HANSER

Leseprobe

zu

„Funktionale Sicherheit im Automobil“

von Hans-Leo Ross

Print-ISBN: 978-3-446-45841-3
E-Book-ISBN: 978-3-446-45842-0

Weitere Informationen und Bestellungen unter
http://www.hanser-fachbuch.de/978-3-446-45841-3
sowie im Buchhandel

Vorwort

Wenn man das Vorwort der ersten Auflage meines Buches liest und diese Gedanken auf die zweite, vollständig überarbeitete Auflage überträgt, dann gibt es viele Punkte, die einen komplett neuen Inhalt erfahren, wenn man sie aus einem anderen Blickwinkel betrachtet.

Sprach ich im Vorwort der ersten Auflage noch von 20 Jahren Erfahrung im Bereich Funktionssicherheit, so sind es heute Aspekte aus über 35 Jahren Berufserfahrung. Dazu zählen auch Aspekte aus meiner Berufsausbildung als Fernmeldehandwerker – so hieß damals die Ausbildung bei der Deutschen Bundespost (nun Telekom), heute würde man wohl sagen: Ausbildung zum Kommunikationselektroniker –, die heute in einem neuen Licht erscheinen. Als ich mich 1992 als Diplom-Ingenieur ins Berufsleben stürzte, war der Anlagenbau von verschiedenen Katastrophen wie Bhopal und Seveso geprägt. Dass nun in der zweiten Auflage sogar die Seveso-III-Richtlinie erwähnt wird, zeigt, wie sich das Thema Sicherheit über viele Jahre verändert hat. In der ersten Auflage verwies ich auf die VDI/VDE-Richtlinie 2180 „Sicherung von Anlagen der Verfahrenstechnik“ aus dem Jahr 1966, meinem Geburtsjahr. Durch die Elektromobilität muss man auch auf die VDE 100 eingehen, die ihren Ursprung laut VDE im Jahre 1895 hat. Sie handelte damals nicht nur von elektrischen Verbrauchern, sondern auch von Transformatoren, Kabeln/Schienen sowie dem Einsatz von Messtechnik. Im Jahr 1984 wurde die VDE/VDE-Richtlinie 2180 erweitert. Der Begriff „Anlagensicherung mit Mitteln der Mess- und Regeltechnik“ wurde in der Norm eingebracht. Welche Aufgabe haben Sensoren in Fahrzeugregelsystemen wie Lenkung, Bremse und Antrieb? Dies wird heute für Radar, Lidar oder Kamerasysteme im Auto hinterfragt. Welche neuen Sicherheits- oder Schutzfunktionen braucht man für automatisierte Fahrfunktionen? Wie automatisierte man Funktionen, die bisher der Fahrer ausgeführt hat? Man machte einen Unterschied zwischen Betriebs- und Sicherungseinrichtungen sowie Überwachungs- und Schutzeinrichtungen. In der zweiten Auflage wird nun neben den Funktionssicherheitskonzepten auch auf Betriebssicherheits-, Fahrzeugsicherheits- und Datensicherheitskonzepte verwiesen. Das heißt, die alten Perspektiven werden auf neue Technik angewendet.

Die DIN VDE 31000 „Allgemeine Leitsätze für das sicherheitsgerichtete Gestalten technischer Erzeugnisse“ wird heute mit ganz neuen Augen betrachtet. Die Zusammenhänge zwischen Risiko, Sicherheit und Gefahr, die hier beschrieben wurden, müssen nun auf das automatisierte Fahren abgebildet werden. Die Frage nach dem Grenzrisiko, die in der Norm eingeführt wurde, wird ganz neu gestellt. Zu dieser Zeit waren noch Maschinenstandards gültig, die die Nutzung von Mikrocontrollern für Sicherheitsaufgaben verboten haben. Es gab jedoch bereits einen akzeptierten Markt für Sicherheitssteuerungen. Verschiedene Normen und Standards definierten die Grundlage für Prüfung, Zertifizierung und Auslegung dieser Sicherheitssteuerungen. Sie wurden in Anforderungsklassen (AK 1–8) gemäß der DIN V 19250 klassifiziert. Diese Norm war anwendungs- und technologieunabhängig und beschrieb anhand eines Risikographen ein qualitatives Verfahren zur Risikoabschätzung. Die Beschäftigung mit Risiken, Prüfung und Zertifizierung sind neue Themen, die heute aktuell auch auf die Fahrzeugtechnik abgebildet werden müssen. 1990 erschien die DIN V VDE 0801 „Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben“. In der Revision von 1994 wurden Begriffe wie „betriebsbewährt“ und der Einsatz einer „Betrachtungseinheit“ eingeführt. Als Antwort auf die unterschiedlichen Risiko- oder Anforderungsklassen kannte man aber weitgehend nur Redundanz. Scheinbar ist beim Einsatz von Mikroprozessoren und Multi- bzw. Many-Core-Konzepten Redundanz heutzutage die einzige Möglichkeit, solche hochkomplexen Daten- und rechenintensive Systeme noch beherrschen zu können. Selbst der Mensch mit seinen zwei Gehirnhälften setzt auf Redundanz, um sich zu vergewissern, ob er Situationen richtig erfasst. Scheinbar erfasst die eine Gehirnhälfte mehr den Kontext und die andere fokussiert sich auf das Erfassen von konkreten Informationen wie zum Beispiel der Schrift. Bei Zwillingen kann man oft feststellen, dass der oder die eine besser in der Kontexterfassung ist und der oder die andere besser beim Erfassen der beabsichtigten Information. Wer ist die oder der Intelligentere? Oder ist es so, dass die Güte zwischen den beiden Gehirnhälften die wahre Intelligenz ausmacht? Wahrscheinlich wird der eine Zwilling bei jedem Intelligenztest die besseren Ergebnisse haben, der andere wird wohl den höheren EQ haben. Welche Fähigkeit wird bei welchem Test tatsächlich gemessen? Ist dies auch eine Antwort auf die Ideen zur künstlichen Intelligenz? In der Mess- und Regelungstechnik wurden jedoch auch schon diversitäre Messprinzipien genutzt, um Gefahrenszenarien frühzeitig zu entdecken. Heutzutage hat man die Erfahrung gemacht, dass es ein perfektes Messsystem zur Erfassung der Verkehrsumgebung nicht geben kann. Wahrscheinlich wird man auch auf intelligente Sensorfusionen basierende, diversitäre Sensorik und verschiedene logische Algorithmen setzen müssen. Die technischen Regeln für Dampf oder Richtlinien für Druckbehälter schrieben schon die redundante Messung von Druck und Temperatur aus Sicherheitsgründen vor. Selbst das Wasserhaushaltsgesetz kannte die Begrenzung der Füllmenge von Behältern durch Vorschrift oder Regelung sowie die unabhängige

Überfüllsicherung als Sicherheitsmaßnahme. Viele dieser Sicherheitsprinzipien waren in den Sicherheitsstandards der Anlagenbetreiber entstanden und dienten sogar als Grundlage für behördliche Genehmigungen. An all diese Prinzipien müssen wir uns nun bei den Themen Wasserstoff im Fahrzeug oder der Brennstoffzelle zurückerinnern. Als ich 1998 mit dem Vertrieb von Sicherheitssteuerungen begann, wurden besonders in England, den Niederlanden und Norwegen die Entwürfe der IEC 61508 diskutiert. Man kannte die skalierbare Redundanz und es wurde zwischen Redundanz für Sicherheit und Verfügbarkeit unterschieden. Mikrocontroller wurden auch im Lockstep-Prinzip gekoppelt und konnten im laufenden Betrieb der Anlage den Programmablauf oder die Steuerungslogik ändern. Es waren Programmierprogramme verfügbar, die die Sicherheitslogik zwischen einer definierten Laufzeitumgebung konfigurieren konnten. Leider hat man heute feststellen müssen, dass ein Lockstep absolut keine Lösung zur Beherrschung von systematischen Fehlern ist. Wer dies für Software-Fehler nutzen möchte, unterliegt wohl einem systematischen Irrtum.

Mit der Veröffentlichung der IEC 61508 wurde ein Lebenszyklusansatz für Sicherheitssysteme vorgestellt. Des Weiteren wurden die Prozessbetrachtung der Produktentwicklung und der Bezug zu den Qualitätsmanagementsystemen formuliert. Während meines Masterstudiums am Wirtschaftswissenschaftlichen Institut der Universität Basel durfte ich auch die Vorlesung von Professor Dr. Walter Masing genießen, der die Qualitätsmanagementsysteme in Deutschland sehr geprägt hat. Wo sind unsere standardisierten Prozesse für die automatisierten Fahrfunktionen? Wo sind diese für die neuen Antriebssysteme? Wer harmonisiert die Prozesse, um die Fahrzeuge in die neue Verkehrsumgebung systematisch einzubringen? Kann man mit Big-Data und Agilität dies alles ohne Prozesse umsetzen? Die IEC 61508 kannte die Unterscheidung zwischen der beabsichtigten Funktion und den notwendigen Sicherheitsintegritätsmaßnahmen, um eine Anlage oder Maschine absichern zu können. Das „Equipment under Control“, also die zu steuernde Anlage oder Maschine, stand im Fokus der Betrachtung. Ist nicht das automatisierte Fahrzeug im Verkehrsumfeld die zu sichernde Mobilitätsmaschine? Die Einführung der Diagnose zur Sicherung der Funktion bzw. der elektrischen Trägersysteme der Funktion erweiterte den Gedanken der Sicherheitsarchitektur. Heute ergänzen wir die Ideen aus der Medizin- und Flugzeugtechnik. Man setzt auf prädiktive Gesundheitsvorsorge für technische Systeme. Das heißt, man versucht Systemschwächen zu entdecken, bevor sie sich gefährlich auswirken können. 1998 durfte ich in Birmingham das erste passive elektronische System vorstellen, welches bis SIL 4 gemäß IEC 61508 zertifiziert war. Auf einer VDMA-Veranstaltung berichtete ich über die Erfahrung mit der IEC 61508 im Anlagenbau und deren Einfluss auf die Entwicklung von sicherheitsgerichteten Steuerungssystemen. Die ersten Erfahrungen mit Ethernet in der Sicherheitstechnik verwunderte doch viele. Die Maschinenbauindustrie war damals noch sehr stark von Relaistechnik geprägt. Dass die software-

basierende Sicherheitstechnik diese Branche so schnell mit neuen Lösungen und Systemen verändern würde, wollte damals kaum jemand glauben. 80 % der Kommunikation im Fahrzeug sind CAN-Busse, Ethernet existiert in den heutigen Systemen noch immer nicht als Netzwerk. Als ich 2001 die Leitung des Produktmanagements übernahm, galt es, neue Anwendungen für neue Sicherheitssysteme zu finden. Ein weiterer Themenschwerpunkt wurde die vernetzte Sicherheitstechnik, die bis dahin auf seriellen Datenbussen beruhte. Jetzt mussten verteilte und dezentrale Sicherheit sowie dynamische, situations- oder zustandsabhängige Sicherheitssysteme realisiert werden. Als Lösung kam nur noch Ethernet in Frage. Wichtig war hier, die vorhandene Datentechnik für die Sicherheitstechnik handhabbar zu machen. Im Rahmen von Diplomarbeiten wurden Sicherheitssteuerungen in ganz Norwegen verteilt, die auf dem Datennetz der norwegischen Mineralölgesellschaft Statoil sicherheitsrelevante Daten austauschten. Die Erfahrungen mit Datenübertragung über Satelliten zwischen Ölplattformen und Landanlagen oder zwischen Norwegen und Deutschland sowie verschiedenen Lösungen zur Pipelineüberwachung über Funksysteme zeigten, dass sicherheitstechnische Datensysteme auch auf Basis von Ethernet realisierbar sind.

Durch die Veröffentlichung der IEC 61508 als DIN EN 61508 (VDE 0803) „Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme“ im Jahre 2001 wurde die deutsche Automobilindustrie auf das Thema aufmerksam. Öffentlicher Schriftverkehr zwischen dem VDA und den VDTÜVs führte zur Gründung des AK16 im FAKRA (Facharbeitskreis Automobil). Durch meinen Wechsel zu Continental Teves wurde ich 2004 Mitglied in diesem Arbeitskreis. Noch im selben Jahr wurden die ersten Strukturen für die spätere ISO 26262 entworfen und man nahm Kontakt zu weiteren Automobilnormungsgremien in anderen Ländern auf. Insbesondere mit Frankreich wurden konkrete Rahmenbedingungen für die Norm ausgearbeitet. Die erste Sitzung der ISO/TC22/SC03/WG16 fand vom 31.10. bis 2.11.2005 in Berlin statt. Die Arbeitsgruppen aus Frankreich und Deutschland bildeten die größten Fraktionen neben anderen Ländervertretungen aus Japan, USA, Schweden, Großbritannien usw. Bis zu diesem Zeitpunkt kursierte die ISO 26262 unter dem Namen „FAKRA-Norm“. Die safetronic 2005 adressierte bereits die ersten Ideen der zukünftigen Automobilnorm und es wurden Vorträge zu „Best Practices“ und Methoden präsentiert. So konnte ich mit einem Kollegen die neuen Ideen der Sicherheitstechnik zeigen, beispielsweise wie eine Hinterachslenkung die Fahrdynamik erhöhen oder eine Steer-by-Wire-Lösung den Fahrkomfort verbessern kann. Richtige Steer-by-Wire-Systeme sind bisher in keinem Großserienfahrzeug eingesetzt. Für zukünftige automatisierte Fahrfunktionen werden by-Wire-Systeme unumgänglich sein. Woher nehmen wir die Erfahrung, wie solche Systeme in der Verkehrsumgebung und auf den Fahrer einwirken?

Es zeigt sich, dass viele Errungenschaften aus der Ingenieurwissenschaften immer wieder neu erfunden werden müssen, weil sich der Kontext ändert, früher sagte

man, weil sich die Zeiten ändern. Wir müssen uns wohl an die alten Philosophen zurückerinnern, die durch Beobachten der Natur bestimmte Zusammenhänge erklären wollten. Durch Induktion wollte man vom Speziellen auf das Allgemeine schließen. Es sieht so aus, dass wir wieder mehr beobachten müssen und das Gesehene in dem wahrgenommenen Kontext beschreiben. Die Metaphysis hat so ihre Hypothesen erstellt.

Viele dieser Aspekte haben gezeigt, dass die ISO 26262 ein wirklich sehr umfangreiches Rahmenwerk ist, doch für die neuen Mobilitätssysteme werden wir alle Risiken betrachten müssen. Dabei müssen wir auch auf das Sicherheitsbedürfnis der Gesellschaft achten und werden die neue Technik aus sehr vielen Perspektiven betrachten müssen. Gesetze wie auch Systeme können nur im beabsichtigten Zielkontext betrachtet und bewertet werden, daher müssen wir lernen, wie sich der Kontext auf die Systeme auswirkt. Ohne eine hinreichende Kontextbetrachtung wird eine Sicherheitsargumentation immer unvollständig sein und weitere Risiken für Leib und Leben in sich bergen.

Dankwort des Autors

Die Erfahrung, die ich in all den Projekten gesammelt habe, die Diskussionen mit den Experten, den Kollegen, in den Arbeitskreisen, mit Hochschulen und bei Vorträgen sowie die Erkenntnisse aus Diplomarbeiten und Förderprojekten haben zu diesem Buch beigetragen. All den beteiligten Menschen möchte ich für die Leidenschaft danken, mit der sie das Thema Mobilität und Sicherheit mit mir betrachtet haben. Neben all den Experten gilt der besondere Dank meiner Familie. Meiner Frau, weil sie geduldig meine Arbeiten begleitet hat und auch meinen Kindern, die zu vielen Zeitpunkten lieber mit mir gespielt hätten. Ich habe es aber auch sehr genossen, mit meiner Tochter auf dem Schoß die lustigen Bilder in diesem Buch anzuschauen. Meine Familie brachte viel Verständnis auf und gab mir den Freiraum, dieses Buch zu schreiben.

Inhalt

Der Autor

Hans-Leo Ross ist seit 2019 bei der Robert Bosch GmbH für Fahrzeugsicherheit verantwortlich. Von 2015 bis 2018 war er bei der Bosch Engineering GmbH unter anderem für die Sicherheitsaktivitäten in Fahrzeug- und Luftfahrtprojekten verantwortlich. Dabei entwickelte er auch erste Sicherheitskonzepte für hochautomatisierte Fahrfunktionen. Von 2014 bis 2015 war er bei der Mando Europe verantwortlich für den Infrastrukturaufbau der europäischen Entwicklungsaktivitäten. Dabei wurden in seinem Bereich auch die Basis-Software für zukünftige ESP-Systeme sowie die ersten Kundenprojekte für elektronische Parkbremsen nach Sicherheitsstandards aktueller Normen und gemäß dem Autosar-Standard entwickelt. Davor war der Autor 10 Jahre bei Continental für die Einführung der Funktionalen Sicherheit verantwortlich und koordinierte alle geschäftsbereichsübergreifenden Sicherheitsaktivitäten. Während dieser Zeit leitete er unter anderem die deutsche Arbeitsgruppe zur ISO 26262 im VDA und vertrat die Interessen vor internationalen Gremien. Zeitweise leitet er auch die Abteilung für Entwicklungsprozesse, Methoden und Tools in den Continental Automotive-Bereichen. Für die Preussag-Noell-LGA Gastechnik plante und realisierte er sicherheitsrelevante Anlagen und Systeme für die Öl- und Gasindustrie. In der Firma HIMA war er zuerst für den Vertrieb von sicherheitsrelevanten Steuerungen in UK sowie Nord- und Osteuropa zuständig, bevor er die Leitung des Produktmanagements übernahm.

Hans-Leo Ross absolvierte sein Ingenieurstudium an der Uni-GH-Paderborn im Fachbereich Elektrotechnik mit dem Schwerpunkt Nachrichtentechnik. Einen Master of Advanced Studies mit Schwerpunkt Betriebswirtschaft und Marketing schloss er berufsbegleitend an der Uni Basel ab.

■ 7.3 Schutzebenen und Barrieren

Wie bereits vorher beschrieben, können Fehler und funktionale Effekte in beliebiger Form zu Störfällen und Unfällen führen. Die Effekte und Fehler können in horizontaler Ebene (zum Beispiel vom Sensor über die Verarbeitung hin zum Aktuator) propagieren, oder vertikal vom physikalischen Effekt zum Beispiel in der Elektronikhardware hin zu einem Störfall oder Unfall. Daher ist es notwendig, Schutzebenen oder Barrieren einzuplanen.

7.3.1 Fehler- und Risiko-Pyramide

Bei automatisierten Fahrfunktionen, die man in dem Kontext der jeweiligen Verkehrssituation betrachten muss, wird schnell transparent, dass eine Fehlerpyramide sehr viele Ebenen hat.

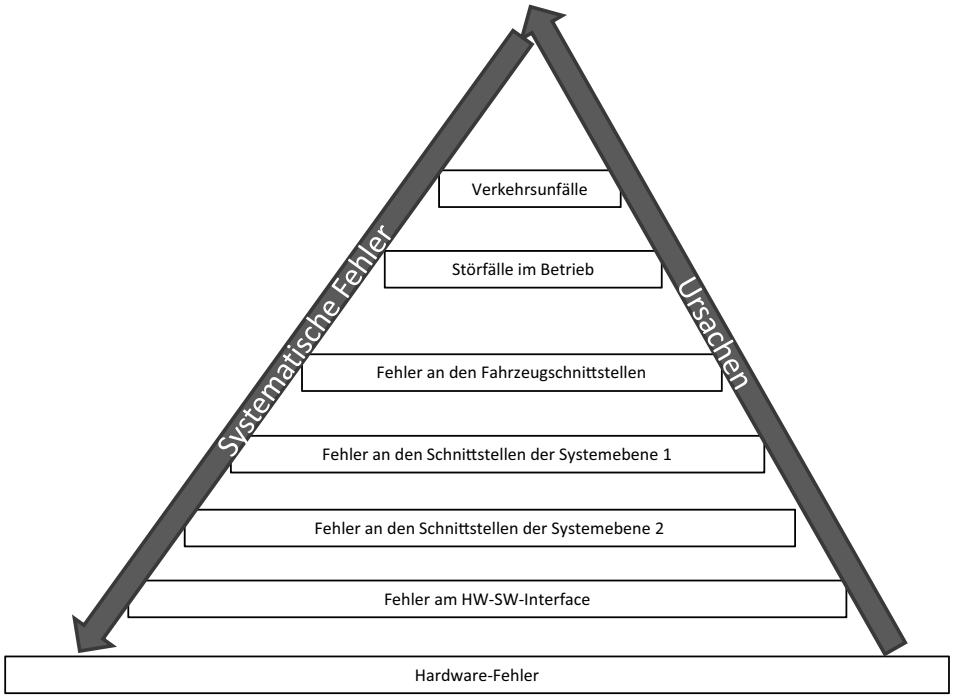

Bild 7.28 Fehler- und Risikopyramide

Die systematischen Fehler (nicht nur die gemäß ISO 26262), wie Spezifikationsfehler, falsche Einschätzungen von Situationen, Irrtümer, nicht geeignete Komponenten oder Algorithmen und Abhängigkeiten, vererben sich bis in die Hardware-Design-Entscheidungen beziehungsweise die physikalische Ebene hinunter. Defekte und die Auswirkungen von Designfehlern gehen von der physikalischen Ebene

über alle Fehler an den Schnittstellen nach oben, bis es zu Unfällen im Verkehr kommt. Eine solche Pyramide kann nicht wirklich von Menschen, auch mit allen technischen Hilfsmitteln, über Ursache-Wirkungs-Analysen analysiert werden.

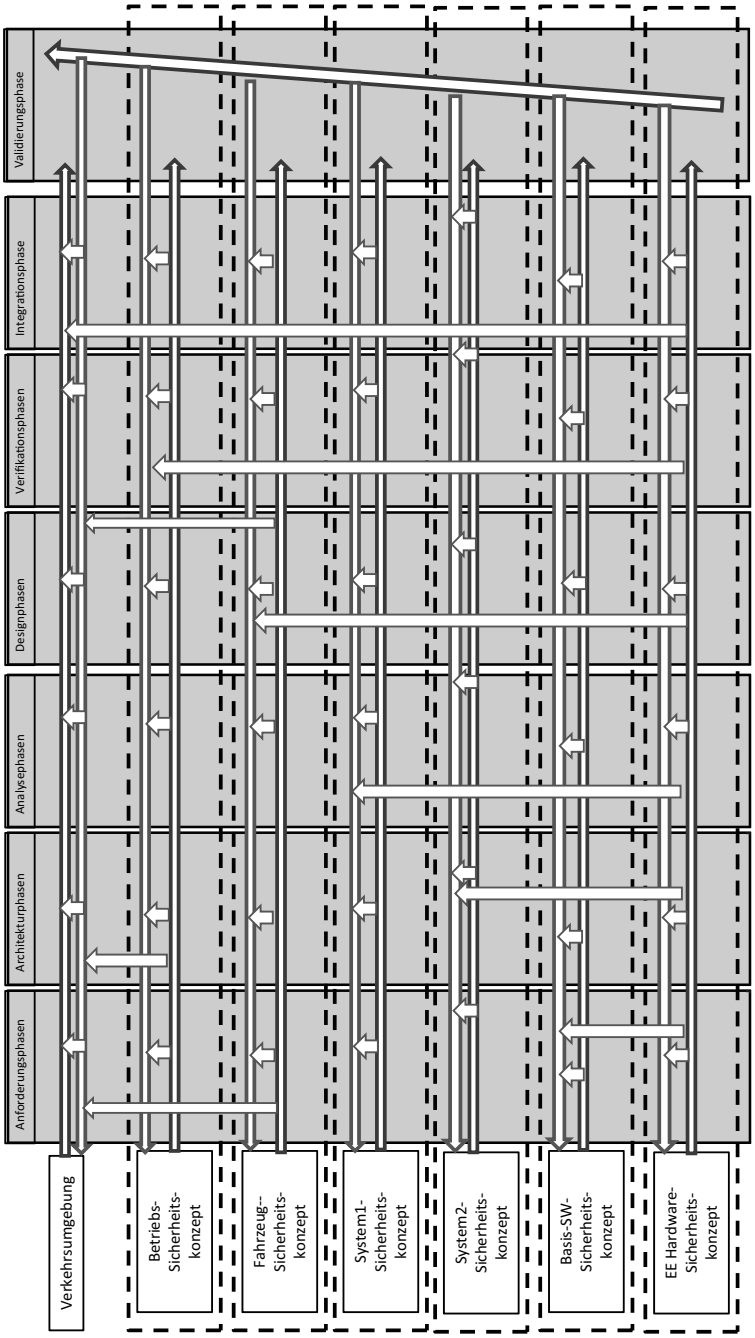

Bild 7.29 Ebenen der horizontalen Systemabsicherung

Grundsätzlich muss von den Maßnahmen in den verschiedenen Ebenen, ausgehend von Maßnahmen in der Verkehrsumgebung bis zu Maßnahmen auf der unteren physikalischen Ebene (z. B. EE-Hardware), derselbe grundsätzliche Prozess abgearbeitet werden.

Der Prozess muss die üblichen Phasen betrachten:

- Anforderungsphase,
- Architekturphase,
- Analysephase,
- Designphase,
- Verifikationsphase,
- Integrationsphase,
- Validationsphase.

Die Phasen werden wie in jeder Entwicklung keiner eindeutigen Sequenz folgen, die Aktivitäten müssen aber in jeder dieser Ebenen durchgeführt werden.

Sämtliche Architektur- oder Designentscheidungen, logischen Zuordnungen, organisatorischen Schnittstellen sind rein willkürlich und entstammen den Rahmenbedingungen und Einschränkungen des Produktentstehungsprozesses.

- Funktionales Verhalten,
- Systemverhalten,
- zeitliche Abhängigkeiten,
- eingeschränkte Fähigkeiten von System, Komponenten und Algorithmen sowie
- Fehler, Fehlverhalten und Fehlerpropagationen

werden durch solche in der Entwicklung festgelegten Schnittstellen nicht beeinflusst.

Einen solchen Zusammenhang hat Reason 1990 bereits mit seinem Schweizer-Käse-Modell beschrieben.

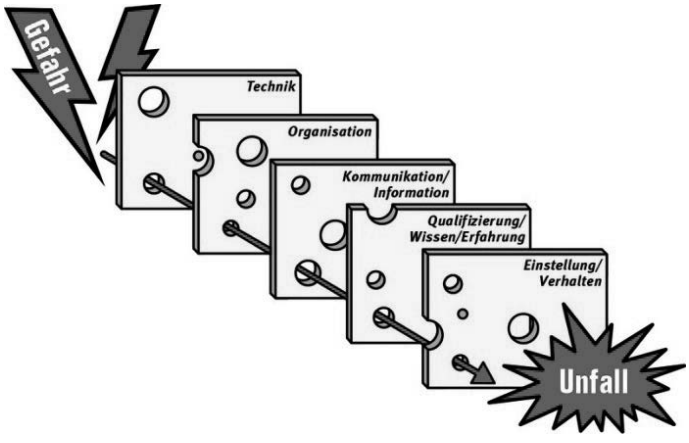

Bild 7.30 Schweizer-Käse-Modell (Quelle: Reason 1990)

Die Kette zeigt Fehler an den Organisationsschnittstellen auf. Die Kette hier verdeutlicht, dass latente Fehler (Fehler, die im Produktdesign schlummern) über

- die Technik zur
- Organisation, weiter zu
- Fehlern in der Überwachung, zu
- Fehlverhalten des Systems oder Flugzeugs oder Fahrzeugs bis hin zu
- Unfällen führen.

Ähnliche Ketten sehen die Ursache

- in der Technik,
- der Organisation,
- der Kommunikation der Informationen (Spezifikation, Instruktionen etc.),
- der Qualifikation der Agierenden,
- dem Verhalten und der Einstellung der Protagonisten.

Protagonisten können Hersteller, Vertreiber, Händler, Anwender und auch Verkehrsteilnehmer als die Gefährdeten sein, aber auch als Ursachen für den Fall, dass durch ihr Verhalten andere gefährdet werden.

7.3.2 Diversität zur Risikoreduzierung

In einigen Veröffentlichungen zur ISO 26262 wurde das Schweizer-Käse-Modell auch für die ASIL-Dekomposition angewendet. Leider wurde in keiner der Veröffentlichungen darauf hingewiesen, dass es das Ergebnis einer Analyse und eine Architekturmaßnahme ist, die Käsescheiben so anzuordnen, dass zum Beispiel Fehler nicht durch alle Löcher durchpropagieren. Weiter hat man in anderen Branchen schon festgestellt, dass man nicht einfach Käsescheiben aus der französischen Schweiz und der italienischen Schweiz als diversitäre Käsesorten deklarieren und davon ausgehen kann, dass sich dadurch die Löcher an verschiedenen Stellen befinden. Dies gilt natürlich für jeden anderen löchrigen Käse genauso. Hier kommt man wieder schnell zu dem Schluss, dass ein diversitäres Systemdesign oder diversitäre Funktionen und Algorithmen überhaupt keinen generischen Vorteil für die Sicherheitstechnik haben. Homogene Redundanzen lassen sich sogar viel schneller synchronisieren und damit vergleichbar machen, damit man potentielle Quellen von latenten Fehlern vor der Fehlerauswirkung entdecken kann. Dies heißt nicht, dass man Objekterkennungen oder auch Zustandserkennungen auf verschiedenen logischen Prinzipien erstellen sollte.

Mikrocontroller und Mikroprozessoren arbeiten weitgehend auf demselben Prinzip, daher kann selbst die parallele Verwendung von Mikrocontrollern und Mikroprozessoren zu sehr vielen ähnlichen Verhaltensweisen führen, die eine Erkennung von systematischen Fehlern nicht erlauben werden. Eine parallele Verwendung von

Mikrocontrollern verschiedener Hersteller wird erst recht kein Ausschlusskriterium für systematische Fehler sein, weil nur Mutmaßungen existieren können, wo sich die Lücken im Design oder Ähnliches durch die redundante Verwendung finden.

Die Druckkesselverordnung (zum Beispiel Druckgeräterichtlinie 2014/68/EU) geht auf die Bierbrauer von Mannheim und Heilbronn zurück. Hier legte man vor mehr als 100 Jahren fest, dass die Temperatur, der Druck und der Flüssigkeitsstand zu messen sei. Die Abhängigkeit dieser Größen ist durch das Design des Druckkessels gegeben. Wird eine dieser Größen außerhalb der Spezifikation für den jeweiligen Betriebsfall betrieben, kann dies zur Gefährdung führen. Der Kessel wird gekühlt, es wird Druck abgelassen, der Füllstand wird reduziert und andere Maßnahmen können eingeleitet werden. Die Bierbrauer haben aber bewusst lieber schlechtes oder weniger Bier gebraut, als die gesamte Brauerei durch eine Explosion zu verlieren. Das gleiche Prinzip gilt für ein Sicherheitssystem für eine Lithium-Ionen-Batterie:

- Temperatur,
- Spannung und
- Ströme

müssen zu jedem Betriebszeitpunkt in einem bestimmten Verhältnis zueinander innerhalb der Spezifikation stehen, sonst riskiert man einen Brand oder die Explosion der Batterie.

Bei dem Braukessel wie bei der Batterie gilt, dass man durch logische physikalische Zusammenhänge immer die Größen gegeneinander überprüfen kann. Somit werden viele systematische und sporadische Fehler entdeckbar. Dieser Effekt wird heute auch bei der Umfelderfassung notwendig sein, da es keine Sensoren gibt, die alle notwendigen Situationen, das Verhalten und so weiter in dem jeweiligen Kontext hinreichend erfassen können.

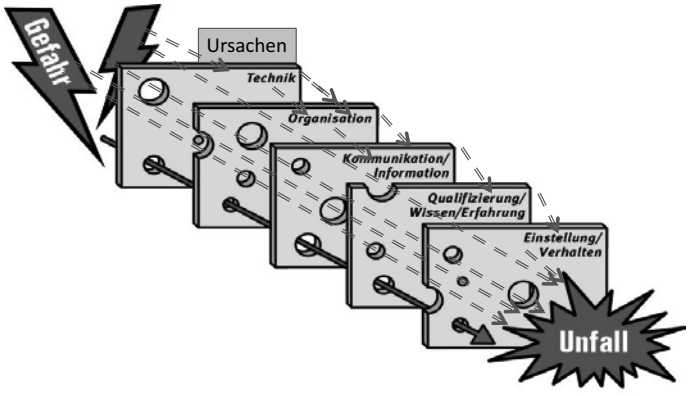

Bild 7.31 Ursache/Wirkung und Propagation von Eigenschaften, Funktionen und Fehlern

Ursachen können durch jede Ebene entstehen und von dieser Ebene aus propagieren. Für welche Propagation von Verhalten und Fehlern tatsächlich kein „Loch im Käse“ vorhanden ist, muss systematisch geplant werden.

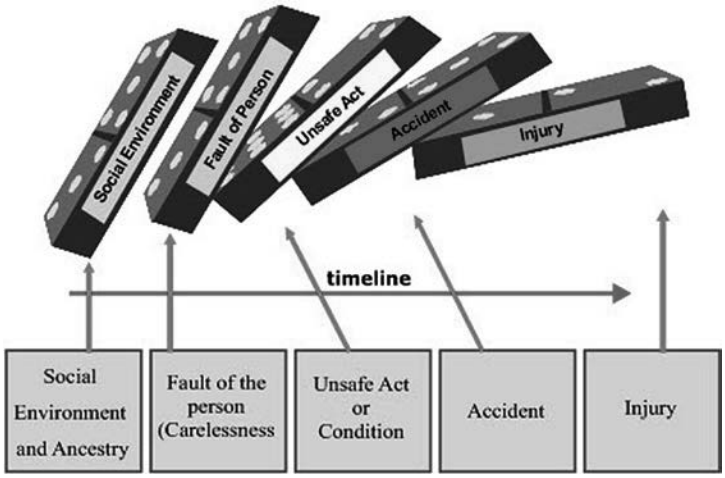

Bild 7.32 Dominoeffekt zu Unfällen und Verletzungen nach Heinrich 1931 (Quelle: Disaster Management Institute, Bhopal, Online Explanation of Domino theory)

Heinrich zeigt die soziale Umgebung und das Umfeld des Entwicklers auf, welches nur einen geringen Einblick in die Anwendungen haben kann; seine Fehler und Irrtümer propagieren aber auch möglicherweise bis hin zu einem Unfall.

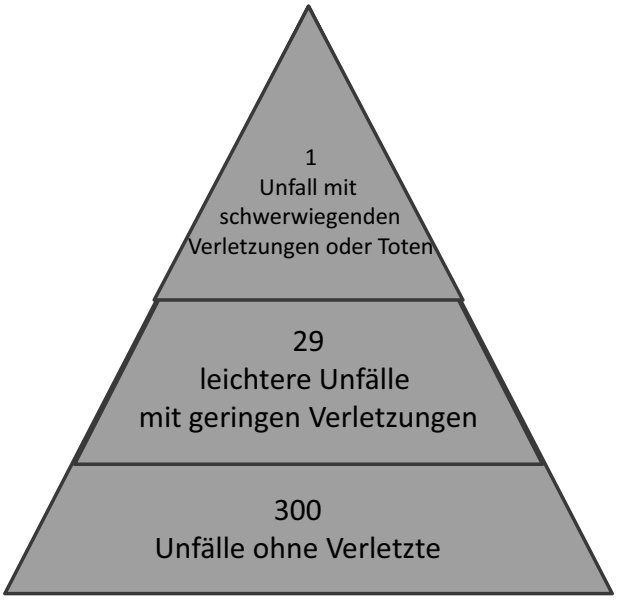

Bild 7.33 Heinrich-Pyramide

Heinrich formulierte auch den Pyramideneffekt, jedoch schloss er darauf, dass man durch effiziente Maßnahmen an den Ursachen viele Fehlereffekte, die zu großen Schäden führen, arbeiten kann. Diese Erkenntnis geht in die FMEA-Methodik ein, bei der man das Vermeiden von Fehlerursachen als effektivste Maßnahme ansieht. Eine der wesentlichen Motivationen der Lebenszyklusansätze war die, dass Ursachen nicht nur in der Technik und im Design verankert sind, sondern auch in vielen anderen Zusammenhängen der Produktentstehung bis hin zum Ausphasen eines Produktes. In heutigen Systemen wird also durch das technische Design kaum ein Produkt definierbar sein, welches frei von Sicherheitsrisiken ist.

Diese Zusammenhänge, die immer wieder aufgezeigt werden, sind heute nicht durch ein Wunder gelöst und werden auch nicht durch so etwas wie künstliche Intelligenz gelöst werden können. Wir fordern heute, dass wir zufällige Hardwarefehler mit einer Diagnosedeckung von 99 % absichern können, und argumentieren immer noch mit Zuverlässigkeitsdaten von Siliziumspeichern aus den 70er Jahren in der Hardwaresicherheit. Wir sprechen von sicheren Hardwarefehlern in Mikroprozessoren, bei denen kein Mensch weiß, welcher Speicher für welche Aufgabe verwendet wird. Geschweige denn, wie diese Fehler in Mikroprozessoren zu einer Gefährdung führen können. Ähnliche Irrtümer wie dieser können an jeder technischen, logischen, organisatorischen Schnittstelle geschehen, ohne dass eine Systematik dies verhindern kann.

Also, wollen wir auf verteilte Entwicklung, künstliche Intelligenz, Hochleistungsrechner verzichten? Im digitalen Zeitalter doch wirklich nicht.

Ein Hardware-Elektroniker kennt seine Hardware am besten, der Software-Ingenieur seine Software, aber die unterschiedlichen Betriebsszenarien und die Reaktionen der Personen im Verkehrsumfeld werden beide nicht systematisch bearbeiten oder analysieren können. Die Effektivität von Maßnahmen in all den Ebenen wird auch nie ein einziger Assessor beurteilen können.

7.3.3 Künstliche Intelligenz und Sicherheit

Wesentlich ist die Frage, was ist künstliche Intelligenz und wozu setzt man diese sinnvoll ein. Schon vor 20 Jahren hat man im Anlagenbau sogenannte „Fuzzy-Regler“ eingesetzt. Diese konnten die Regelstrecke einlernen, aber auch das Verhalten von möglichen Störgrößen erlernen, um damit die Regelparameter zu optimieren. Um einen nach den Regeln der Sicherheitstechnik implementierten Regler abzusichern, ist es vollkommen irrelevant, ob die Regelparameter korrekt oder falsch während der Laufzeit „weglaufen“, die Reglerabsicherung muss eine Abweichung, die zu einer Gefahr werden kann, erkennen und entsprechende Gegenmaßnahmen initiieren. Bei großen kontinuierlichen Anlagen wie einer Destillationskolonne einer Raffinerie wäre es nicht nur ein wirtschaftlicher Schaden, sondern auch ein

Sicherheitsrisiko, eine Anlage plötzlich einfach abzuschalten. Also wird wie bei einem Kernkraftwerk oder einem Flugzeug auf eine sichere Steuerung des Antriebs oder der Anlage umgeschaltet.

Warum dies nicht auch eine Lösung oder gar eine Anforderung für das automatisierte Fahren ist, leuchtet nicht wirklich ein. Einen Regler zum Fahren, Lenken und Bremsen im Fahrzeug würde man nie unüberwacht implementieren, warum will man dies machen, wenn man künstliche Intelligenz einsetzt?

Die heute als schnelle und effiziente Anwendung gepriesene „End2End-KI" wird aus gesellschaftlichen Interessen heraus zu viele Risiken bergen, als dass man eine Akzeptanz dieser Technologie erfahren wird. End2End-KI wird oft als eine Algorithmik verstanden, die von der Erkennung durch Sensoren ausgehend auch die geeignete Reaktion am Aktuator erzeugt.

Dazu muss geklärt werden, ob man KI als Funktion für

- die Nominalfunktion,
- als Schutzfunktion oder
- Sicherheitsmechanismus

einsetzt.

Weiter muss sichergestellt werden, ob

- die Funktion geeignet ist für die Aufgabe,
- die Eigenschaften und Features der KI-Funktion hinreichend sind,
- die KI-Funktionen selbst geeignet sind,
- das System geeignet ist, die Funktionen hinreichend und rechtzeitig auszuführen,
- die Sensoren und Aktuatoren geeignet sind und
- die Regelkreise mit den richtigen Parametern angewendet werden können.

Die weiteren Fragen danach, ob die richtigen Trainingsdaten und Validierungsstrategien angewendet werden können, sind dem nachgelagert.

Die Frage ist: Was ist künstliche Intelligenz (KI)? Bedeutet es: Alles, was der Mensch kann, wird durch eine Maschine umgesetzt? Vielleicht sogar durch eine intelligentere Maschine, als sie der Mensch je sein kann, weil die Summe der Intelligenz aller Menschen in einem System eingebracht wird? Oder ist KI doch nur ein lernender Regler und Speicher, der auf die Reize reagieren kann, die bewusst dem System zugeführt werden? Wie viel Intelligenz bekommt der Mensch durch die Gene von den Vorfahren geliefert und wie viel brauchen wir davon für das automatisierte Fahren?

Künstliche Intelligenz (AI, Artificial Intelligence) ist heute ein Sammelbegriff für

- maschinelles Lernen (Machine Learning),

- Verarbeitung natürlicher Sprache (NLP, Natural Language Processing),
- künstliche neuronale Netze (Deep Learning ist oft Methodik und nicht immer deckungsgleich mit KNN oder anderen Abkürzungen und Bezeichnungen).

Die Begriffe werden heute in unterschiedlichen Branchen und Kontexten verschieden verwendet.

Wissensbasierte Systeme oder sogenannte Expertensysteme bezeichnen modellierte Systeme, die aus formalisiertem Wissen logische Schlüsse ziehen können. Sie werden zum Beispiel in der Medizintechnik zur Diagnostik eingesetzt. Zur Fehleranalyse oder präventiven Diagnose wären sie auch in technischen Systemen sinnvoll einsetzbar.

Musteranalyse und Mustererkennung sind bereits bei der Zutrittskontrolle oder als Iris-Erkennung oder Fingerabdruckerkennung allen Mobiltelefonnutzern bekannt. Für Objekterkennung, Straßenzustandserkennung (AI sollte den aktuellen Reibwert der Straße besser erfassen können als die Reibwertschätzung über Raddrehzahlsensoren bei einem heutigen ABS), Bewegungsprofile von Menschenmengen oder auch Verkehrsströmungen aus der Cloud oder Verkehrsschildererkennung sollte die Technik durchaus sinnvoll sein. Auch bei der Belegung von virtuellen Rasterflächen, wie in der Robotik bekannt, sollten solche Systeme technische Vorteile haben können.

Sprachliche Intelligenz ist zur Sprachsynthese und umgekehrt von Siri und Alexa bereits bekannt, als Schnittstelle zu Navigationssystemen wird dies heute bereits verwendet.

Die Mechanismen der Musteranalyse, Mustererkennung oder Sprecherkennung können auch umgekehrt zur Mustervorhersage genutzt werden. Wie bei einem Kalmanfilter kann durch weitere Messwerte eine Hypothese plausibilisiert oder bewertet werden. Hierzu ist auch der hierarchische Temporalspeicher von Jeff Hawkins bekannt.

In der Robotik manipuliert man auch bewusst künstliche Intelligenz. Minensuche, Schweißroboter und so weiter erkennen anhand von Lernalgorithmen bestimmte Risiken und initiieren entsprechende risikominimierende Maßnahmen.

In der Medizintechnik setzt man auch immer mehr auf lernende künstliche Systeme, um Prothesen für Gliedmaßen optimal an das Verhalten der Menschen anzupassen.

Alexander Wissner-Gross beschreibt ein intelligentes System, welches Entropiekräfte modelliert. Anhand der Umgebung versucht man einen Zustand zur ermitteln und durch eine Aktivität bei möglicher Ausnutzung der verfügbaren Freiheitsgrade einen zukünftigen Zustand zu erreichen. Zur Navigation und zur Ermittlung der optimalen Trajektorie wäre dies eindeutig auch fürs automatisierte Fahren denkbar.

Dies sind nur wenige Beispiele, bei denen künstliche Intelligenz sinnvoll auch für Sicherheitsanwendungen einsetzbar ist oder gar zur Verbesserung der Sicherheit eingesetzt werden kann. Die Ingenieure, die solche Systeme integrieren, sollten die allgemeinen Regeln der Sicherheitstechnik kennen und beherrschen.

Wenn man künstliche Intelligenz einsetzen möchte, dann sollte klar sein, dass der allgemeine breite End2End-Einsatz keine Lösung für die unterschiedlichen Stakeholder der Gesellschaft sein kann. Zielgerichtet muss man prüfen, welche Risiken durch solche Systeme und Funktionen tatsächlich mit welchen Maßnahmen sinnvoll zu beherrschen sind.

Die notwendigen Sicherheitsmechanismen im Fahrzeug, aber auch in der Verkehrslenkung oder Verkehrsüberwachung sollten nach den geeigneten Sicherheitsintegritätsstandards wie ISO 26262 oder IEC 61508 entwickelt werden.

7.3.4 Mehrebenenabsicherung

Aber wie sind wir dann vor bereits 50 Jahren auf den Mond gekommen? Ist es wirklich nur eine Hollywood-Kulisse und ein Schauspiel, was wir alle gesehen haben? Vermutlich nicht. Was wussten die Protagonisten von damals mehr als wir heute? Wahrscheinlich waren sie demütiger und haben sich nicht von Lobbyismus, Aktienkursen und Marketing-Events blenden lassen.

Eine der ältesten Erkenntnisse des Systemengineerings ist, dass man unerwünschte Effekte und Verhalten vermeidet mit den Maßnahmen, die auch analysierbar und bewertbar sind. Aus dieser Idee entwickelte sich die

- Layer-of-Protection-Analyse (LoPA) oder
- Layer-of-Defense (LoD), auch Line-of-Defense.

In der LoPA geht man davon aus, dass die Ursachen für Risiken in jeder Ebene existieren und alle positiven und negativen Effekte Ursache für Risiken in der höheren Ebene sind. Somit kommt man nicht umhin, in jeder Ebene eine Zielüberprüfung, also eine Validierungsphase in Ergänzung zu den Analysen und Verifikationen, zu ergänzen.

Beginnt man von unten in der physikalischen oder der Hardware-Ebene, bringt die ISO 26262 einige Maßnahmen und Methoden mit, die eine solche Betrachtung unterstützen. Kombiniert man eine System-FMEA und eine quantitative Analyse, so erhält man schon einen Überblick über die möglichen systematischen Fehler und die zufälligen Fehler aus der EE-Hardware. Natürlich müssen aus der EE-Mechanik oder anderen nicht elektrischen Komponenten die Fehler auch betrachtet werden, aber dies ist in allen Qualitätsmanagementsystemen ja sowieso schon so gefordert. Natürlich sind bei Kommunikationssystemen wie CAN-Bus, FlexRay oder Ethernet die entsprechenden Ebenen hinunter bis zur

physikalischen Ebene zu berücksichtigen, jedoch kann man sich hier gut am ISO/OSI-Schichtenmodell orientieren. Handelt es sich um reine Sicherheitsintegritätssysteme, bei denen der energielose Zustand der „sichere Zustand“ ist, können die Metriken der ISO 26262 angewendet werden. Es sollte jedem jedoch klar sein, dass eine PMHF von 10E-8 und einer SPFM von mehr als 99 % nicht heißt, dass die relevanten EE-Fehler nicht auftreten; sie treten nur statistisch gesehen hinreichend selten auf. Davon auszugehen, dass die Fehler nicht über die Systemebene hinaus auch zu Gefährdungen propagieren, wäre ein Irrtum und ein systematischer Fehler.

Geht es jedoch um Risiken wie

- die Gebrauchssicherheit,
- aktive Sicherheitsfunktionen oder Schutzfunktionen,
- die mit der Unverfügbarkeit eines Systems oder einer Funktion einhergehen und so weiter,

wird ein „sicherer Fehler“ womöglich auch ein Fehler sein, der das Potential hat, Ursache für eine Gefährdung zu sein.

Daher wird es Ziel der Validierung sein, abzuwägen, welches Ziel mit der Komponente dem Nutzer oder Anwender versprochen wird. Konsequenterweise benötigt man dann wie bei einer Zertifizierung im Flugzeugbau einen kompletten Safety Case, der das Verhalten im Positiven inklusive aller

- Nominalfunktionen innerhalb ihrer Performancegrenzen,
- aller aktiven Sicherheitsfunktionen und Schutzmechanismen innerhalb der geprüften Betriebsgrenzen,
- aller Verhaltensweisen im Fehlerfall und
- aller Sicherheitsmechanismen und deren geprüften Fähigkeiten, Fehler zu beherrschen, sowie aller
- Trennmechanismen und Barrieren,
- Maßnahmen gegen vorsehbaren und aktiven Missbrauch beinhaltet.

Alles, was vom Hersteller nicht spezifiziert und nachgewiesen ist, bedeutet, dass die Komponente oder das System nicht geeignet ist.

Dieser Prozess wird ebenfalls insbesondere für SW-intensive Systeme an allen darüber liegenden Systemgrenzen notwendig sein, weil schon jemand, der eine Anwendersoftware auf einem System installieren möchte, die Parameter, das Verhalten und die Eigenschaften der Mikrocontroller oder Mikroprozessoren nicht mehr beurteilen kann.

Liefert der Hardwarehersteller keine vollständige Basis-Software, ist es sinnvoll, auch an der Schnittstelle zwischen Basis-Software und Anwender-Software eine solche Trennlinie, also eine Schutzebene, zu installieren.

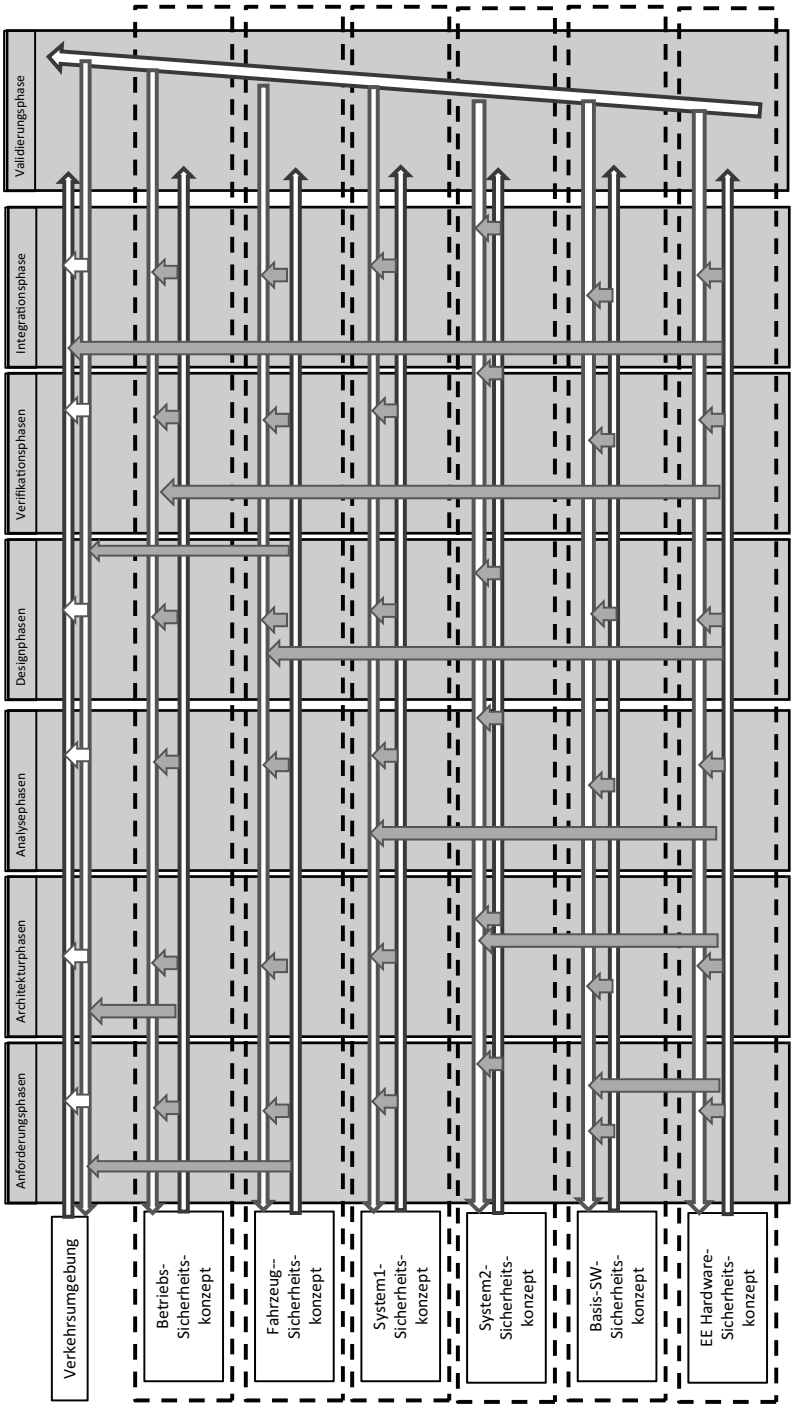

Bild 7.34 Ebenen zur Analyse der Risikoursachen und deren Propagationspotential

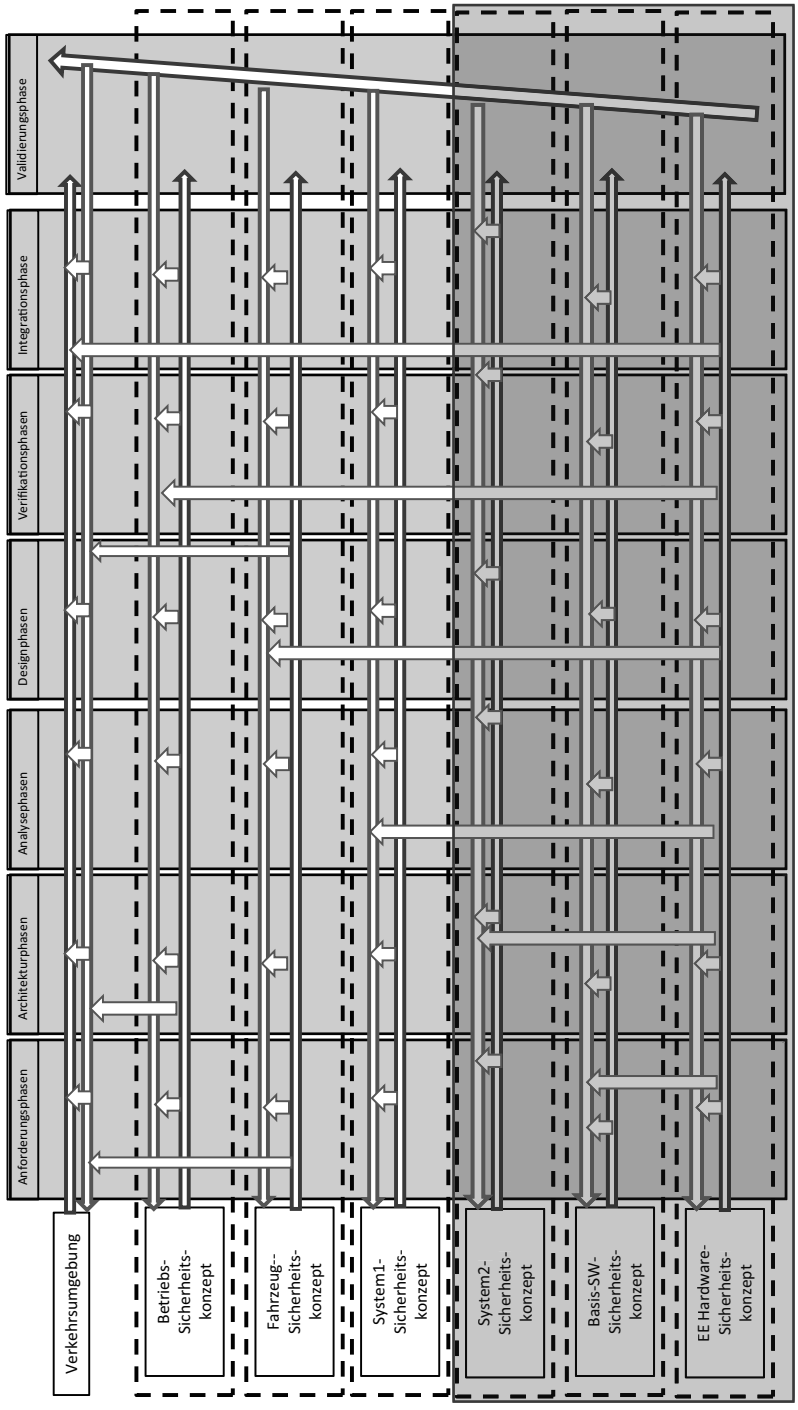

Bild 7.35 Absicherungsebenen in einem Steuergerät

Vergleicht man die Prinzipien, sieht man in einem typischen VDA-3-Ebenen-Sicherheitskonzept, wie EGAS,

- die Ebene 1 für die Nominalfunktion (Motoransteuerung),
- die Ebene 2 für die Funktionsüberwachung (hier vergleichbar mit der System-2-Ebene) und
- die Ebene 3 für die EE-Hardware-Überwachung.

Die Basis-SW ist nicht als Trennmechanismus im Allgemeinen im EGAS ausgeprägt, jedoch wird bei Systemen mit unterschiedlichen ASILs eine solche Ebene notwendig, um Trennebenen oder Barrieren zu implementieren, die die Partitionen zum Beispiel hinreichend trennen.

Die Trennung zwischen Basis-Software und Anwender-Software entsprechend auszubauen, macht schon deswegen Sinn, weil die Entwicklungsparteien hier aus unterschiedlichen Organisationen kommen und somit auch eine Kompetenz dafür angezweifelt werden kann, ob die verantwortliche Organisation für die Anwender-Software überhaupt noch die Verhaltensweisen und Eigenschaften an den Schnittstellen zur Basis-Software und dem Mikrocontroller oder Prozessor beurteilen kann. Einen geeigneten oder „Fähigen Assessor“ zu finden, der so etwas beurteilen kann, mag noch mehr angezweifelt werden.

Ab der Fahrzeugebene wird die Interaktion mit dem Fahrer und anderen Protagonisten, wie Passagieren und anderen Verkehrsteilnehmern, im Vordergrund stehen. Daher wird im Anlagenbau in den oberen Ebenen mehr mit Alarmen und Warnanzeigen etc. gearbeitet. Auf der Betriebsebene werden dann Straßenverkehrsregeln und die Interaktion der Fahrzeuge mit der Infrastruktur im Vordergrund der Maßnahmen stehen, die gewährleisten sollen, dass Fehler der Verkehrsteilnehmer nicht zu Unfällen führen.

7.4 AD-Sicherheitsfunktionen

Um ein Fahrzeug von einem System steuern zu lassen, muss das System die Aufgaben des Fahrers übernehmen. Bei AD-2-Systemen darf der Fahrer praktisch gar nicht die Hände vom Lenkrad lassen und bei AD-Level 3 muss er je nach Funktion innerhalb einer sehr kurzen Zeit die Fahrzeugsteuerung und die Verkehrsraumbeobachtung wieder übernehmen müssen.

Der menschliche Fahrer lernt die unterschiedlichen Situationen und Gegebenheiten während seiner Führerscheinausbildung. In Deutschland machen die Kinder mit zehn Jahren bereits eine Fahrradfahrerausbildung, während der man lernt sich im öffentlichen Verkehrsraum als Fahrradfahrer zu behaupten. Im Kinder-

Index

W

Z