Systemsicherheit des Active Front Steering

Active Front Steering – System Safety

Wolfgang Reinelt, Willy Klier und Gerd Reimann

Active Front Steering ist ein elektronisch geregeltes Lenksystem für Kraftfahrzeuge, das situationsabhängig eine Überlagerung eines Winkels zum Lenkradwinkel erlaubt und somit eine Variation der Lenkübersetzung ermöglicht. Für ein solches System muss die funktionale Sicherheit gewährleistet sein. Ziele der funktionalen Sicherheit werden erläutert und messbare Kriterien und deren Nachweisbarkeit dafür diskutiert. Der Analyseprozess, der Sicherheitsintegritätslevel des Systems und der Komponenten bestimmt, wird erläutert, gefolgt von der Spezifikation der Sicherheitsanforderungen und Überwachungsfunktionen. Zum Schluss werden einige modellbasierte Überwachungsfunktionen beschrieben, wie sie im technischen Sicherheitskonzept, speziell in der Verifikation der Eingangssignale des Active Front Steering der Nachfolgegeneration Anwendung finden sollen.

Active Front Steering is an electronically controlled steering system for passenger cars. It enables superposition of an angle to the hand wheel angle and hence the variation of the steering ratio dependent on the situation. For such systems functional safety must be guaranteed. Goals of functional safety are described along with criteria for their measurement. The validation aspect of these criteria is discussed as well. The analyses that determine the system's and the components' integrity are explained. Additionally specification of safety requirements and safety measures is discussed. Finally some model-based monitoring functions that will be used in the technical safety concept, particulary the signal verification layer are presented; focus are Active Front Steering systems of the second generation.

Schlagwörter: Lenksysteme für Kraftfahrzeuge, variable Lenkübersetzung, funktionale Sicherheit, Sicherheitsnachweis, Spezifikation von Sicherheitsanforderungen, Validierung und Verifikation

Keywords: Steering systems for passenger cars, variable steering ratio, functional safety, safety case, specification of safety requirements, validation and verification

1 Einleitung

Elektronisch geregelte Lenksysteme halten im Kraftfahrzeug zunehmend Einzug. Seit längerem bekannt sind z. B. Systeme wie die Elektrolenkung und die Elektrohydraulische Lenkung, die das *Moment* des Lenksystems abhängig von der Fahrsituation beeinflussen. Dementgegen und recht neu auf dem Markt stellt die sog. Aktivlenkung, oder auch Active Front Steering genannt, eine elektronisch geregelte Überlagerung eines *Winkels* zum Lenkradwinkel dar.

Active Front Steering ermöglicht sowohl einen vom Fahrer abhängigen als auch einen aktiven Lenkeingriff an der Vorderachse, ohne die mechanische Kopplung zwischen Lenkrad und Vorderachse auftrennen zu müssen (vgl. Bild 1). Der zusätzliche Freiheitsgrad ermöglicht die kontinuierliche und situationsabhängige Adaption der Lenkeigenschaften. Eine der Hauptfunktionen ist dabei die geschwindigkeitsabhängige Variation des Übersetzungsverhältnisses zwischen (Hand-)Lenkrad und (Straßen-)Rad. Dies hat zur Folge, dass bei niedrigen Geschwindigkeiten, etwa beim Parkieren, die Lenkung sehr direkt ist (z. B. ist weniger als eine Umdrehung am Lenkrad notwendig, um das Rad an den Anschlag zu lenken). Bei höheren Geschwindigkeiten wird die Lenkung im Gegenzug indirekter. Komfort, Lenkaufwand und Lenkdynamik werden somit aktiv angepasst und optimiert. Darüber hinaus sind auch Lenkeingriffe zur Verbesserung der Fahrzeugstabilisierung möglich.

Nach der erfolgreichen Markteinführung des Systems in der neuen BMW 5er Limousine, stehen für ZF Lenksysteme die Fragen der Modularisierung und der Systemsicher-

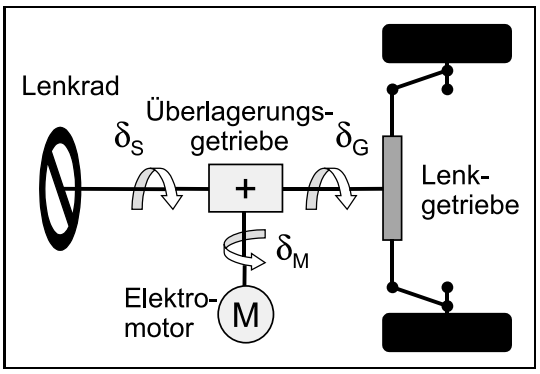

Bild 1: Prinzip der Überlagerungslenkung. Ein Elektromotor überlagert den Winkel δ_M zum Lenkradwinkel δ_S. Als Resultat ergibt sich der Ritzelwinkel δ_G am Lenkgetriebe als gewichtete Summe der beiden Winkel. Mithilfe des Motorwinkels δ_M kann somit die Lenkübersetzung, das Verhältnis zwischen Lenkradwinkel δ_S und Ritzelwinkel δ_G, variiert werden.

heit für Nachfolgeprojekte im Vordergrund. System und Funktionsumfang werden in [11; 12] beschrieben. Dieser Beitrag diskutiert die Systemsicherheit. Der Begriff „Sicherheit“ wird in diesem Beitrag im Sinne von funktionaler Sicherheit gebraucht. Funktionale Sicherheit bezeichnet diejenigen Maßnahmen, die sicherstellen, dass ein programmierbares elektronisches System das leistet, was es leisten soll, und insbesondere keine Gefährdungen durch etwaige Fehlfunktionen auslöst. Solche Systeme werden auch sicherheitsrelevant oder sicherheitskritisch genannt.

Dementgegen stehen die Begriffe aktive oder passive Sicherheit, die Systeme bezeichnen, die gefährliche Situationen verhindern oder zumindestens abmildern. Beispiele hierfür sind Fahrstabilisierungssysteme wie ESP (aktive Sicherheit) oder Airbags und Gurtstraffer (passive Sicherheit).

Zur Gruppe der sicherheitsrelevanten Fahrzeugsysteme gehören offensichtlich die aktiven und passiven Sicherheitssysteme, da diese durch Fehlverhalten Gefährdungen auslösen können; aber auch andere Fahrwerkssysteme, die programmierbare elektronische Komponenten enthalten, wie z. B. elektronische Kraftstoffeinspritzung, elektronische Bremse, elektronische Lenksysteme usw. Der vorliegende Beitrag beschäftigt sich mit der funktionalen Sicherheit des Active Front Steering.

2 Elemente der Funktionalen Sicherheit

2.1 Übersicht

Funktionale Sicherheit von programmierbaren elektronischen Systemen wird in internationalen Normen wie beispielsweise der IEC 61508 [10] behandelt, Übersichten über weitere Sicherheitsnormen finden sich in [5; 23]. Die technischen Kernthemen aller Normen lassen sich wie folgt beschreiben:

1. Risikoanalyse des Systems und der Komponenten
2. Spezifikation von Sicherheitsanforderungen auf System- und Komponentenebene
3. Sicherheitsgerichtetes System- und Komponentendesign
4. Validierung und Verifikation der Sicherheitsanforderungen

Das technische Sicherheitskonzept behandelt dabei vornehmlich den zweiten Punkt und spezifiziert nicht nur (umzusetzende) Sicherheitsmaßnahmen, sondern erläutert auch, warum diese zu einem hinreichend sicheren System führen. Nach Erläuterung einiger wesentlicher Begriffe werden Elemente des technischen Sicherheitskonzeptes des Active Front Steering vorgestellt. Initiiert werden die oben genannten Punkte von einem begleitenden Sicherheitsentwicklungsprozess, vgl. [1; 19].

2.2 Messbarkeit und Messung von „Sicherheit“ und „Risiko“

Die Wahrscheinlichkeit, durch einen Unfall im Straßenverkehr tödlich zu verunglücken, beträgt etwa 10^{-6} bis 10^{-5} pro Jahr. Von der Öffentlichkeit wird allgemein akzeptiert, dass die Vorteile des eigenen Kraftfahrzeuges diese erhöhte Wahrscheinlichkeit, ums Leben zu kommen, zumindest kompensieren [6]. Basierend auf diesen Zahlen werden für technische Systeme im Einzelkraftfahrzeug Wahrscheinlichkeiten für sicherheitsrelevante Ausfälle von kleiner als $10^{-8}, \ldots, 10^{-5}$ pro Stunde gefordert. Die genaue Größe wird dabei durch die sog. Sicherheitsintegrität des Systems bestimmt, die abhängig von Ausmaß, Auftretenswahrscheinlichkeit und Beherrschbarkeit der möglichen Systemfehler in der sog. Risikoanalyse ermittelt wird [10, Teil 5]. Die Sicherheitsintegrität wird nach [10] in diskreten Stufen, dem sog. SicherheitsIntegritätsLevel (SIL 1 bis 4) gemessen. Je höher diese Stufe, desto höher ist die Anforderung an die Integrität des Systems und desto höher sind auch die Anforderungen an dessen funktionale Sicherheit. Die geforderten Wahrscheinlichkeiten stellen das sog. vertretbare Risiko dar, siehe Bild 2. Ausfälle sind hierbei als Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion (korrekt) auszuführen, definiert [10, Teil 4]. Die üblicherweise in Qualitätszielen vereinbarten Kennzahlen in ppm/a[1] und FIT[2] liegen höher, was dadurch zu erklären

[1] Definiert als Anzahl der Ausfälle pro 1 Million Stück pro Jahr.
[2] Abkürzung für *Failure In Time* und definiert als Anzahl der Ausfälle pro 1 Milliarde Betriebsstunden.

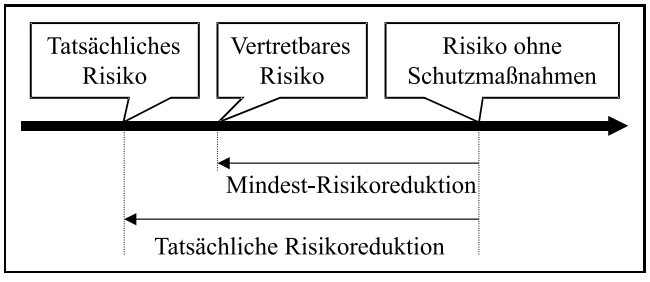

Bild 2: Das vom System ausgehende Risiko muss mithilfe geeigneter Sicherheitsmaßnahmen auf ein akzepiertes Niveau reduziert werden (oder darunter).

ist, dass diese auf alle möglichen Ausfälle bezogen sind, während die in [10] geforderten Grenzwerte sich auf die Untermenge der sicherheitsrelevante Ausfälle beziehen.

2.3 Validierung von Obergrenzen für Ausfallwahrscheinlichkeiten

Was bedeutet es nun, für ein technisches System eine Ausfallwahrscheinlichkeit von $p < 10^{-8}, \ldots, 10^{-5}$ pro Stunde zu fordern? Möchte man diese statistisch zuverlässig mittels eines einfachen Hypothesentests nachweisen, so gilt folgendes: Man betreibe das System n Stunden unverändert, während dieser Zeit zeige es z sicherheitsrelevante Ausfälle. Mit einer Wahrscheinlichkeit (Signifikanzniveau) von 95% soll die Aussage, das System habe höchstens $p \in [10^{-8}/\text{h}, \ldots, 10^{-5}/\text{h}]$ sicherheitsrelevante Ausfälle, bestätigt werden (d. h. bei höchstens 5% aller Fälle zieht man aus dem Test den falschen Schluss). Unter der Annahme, daß die Ausfälle normalverteilt sind, ergibt sich die in Tabelle 1 dargestellte Situation. Um etwa bei einem System statistisch zuverlässig nachweisen zu können, dass die Wahrscheinlichkeit für sicherheitsrelevante Ausfälle kleiner als $p = 10^{-7}/\text{h}$ ist, muss man das System zirka 600 Jahre durchgehend und unverändert betreiben. Tritt höchstens $z = 1$ sicherheitsrelevanter Ausfall auf, kann die oben anvisierte Wahrscheinlichkeit als nachgewiesen gelten. Im Automobilbereich könnten z. B. in einer halbjährigen C-Musterphase 1200 Versuchsträger (unverändert) im Dauerlauf diesen Nachweis erbringen.

Verbindet man Statistik und Praxis, so ist es also nahezu unmöglich, angestrebte Obergrenzen für Ausfallraten nachzuweisen [22]. Dieses gilt für alle Bereiche mit sicherheitsrelevanten Anwendungen, und zwar umso mehr, je weniger Prototypen oder Entwicklungszeit zur Verfügung stehen.

Unter der Voraussetzung, dass ein Nachweis der geforderten Ausfallraten durch Validierung (auf Systemebene, d. h. durch Fahrzeugtests) nicht möglich ist, wie soll dann der Sicherheitsnachweis für sicherheitsrelevante Systeme, die programmierbare Elektronik nebst Software enthalten, geführt werden? Neben den zufälligen Fehlern während des Betriebs des Systemes, die von Überwachungsmaßnahmen entdeckt werden, sind insbesondere systematische Fehler im Entwurf zu beseitigen. Dieses wird durch den *sicherheitsgerichteten Entwicklungsprozess* gewährleistet. Da systematische Fehler in der Software einen Teil der sicherheitsrelevanten Ausfälle bilden, schreiben Softwareentwicklungsprozesse üblicherweise eine Reihe von Modultests mit einer vorgeschriebenen (Pfad-)Abdeckungsrate vor. Dabei werden gängige Tools zur statischen Codeanalyse wie PolySpace, CodeSurfer, Safer C etc. eingesetzt. [4] stellt fest, dass lediglich 19.8%[3] aller sicherheitsrelevanten Fehler durch diese Tests entdeckt werden, weitere 25.8% durch zusätzliche Analysen wie Code- oder Dokumentationsbegutachtung. Die restlichen 54.4% werden durch Felderfahrung entdeckt, vgl. Tabelle 2. Gründe für den niedrigen Aufdeckungsgrad durch statische Codeanalyse mögen u. a. sein, dass statische Analysetools den Code in Gleichungssysteme umwandeln, während der Code letztlich Differentialgleichungen beschreibt (die Dynamik im Test also höchstens approximiert wird), oder dass z. B. Fahrzeugtests die implementierte Software gegen das prüfen, was das System leisten soll, statt lediglich gegen die (gegebenenfalls schon fehlerbehafteten) Spezifikationen [9; 13]. Vergleicht man diese Tatsache mit der Entwicklung nach dem V-Modell, so ist es auch die Aufgabe von (z. B. statischen) Softwaretests gegen die Softwarespezifikationen zu testen (Verifikation) und nicht gegen die Spezifikationen auf Systemebene. Dies ist die Aufgabe der Validierung, zu der auch die Fahrzeugtests zählen. Da Fahrzeugtests allein aus den oben genannten Gründen nicht den statistischen Nachweis einer gewissen Ausfallrate erbringen können, müssen andere, im sicherheitsgerichteten Entwicklungsprozess verankerte Verifikations- und Validierungsaktivitäten einen erheblichen Teil beitragen. Insgesamt bleibt jedoch festzuhalten, dass Fahrzeugversuche im Automobilbereich ein wesentlicher und wichtiger Bereich für den sicherheitsrelevanten Test sind.

Des Weiteren kann aus Tabelle 2 geschlossen werden, dass die Mehrzahl der „major safety“ Fehler auf unzureichende Spezifikationen zurückzuführen sind, was ebenfalls in [9] ausgeführt wird. Daher ist auf die korrekte Spezifikation

Tabelle 1: Betriebszeit eines Systems, die zum Nachweis einer bestimmten Ausfallrate notwendig ist.

Ausfallrate p	Betriebsjahre	Anzahl erlaubter sicherheitsrelevanter Ausfälle z, die noch zum Sicherheitsnachweises führen
$10^{-9}/\text{h}$	57078	≤ 1
$10^{-8}/\text{h}$	5708	≤ 1
$10^{-7}/\text{h}$	571	≤ 1
$10^{-6}/\text{h}$	57	≤ 1
$10^{-5}/\text{h}$	6	≤ 1

[3] bezogen auf die $(17{,}3 + 30{,}7)\%$ der major und minor safety Spalten

Tabelle 2: Entdeckte Fehler, Abweichungen oder Ausfälle, aufgeschlüsselt nach deren Sicherheitsrelevanz und Möglichkeit zur Aufdeckung nach [4].

	Major Safety	Minor Safety	Significant Violation	Minor Violation	All
Static analysis	0,0	9,5	7,1	39,0	55,6
Additional analysis	2,4	10,0	0,0	5,9	18,3
Field experience	14,9	11,2	0,0	0,0	26,1
Total	17,3	30,7	7,1	44,9	100,0

von Anforderungen, insbesondere der Sicherheitsanforderungen, ein besonderer Wert zu legen. Einige Details dazu finden sich in [19].

2.4 Spezifikation von Sicherheitsanforderungen

Die Risikoanalyse, etwa nach den in [10, Teil 5] referenzierten Methoden, zeigt diejenigen Gefährdungen auf, die vom System (ohne jegliche Schutzmaßnahme) ausgehen. Zusätzlich dazu wird die Sicherheitsintegrität des Systems, ausgedrückt als SIL, ermittelt.

Gefährdungen und Sicherheitsintegrität müssen dann auf einzelne Komponenten heruntergebrochen werden, um die sicherheitsrelevanten Fehlfunktionen der Komponenten zu identifizieren und geeignete Überwachungsfunktionen zu spezifizieren. Die Summe der notwendigen Überwachungsfunktionen bildet den zu implementierenden Teil des technischen Sicherheitskonzeptes. Komponenten in diesem Sinne sind Mechanik, Hydraulik, Sensorik, Steuergerät und Softwaremodule.

In der sog. Kritikalitätsanalyse werden die Komponenten nun mit einzelnen Funktionen belegt und somit die Sicherheitsintegritätslevel der Komponenten ermittelt. [16; 20] stellen qualitative Verfahren für Kritikalitätsanalysen dar. Bild 3 zeigt dies am Beispiel des Ritzelwinkelsensors. Ausgehend vom Sicherheitsintegritätslevel der Gesamtfunktion „Winkelüberlagerung" wird diese entgegen dem logischen Signalfluss auf die Komponenten vererbt. Dabei wird davon ausgegangen, dass fehlerhaftes Verhalten einer Komponente einerseits von der Komponente selbst oder von fehlerhaften Eingängen herrühren kann. Je nach Auswirkung des fehlerhaften Verhaltens kann der SIL für Komponenten kleiner sein als der System SIL.

Fehlfunktionen treten in den einzelnen Komponenten mit unterschiedlicher Häufigkeit auf. Im Allgemeinen wird angenommen, dass Fehler in der Aktuatorik am häufigsten auftreten, gefolgt von Fehlern in Sensorik oder der Übertragung der Signale an den gewünschten Ort, zum Schluss folgt das Steuergerät [15]. Schlüsselt man das Steuergerät weiter auf, so treten Fehler in Form von Softwarefehlern, Spezifikationsfehlern und schlussendlich Elektronikfehlern auf (dieses gilt zumindestens für die zur Zeit im Automobilsektor verwendete Steuergeräteelektronik). Bei Software- und Spezifikationsfehlern handelt es sich um systematische Fehler, die, wie bereits diskutiert, nur durch den Entwicklungsprozess herausgefiltert werden können. Im Falle von zufälligen Elektronikfehlern im Steuergerät fordert [10, Teil 3, Abschn. 7.4.3.2 c], dass alle Hardware-Software Interaktionen beschrieben und deren Signifikanz bewertet werden muss. Die Hardwarearchitektur des Steuergerätes muss also von vorne herein in Design und Sicherheitskonzept mit einbezogen werden. Sammlungen wie [10, Teil 3] geben genügend Handhabe zur Auswahl geeigneter Überwachungsfunktionen (im Folgenden „elektronikabhängige Überwachungsfunktionen" genannt). Zur Auslegung der elektronikabhängigen Überwachungsfunktionen ist daher keine oder nur sehr wenig Kenntnis der auf dem Steuergerät abgebildeten Funktionalität/Applikation notwendig. Der Vorteil dieser Überwachungsfunktionen besteht darin, dass sie bei Verwendung der Komponente in einer anderen Applikation wiederverwendet werden können und somit eine sog. Plattformsicherheit bieten. Diese Überwachungsfunktionen reagieren in allen Situationen gleich, können jedoch nicht alles abdecken. Beispielsweise kann bei der applikationsunabhängigen Überwachung der Analogspannung als Ausgangssignal eines Sensors überprüft werden, ob die Spannung die richtige Größenordnung hat. Es kann jedoch nicht überprüft werden, ob die der Spannung zugeordnete Systemgröße (z. B. ein Winkel) zur derzeitigen Situation passt bzw. mit anderen Systemgrößen kompatibel ist. Letzteres kann nur von applikationsabhängigen Überwachungen geleistet werden. Anwendungsbereich und Anforderungen an solche applikationsabhängigen Überwachungen können mit Hilfe der FMEA[4] oder FTA[5] hergeleitet werden. Um in diesen Situationen den notwendigen Aufdeckungsgrad zu haben, sind die sog. „applikationsabhängigen Überwachungsfunktionen" notwendig, die im Allgemeinen Sensorik und Aktuatorik überwachen. Da diese in Bezug auf Spezifikation und Umsetzung einen hohen Anspruch haben, sollte die Umsetzung des technischen Sicherheitskonzeptes mit diesen starten. Gleichwohl sei betont, dass elektronikabhängige sowie applikationsabhängige Überwachungsfunktionen gleichwichtige Pfeiler zur Aufdeckung zufälliger Fehler bilden. Das Ziel ist jedoch, möglichst viel applikations-

[4] Failure Modes and Effects Analysis
[5] Fault Tree Analysis

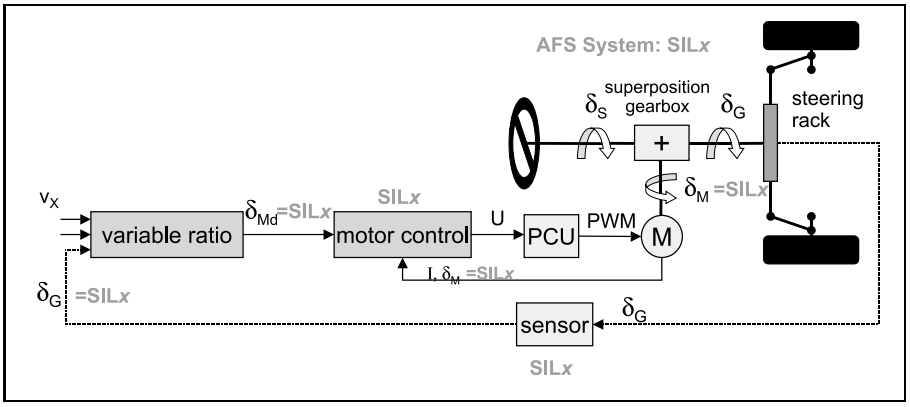

Bild 3: Beispiel aus der Active Front Steering Kritikalitätsanalyse: Ausgehend von dem in der Risikoanalyse ermittelten SIL der Funktion „Winkelüberlagerung" wird dieser SIL auf Funktionen bzw. deren Eingänge heruntergebrochen. In diesem Falle hätte der Ritzelwinkelsensor den gleichen SIL wie die Gesamtfunktion.

unabhängige/elektronikabhängige Überwachungsfunktionen zu entwickeln, um eine wiederverwendbare Plattformsicherheit zu schaffen.

2.5 System- und Komponentendesign

Nach der Spezifikation der technischen Maßnahmen, die die funktionelle Sicherheit des Systems gewährleisten soll, müssen diese für die einzelnen Komponenten umgesetzt werden. An dieser Stelle werden die Sicherheitsanforderungen mit den Funktionsanforderungen, auch mit denen für nicht sicherheitsrelevante Teile, vereint zu den Gesamtanforderungen. Insbesondere die Sicherheitsrelevanz der Software hat einige Implikationen auf das Software- und Systemdesign zur Folge:

„Wenn Software sicherheitsrelevante Funktionalitäten unterschiedlicher Integrität implementiert, ist die gesamte Software als sichheitsrelevant mit höchster Integrität zu betrachten, sofern nicht adäquate Unabhängigkeit zwischen den Funktionalitäten im Software-Design nachgewiesen werden kann“ [10, Teil 3, Abschn. 7.4.2.7+8]. Im Falle des Active Front Steering sind sicherheitsrelevante und nicht sicherheitsrelevante Funktionalitäten im Design nicht trennbar bzw. nur sicherheitsrelevante Funktionalitäten enthalten, was impliziert, dass die nicht sicherheitsrelevante Software nach demselben Prozess entwickelt und getestet wird wie die sicherheitsrelevante. Im Umkehrschluss muss jedoch vermieden werden, nicht sicherheitsrelevante Funktionalitäten, die nicht dem Active Front Steering funktionell zuzuordnen sind (z. B. das elektrische Schiebedach), in diesem Steuergerät zu platzieren (um den Enwicklungsaufwand nicht unnötig aufzublähen). Die Ziele von Schnittstellen- und Architekturgremien wie z. B. [2] fordern u. a. „Verschiebbarkeit von Funktionen“. Gemeint ist, die Software-Architektur im Steuergerät so zu standardisieren und mit einer „Basissicherheit“ auszustatten, dass Funktionen dort ohne größeren Adaptionsprozess integriert werden können. Offensichtlich ist darauf zu achten, dass der Sicherheitsintegritätslevel des Steuergerätes samt Basissicherheit mit der zu integrierenden Funktion kompatibel ist. Die Verschiebbarkeit von Funktionen geschieht einmalig während des Systemdesigns und ist daher grundsätzlich von der sog. dynamischen Rekonfiguration zu unterscheiden. [10, Teil 7, C3.13] definiert den Begriff „Dynamische Rekonfiguration“ derart, dass ermöglicht wird, „die logische Architektur des Systems auf andere (derzeit verfügbare) Teilsysteme ganz oder teilweise abzubilden“ (gemeint ist: im laufenden Betrieb). Für sicherheitsrelevante Systeme mit höherem SIL (2–4) ist dieses jedoch nach [10, Teil 3, Tab.A2] nicht erlaubt.

3 Beispiele aus dem Sicherheitskonzept des Active Front Steering

3.1 Generelles

Die Kritikalitätsanalyse enthält etwa 500 Einträge von Fehlfunktionen auf (funktionaler) Komponentenebene, die sicherheitsrelevante Auswirkung auf die Systemfunktion „Winkelüberlagerung“ haben. Für diese Fehlfunktionen sieht das technische Sicherheitskonzept Überwachungsfunktionen entsprechender Integrität vor. Diese umfassen z. B.:

- Applikationsunabhängige Überwachung der elektronischen Komponenten wie Sensorik, Steuergerät etc. in Form von Überwachung analoger Signale, Speichertests usw.
- (Applikationsabhängiges) diversitäres Rechnen.
- Applikationsabhängige Plausibilisierung der Nutzsignale gegeneinander und gegen die Fahrsituation.
- Absicherung der Kommunikationswege zum und vom Steuergerät.
- Applikationsabhängige Überwachung der Aktuatorik.

Aus regelungstechnischer Sicht am interessantesten sind die applikationsabhängigen Überwachungsfunktionen, da im Allgemeinen aufwändige Modellbildung und Parameteridentifiation von Gesamtsystem oder Komponenten notwendig sind. Zusätzliche Herausforderungen stellen sich in Form von Beoachterentwurf, Anfangswertschätzung und Rechenzeit. Diese sind vornehmlich bei Aktuatorik- und Nutzsignalüberwachung zu finden. Letztere soll im Folgenden exemplarisch betrachtet werden.

3.2 Nutzsignalüberwachung

Die zum Betrieb der Active Front Steering Funktionalität notwendigen Signale sind im Wesentlichen der Lenkradwinkel δ_S, der Motorwinkel δ_M, der Ritzelwinkel δ_G und die Fahrzeuggeschwindigkeit v_X; [11] stellt die vollständige Schnittstelle dar. Der Lenkradwinkel δ_S ist ein externes Signal und als solches in der Schnittstelle als hinreichend plausibilisiert[6] definiert. Weiters sind Ritzelwinkel δ_G sowie der Motorwinkel δ_M zum Betrieb der Lenkassistenz- und Aktuatorfunktionen notwendig. Zur Plausibilisierung stehen noch die vier Raddrehzahlen ω_{ij} zur Verfügung, die im Wesentlichen die Fahrzeuggeschwindigkeit repräsentieren. Alle Signale werden eingangs mit einer Kommunikationsüberprüfung zur Quelle hin, einer Sensordiagnose und einer Bereichs- und Gradientenüberprüfung versehen. Diese Überwachungsfunktionen gehören zur Klasse der elektronikabhängigen Sicherheitsfunktionen. Um bei den sicherheitsrelevanten Nutzsignalen δ_G, δ_M einen hinreichenden Aufdeckungsgrad für zufällige Fehler zu gewährleisten, wird ein virtueller zweiter Signalkanal mithilfe unabhängiger Signale errechnet, siehe Bild 4 oder [21]: zur Berechnung des Signals steht ein validiertes Modell zur Verfügung, dessen Eingänge zunächst aufbereitet werden. Der Unterschied zwischen gemessenem und errechnetem Signal wird dann in seiner Größe beurteilt, die Qualitätsaussage gegebenenfalls über einen gewissen Zeitraum gefiltert [8]. Zudem muss entschieden werden, ob das Modell im derzeitigen Fahrzustand gültig ist. Diese Überwachungsfunktionen gehören zur Klasse der applikationsabhängigen Sicherheitsfunktionen. Zur Beurteilung der einzelnen Signale

[6] D. h. entsprechend ihrer, durch Kritikalitätsanlayse ermittelten, SIL

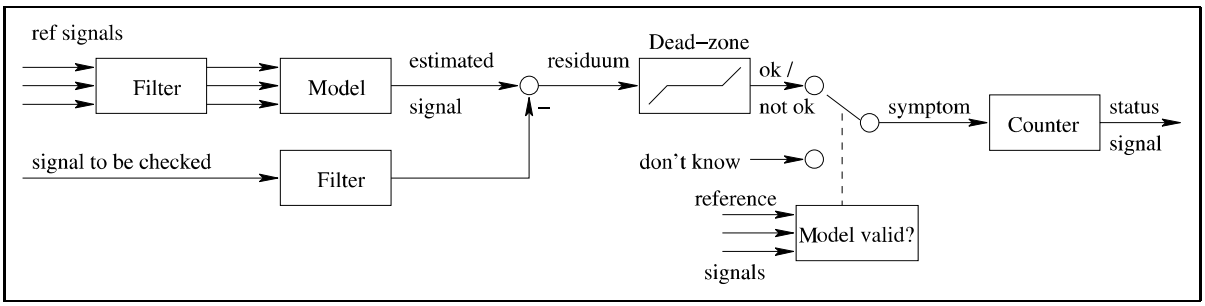

Bild 4: Generische Struktur einer modellbasierten Überwachungsfunktion.

müssen dann die Informationen aus allen beteiligten Überwachungsfunktionen ausgewertet werden. Je nach Status der Nutzsignale werden dann die Lenkassistenzfunktionen in entsprechende Modi überführt.

3.3 Summengleichungsüberwachung

Diese Überwachungsfunktion überwacht die kinematische Zwangsbeziehung zwischen den drei Winkeln der Überlagerungslenkung: $\delta_S/i_D + \delta_M/i_M = \delta_G$. Es ist jedoch unzureichend diese Beziehung als lineares, statisches Modell anzusetzen. Da der Lenkradwinkelsensor am oberen Ende der Lenksäule plaziert ist, müssen Torsion und Kardangelenke der Lenksäule mit berücksichtigt werden. Ein Mehrkörpermodell liegt vor [12], das jedoch aus Rechenzeitgründen auf dem Steuergerät nicht verwendet werden kann. Daher wurde eine einfachere Lösung verfolgt und die Torsion der Lenksäule (die linear angesetzt werden kann) und die Kardangelenke (die mittels einer nichtlinearen statischen Beziehung modelliert werden können) wurden durch den folgenden Wiener-Ansatz modelliert:

$$\dot{x}(t) = Ax(t) + b\left(\delta_G^{\#}(t) - \delta_M^{\#}(t)\right);\ x(0) = x_0 \qquad (1)$$

$$\hat{\delta}_S(t) = J\left(Cx(t)\right)\ , \qquad (2)$$

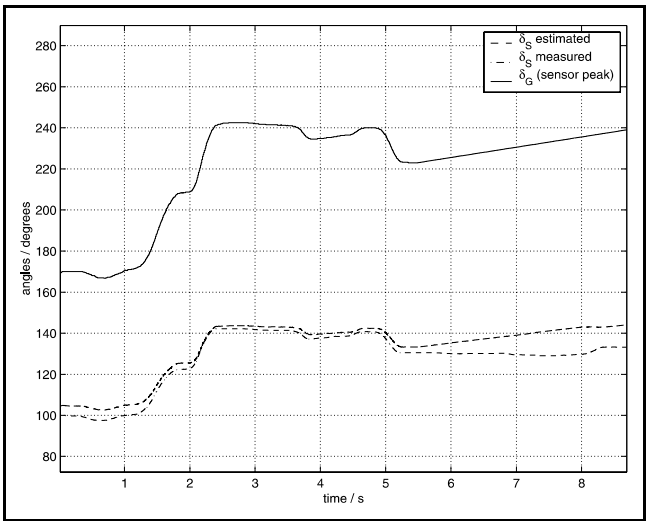

Bild 5: Überwachung der Summengleichung während eines Fahrdynamikmanövers. Eine Signaldrift wurde in den Ritzelwinkelsensor injiziert (bei 5,2 s). Gemessener Lenkradwinkel (strichpunktiert), berechneter Lenkradwinkel (gestrichelt) und driftender Ritzelwinkel (durchgehend).

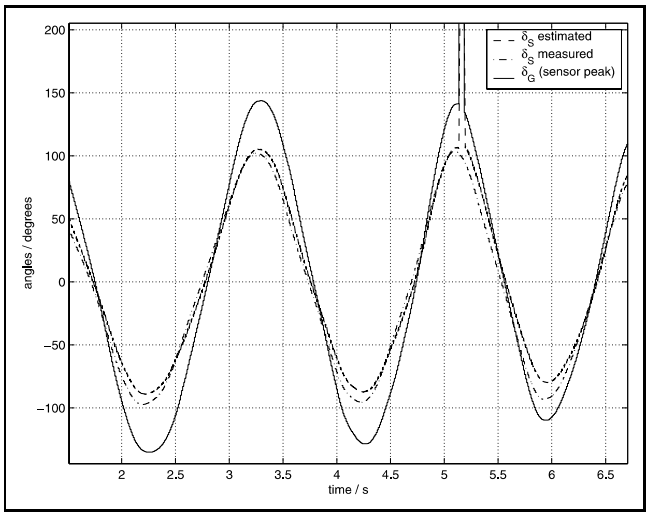

Bild 6: Überwachung der Summengleichung während eines Fahrdynamikmanövers. Ein Signalausreisser wurde in den Ritzelwinkelsensor injiziert (bei 5,14 s). Gemessener Lenkradwinkel (strichpunktiert), berechneter Lenkradwinkel (gestrichelt) und driftender Ritzelwinkel (durchgehend).

wobei $\delta_M^{\#}$ und $\delta_G^{\#}$ der Motor- bzw Ritzelwinkel sind, jedoch bezogen auf den Lenkradwinkel. Das lineare zeitinvariante System mit Zustandsdarstellung (A, b, C) modelliert dabei die Torsion (und benutzt im Wesentlichen die Lenkgeschwindigkeit $\dot{\delta}_S$), während die statische Nichtlinearität J die Kardangelenke modelliert; dabei handelt es sich um eine Vereinfachung des exakten analytischen Ausdrucks. Die Parameter des linearen und nichtlinearen Teils wurden getrennt identifiziert, basierend auf Fahrzeugdatensätzen, die hinreichende Informationen im gewünschten Frequenzbereich enthalten, vgl. [14, Kapitel „Experiment Design“]. Bilder 5 und 6 zeigen einige repräsentative Ergebnisse. Bei einem Fahrdynamikmanöver wurde beim Test in Bild 5 eine Drift des Ritzelwinkelsensors simuliert, was sich in einer ansteigenden Abweichung zwischen gemessenem und geschätztem Lenkradwinkel äußert. Beim Test in Bild 6 wurde ein Signalausreisser des Ritzelwinkelsensors simuliert, was sich in einer punktweisen Abweichung zwischen gemessenem und geschätztem Lenkradwinkel äußert.

3.4 Plausibilisierung des Ritzelwinkels

Berechnet wird hier der Ritzelwinkel δ_G aus den beiden vorderen Raddrehzahlen. Grundlage für die Funktion ist

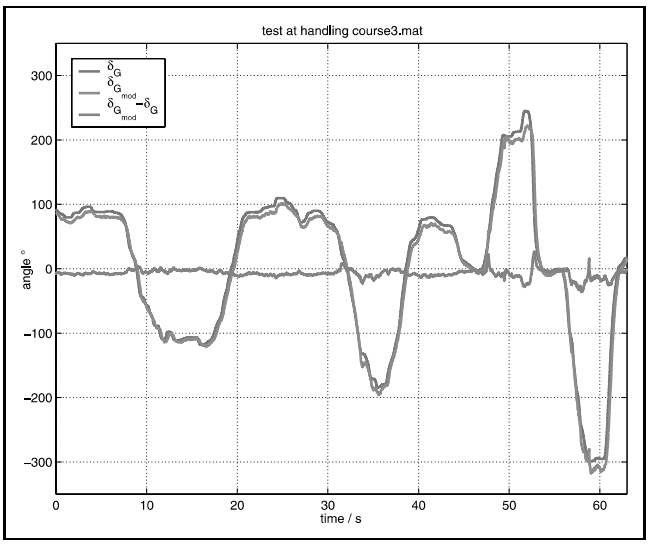

Bild 7: Ritzelwinkelschätzung während eines Handlingkursmanövers: geschätzter Winkel und gemessener Winkel sowie deren bei Null liegende Differenz.

folgende analytische Beziehung, die aus der Fahrzeuggeometrie hergeleitet werden kann [7]:

$$\tan \delta_i = \frac{-I(\omega_i^2 - \omega_o^2)}{S_L \omega_i^2 + \sqrt{S_L^2 \omega_i^2 \omega_o^2 - I^2(\omega_i^2 - \omega_o^2)^2}}. \qquad (3)$$

Hier sind I und S_L Achsabstand bzw. Spurweite, δ_i der Winkel des kurveninneren Rades und ω_i, ω_o die kurveninnere bzw. kurvenäußere Raddrehzahl. Aus Radwinkel δ_i wird dann mittels Lenkgeometrie auf den Ritzelwinkel zurückgerechnet. In Summe entsteht ein Modell mit den beiden Raddrehzahlen als Eingang, den Fahrzeuggeometriedaten in (3) und der Lenkgeometrie als Parameter und dem Ritzelwinkel als Ausgang. Konsequenterweise wurde die Parameteridentifikation in zwei Schritten durchgeführt: Nach Messung von Achsabstand bzw. Spurweite wurde die Lenkgeometrie identifiziert [17], der zweite Schritt ist im Wesentlichen die Identifikation eines Wiener-Modells [3]. In einem weiteren Schritt können dann die Fahrzeugparameter weiter optimiert werden (nichtlineare Optimierung). Wie in [18] kann diese Prozedur dann iterativ fortgeführt werden. Bild 7 zeigt ein Beispielergebnis.

4 Zusammenfassung

Ausgehend vom Begriff „funktionale Sicherheit“ wurden Kennzahlen für sicherheitsrelevante Systeme, insbesondere Obergrenzen für die Wahrscheinlichkeit sicherheitsrelevanter Ausfälle diskutiert. Da eine statistisch zuverlässige Validierung dieser Obergrenzen bei wenigen Prototypen oder kurzer Entwicklungszeit nicht möglich ist, wurde der Zusammenhang zwischen sicherheitsgerichtetem Entwicklungsprozess und sicherheitsrelevante Tests diskutiert. Ein Analyseprozess zur Herleitung von Überwachungsfunktionen aus den obersten Sicherheitsanforderungen wurde skizziert. Schlussendlich wurden zwei modellbasierte Überwachungsfunktionen vorgestellt, die zur Absicherung der Eingangssignale des Active Front Steering der nächsten Generation zum Einsatz kommen werden.

Danksagung

Die Verfasser bedanken sich bei Alexander Krautstrunk und Christian Lundquist für viele wertvolle Hinweise und fruchtbare Diskussionen.

Literatur

[1] S. Amberkar, J.G. D'Ambrosio, B.T. Murray, J. Wysocki and B.J. Czerny. System-Safety Process For By-Wire Automotive Systems. SAE technical paper 2000-01-1056. *SAE World Congress*, Detroit, MI, USA, March 2000.

[2] AUTomotive Open System ARchitecture – AUTOSAR www.autosar.org.

[3] D. Bauer and B. Ninness. Asymptotic Properties of Least Squares Estimates of Hammerstein Wiener Model Structure. *International Journal of Control*, 75(1): 34–51, 2002.

[4] P. Bishop, R. Bloomfield, T. Clement, S. Guerra and C. Jones. Integrity Static Analysis of COTS/SOUP. Proc SAFECOMP, pp.63–76. Edinburgh, Scotland, Sep 2003.

[5] B.J. Czerny, J.G. D'Ambrosio, P.O. Jacob and B.T. Murray. Identifying and Understanding Relevant System Safety Standards for Automotive Systems. SAE technical paper 2003-01-1293. *SAE World Congress*, Detroit, MI, USA, March 2003.

[6] R.J. Evans and J.D. Moffett. Derivation of Safety Targets for Random Failures of Programmable Vehicle based systems. Proc SAFECOMP, Rotterdam, NL. Oct 2000.

[7] T.D. Gillespie. Fundamentals of Vehicle Dynamics. Society of Automotive Engineers, Inc., Warrendale, PA, USA, 1992.

[8] F. Gustafsson. Adaptive Filtering and Change Detection. John Wiley and Sons, Ltd, 2000.

[9] J. Howard. Preserving System Safety Across the Boundary Between System Integrator and Software Contractor. SAE technical paper 2004-01-1663. *SAE World Congress*, Detroit, MI, USA, March 2004.

[10] IEC 61508 – Functional Safety of E/E/PES Systems. International Electrotechnical Commission. Geneve, Switzerland. Oct 1998.

[11] W. Klier, G. Reimann and W. Reinelt. Active Front Steering: Systemvernetzung und Funktionsumfang. VDI Bericht 1828, pp.569–583. Proc AUTOREG. Wiesloch, Germany, Mar 2004.

[12] W. Klier and W. Reinelt. Active Front Steering (Part 1): Mathematical Modeling and Parameter estimation. SAE technical paper 2004-01-1102. *SAE World Congress*, Detroit, MI, USA, March 2004.

[13] J.C. Laprie. Dependable Computing: Concepts, Limits, Challenges. Proc IEEE Intrnational Symposium on Fault Tolerant Computing, Pasadena, CA, USA, 1995.

[14] L. Ljung. System Identification – Theory For the User. Prentice Hall, Upper Saddle River, NJ, USA, 2nd edition, 1999.

[15] MIL-STD-217F: Reliability Prediction Of Electronic Equipment. US Dept of Defense, Washington DC, USA Military Standard 217F, Notice2. Aug 1998.

[16] MIL-STD-1629A: Procedures for performing a FMECA. US Dept of Defense, Washington DC, USA Military Standard 1629A Feb 1998.

[17] W. Reinelt, A. Garulli and L. Ljung. Comparing different approaches to model error modeling in robust identification. *Automatica*, 38(5):787–803, May 2002.

[18] W. Reinelt and S.O. Reza Moheimani. Identification of a flexible beam. Proc. of the 8th International Mechatronics Conference. Enschede, The Netherlands, June 2002.

[19] W. Reinelt and A. Krautstrunk. Safety related development process for electronic steering systems. *SAE World Congress*, Detroit, MI, USA, April 2005. To appear.

[20] SAE ARP 926: Design Analysis Procedure for Failure Modes, Effect and Criticality Analysis. SAE, Troy, MI, USA.

[21] A. Schwarte and R. Isermann. Model-Based Fault Detection of Diesel Intake With Common Production Sensors. SAE technical paper 2002-01-1146. *SAE World Congress*, Detroit, MI, USA, Mar 2002.

[22] M. Thomas. Issues in Safety Assurance. Keynote Talk. Proc of SAFECOMP, pp.1–8, Edinburgh, Scotland, Sep 2003.

[23] M. Woltereck, C. Jung and G. Reichart. How to achieve functional safety and what safety standards and risk assessment can contribute. SAE technical paper 2004-01-1662. *SAE World Congress*, Detroit, MI, USA, March 2004.

Manuskripteingang: 15. Juni 2004.

Dr.-Ing. Wolfgang Reinelt ist seit 2001 als Entwicklungsingenieur bei der ZF Lenksysteme GmbH, derzeit als Teamleiter für funktionale Sicherheit von aktiven Lenksystemen tätig. Seine Hauptinteressensgebiete sind funktionale Sicherheit, Automotive-Anwendungen, robuste Regelungen, Identifikation nichtlinearer Systeme.

Adresse: ZF Lenksysteme GmbH, Richard Bullinger Str. 77, 73527 Schwäbisch Gmünd, Tel.: +49-7171-313110, Fax: +49-7171-3163110,
E-Mail: wolfgang.reinelt@zf-lenksysteme.com

Dr.-Ing. Willy Klier ist seit 2000 als Entwicklungsingenieur bei der ZF Lenksysteme GmbH, derzeit als Teamleiter für Algorithmenentwicklung aktiver Lenksysteme tätig. Seine Arbeitsschwerpunkte sind Nutz- und Sicherheitsfunktionen, Aktuatorregelung, Systemschnittstelle und Systemvernetzung.

Adresse: ZF Lenksysteme GmbH, Richard Bullinger Str. 77, 73527 Schwäbisch Gmünd,
Tel.: +49-7171-312589, Fax: +49-7171-3162589,
E-Mail: willy.klier@zf-lenksysteme.com

Dipl.-Ing. Gerd Reimann ist seit 2000 bei ZF Lenksysteme als Projektleiter für das AFS-System (Active Front Steering/Aktivlenkung) und Leiter der AFS-Grundlagenentwicklung beschäftigt.

Adresse: ZF Lenksysteme GmbH, Richard Bullinger Str. 77, 73527 Schwäbisch Gmünd, Tel.: +49-7171-313193, Fax: +49-7171-3163193,
E-Mail: gerd.reimann@zf-lenksysteme.com

Vorschau auf Heft 2/2005

In unserem nächsten Heft finden Sie unter anderem folgende Themen:

- *J. F. Seara, G. Schmidt:* Gaze Control Strategy for Vision-Guided Humanoid Walking
- *Ch. Brenneke, O. Wulf, B. Wagner:* Autonome Navigation mobiler Systeme in natürlichen Umgebungen durch die Integration von 3D-Laserdaten
- *J. Ch. Schlake, Ch. Preusse, J. Winkelhake, U. Konigorski:* Modellierung einer Direkt-Methanol-Brennstoffzelle

Weitere Informationen über geplante sowie ausführliche Informationen über die in den letzten Heften der **at** erschienenen Beiträge finden Sie im Internet unter http://www.oldenbourg.de

Hinweise für Autoren finden Sie unter
http://www.oldenbourg.de/verlag/stylefiles/autorenhinweise.htm