- und Einflussanalyse erarbeitet und implementiert.

ISBN 978-3-8396-0644-5

9 783839 606445

FRAUNHOFER VERLAG