



FAKULTÄT FÜR **INFORMATIK**

X-by-Wire

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Informatik

eingereicht von

Gerd Wielander

Matrikelnummer 0026165

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung:
Betreuer: Univ.-Prof. Dr.Ing. Gerhard H. Schildt

Wien, 31.10.2008

(Unterschrift Verfasser)

(Unterschrift Betreuer)

Kurzfassung

Der Einsatz von elektronischen Systemen zur Steigerung der Sicherheit und Erhöhung des Komforts hält nun schon seit geraumer Zeit Einzug im Automobilbau. Bremskraftregelung, um blockierenden Rädern entgegenzuwirken, Antiblockiersystem, für eine kontrollierte Abbremsung, Motorsteuerung, für optimierte Effizienz und Dynamik des Antriebsstranges, elektronisches Stabilitätsprogramm, um das Ausbrechen des Fahrzeuges zu verzögern, sind einige der heute bereits bekannten Systeme und haben sich im Automobilbereich etabliert. Die eingesetzten Komponenten sind meist alleinstehende Systeme mit mechanischer Rückfallebene. So werden keine Informationen unter den Komponenten ausgetauscht und die elektronisch bereitgestellten Funktionalitäten spielen lediglich eine übergeordnete Rolle. Ein Ausfall führt dazu, dass das System auf die mechanische Ebene zurückfällt, wodurch die Grundfunktionalität (Lenkung, Bremse) weiterhin gewährleistet ist.

Ein nächster Schritt in der Entwicklung des Fahrzeugbaues ist, die Komponenten untereinander zu vernetzen, wodurch Synergien entstehen und genutzt werden können. Zudem wird angestrebt, die im Prinzip redundant verbaute, mechanische Rückfallebene, durch fehlertolerante elektronische Komponenten zu ersetzen. Harte Echtzeiteigenschaften und Verlässlichkeit sind Voraussetzungen für die Grundfunktionen. Die durchgängige Realisierung auf mehrfach redundanten Systemkomponenten ist erforderlich, so müssen Stromzufuhr, Kommunikationskanäle, Recheneinheiten, Sensoren und Aktuatoren in mehrfacher Ausführung verbaut werden. Mögliche Gefahren durch externe Einflüsse, wie Witterung, Abnutzung, NEMP, usw. müssen in der Architektur berücksichtigt werden. Neue Mensch-Maschine-Schnittstellen werden diskutiert, welche die Benutzerfreundlichkeit, Ergonomie und Sicherheit erhöhen und zudem neue Möglichkeiten der Fahrzeuginnenraumgestaltung bieten. Der Vergleich der Kommunikationsprotokolle CAN und TTP/C diskutiert Vor- und Nachteile. Das gesamte by-Wire-System muss von einer ausfallsicheren Stromversorgung gespeist werden. Hierzu werden redundante Bauweisen lokalen Reserven gegenübergestellt. Nicht vernachlässigt werden dürfen Softwarefehler und müssen durch Softwarediversität und Programm-

ablaufüberwachung vorgebeugt werden.

Ein Ausblick in die Zukunft erlaubt das Thema der Full Collision Avoidance zu diskutieren, wo durch Zusammenspiel der einzelnen Komponenten und die Überwachung des Fahrzeugumfeldes weitgehend alle lauernden Gefahren erkannt und rechtzeitig Vorkehrungen zur Vermeidung von Unfällen getroffen werden können. Interessant wird auch die Kommunikation zwischen Fahrzeugen, was z.B. einen geregelten Kolonnenverkehr ermöglichen würde, oder die Fernsteuerung des Fahrzeuges durch einen Leitreechner.

Abstract

The employment of electrical systems in the automotive area, mostly for security and dynamic reasons, is already known. Braking control, to avoid blocking wheels, anti-lock braking system, for controlled braking, control of the engine, for optimized efficiency and dynamic, electronic stability program, to avoid critical situations, are some of the actually used systems. The build-in components are mostly standing alone systems with a mechanical fall-back level. There is no communication between the systems, and the electronic components work for a higher functional level. The failure of an actually used electronic system, causes the fall-back to the basic functionalities (steering, braking), which are served by the mechanical technology.

A next step in the development is to wire the single components and to make a communication possible. The replacement of the redundantly build mechanical level with fail operational, electric systems follows. A system with hard real-time properties and a high dependability is a precondition for every basic functionality. The use of multiple redundant components in every part of the system (electrical supply, communication, central processor, sensors, actuators) provides a safe functionality. Possible risks of external influences, as like as weather, wear and tear, NEMP, ecc. must be studied and regarded in the architecture. New developed human interfaces are user-friendlier, better for ergonomic and safety reasons and make a new design of the interior fittings possible. The communication protocols CAN and TTP/C are discussed and the use in automobiles is analysed. To provide a fail-safe power supply, the redundant power architecture must be confronted with local power resources. A further, very important topic is the evolution of a safe software. Terms as software diversity and control of the program process are explained and discussed.

Making some future prospects, it becomes interesting to discuss the full collision avoidance, where the whole components are communicating through a common network and, in addition, the environment of the automobile is kept under surveillance by various sensors. So it is possible to prevent for recognized danger. Very interesting is also the communication between au-

tomobiles, what makes an automatic driving in a lane possible. A remote control of a car becomes also makeable, so a centralized host computer can route a car safely.

Inhaltsverzeichnis

1	Themenbeschreibung	1
2	Einleitung	4
2.1	Elektronische Subsysteme	5
2.1.1	Anti-Blockier-System (ABS)	5
2.1.2	Anti-Schlupf-Regelung (ASR)	9
2.1.3	Motorschleppmomentregelung (MSR)	10
2.1.4	Bremsassistent (BAS)	11
2.1.5	Fahrdynamikregelung(FDR - ESP)	12
2.1.6	Brake-by-Wire	17
2.1.6.1	Architektur des Brake-by-Wire Systems	19
2.1.6.2	Elektro-hydraulisches Bremssystem (EHB)	21
2.1.6.3	Elektro-mechanisches Bremssystem (EMB)	22
2.1.7	Steer-by-Wire	23
2.1.7.1	Architektur des Steer-by-Wire Systems	23
2.1.7.2	Eigenschaften	25
2.1.8	Der Weg zu Full Collision Avoidance (F'CAS)	28
2.2	Neue Bedienelemente	31
2.2.1	Sticksteuerung	32
2.2.2	Das Bedienkonzept X-Drive	34
2.2.3	Bedienung mit Lenkrad und Pedalen	35
2.3	Wirtschaftlichkeit	36
2.4	Fly-by-Wire vs. Drive-by-Wire	37
3	Grundlagen und Sicherheitsaspekte	40
3.1	Begriffserklärungen	41
3.1.1	Sicherheit & Zuverlässigkeit	41
3.1.2	Hazards & Risiko	46
3.1.3	Fehler, deren Quellen und Auswirkungen	50
3.1.4	Fehlertoleranz	51
3.1.4.1	Redundanz	54

3.1.4.2	Diversität	57
3.1.4.3	Möglichkeiten für ein Recovery	58
3.2	Der sichere Zustand im KFZ	59
3.3	Elektromagnetische Verträglichkeit - EMV	62
3.4	Gefahr durch NEMP und HPM	65
4	Systemarchitektur	67
4.1	Grundlegende Elemente der X-by-Wire Architektur	68
4.1.1	Zeitbasis	71
4.1.2	Zeitgesteuert - Ereignisgesteuert	73
4.2	Sensoren	74
4.3	Rechnersysteme	79
4.4	Kommunikation	84
4.4.1	CAN - TTCAN	87
4.4.2	TTP	89
4.5	Aktuatoren	93
4.5.1	Aktuatoren für die Bremsanlage	95
4.5.2	Aktuatoren für das Lenksystem	97
4.6	Stromversorgung	98
4.6.1	Lokale Reserven	100
4.6.2	Redundante Energiekreise	101
4.7	Sichere Software	103
4.7.1	Softwarediversität	104
4.7.2	Programmablaufüberwachung	106
4.7.2.1	Zeitliche Programmablaufüberwachung	107
4.7.2.2	Logische Überwachung	108
5	Zusammenfassung & Ausblick	112
5.1	Zusammenfassung	112
5.2	Ausblick	115
	Abkürzungsverzeichnis	A
	Abbildungsverzeichnis	B
	Tabellenverzeichnis	C
	Literaturverzeichnis	D

Kapitel 1

Themenbeschreibung

Im Automobilbereich wird bereits seit mehreren Jahrzehnten der Einsatz von fahrerunterstützenden Systemen zur Steigerung der Sicherheit und Erhöhung des Fahrkomforts forciert. Anfänglich wurden mechanische Systeme entwickelt, welche etwa den Antriebsstrang oder das Bremssystem beeinflussen und dadurch zu einer höheren Sicherheit beitragen. Mit der zunehmenden Forschungsarbeit im Bereich der Mikroprozessoren, deren zunehmender Verbreitung auf dem Markt und die dadurch sinkenden Kosten sowie parallel steigende Performance, wurde der Einsatz im Automobilbereich immer interessanter. Zudem war man mit herkömmlichen, mechanischen Systemen bereits auf Grenzen gestoßen und die geforderte Dynamik in hochsensiblen Regelkreisen, wie der Bremskraftregelung, das Antiblockiersystem, sowie Steuerungen der Motoren oder des Einspritzsystems, drängte zur Entwicklung von dynamischen und flexiblen Lösungsansätzen. Als Konsequenz wurde der Einsatz erster elektronischer Steuerungen in der Kraftfahrzeugtechnik erprobt und schon bald überschritten diese neuen Systeme die Dynamik und Präzision der etablierten mechanischen Vorgängermodelle. Die generelle Skepsis gegenüber elektronischer Steuerungen, besonders im Bereich von sicherheitskritischen Anwendungen, ist jedoch bis heute merklich spürbar und hemmt die Entwicklung und den Serieneinsatz solcher Systeme. Bis heute sind elektronische Regelsysteme im Kraftfahrzeug, welche sicherheitskritische Aufgaben erfüllen, lediglich als übergeordnete Systeme realisiert. Das heißt, dass bei einem eventuellen Ausfall des elektronischen Systems auf das darunterliegende, mechanische System zurückgegriffen werden kann, und somit die Grundfunktionalität in gewissem Maße, trotz Elektronikfehler erhalten bleibt.

Alle Automobilhersteller haben bereits eine Fülle von elektronischen Systemen im Angebot, wie elektronische Bremskraftverteilung (EBV), allseits bekannte ABS-Systeme, Antriebs-Schlupf-Regelung (ASR), verschiedene Fahrdynamikregelungen (darunter fällt unter anderem ESP), elektrohydraulische

Bremse (EHB), automatische Distanzregelung, elektrische Lenkhilfe, Überlagerungslenkung mit Seitenkraftkompensation, Einparkunterstützung, Line-Control, Tote-Winkel-Überwachung u.a.m. Neben den hier genannten Systemen sind aktuelle Fahrzeuge mit einer Fülle von weiteren elektrischen Komponenten ausgerüstet, welche im Bereich Komfort (elektrische Sitzverstellung, automatische Klimatisierung, elektrische Fensterheber, Regensensoren, Lichtsensoren usw.) und multimediale Extras (Radio, Navigation usw.) angesiedelt sind. Bereits bei heutigen Systemen ist eine günstige und zuverlässige Kommunikation zwischen den einzelnen Komponenten dringend erforderlich, welche bereits anhand eines Datenbusses realisiert wird. Die geforderte Interaktion der Subkomponenten nimmt in der Automobilbranche eine zunehmend wichtige Rolle ein, da einerseits die neuen, immer stärker vernetzten Module darauf aufbauen und andererseits die Diagnosefunktionen der Gesamtanlage über die Kommunikationsschnittstelle abgerufen wird. Die Problematik der überdurchschnittlich hohen Ausfallquote und mangelnden Diagnosefähigkeit bei stark vernetzten Oberklassefahrzeugen wurde bereits öffentlich bekannt und mehrere Forschungsgruppen versuchen in diesem Bereich Lösungsansätze zu finden.

Aufbauend auf die aktuellen Systeme existieren einige Pilotprojekte, welche den gesamten Bereich der heute verwendeten elektronischen Komponenten im Fahrzeug revolutionieren und die komplette Steuerung des Fahrzeugs umfassen. Dabei wird versucht, das heute angewandte zwei-Ebenen-System¹ zu eliminieren und diese durch rein elektronische Systeme zu ersetzen. Offensichtlich werden dadurch viele platz- und gewichtsintensive Komponenten am Fahrzeug überflüssig, man denke lediglich an die Bremsleitungen, oder das Lenkgestänge. Der frei gewordene Platz kann für eine neue, sicherheitsgerichtete und ergonomische Bauweise genutzt werden, während durch die Gewichtseinsparung Vorteile im Bezug auf Fahreigenschaften und Verbrauch, und somit des Umweltschutzes, errungen werden. Allerdings müssen die elektronischen Regelkreise in einem derartigen Einsatzgebiet höchste Sicherheitskriterien erfüllen, denn ein Versagen kann verheerende Folgen für Menschen und Material haben und muss deshalb unter allen Umständen verhindert werden.

Im Rahmen dieser Arbeit wird der Einsatz von elektronischen Systemen im Automobilbereich, speziell in sicherheitskritischen Bereichen, untersucht und verschiedene Lösungsansätze gegenübergestellt. Zudem wird das Hauptaugenmerk auf die mögliche Architektur eines X-by-Wire Fahrzeuges gelegt und deren Anforderungen in den Bereichen der Hardware- und Software ana-

¹In aktuellen Fahrzeugen werden in sicherheitskritischen Bereichen mechanische (hydraulische) Rückfallebenen, mit lediglich übergeordneter Elektronik, eingesetzt

lysiert.

Einführend werden grundlegende Begriffe und Prinzipien der elektronischen Komponenten in heutigen Automobilen beschrieben, sowie deren Einsatzgebiet und Funktionsweise kurz erklärt. Dabei wird auf die mögliche Erweiterung derartiger Systeme bezüglich verstärkter by-Wire Technologie eingegangen, und darauf aufbauend die verschiedenen Aspekte kompletter X-by-Wire Systeme erörtert. Anschließend folgt eine Abhandlung der Grundlagen im Bereich der technischen Sicherheit und Fehlertoleranz. Als Schwerpunkt steht das Kapitel über fehlertolerante Rechnersysteme (Hardware, Software, Kommunikation, Sensoren, Aktuatoren, usw.), worin die jeweiligen Architekturen und möglichen Integrationsmodelle beschrieben und einem Vergleich unterzogen werden. Abschließend folgt eine Zusammenfassung der abgehandelten Thematik, sowie die Stellungnahme des Autors.

Kapitel 2

Einleitung

In X-by-Wire-Systemen steuert der Lenker das Fahrzeug nicht direkt über mechanisch verbundene Komponenten, sondern die Steuerbefehle werden elektronisch (by-wire) an den jeweiligen Aktuator weitergegeben und dort ausgeführt. Die X-by-Wire-Steuerung umfasst mehrere Komponenten - Bremsen, Lenkung, Motorsteuerung usw. - für alle diese Steuerbereiche steht das X. Im Grunde ist dabei die Betätigung der Steuerelemente durch den Fahrer, mit der darauf folgenden Ausführung des Steuerbefehls am entsprechenden Fahrzeugteil (z.B. Anziehen der Bremszangen beim Bremsen), energetisch entkoppelt. In Flugzeugen hielt dieses Steuerprinzip bereits seit Ende der 70er Jahre Einzug. Im Automobilbereich haben sich by-Wire-Systeme bisher lediglich in beschränktem Ausmaß etablieren können. Als Beispiel sind die elektronische Motorsteuerung und die Tiptronic-Getriebesteuerung (Shift-by-Wire) zu erwähnen, welche bereits in aktuellen Kraftfahrzeugmodellen nahezu flächendeckend eingesetzt werden.

Der Bedarf an elektronischen Bauteilen und Regelungen bestand bereits lange vor deren ersten effektiven Einsatz. Dies aus dem Grund, da Mikroprozessoren gerade für Steuerungs- bzw. Regelungsaufgaben hervorragend geeignet sind und gegenüber mechanischen Steuerungen sowohl qualitativ als auch quantitativ enorme Vorzüge aufweisen. Jedoch war die Akzeptanz und das Vertrauen in rein elektronische Systeme aufgrund ihrer Unzuverlässigkeit noch keinesfalls gegeben, und die Technologie erster Prototypen war noch keinesfalls für den Serieneinsatz ausgereift.

Durch die zunehmende Miniaturisierung und die gleichzeitige Performancesteigerung der elektrischen Bauteile, wurde die Realisierung immer komplexerer Systeme möglich. Der weit verbreitete Einsatz von Elektronikelementen trieb die Forschung und Entwicklung in diesem Bereich stark an. Als dessen Konsequenz findet man heute bereits in allen Fahrzeugen elektronische Regelungssysteme. Nach der Markteinführung und Serienfertigung in ver-

schiedenen Automodellen, fand eine durchaus positive Preisentwicklung im Segment der Elektronikkomponenten statt, was natürlich weitere Möglichkeiten für deren Einsatz eröffnete.

Beobachtet man die letzten Jahre des Automobilbaues, so kann man den immer stärker werdenden Einsatz von elektronischen Subsystemen, welche den Fahrer in den verschiedensten Situationen unterstützen, deutlich beobachten. Der Einsatz der neuen Technologien ermöglicht die automatische Regelung von immer komplexeren Bereichen. Diese Systeme werden anfänglich meist als zusätzliche Optionals angeboten, halten aber nach deren Etablierung schon bald als Serienausstattung in den verschiedensten Modellen ihren Einzug.

2.1 Elektronische Subsysteme

In den Kraftfahrzeugen werden heute bereits eine große Anzahl an elektronischen Systemen in den verschiedensten Bereichen eingesetzt. Systeme wie AntiBlockierSystem, Antischlupfregelung, Fahrdynamikregelung, automatische Klimaanlage, Navigationssysteme, Multimediazentren und dergleichen sind bereits allseits geläufige Begriffe und jeder Autohersteller hat derartige Subsysteme im Sortiment. Im folgenden wird auf die wichtigsten der heute eingesetzten Systeme eingegangen und deren Zusammenhänge erklärt. Dies soll weitere Möglichkeiten zur Interaktion der einzelnen Komponenten aufdecken und Vorteile und Vorzüge der elektronischen Steuerung und deren Vernetzung darlegen.

2.1.1 Anti-Blockier-System (ABS)

Auf die sicher längste Historie unter den elektronischen Systemen im Automobilbereich kann das, inzwischen serienmäßig eingesetzte, Antiblockiersystem zurückblicken.

Die Problematik des blockierenden Rades beim starken Bremsen beschäftigte Wissenschaftler bereits lange vor der Fertigung des ersten Automobils. Bereits bei Zugbremsen war das Blockieren der Räder ein ungewünschter Zustand, weil dadurch die Räder abgeplattet wurden und somit ihren Rundlauf verloren. Der längere Bremsweg bei stehenden Rädern war damals noch weniger ausschlaggebend für die Suche nach einem möglichen Lösungsansatz. Bereits im Jahre 1903 wurde deshalb ein „Bremskraftregler bei Luftbremsen zur selbsttätigen Verhinderung des Schleifens der Räder von Eisenbahnfahrzeugen“ beim kaiserlichen Patentamt angemeldet. Die Steuerung dieses ersten „Antiblockiersystems“ erfolgte mit, an den Rädern angebrachten, Fliehkraft-

reglern, Seilzügen und Luftauslasshähnen [Rei03]. Dieses Konzept war allerdings alles andere als fehlerunanfällig und robust. Es folgten eine Anzahl verschiedener Lösungsansätze, welche durch Anbringung einer Schwungmasse am jeweiligen Rad die Differenz der Geschwindigkeit dieser trägen Masse und des Rades selbst ermittelten und bei Überschreitung eines bestimmten Schwellwertes die Bremskraft kurz wegnahmen. Für Zugräder waren solche Systeme akzeptabel, da nicht jedes Rad einzeln gebremst werden musste, sondern das Bremsen einer Achse bereits ausreicht. Weiters ist der Freiraum am Rad nicht so eng bemessen wie bei einem Automobil, und auch das zusätzliche Gewicht ist nicht dermaßen ausschlaggebend. Eine weitere Problematik war, dass sämtliche mechanische Systeme für die Bremskraftanpassung viel zu träge reagierten, um damit optimale Werte zu erhalten. Dies stellte Ostwald bereits im Jahre 1940 in seiner Diplomarbeit fest und entwickelte darauf aufbauend ein System, welches die Bremskraft der einzelnen Räder über Magnetventile regulierte [Rei03]. Damit bestand erstmals in der Geschichte der Automobilindustrie das Bedürfnis nach elektromagnetischen Aktuatoren - in diesem Fall nach elektromagnetischen Ventilen.

Nach dem 2. Weltkrieg wurden sogenannte Bremsschlupfregler für Flugzeuge entwickelt, welche das Durchscheuern der Reifen beim Aufsetzen des Flugzeuges verhindern sollten. Erste Aufzeichnungen für den Einbau ähnlicher Anlagen in Personen- und Lastkraftwagen stammen jedoch erst aus dem Jahre 1960. Pilotsysteme wurden zuerst in Rennwagen und teilweise in Polizeifahrzeuge eingebaut. Der Serieneinsatz von ABS-Systemen in Automobilen wurde weiter verzögert, ein Grund dafür war die mangelnde Zuverlässigkeit und Akzeptanz der verwendeten Schaltungstechniken. Erst in den 80er Jahren war das Antiblockiersystem für Automobile erhältlich und fand aufgrund der eindeutigen Vorteile und der mittlerweile ausgereiften Technik auch schleunigst Zustimmung bei den Abnehmern. Die Problematik im Automobilbereich war bzw. ist, dass das Fahrzeug bei einer Vollbremsung mit blockierenden Rädern instabil wird. Zum einen blockieren die Räder bei gleichmäßig verteilter Bremskraft an der Hinterachse schneller als an der Vorderachse, das Fahrzeug wird instabil, neigt dazu ins Schleudern zu geraten und ist nicht mehr kontrollierbar. Weiters erlauben blockierende Vorderräder keine Lenkkorrekturen des Fahrers, da das Fahrzeug über die Vorderachse geradeaus „schiebt“. Ein durchschnittlicher Fahrzeuglenker, welcher nicht für solche Extremsituationen trainiert ist, verliert in solch einem Fall schnell die Kontrolle über das Fahrzeug, was offensichtlich vermieden werden sollte.

Für die Entwicklung von Bremssystemen stellt also neben dem bestmöglichen Verzögerungswert auch die Stabilität und Kontrollierbarkeit des Fahrzeuges ein wichtiges Augenmerk dar. Die Regelungsanlage muss in einem breiten Geschwindigkeitsbereich korrekt funktionieren (etwa von 250 km/h

bis zum Stillstand), und soll sich auch an verschiedene Beschaffenheiten der Fahrbahnoberfläche (Splitt, Eis, Schnee, Regen, u.a.) anpassen. Darüber hinaus muss das System robust gegen auftretenden Fehlern sein.

Aktuelle Systeme verwenden Massesensoren, um die Drehverzögerung bzw. -beschleunigung der einzelnen Räder zu messen. Diese Daten werden an ein elektronisches Steuergerät weitergeleitet, welche die einzelnen Daten filtert und aufbereitet, die momentane Radgeschwindigkeit und Fahrzeuggeschwindigkeit errechnet und anhand der aktuellen Pedalstellungen die Stellbefehle für die ABS-Magnetventile erzeugt. Letztere regulieren die Bremskraft an den einzelnen Rädern und verhindern durch kurzen Druckablass das Blockieren derselben. Moderne ABS-Anlagen steuern die einzelnen Räder gezielt mit den optimalen Brems Eingriffen an.

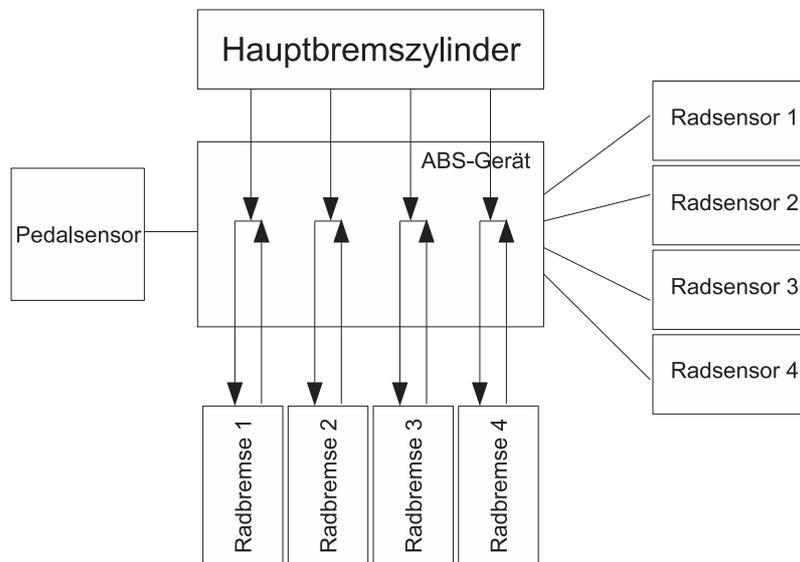


Abbildung 2.1: Aufbau eines ABS-Gerätes

Für die Umsetzung dieser hoch-präzisen Bremsbefehle reicht der herkömmliche zweigeteilte, hydraulische Bremskreis nicht mehr aus, sondern muss durch entsprechende Komponenten erweitert werden, um eine höhere Dynamik beim Abbremsen eines einzelnen Rades zu erreichen. Dazu werden die vom Hauptbremszylinder zu den einzelnen Radbremszylindern führenden Bremsleitungen in jeweils doppelte Kanäle getrennt. Hochdynamische Elektromagnetventile können den Durchfluss in jeder Leitung schnell schließen bzw. öffnen und führen dadurch die von der ABS-Steuerung errechneten Eingriffe am entsprechenden Radbremszylinder aus. Im Normalzustand sind die vier Zuleitungen zu den Radbremsen geöffnet, während die jeweiligen

Rückleitungen, die für den Druckablass beim Blockieren der Räder verwendet werden, geschlossen sind.

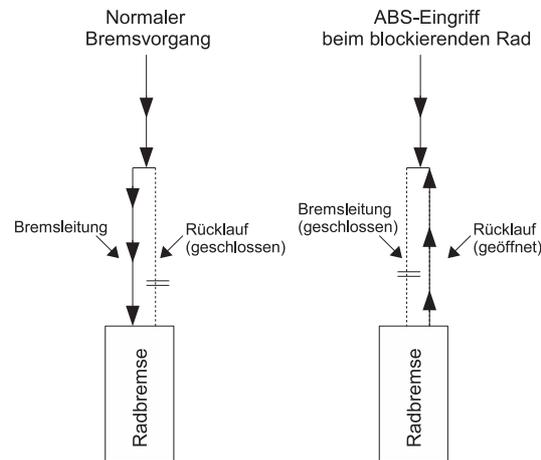


Abbildung 2.2: Eingriff des ABS-Systems

Der Einbau mechanischer Druckfedern in allen Elektromagnetventilen sorgt auch bei einem Ausfall der elektronischen Ebene, für die Gewährung der Bremsleistung. Wird das Bremspedal betätigt, wirkt der Bremsdruck vom Hauptzylinder über die offenen Kanäle direkt auf die Radbremszylinder. Das ABS-Gerät wertet periodisch die Radbeschleunigung aller vier Räder aus und erkennt durch einen überdurchschnittlich negativen Beschleunigungswert, dass das entsprechende Rad zum Blockieren neigt. Um dem entgegenzuwirken, wird zunächst das offene Ventil geschlossen, um den im Bremszylinder erreichten Druck konstant zu halten. Nimmt die Blockierneigung dadurch nicht ab, wird die Rückleitung durch das, bis dahin geschlossene Ventil, kurz geöffnet. Die Bremsflüssigkeit gelangt nun zurück in die Bremsleitung zwischen Hauptbremszylinder und geschlossenem Ventil. Der Bremsdruck am Radzylinder sinkt und die Radbeschleunigung wird wieder positiv, worauf sich das zuvor geschlossene Ventil wieder öffnet und der Regelkreis beginnt erneut (Abb.2.2). Die Grenzen der Regelung in dieser Bauweise sind gleich der physikalischen Grenzen der Hydraulik. Um die Dynamik der ABS-Anlage weiter zu steigern, bedarf es neu konzipierter und speziell auf derartige Anforderungen abgestimmter Bremskomponenten, wie elektromagnetische Bremsaktuatoren. Die Leistung letzterer kommen allerdings erst in Kombination mit einer kompletten Brake-by-Wire Lösung vollständig zum Tragen.

2.1.2 Anti-Schlupf-Regelung (ASR)

Mit der Entwicklung des ABS eng verbunden sind die Anti-Schlupf-Regelungssysteme bzw. Systeme zur Traktionskontrolle. Sie verhindern das Durchdrehen der Räder bei der Beschleunigung des Fahrzeuges und erhöhen dadurch die Fahrstabilität. Die Geschwindigkeiten der angetriebenen Räder werden jenen der nicht angetriebenen Achse (entspricht der tatsächlichen Fahrzeuggeschwindigkeit) gegenübergestellt, wodurch ein zu starker Schlupf erkannt werden kann¹. Es kann nun auf zwei verschiedene Wege eingegriffen werden, um einen bevorstehenden Traktionsverlust zu vermeiden. Als erster Lösungsansatz kann ein kurzer Bremsengriff am entsprechenden Rad vorgenommen werden. Dadurch arbeiten jedoch Motor und Bremse gegeneinander, weshalb die Dauer des Bremsengriffes streng überwacht werden muss. Um eine Beeinträchtigung des Bremssystems zu vermeiden, darf die Intensität des Bremsengriffes eine bestimmte Obergrenze keinesfalls überschreiten. Die zweite, und komponentenschonendere Variante, ist die Drosselung der Motorleistung. Die einfache Gaswegnahme ist dafür jedoch zu unpräzise und nicht fein genug dosierbar. In die Nähe der gewünschten Eigenschaften gelangt man durch zusätzliche Verstellung der Drosselklappen (nur bei E-Gas²), durch Verstellen des Zündzeitpunktes oder durch eine kurzfristige Kraftstoffabschaltung für einen einzelnen oder alle Zylinder.

Beide Systeme haben Vorzüge aber auch Nachteile und keine der angeführten Lösungsansätze befriedigte die Fahrzeugingenieure durchaus. Deshalb hat man eine Kombination von Brems- und Motoreingriff für die weitere Entwicklung von Traktionskontrollen in Betracht gezogen. Die Art und Weise der Regelung ist jedoch von mehreren Faktoren abhängig. So beeinflusst das Drehmoment des Motors und die Art der Bremsanlage (ABS, Bremssysteme mit Hochdruckspeicher) die Regelung bereits deutlich. Zudem muss die Anwendung in mehrere Bereiche eingeteilt werden: Verstärkte Reduzierung des Motordrehmoments sowie gezielte Bremsengriffe beim Anfahren (unter 10 km/h). Bei hohen Geschwindigkeiten wird das Motormoment bereits bei beginnender Tendenz zum Durchdrehen zurückgenommen, während Bremsengriffe in diesem Zustand äußerst unwahrscheinlich sind, da die Fahrstabilität dadurch negativ beeinträchtigt werden könnte.

Die ASR-Regelung verfügt also neben dem ABS über ein weiteres Regel-

¹Bei allradgetriebenen Fahrzeugen werden die Radgeschwindigkeiten untereinander gegenübergestellt. Differenzen über einem bestimmten Schwellwert bzw. physikalischen Beschleunigungsgrenzen, lassen auf Schlupf schließen.

²Bei E-Gas oder Throttle-by-Wire Systemen wird die Position am Gaspedal durch Sensoren ermittelt und über elektronische Regelungssysteme an das ebenfalls elektronische Motormanagement weitergegeben

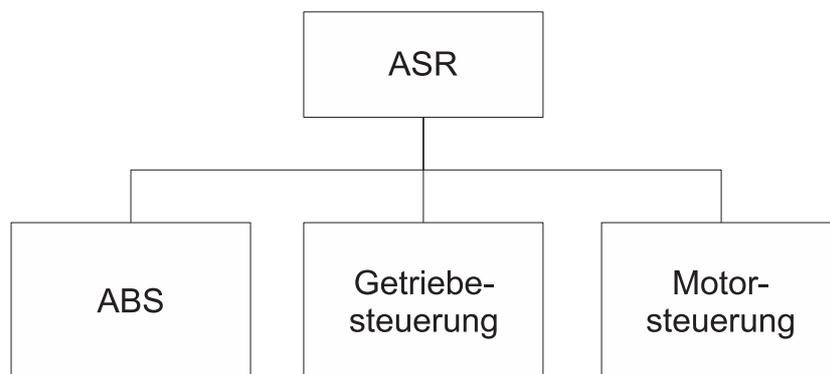


Abbildung 2.3: Aufbau einer ASR-Steuerung

system, welches jedoch teilweise die selben Komponenten der ABS-Anlage verwendet (Sensoren, Magnetventile). Des weiteren müssen die Bremsen bei Verwendung des ASR-Systems auch einzeln ansteuerbar sein, was zusätzliche Trennventile in den Bremskreisen erfordert, welche den Bremskreis auf ein einzelnes Rad abtrennen. Diese Modifikation erfordert zudem einen ASR-Druckbegrenzungsventil, was überschüssige Bremsflüssigkeit umleitet und eine Beschädigung des Bremskreislaufes verhindert. Es wird also bereits offensichtlich, dass der verstärkte Einsatz von vernetzten elektronischen Komponenten vorteilhaft und teilweise signifikant einfacher wäre. So wäre das ASR-System mit vorhandenen Brake-by-Wire und Throttle-by-Wire Systemen lediglich eine zusätzliche Anforderung im vernetzten Regelsystem bzw. sogar durch ein Update an der Regelungssoftware realisierbar, während auf eine umständliche Modifikation der bestehenden Brems- bzw. Hydraulikanlage verzichtet werden könnte.

2.1.3 Motorschleppmomentregelung (MSR)

Das Motorschleppmoment oder Motorbremsmoment hat, besonders bei stark motorisierten und hinterradgetriebenen Personenwagen, deutlich spürbare Auswirkungen auf die Stabilität des Fahrzeuges und muss deshalb überwacht werden. Bei der Gaswegnahme entsteht ein Schleppmoment, wodurch das Fahrzeug über die Antriebsräder gebremst wird. Dabei entsteht besonders auf glatter Fahrbahn ein nicht zu vernachlässigender Bremsschlupf. Auch das Zusammenspiel mit einem ABS-System ist in solch einer Situation nicht mehr einwandfrei. Abhilfe schafft nur eine zusätzliche Motor-Schleppmoment-Regelung (MSR). Auch diese interagiert mit dem ABS-System und informiert letzteres über den auftretenden Bremsschlupf an den jeweiligen Rädern. Zusätzlich kommuniziert das MSR-System mit dem Getriebe- und Motorma-

nagement, wodurch der Bremsschlupf durch eine Leerlaufstellung des Antriebsstranges beseitigt wird. Dies erfordert aber das Vorhandensein eines E-Gas-Systems.

Die starke Verbindung zwischen den einzelnen Komponenten ist offensichtlich feststellbar und die problematische Adaptierung der bestehenden Komponenten wird immer deutlicher erkennbar.

2.1.4 Bremsassistent (BAS)

Der Bremsassistent greift bei einer Notbremsung des Fahrzeuges aktiv ein und unterstützt den Fahrzeuglenker in dieser Gefahrensituation. Bei der Untersuchung typischer Notsituationen, welche zu einer Vollbremsung führen, wurde festgestellt, dass sich Fahrer, welche für eine derartige Gefahrensituation nicht genügend Erfahrung haben, durchaus verschieden reagieren und oftmals nicht die gewünschten maximalen Verzögerungswerte erreichen. Durch die Schockreaktion wird das Bremspedal zwar schnell betätigt, der erforderliche Druck auf das Bremspedal wird jedoch oft nur kurz aufgebracht oder erst gar nicht erreicht. Die Gründe dafür sind vielfältig, unter anderem das typische Vibrieren am Bremspedal, herbeigeführt durch das Regelungssystem des ABS. Durch die nicht optimale Betätigung der Bremsen, verlängert sich der erforderliche Bremsweg deutlich, was unter Umständen zu einem Unfall führen kann. In diesem Bereich setzt der elektronische Bremsassistent an und versucht den Fahrzeuglenker in derartigen Situationen aktiv zu unterstützen.

Die erste Anforderung an das BAS-System ist offensichtlich die Erkennung einer anstehenden Gefahrensituation. Dies scheint für ein automatisiertes System auf den ersten Blick eine nicht triviale Herausforderung darzustellen, da natürlich unzählige Faktoren für solche Entscheidung berücksichtigt werden müssen und deren Erkennungsmerkmale lediglich unscharf definiert werden können. Untersuchungen ergaben jedoch, dass die Fahrzeuglenker in kritischen Situationen, nach Überwindung einer gewissen Schreckenssekunde, das Bremspedal deutlich schneller (etwa 3 mal so schnell) betätigen als bei der Bremsung in einer normalen Verkehrssituation. Zudem kann eine abnormale, übermäßig schnelle Bewegung bereits bei der Gaswegnahme erkannt werden. Um dies zu erkennen, muss die Pedalgeschwindigkeit, mit welcher Gas und Bremse vom Fahrer betätigt werden, überwacht werden. Da das Bremspedal in herkömmlichen Automobilen direkt mit der Membran des Unterdruckverstärkers verbunden ist, kann die Pedalgeschwindigkeit direkt aus dem Membranweg, differenziert nach die Zeit, errechnet werden, oder es werden spezielle Sensoren in die Pedalerie integriert, welche die gewünschten

Informationen ermitteln.

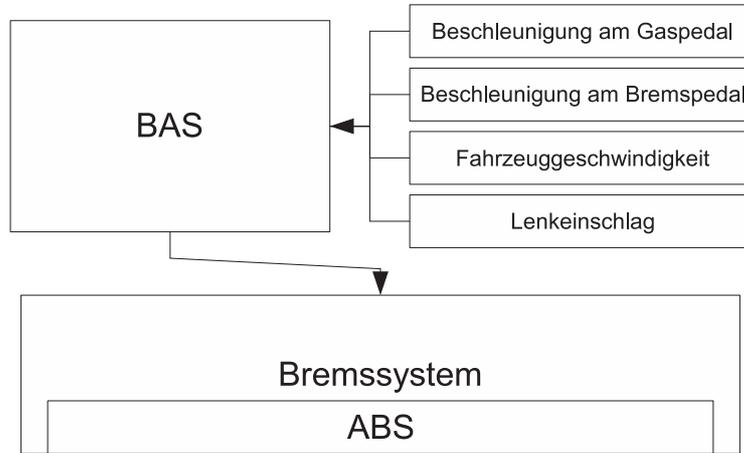


Abbildung 2.4: Aufbau eines Bremsassistenten

Zudem werden Bremspedalweg und ein Lernalgorithmen, welcher das Zusammenspiel von Bremspedal und Fahrzeugverzögerung in den normalen Situationen vergleicht, analysiert, um eine vorliegende Notsituation mit einer gewissen Sicherheit erkennen und klassifizieren zu können. Wird eine Notbremssituation festgestellt, sorgt das BAS-System für die Erzeugung der vollen Bremskraft, auch wenn die aktuelle Pedalstellung lediglich zu einer geringeren Bremskraft führen würde. Das Blockieren der Räder wird durch das parallel in Kraft tretende Regelungssystem des ABS verhindert. Einen Abbruch der Notbremsung deutet der Fahrer mit der Zurücknahme des Bremspedals an. Heute eingesetzte BAS-Steuergeräte sind oftmals über einen CAN-Bus mit der restlichen Fahrzeugelektronik verbunden und entscheiden in kurzen Perioden immer wieder ob eine Notbremssituation vorliegt. Anzumerken ist erneut die Interaktion zwischen mehreren Subsystemen, sowie die Steuerung auf elektronischer Ebene, während die Ergebnisse an das darunterliegende hydraulische System weitergegeben und von diesem ausgeführt werden. Diese mehrmalige Energieumwandlung beeinflusst die Dynamik des Regelungssystems und ist ausschlaggebend für gewisse Abstriche in der Performance.

2.1.5 Fahrdynamikregelung(FDR - ESP)

Aufbauend auf die Systeme ABS und ASR dient das Fahrdynamiksystem zur weiteren Stabilisierung des Fahrzeuges. Es wird dabei die Querdyna-

mik des Automobiles in allen Zuständen miteinbezogen³, und mittels kurzen Bremsingriffen wird im Rahmen der physikalischen Möglichkeiten versucht, ein neutrales Fahrverhalten zu bewahren. Besonders bei Kurvenfahrten mit hoher Geschwindigkeit oder bei unvorhersehbaren Ausweichmanövern (legendärer Elchtest) tritt das ESP in Kraft. Das System kann erweitert werden, indem zusätzlich einstellbare Federbeine eingebaut werden. Damit können im Rahmen der verbesserten Querdynamik, zusätzliche Adaptierungen vorgenommen, und dadurch eine bessere Straßenlage erzielt werden. Wiederum soll das System den Normalfahrer lediglich in Extremsituationen unterstützen, und dies auf eine für den Fahrer möglichst transparente Art - sodass der Fahrer die Eingriffe im besten Fall gar nicht bemerkt.

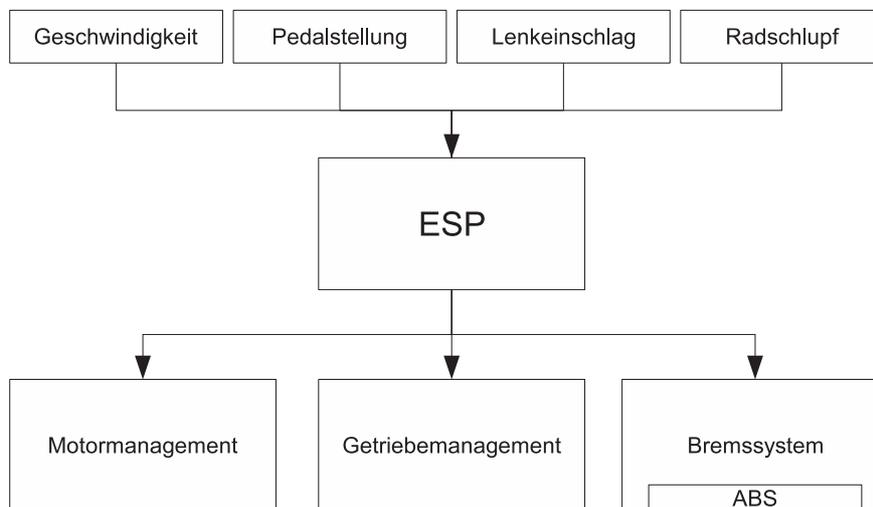


Abbildung 2.5: Aufbau einer ESP-Steuerung

Das System funktioniert, indem das vom Fahrzeuglenker vorgegebene Sollverhalten erfasst und mit dem Istverhalten des Fahrzeuges abgeglichen wird. Das Sollverhalten wird durch Stellung des Gaspedals, dem Bremsdruck im Bremssystem und dem Einschlag des Lenkrades ermittelt. Der laufend aktualisierte Zustand des Fahrzeuges wird anhand mehrerer Sensoren ermittelt und setzt sich primär aus Raddrehzahl, Querbewegung, Bremsdruck und Giergeschwindigkeit⁴ zusammen. Dieser Fahrzustand wird periodisch (ca. 150 mal pro Sekunde) mit dem Sollzustand, welchen der Fahrer vorgibt, abgeglichen. Wird eine deutliche Abweichung zwischen Soll- und Istzustand

³Im Gegensatz zur hier beschriebenen Fahrdynamikregelung, regelt das ABS die Stabilität lediglich während der Betätigung des Bremspedals

⁴Giergeschwindigkeit: Geschwindigkeit der Drehbewegung des Fahrzeuges um seine Hochachse, d.h. Änderung der Fahrzeugposition im Vergleich zur Fahrtrichtung

festgestellt, so greift das Stabilitätsprogramm ein, indem, ähnlich wie beim ABS und ASR, Eingriffe in das Motormanagement und das Bremssystem vorgenommen werden. Die permanente Berechnung dieser Stellgrößen aus den Mess- bzw. Schätzwerten (Fahrzeuggeschwindigkeit, Reifenschlupfwert) ist keineswegs trivial und erfordert beträchtliche Rechenleistung. Deshalb werden Mikroprozessoren eingesetzt, um die komplexen Rechenschritte mit vordefinierter Antwortzeit durchführen zu können. Da das ESP-Modul Sensorwerte (Raddrehzahl, Motorendrehzahl, Pedalstellungen, usw.) und Aufgaben anderer Steuergeräte (Bremseingriffe über ABS-Anlage, Eingriffe in Zündzeitpunkt oder Kraftstoffeinspritzung über Motorenmanagement) und benötigt, wird auch hier wieder eine Kommunikation zwischen den einzelnen Sensoren und Steuergeräten erforderlich.

Die hier beschriebenen Systeme sind heute bereits in vielen Automodeln serienmäßig integriert, die elektronische Steuerung ist jedoch zum großen Teil durch ein herkömmliches, mechanisches Backup gesichert. Dabei wird die eigentliche Umsetzung der Stellbefehle durch mechanische Systeme bewerkstelligt. Diese werden dem Einsatz übergeordneter Systeme, mit teilweise recht komplexen Regelungssystemen, entsprechend adaptiert (wie im Beispiel des ASR bereits beschrieben). Die Ideen und Möglichkeiten für weitere unterstützende Funktionen wachsen aber ständig und die Realisierung der unteren (Ausführungs-)Ebene stellt zunehmend ein Hindernis dar, welches momentan anhand zusätzlicher Modifikationen umgangen wird.

Automatische Distanzregelung (ADR), welche den Abstand zum nächsten Fahrzeug anhand eines Radargerätes misst und, falls notwendig, das Fahrzeug selbständig bremst, ist in Oberklassefahrzeugen bereits erhältlich. Darauf aufbauend wird an einem System F2S (Follow to Stop) bzw. Stop and Go entwickelt, welches in der Lage ist, das Fahrzeug, hinter einem vorausfahrenden Mobil, bis zum völligen Stillstand zu bringen. Zusätzlich ist mit einem solchen System der Grundstein für eine automatische Notbremse gelegt, was den unmittelbar bevorstehenden Aufprall bei einem Unfall, durch Detektion eines Hindernisses erkennt und völlig automatisch eine Notbremsung einleitet. Dadurch wird versucht den Unfall noch rechtzeitig zu vermeiden, bzw. dessen Folgen bestmöglich zu lindern.

Mit dem Einsatz von Line-Control-Systemen, welche den Fahrer bei unbeabsichtigtem Verlassen der Fahrspur warnen, werben einige Automobilhersteller bereits massiv. Solche Systeme überwachen mit Kameras die Fahrspur und erkennen die Überquerung der Fahrbahnmarkierungen. Zusätzlich wird an sogenannten Aufmerksamkeitskontrollen (AMK) gearbeitet, die durch eine im Fahrzeuginnenraum installierte Kamera den Lidschlag des Fahrzeuginsassers

beobachtet. Bei voller Aufmerksamkeit des Fahrers sind die Augen weit geöffnet, der Lidschlag ist kurz und erfolgt in relativ langen Intervallen. Ermüdet der Fahrer, nimmt die Augenöffnung ab und der Lidschlag häufiger. All diese gemessenen Daten werden vom AMK-System analysiert. Überschreiten die Messdaten einen Schwellwert, so wird der Fahrer gewarnt und zum Einlegen einer Erholungspause aufgefordert. So will man dem Problem des Sekundenschlafes entgegenwirken. Des Weiteren sind bereits Projekte angefallen, welche automatisch die Verkehrsschilder entlang der Fahrbahn erkennen und die aktuell geltenden Vorschriften digital im Cockpit anzeigen, wodurch der Fahrzeuginsasse sich nicht mehr dermaßen auf die Verkehrsschilder konzentrieren muss. Die Firma Siemens VDO hat bereits im Jahr 2006 die Verkehrszeichenerkennung aus dem Projekt pro.pilot vorgestellt. Das sogenannte TSR-System (Traffic Sign Recognition) von VDO beobachtet die Fahrzeugumgebung mit einer Kamera. Die Auswertungs Elektronik des Bordcomputers wertet die gefilmten Daten aus und überschlägt diese zudem mit den Informationen aus dem gekoppelten Navigationssystem. Die ermittelten Informationen werden dem Fahrer über ein Kombiinstrument oder ein Head-up-Display eingeblendet. Eine automatische Anpassung der Geschwindigkeit an die erlaubte Höchstgeschwindigkeit wäre darüberhinaus durchaus denkbar.

Im Bereich der Fahrdynamikregelung wird zur Zeit noch stark entwickelt. Auf dem Markt existieren bereits einige integrale Fahrdynamikregler, welche alle betroffenen aktiven Komponenten (Antrieb, Bremse, Lenkung und Fahrwerk) in die Regelung mit einbeziehen. Dadurch erhält man bessere Voraussetzungen für einen elektronischen Regelungseingriff und nähert das Fahrverhalten weiter an die physikalischen Grenzen an. Die Systeme erlauben auch verschiedene Einstellungsmöglichkeiten direkt per Knopfdruck, so kann beispielsweise zwischen sportlicher oder komfortabler Fahrdynamikregelung selektiert werden.

Einige Fahrzeughersteller (Mercedes, BMW, VW) haben bereits automatische Einparksysteme vorgestellt, welche das Fahrzeug eigenständig in eine Parklücke rangieren. Diese Thematik erscheint zwar recht spektakulär, weshalb die weitverbreitete Meinung existiert, die dahinterliegende Technik sei enorm aufwendig und nur schwer realisierbar. Eine Kombination aus Steer-by-Wire und elektronischer Motorsteuerung, sowie den notwendigen Abstandssensoren am Fahrzeug, ermöglicht das automatische Einparken jedoch ohne großem Zusatzaufwand. Die benötigten Komponenten wären in einem kompletten X-by-Wire Fahrzeug ohnehin bereits vorhanden.

Im Rahmen der Sicherheit sind zunehmend starke Entwicklungen im Bereich der Tote-Winkel-Erkennung und der Rundumüberwachung zu verzeichnen. Sensoren rund um das Fahrzeug nehmen die aktuelle Situation wahr

und rekonstruieren diese modellartig. Gewisse Gefahrensituationen können dadurch erkannt, und gegebenenfalls Gegenmaßnahmen eingeleitet werden. Eine Weiterentwicklung solcher Systeme ist die sogenannte Enhanced Night Vision [ENV]. Ziel ist es bei nächtlichen Fahrten, anhand infrarotgestützter Sensoren, mögliche Gefahrenquellen (Personen, Hindernisse) zu erkennen und den Fahrer bereits zu warnen, bevor dieser das bevorstehende Hindernis erblicken kann. Ähnliche Systeme werden für den Einsatz bei schlechtem Wetter (Nebel, Schneefall, Regen) entwickelt.

Als Krönung der heutigen Entwicklungsergebnisse haben die verschiedenen Automobilhersteller Fahrzeuge mit Full Collision Avoidance (F'CAS) im Visier. Das Zusammenspiel der verschiedenen hier beschriebenen Komponenten soll es zukünftig ermöglichen, Gefahren sicher zu erkennen und diese bereits im Vorfeld zu eliminieren.

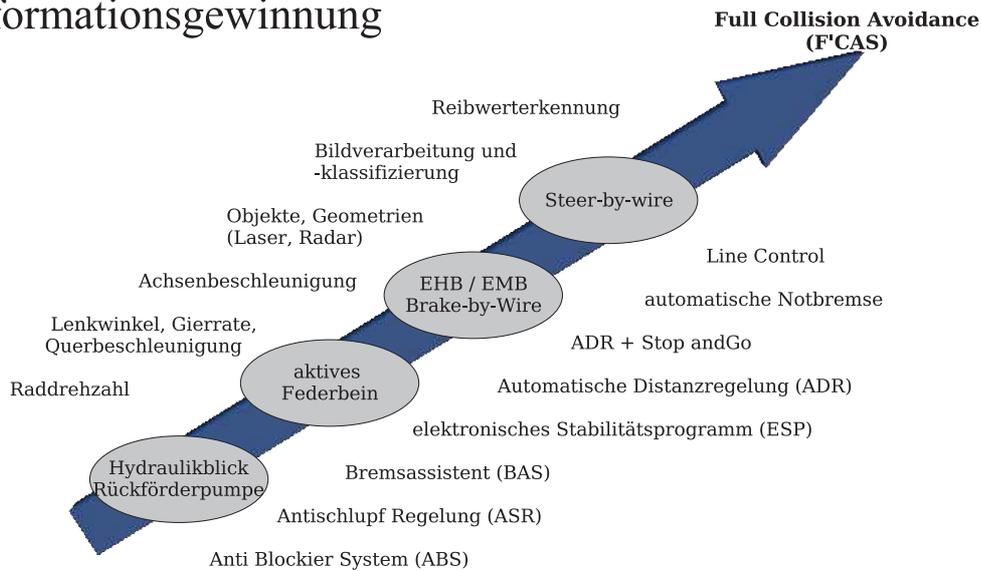
Auch die neu eröffneten Möglichkeiten im Bereich der Kommunikation und Navigation sind enorm. So wäre es technisch realisierbar, dass Fahrzeuge durch zentrale Leitreechner automatisch ferngesteuert werden, oder mit futuristischen Multimediakomponenten für ein mobiles Büro ausgestattet werden. Diese Bereiche fallen weniger in den Bereich der aktiven Fahrsicherheit und werden an dieser Stelle nicht weiter diskutiert.

Einige der hier genannten Systeme sind weder voll ausgereift, noch bereit für den Serieneinsatz, aber die zunehmende Rechenleistung und Speicherkapazität, bei gleichzeitig fallenden Kosten im Mikroelektronikbereich, fördert die Entwicklung ungemein. Deshalb ist man an dem Punkt angelangt, wo die mechanischen Systeme eigentlich die Entwicklung des Fahrzeuges hemmen, und es wird an eine Ersetzung der, bisher kosten- und zieloptimierten Hardware, durch eine leistungsfähige, umfangreiche und zuverlässige elektronische Regelung gedacht bzw. bereits gearbeitet. Dabei entfällt die heute übliche mechanische Verbindung zwischen den verschiedenen Bedienelementen im Fahrzeuginneren und dem jeweiligen Wirkungsfaktor und wird durch eine elektronische Übertragung ersetzt. In einem solchen Konzept wäre die Installation eines neuen Systems oftmals denkbar einfach, indem den bereits vorhandenen Reglern eine modifizierte Software mit den neuen Funktionalitäten eingespielt wird. Als Beispiel kann bei vorhandener ABS und Motorsteuerung eine zusätzliche Antischlupfregelung auf diesem Wege eingebaut werden, da benötigte Sensoren, Aktuatoren und Kommunikationskanäle bereits vorhanden sind und dafür genutzt werden können.

Um solche, heute noch futuristischen Projekte zu realisieren, muss im Vorfeld die grundlegende Fahrzeugsteuerung (Lenkung, Antrieb und Bremse) durch by-Wire Systemen realisiert werden, damit später übergeordnete Systeme auf deren Funktion zugreifen können. Da die Motorsteuerung und die Getriebesteuerung heute bereits auf elektronischem Wege geregelt wird,

und bereits auf dem Markt ist, wird auf deren Ausführungen hier verzichtet. Die beiden folgenden Abschnitte beschreiben die Funktionsweise von Brake-by-Wire-Systemen und Steer-by-Wire-Systemen.

Informationsgewinnung



Mechatronik Assistenzsysteme

Abbildung 2.6: Entwicklung der Informationsgewinnung und Assistenzsysteme im Fahrzeug

2.1.6 Brake-by-Wire

Definition: Das Brake-by-Wire-System leitet den Bremsbefehl, welcher mittels eines Sensors am Bremspedal erfasst wird, an ein Steuergerät. Der dort berechnete Output gelangt auf elektrischem Weg zu den Aktuatoren (Stellleinheit am Bremssattel). Der in konventionellen Bremssystemen übliche mechanische (hydraulische) Kraftschluss vom Pedal zu den Bremsen entfällt hierbei gänzlich.

In Serienfahrzeugen werden heute keine reinen Brake-by-Wire Bremssysteme eingesetzt. Darüber hinaus schreibt der Gesetzgeber das Vorhandensein einer mechanischen Rückfallebene vor, da die Mindestbremsleistung auch bei ausgefallenen elektrischen Systemen gewährleistet werden muss [BBW]. Momentan befinden sich erste elektro-hydraulische-Systeme (EHB) auf dem

Markt. Ähnliche Konzepte werden für aktuelle Parkbremsen eingesetzt, wodurch die klassische Handbremse mit zugehörigem Seilzug durch einen einfachen Knopf ersetzt wurde.

Die hydraulische Bremse wurde vor allem im Laufe der letzten Jahre immer mühsamer an die Erfordernisse der aktuell eingesetzten Mechatroniksysteme (ABS, ASR, ESP) angepasst. Diese Systeme erfordern, wie bereits in den vorangehenden Kapiteln beschrieben, radselektive Bremsengriffe, weshalb die ursprünglichen zwei Bremskreise um zusätzliche Hydropumpen und Magnetventile erweitert werden mussten. Dies erschwert den ohnehin bereits komplizierten Einbau der Bremsleitungen, welche mit Bremsflüssigkeit gefüllt, entlüftet und auf Dichtigkeit hin geprüft werden müssen. Zudem hat die hydraulische Bremse folgende prinzipielle Nachteile:

- Mehrfache Energieumwandlung. Die Bremskraft aus der Betätigung des Bremspedals wird zunächst im Unterdruckverstärker (sofern Servobremse vorhanden) verstärkt, danach im Hauptbremszylinder in hydraulischen Druck umgewandelt. Dieser gelangt über die Bremsleitung an die Radbremszylinder, wo der Druck in eine Zuspännkraft umgesetzt wird.
- Einbauort. Der Druckverstärker liegt, aufgrund der mechanischen Verbindung zum Pedal, direkt im Motorraum, wo er kostbaren Platz wegnimmt.
- Unterschiedliche Verzögerungswerte. Die Bremskraft des Fahrers führt nicht immer zur gleichen Fahrzeugverzögerung, sondern ist von mehreren Faktoren wie Beladung oder Zustand der Bremsen (Temperatur, Abnutzung) abhängig.
- Störung. Der, die Bremskraft verstärkende Unterdruckverstärker benötigt Vakuum, welches vom Verbrennungsmotor erzeugt wird. Die Entnahme dieses Vakuums kann die Abgasregelung des Ottomotors stören.

All diese negativen Eigenschaften der herkömmlichen (hydraulischen) Bremsanlage treiben die Industrie zur Entwicklung eines neuartigen Konzeptes, wo der eigentliche Bremswunsch des Fahrers und die daraus resultierende Bremsbetätigung nicht mehr direkt verbunden sind, sondern an ein leistungsfähiges Regelsystem übermittelt und von diesem optimiert wird. Dieser Zentralrechner bestimmt die von der aktuellen Situation abhängige, optimale Stellgröße der Radbremsen und übermittelt diese an die jeweiligen Aktuatoren. Solch ein System lässt sich mit dem heutigen Stand der Technik nur durch ein voll elektronisch arbeitendes Bremssystem (Brake-by-Wire oder elektro-mechanische Bremse EMB) erreichen.

Diese Art der Bremstechnik macht den Einsatz von sperrigen Komponenten wie Unterdruckverstärker, Bremszylinder und Bremsleitungen überflüssig und bietet dadurch mehr Freiraum im Motorraum. Weiters bietet diese Technologie großen Spielraum im Bereich des Package des Fahrzeuges. Beispielsweise sind beim Ausbau des Cockpits weniger Randbedingungen zu beachten, da die Verbindung lediglich über leicht zu verlegende Datenbussleitungen stattfindet und nicht mehr durch direkter mechanischer Kopplung.

2.1.6.1 Architektur des Brake-by-Wire Systems

Der Umstieg vom herkömmlichen, bereits über viele Jahrzehnte eingesetzten und immer weiter verbesserten mechanischen Bremssystem auf ein neues, elektronisch geregeltes System sehr schwierig und bedarf einer enormen Überzeugungsarbeit. Neben der Entwicklung eines zuverlässigen Systems, muss dieses vom Gesetzgeber erst anerkannt werden, denn das Vorhandensein einer mechanischen Rückfallebene bei Bremssystemen ist gesetzlich vorgeschrieben. Weiters muss sich der Normalfahrer an das neue System gewöhnen, die von ihm gebotenen Vorzüge kennenlernen und es letztlich akzeptieren. Dazu bedarf es ausfallsicherer und über lange Zeit zuverlässig betreibbarer Elektronikkomponenten, welche den Entwurf einer sicherheitsrelevanten Architektur erlauben. Zudem muss die Fehlerdiagnose vereinfacht werden und eine serienreife Anwendung erlauben.

Das zukünftige Brake-by-Wire System kann in mehrere Ebenen geteilt werden, welche über Datenbussysteme miteinander verbunden sind. Die oberste Ebene stellt die Schnittstelle zum Fahrer dar. Bei der Realisierung dieser Schnittstelle herrscht, dank der by-Wire Technologie, große Freiheit. Es kann weiterhin mit Fußpedalen gearbeitet werden, wo redundante Sensoren den Bremswunsch des Fahrers ermitteln. Denkbar wäre beispielsweise auch ein Drehpotentiometer am Lenkrad, oder ein Stick in der Mittelkonsole, oder an der Türinnenseite (ähnlich wie sie in der Luftfahrt zunehmend eingesetzt werden).

Die nächste Ebene stellt das zentrale Bremsenmanagement für das Fahrzeug dar, welches die gemessenen Daten an der Benutzerschnittstelle sowie jene der restlichen Sensoren im Fahrzeug erhält. Zusatzfunktionen wie ABS, ASR, ESP usw. werden hier zentral realisiert. Prinzipiell kann der Funktionsumfang durch Veränderung der Software beliebig angepasst und erweitert werden. Dieser Zentralrechner muss fehlertolerant (fail operational) arbeiten. Das bedeutet, dass die Grundfunktion des Bremssystems trotz auftretendem Fehler erhalten bleiben muss. Um das zu erreichen, muss die Anlage mindestens aus drei parallelen Systemen bestehen, deren Ergebnisse einem Vergleich (auch der Vergleich muss fail-safe arbeiten) unterzogen werden. Stimmen die

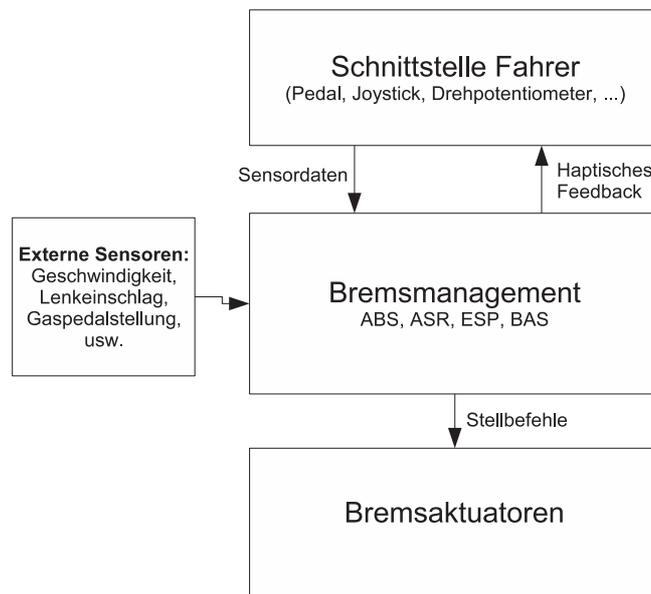


Abbildung 2.7: Prinzipaufbau des Brake-by-wire-Systems

Ergebnisse nicht überein, so kann das fehlerhafte System erkannt werden, während die Gesamtfunktion, durch die restlichen beiden Systeme, gewährleistet wird (2 von 3 System). Um die Wahrscheinlichkeit eines Ausfalles weiter zu senken, bzw. Fehlertoleranz mehrerer gleichzeitiger Fehler zu gewährleisten muss die Anzahl der parallelen Systeme (heiße Reserven) erhöht werden.

Die unterste Ebene bilden die vier Radbremsmodule, welche jeweils aus einem Mikrocontroller und einer elektromotorischen Bremse (Aktuator) bestehen. Diese führen die Befehle des Zentralrechners aus der mittleren Ebene aus. Realisiert werden die Aktuatoren durch Elektromotoren, kombiniert mit geeigneten Getrieben. Innerhalb von Millisekunden muss ein Druck von mehreren Tonnen aufgebracht werden, wozu das heutige Bordnetz mit 12V jedoch nicht mehr ausreicht. Man tendiert hier zu einer Erhöhung der Bordspannung auf 42V, oder die Spannungsspitzen bei geforderten Extrembelastungen (etwa einer Vollbremsung) werden durch Pufferung in zusätzlichen Akku's abgedeckt. Die zusätzliche Pufferung ermöglicht die Funktion der Bremsanlage auch nach einem Ausfall des Hauptgenerators für einige Zeit. Diese Aktoren sind jedoch erst in der Entwicklungsphase. Deshalb kristallisieren sich bei der Realisierung der Brake-by-Wire Lösung folgende Entwicklungsschwerpunkte heraus:

- Die Bedienung. Verwendbare Systeme, welche die Wünsche des Fahrers entsprechend übersetzen, müssen konstruiert und ausreichend getestet

werden.

- Bereitstellung der Bremskraft. Die enormen Bremskräfte, welche bei aktuellen Fahrzeugen benötigt werden, müssen auf elektro-mechanischem Weg bereitgestellt werden. Die Entwicklung neuer, robuster Systeme wird angestrebt.

Da die elektromechanische Bremse noch nicht reif für den Serieneinsatz ist, sondern noch reichlich Entwicklungsarbeit besteht, wurde bis zu deren Lösung eine Zwischenstufe eingeschoben. Als Übergangslösung wird deshalb die elektro-hydraulische Bremse für Kraftfahrzeuge eingesetzt. Dabei regelt eine elektronische oberste Ebene die darunterliegende hydraulische (herkömmliche) Bremsanlage.

2.1.6.2 Elektro-hydraulisches Bremssystem (EHB)

Der Aufbau der EHB ist ähnlich der Architektur des Brake-by-Wire Systems. Unterschiedlich ist lediglich die untere Ebene, welche in diesem Fall hydraulisch realisiert wird. Der am Pedal gemessene und klassifizierte Fahrerwunsch wird an das elektronische Steuergerät übermittelt. Zusätzlich erhält das Steuergerät externe Daten (Raddrehzahlen, Giermoment, Querschleunigung) und ermittelt daraus den Bremsdruck an den einzelnen Rädern. Funktionen wie ABS, ASR usw. sind bereits in dieser zentralen Steuereinheit realisiert. Die resultierenden Outputdaten werden an das hydraulische Steuergerät weitergegeben, welches die darunterliegende, hydraulische Bremsanlage ansteuert. Beim Betätigen des Bremspedals wird das Pedal sofort von der vorhandenen direkten hydraulischen Anlage entkoppelt, auch die Rückmeldungen über das Pedal (angemessener Pedalwiderstand, typisches Ruckeln beim Einsetzen des ABS) werden im Normalfall direkt von der Steuereinheit errechnet und je nach Wunsch im Pedal erzeugt. Erst wenn die obere, elektronische Ebene in einen Fehlerzustand geraten sollte, wird diese komplett vom System getrennt und das hydraulische Bremssystem steht als Notsystem direkt zur Verfügung.

Die in herkömmlichen Bremssystemen eingesetzten Unterdruckverstärker und Hauptbremszylinder werden hier durch ein Motor-Pumpen-Speicher-Aggregat ersetzt. Eine elektrische Pumpe befördert die Bremsflüssigkeit in einen Hochdruckbehälter. Dadurch kann stets, auch ohne Betätigung des Bremspedals, ein stufenlos dosierter Bremsdruck an die Radbremsen weitergeleitet werden, was bei ASR und ESP Regelungen erforderlich ist.

Elektro-hydraulische Bremsen und elektrische Parkbremsen werden heute in Oberklassefahrzeugen bereits eingesetzt, der Einsatz der mechanischen Rückfallebene erfordert jedoch zusätzlichen Gewichtsaufwand und erweist sich deshalb als störend. Zudem erscheint es als sinnvoller, die verwendete

Elektronik mit erforderlichem Mehraufwand für den Einsatz in sicherheitskritischen Anwendungen aufzurüsten, als die geforderte Redundanz mühevoll mit einer mechanischen Rückfallebene zu erreichen.

2.1.6.3 Elektro-mechanisches Bremssystem (EMB)

Im Vergleich zu der EHB entfällt hier das komplette Hydrauliksystem. Vom Bremsbefehl bis hin zum Aktuator erfolgt die gesamte Kommunikation auf elektrischem Weg. Der enorme Vorteil dieses Systems ist der Gewinn an Dynamik. So entfällt das verzögerte Ansprechverhalten des Bremskraftverstärkers, und lästige Geräusche von Hydraulikpumpen und Schaltventilen gehören der Vergangenheit an.

Erste Tests an Prototypen lassen eine Reduzierung des Bremsweges um bis zu 40% erkennen. Aufgrund neuer Bedienelemente, sowie fahrerunterstützenden Systemen, erhält man die Verkürzung der Reaktionszeit des Fahrers bis zu einer halben Sekunde. Zudem erklären das Zusammenspiel der einzelnen Sensoren, die Berechnung der optimalen Bremskräfte je Fahrzeuggrad, sowie die zusätzlich beschleunigte Ausführung der Stellbefehle an den Bremszangen, diese großartigen Ergebnisse.

Synonym zum EHB-Systemen werden die Signale vom Bremspedal, sowie weitere externe Signale, zum Zentralrechner geleitet, welcher wiederum die optimalen Ausgangsgrößen berechnet. Nun müssen diese jedoch nicht mehr in hydraulischen Druck umgewandelt werden, sondern die Soll-Bremsmomente werden direkt an die Mikrocontroller in den einzelnen Radbremsen weitergeleitet. Nach Berechnung der optimalen Stellungen der Bremszangen, werden diese durch elektromechanische Stellmotoren versucht zu erreichen.

Fahrzeugingenieure entwickeln zur Zeit noch daran, den höheren Anforderungen bei der Energieversorgung gerecht zu werden. Es ist unumgänglich, dass das EMB-System über ein redundantes, völlig unabhängiges Energienetz versorgt wird. Der Ausfall der Energie in einem System ohne mechanischer Rückfallebene ist keinesfalls tragbar. Weiters ist die aktuell gängige Bordspannung von 12V entschieden zu gering. An einem Vorderrad benötigt man etwa 500W um eine Bremskraft von 30kN aufzubringen. Diese Leistung kann bei einer Notbremsung unter Umständen über mehrere Sekunden erforderlich sein. Dabei wäre mit dem 12V Bordnetz eine Stromstärke von etwa 42 Amperen erforderlich. Dermaßen hohe Ströme sind herkömmliche Bordnetze nicht gewachsen. Deshalb wird für den Einsatz von EMB-Systemen ein weiteres Bordnetz mit voraussichtlich 42V erforderlich sein.

2.1.7 Steer-by-Wire

Steer-by-Wire ist ein System, bei dem die Lenkbefehle von einem Sensor an der Mensch-Maschine Schnittstelle (z.B. Lenkrad, Steuerstick) ermittelt und über ein zentrales Steuergerät elektrisch zum Aktuator geleitet werden, welcher den Lenkbefehl auf die Räder überträgt.

Parallel zum Brake-by-Wire-Prinzip entfallen auch hier sperrige und schwere mechanische Verbindungen, welche in herkömmlichen Fahrzeugen die einzelnen Komponenten der Lenkung verbinden. Motivation für die Entwicklung dieses neuartigen Lenksystems geben vor allem einige unerwünschte Eigenschaften der herkömmlichen, recht starren mechanischen Kopplung:

- Verletzungsgefahr durch die Lenksäule. Die mechanische Verbindung des Lenkrades erfordert den Einsatz einer Lenksäule. Trotz verstärkten Bemühungen und auch einigen Neuerungen auf diesem Gebiet, ist und bleibt die Lenksäule bei einem Frontalaufprall eine drohende Gefahr für den Fahrer. Lediglich der Verzicht auf diese metallische Verbindung beseitigt diese Gefahr gänzlich.
- Geringe Dynamik. Die mechanische Verbindung ist nur in einem geringen Maß bzw. überhaupt nicht flexibel. Die Lenkübersetzung ist nahezu linear und bietet nicht die Möglichkeit, zwischen langsamen Fahrten (wie in der Stadt, oder beim Parken) und schnellen Fahrten (wie etwa auf der Autobahn) zu differenzieren.
- Nachteile bei der Innenraumgestaltung und Geräuschabdämmung. Die Lenksäule muss in einem gewissen Bereich vom Motorraum ins Fahrzeuginnere reichen. Dies muss einerseits bei der Gestaltung des Fahrzeuginnenraumes berücksichtigt werden, andererseits bedarf es im Motorraum einer gewissen Anordnung der Komponenten. Durch die mechanische Verbindung besteht offensichtlich eine Schwachstelle in der Geräuschdämmung. Motorgeräusche dringen dadurch in den Fahrzeuginnenraum und beeinträchtigen den gebotenen Fahrkomfort.

Da die aktuelle Entwicklung im Kraftfahrzeugbau mit mechanischen Systemen immer häufiger an ihre Grenzen stößt, wird auch im Bereich der Lenkungssysteme versucht, ein neues Konzept, mit verstärktem Einsatz von elektronischen Komponenten, voranzutreiben.

2.1.7.1 Architektur des Steer-by-Wire Systems

Es besteht wiederum der Bedarf eine neue Benutzerschnittstelle zu entwickeln. Auch wenn weiterhin ein Lenkrad zur Angabe des Fahrerwunsches

verwendet wird, überträgt dieses die Lenkbewegungen nicht mehr direkt über eine physische Verbindung, sondern sie werden von verschiedenen Sensoren ermittelt. Zudem erhält der Fahrer bei herkömmlichen Systemen über das Lenkrad Rückmeldungen vom Fahrzeug bzw. von der Untergrundbeschaffenheit (Lenkwiderstand, Vibrationen, usw.). Diese Eigenschaften entfallen bei einer rein elektronischen Kopplung der Komponenten. Deshalb ist man bemüht, derartige Meldungen am Bedienelement künstlich zu erzeugen. Die Tendenz führt dahin, die Rückmeldungen an den Fahrer durch zusätzliche Aktuatoren zu simulieren, welche sich einer Kombination aus akustischen, optischen und haptischen Signalen bedienen.

Nach Erkennung und Klassifizierung des Lenkbefehls durch die Sensoren am Bedienelement, wird dieser über einen Datenbus zum Zentralrechner übertragen. Dieser bestimmt zusätzlich die aktuelle Fahrsituation, indem weitere externe Signale ausgewertet werden. Anhand dieser Informationen bestimmt der Zentralrechner die optimale Sollgröße der Lenkeinstellung, welche wiederum über den Datenbus an die einzelnen Aktuatoren übermittelt werden.

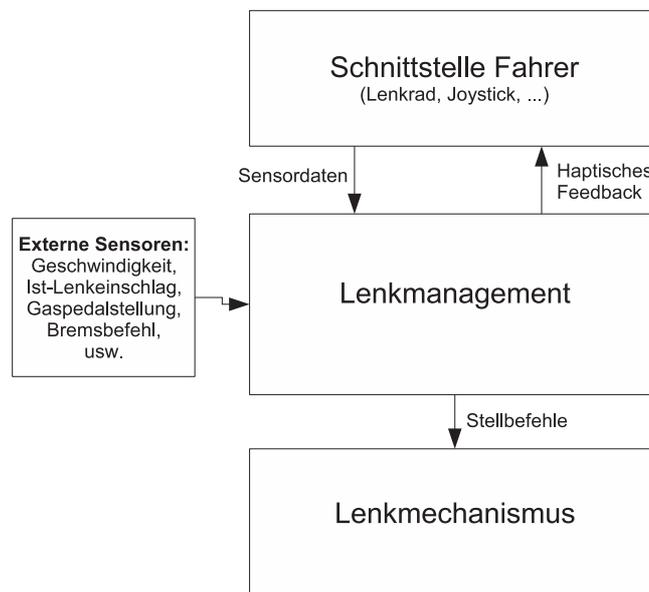


Abbildung 2.8: Diagramm eines Steer-by-wire-Systems

Die an den einzelnen Aktuatoren eintreffenden Daten stellen den Sollzustand der Lenkung dar. Die Aktuatoren selbst sind auch mit Mikrocontrollern ausgestattet, welche laufend damit beschäftigt sind den effektiven Lenkeinschlag, der vom Master erhaltenen Sollvorgabe anzunähern. Über elektromechanische Stellkomponenten wird der Lenkeinschlag der Räder verändert.

Auch in diesem Konzept, wo auf die mechanische Rückfallebene gänzlich verzichtet wird, ist es zwingend erforderlich, die Elektronikkomponenten als ein fehlertolerantes und robustes Energie- und Datennetzwerk auszulegen, welches bestimmte Grundfunktionen auch nach Auftreten von Systemfehlern garantieren kann (fail operational).

2.1.7.2 Eigenschaften

Neben den bereits beschriebenen Eigenschaften bietet ein ausgereiftes Steer-by-Wire System eine Menge positiver Gesichtspunkte [FHK⁺01]. Einige nennenswerte Bereiche dafür sind:

- Package
 - Platzbedarf
 - Umbau Rechts- / Linkslenker
 - Montage
 - Möglichkeiten in der Cockpitgestaltung
- Komfort
 - variable Lenkübersetzung
 - variable Lenkcharakteristik
 - keine Störeinflüsse von Antriebsstrang oder Fahrbahnbeschaffenheit
 - automatisches Einparken
- passive Sicherheit
 - verringerte Lenkradintrusion
 - Alternative Bedienelemente
 - Crashoptimierte Innenraumgestaltung / Package
- aktive Sicherheit
 - Erweiterung der fahrdynamischen Regelungen
 - Höhere Fahrstabilität durch Seitenwindausgleich
 - Interaktion mit ESP

Package. Die Aufgabe des Bereiches Package besteht in der fachübergreifenden Definition und Überprüfung der Bauräume und Referenzmaße des Gesamtfahrzeuges. Dabei müssen neben stilistischen und technischen Gesichtspunkten vor allem Vorgaben im Bereich Usability berücksichtigt werden, da in diesem Entwicklungsschritt stets der Mensch und dessen Interessen als künftiger Fahrzeugnutzer im Mittelpunkt stehen.

Durch die Ersetzung der mechanischen Verbindung vom Lenkrad zu den Rädern durch elektrische Komponenten, entsteht eine Menge freier Bauraum. Dieser kann offensichtlich für ein vorteilhafteres Package verwendet werden. Je nach Art des Bedienelementes sind dennoch einige Randbedingungen gegeben. Wird etwa ein Lenkradaktuator eingesetzt, muss dieser dennoch an der bisher gewohnten Stelle platziert werden, was keinen Platzgewinn im Fahrzeuginnenraum bedeutet. Verwendet man jedoch alternative Bedienelemente, wie z.B. Sidesticks, so gewinnt man auf der Fahrerseite deutlich an Freiraum, was vielfältige Möglichkeiten für die Cockpitgestaltung mit sich bringt. Grundsätzlich ist die Platzierung des Bedienelementes jedoch nicht mehr an einen festen Ort gebunden, sondern kann aufgrund der relativ einfachen und kostengünstigen Verkabelung frei variieren.

Diese angenehmen Nebenerscheinungen der Steer-by-Wire Lenkung bringt vor allem Vorteile bei der Montage. Rechts- und Lenkslenkerfahrzeuge können etwa identisch gebaut werden, lediglich der Platz für das Bedienelement muss beidseitig vorgesehen werden. Zudem erleichtert sich der Arbeitsschritt der „Hochzeit“⁵, da im Bereich der Lenkung keine mechanischen Teile passgenau ineinander geführt, sondern lediglich elektrische Kontakte sicher verbunden werden müssen. Zudem entfällt bei rein elektromechanischen Systemen die Befüllung und Entlüftung des Hydrauliksystems.

Komfort. Ein enormer Vorteil zeichnet sich durch die Möglichkeit der dynamischen Lenkübersetzung aus. Da das Lenkrad mit den Rädern über Datenbusse und dem Zentralrechner verbunden wird, ist es mit geringem Aufwand möglich, die Lenkübersetzung an die fahrdynamischen Eigenschaften des Fahrzeuges anzupassen. So kann die Lenkung bei geringer Geschwindigkeit direkter erfolgen, um den Fahrer das Rangieren auf Parkplätzen oder in engen Straßen, wie etwa in der Innenstadt zu erleichtern, während bei Fahrten mit hohen Geschwindigkeiten die Lenkung zunehmend indirekter abgestuft wird. Dadurch ergibt sich insgesamt eine bessere Kontrollierbarkeit des Fahrzeuges. Bei mittlerer Geschwindigkeit (etwa 80 km/h) soll die Übersetzung jener der konventionellen Lenkung entsprechen.

⁵Im Fahrzeugbau wird als Hochzeit die Zusammensetzung der großen Teilkomponenten, wie Fahrwerk, Motor und Karosserie verstanden

Zudem kann dem Fahrer anhand verschiedener Einstellungen ein individuelles Lenkgefühl vermittelt werden. So kann ein eher sportlicher Fahrer größere Rückstellmomente bevorzugen, während der auf Komfort bedachte Fahrer, im Gegenzug dazu, kleine Momente favorisiert. Derartige Effekte werden durch unterschiedliche Konfigurationen des Lenkaktuators möglich und sind nur ein Teil der denkbaren Individualisierungsmöglichkeiten des Steer-by-Wire Systems. Da auch die Rückmeldung des Antriebes und der Fahrbahnbeschaffenheit ohne direkte mechanische Verbindung entfällt, können in diesem Bereich beliebige Signale⁶ erzeugt werden, welchen den Fahrer etwaige Situationen anzeigen.

Wird das Steer-by-Wire System mit Parksensoren und einer Brake-by-Wire-Anlage kombiniert, ist durch deren Kombination auch eine Realisierung des automatischen Einparkens möglich, wobei sich das Fahrzeug ohne Einwirkung des Fahrzeuginnenlenkers in eine freie Parklücke rangiert.

Passive Sicherheit. Bei konventionellen Lenkungssystemen verbindet die Lenksäule das Lenkrad mit dem Lenkgestänge. Durch die verbindende Anbringung des Lenkrades und der dazugehörigen starren, metallischen Verbindung vor dem Fahrzeuginnenlenker, stellt dies bei einem Frontalzusammenstoß eine Gefahr der Lenkradintrusion ins Fahrzeuginnere dar. Dabei besteht offensichtlich ein enormes Verletzungsrisiko für den Fahrer. Durch den Einsatz einer rein elektronischen Lenkung wird diese Gefahr entschärft, da keine direkte Verbindung besteht, und die meisten Komponenten in nicht crashrelevante Bereiche verlegt werden können. Wird anstatt eines Lenkradaktors eine Sticksteuerung herangezogen, bringt dies verstärkt neues Potenzial im Bereich der passiven Sicherheit. Durch den Entfall des sperrigen Lenkrades vergrößert sich die Bewegungsfreiheit des Fahrers, was parallel eine Vergrößerung des Überlebensraumes bei einem Unfall darstellt. Zudem kann durch den Entfall der Pedale an einer crashoptimierten Fußraumgestaltung gearbeitet werden. Ergänzt wird dieses Sicherheitskonzept durch den Einsatz neuer Airbagkonzepte, welche den Verletzungsgefahren im Fuß-, Oberkörper- und Kopfbereich entgegenwirken.

Aktive Sicherheit. Die Interaktion der einzelnen elektronischen Komponenten, sowie die direkte und gezielte Ansteuerung der Aktuatoren, ohne Verzögerungen und Verzerrungen durch zwischengeschaltete mechanische Komponenten, bietet nun weitaus mehr Möglichkeiten in das Fahrverhalten des

⁶Es besteht die Auswahl zwischen akustischen, optischen oder haptischen Signalen. Jede Art hat ihre Vorteile und auch Kombinationen sind denkbar. Als Grundsatz gilt jedoch, den Fahrer durch übermäßige Interaktivität nicht zu überfordern.

Kraftfahrzeuges einzugreifen. Dabei wird der vom Fahrer am Bedienelement angezeigte Lenkwunsch nicht mehr direkt umgesetzt, sondern dient lediglich als Indikator für die gewählte Fahrtrichtung. Vom Zentralrechner wird indes ein erwartetes Fahrzeugverhalten errechnet, welches mit den gemessenen Daten verglichen wird. Resultierende Abweichungen werden vom Rechner durch Änderung der Winkel an den Vorderrädern autonom korrigiert. Auf diesem Weg ist es möglich in Grenzsituationen (schnellen Spurwechseln, zu hohen Kurvengeschwindigkeiten, drohendes Ausbrechen des Hecks, usw.) zusätzliche Lenkkorrekturen durchzuführen, welche sogar mit gezielten Bremsingriffen des vorhandenen ESP-Systems kombiniert werden können. Im letzteren Fall koordiniert ein überlagerter Fahrdynamikregler Lenk- und Bremsingriffe, wodurch die physikalischen Obergrenzen der Fahrzeugstabilität nahezu erreicht werden, was letztlich der Sicherheit der Fahrgäste zugute kommt.

2.1.8 Der Weg zu Full Collision Avoidance (F'CAS)

Wie in den vorhergehenden Abschnitten bereits deutlich ersichtlich wurde, ermöglicht der zunehmende Einsatz von Sensoren, elektronischen Rechensystemen, elektromechanischen Aktuatoren und deren verstärkte Kommunikation und Interaktion untereinander weitaus größere Unterstützungsmechanismen. In den Augen verschiedener Automobilherstellern gipfelt das Zusammenspiel der verschiedenen Komponenten in der sogenannten Full Collision Avoidance (F'CAS).

Damit solche Systeme die Serienreife erlangen, ist, wie in vielen anderen Fällen, eine schrittweise Vorgangsweise notwendig. Aktuelle Fahrzeuge, vorwiegend aus dem Segment der oberen Mittel- und Oberklasse, bieten bereits einige Pre-Crash Maßnahmen. Das Zusammenspiel verschiedener, bereits bestehender Signale und Auswertungen lässt auf einen unmittelbar bevorstehenden Unfall schließen. In solch einem Fall kann der richtige Einsatz der vorhandenen Schutzmaßnahmen unter Umständen Leben retten.

Die bestehende Vielzahl an Fahrerassistenzsystemen kann hinsichtlich ihres Funktionsumfanges wie folgt klassifiziert werden:

- Assistenzsysteme
 - Informationsvermittlung und Warnung
 - Verbindliche Anweisungen
- Aktiver Eingriff
 - korrigierender Eingriff
 - (teilweise) Übernahme der Fahrzeugbeeinflussung

Analog dazu können die verschiedenen Fahrzustände wie in Abbildung 2.9 kategorisiert werden.

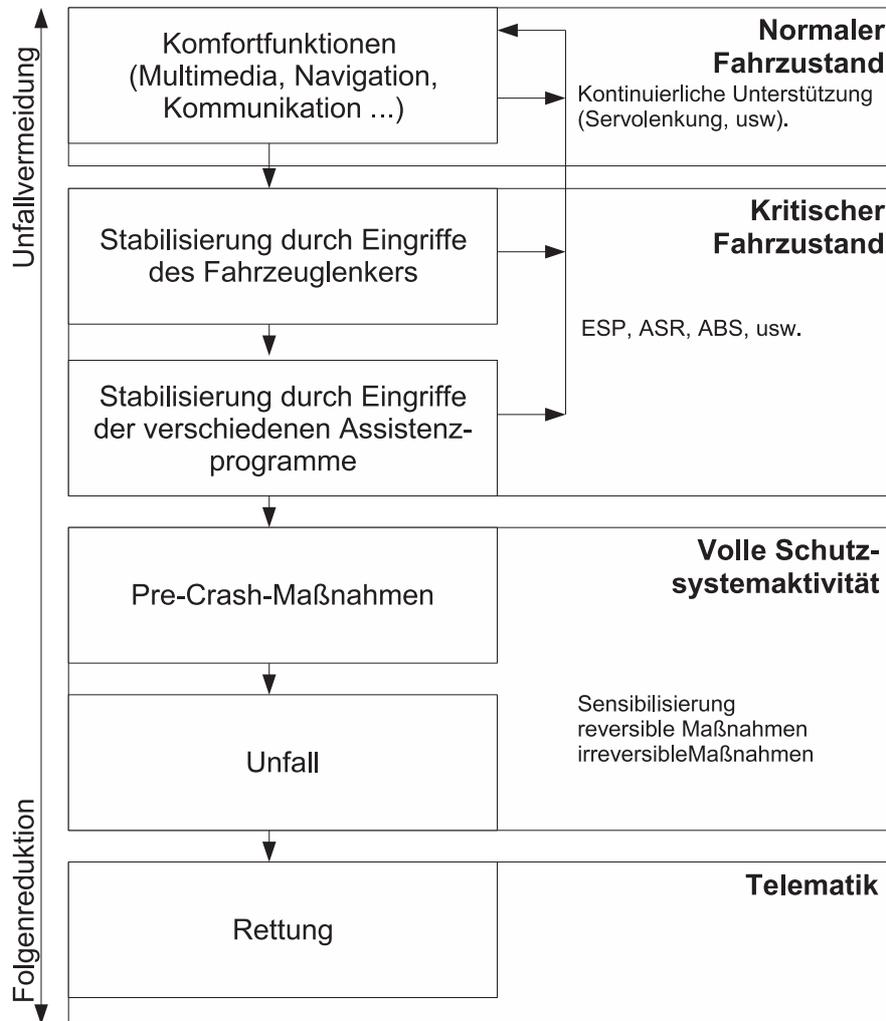


Abbildung 2.9: Assistenzsysteme vom Normalzustand bis zum Unfall

In der ersten Kategorie, dem normalen Fahrzustand, stehen dem Fahrer Navigationssystem, Multimediaunterstützung, automatische Klimatisierung, Sitzpositionsverstellungen usw. zur Verfügung. Sie dienen also hauptsächlich zur Erhöhung des Komforts. Die verschiedenen Sensoren messen laufend die Fahrzeugdaten und erkennen gegebenenfalls einen kritischen Fahrzustand. Je nach Art und Einstufung der Situation wird der Fahrer gewarnt, oder das System versucht selbst in die Dynamik des Fahrzeuges einzugreifen, um dessen Stabilität wiederzuerreichen bzw. zu erhöhen. Sind die Eingriffe vergebens,

begibt sich das Fahrzeug in den Zustand der vollen Schutzsystemaktivitäten. Dabei befindet man sich unmittelbar vor einer Unfallsituation und folgende Pre-Crash Maßnahmen werden durchgeführt:

- Sensibilisierung
 - Sensibilisierung der Steuergeräte (es werden Schwellwerte herabgesetzt, um auf auftretende Situationen empfindlicher zu reagieren, wodurch wertvolle Zeit gewonnen werden kann)
- Auslösen von reversiblen Maßnahmen
 - Moderate Bremsung (automatisch)
 - Reversible Gurtstrammung
 - Fenster und Schiebedach schließen
 - Öffnen der Airbagklappen (ohne diese jedoch aufzublasen)
- Auslösen von reversiblen und irreversiblen Maßnahmen
 - Notbremsung durchführen (Bremsassistent)
 - Notlenkung (um ggf. Hindernissen auszuweichen)
 - Gurtstrammung
 - Auslösen der Airbags

Falls der Unfall durch diese Maßnahmen nicht mehr verhindert werden kann, wird zumindest versucht, die Folgen des Unfalls so weit als möglich zu reduzieren. Im Falle eines aufgetretenen Unfalls wäre es denkbar, dass die Fahrzeugelektronik dies erkennt und automatisch durch einen Notruf die Rettungsmaßnahmen einleitet.

Aufbauend auf diese unfallvermeidenden bzw. folgenlindernden Pre-Crash Maßnahmen sind die Fahrzeugingenieure bestrebt, das System weiter zu verfeinern, um ein System mit Full Collision Avoidance zu entwickeln. Dazu muss in erster Linie die Sensorik am Fahrzeug und die darauf aufbauende Bildverarbeitung entscheidend sensibilisiert und erweitert werden. Immerhin muss das F'CAS-System die aktuelle Verkerssituation und deren potenziellen Gefahrensituationen rechtzeitig erkennen und klassifizieren. Dazu gilt es, neben der Erkennung der Hindernisse, zudem mögliche Ausweichstrecken zu berechnen, was eine Rundumüberwachung des Fahrzeuges erforderlich macht. Erst die Kombination von verschiedenen Sensortypen (Radar, Laser und adäquate Bildverarbeitung) ermöglichen durch ihre individuellen Eigenschaften (Reichweite, Auflösung, Witterungsunabhängigkeit usw.) ein zufriedenstellendes Ergebnis. Das System beeinflusst, nach Klassifizierung der

Gefahrensituation, direkt die Längs- und Querdynamik des Fahrzeuges und versucht dadurch den bevorstehenden Unfall zu vermeiden. Man muss sich jedoch bei derartigen Anwendungen die Komplexität, welche die Erkennung einer Verkehrssituation darstellt vor Augen halten. Einige Faktoren, welche in die Berechnung mit einfließen, sind etwa andere Verkehrsteilnehmer und deren Eigenschaften (Richtung, Geschwindigkeit), feste Hindernisse (Bäume am Straßenrand, Häuser, Mauern), Straßenbeschaffenheit und Ausweichwege. Zudem ist die Entscheidung, ob nun eine Vollbremsung eingeleitet wird, oder versucht wird das Hindernis zu umfahren, keineswegs trivial und in gewissen Fällen auch irreversibel. Deshalb bedarf es in diesem Bereich vor allem Fortschritten in der Bildverarbeitung durch noch leistungsfähigere Rechner, Verbesserung der Sensoren sowie der eingesetzten Algorithmen.

2.2 Neue Bedienelemente

Die konventionelle Steuerung hat sich heute in allen Kraftfahrzeugen etabliert. Gerade in solch einer Situation muss hinterfragt werden, ob diese Bedienungsart auch wirklich die beste ist und ob es keine Schwachstellen bzw. Verbesserungsmöglichkeiten gibt. Die Steuerung des Fahrzeuges geschieht im Groben durch Beeinflussung der Längs- und Querdynamik - lässt sich also anhand Steuerungsbefehlen in zwei Dimensionen bewerkstelligen. Bei der heute üblichen Bedienungsart mit Fußpedalerie, Lenkrad und Schaltknüppel müssen vom Fahrzeuglenker dafür bis zu fünf verschiedene Elemente koordiniert werden und ein gewisser Overhead ist offensichtlich erkennbar. Die herkömmliche Fahrzeugsteuerung ist für den Lenker auch keineswegs eine triviale Aufgabenstellung und bedarf einer gewissen Gewöhnungsphase, was sich durch Tests mit Jugendlichen, welche noch keinen Führerschein besitzen, auch bestätigt hat. Dies ist darauf zurückzuführen, dass die parallele Bedienung der verschiedenen Elemente nicht immer eine direkte Umsetzung resultieren, was nicht für eine intuitiven Bedienung spricht.

Weiters klagen Vielfahrer oft über Verspannungen, welche aufgrund der nicht ergonomischen Anordnung der Bedienelemente, vor allem Lenkrad und Fußpedale, entstehen. Diese Eigenschaft stellt sich effektiv als ein Nachteil dar, welcher durch die mechanische Verbindung zwischen Lenkrad und Lenkgestänge, bzw. Pedalerie und den jeweiligen mechanischen (hydraulischen) Systemen, entsteht. Die Position des Lenkrads lässt sich in heute akuten Automobilen fahrerspezifisch verstellen. Dabei können aber lediglich geringe Bewegungen in Höhe- und Tiefe durchgeführt werden.

Auch bei dem Einsatz der Fußpedale liegen einige offensichtliche Nachteile auf der Hand. Zum einen besteht eine Verletzungsgefahr durch Quetschung

bei einem Unfall, da die Pedale trotz ihrer kompakten Ausführung dennoch einen gewissen Raum der unteren Fahrgastzelle in Anspruch nehmen. Ein anderer Gesichtspunkt ist die Verzögerung beim Pedalwechsel. So muss der Fahrer beim Einleiten einer Bremsung den Fuß vom Gaspedal nehmen und zum Bremspedal hin wechseln. Dabei ergibt sich laut mehreren Testreihen eine messbare Verzögerung von durchschnittlich 0,2 sek, was bereits bei einer Geschwindigkeit von 50 km/h einer Bremswegverlängerung von rund drei Metern entspricht. Dies wiederum kann im Falle eines bevorstehenden Aufpralles die Schwere der Folgen maßgeblich beeinflussen.

Es gibt bereits mehrere Ansätze und mögliche Lösungsvorschläge für alternative Bedienelemente im Fahrzeugbereich. Einige davon werden im nun folgenden Teil vorgestellt.

2.2.1 Sticksteuerung

Das by-Wire-Konzept ist aus der Luftfahrt bereits seit einiger Zeit bekannt. Entwicklungen an der by-Wire Technik starteten dort bereits im Jahre 1960 und deren Einsatz ist in der heutigen Luftfahrt nicht mehr wegzudenken. So wird dort dem Piloten in den meisten Fällen ein Sidestick zur Steuerung zur Verfügung gestellt. Dieses Prinzip ist nun auch für eine Automobilsteuerung denkbar. Die entscheidenden Vorteile sind in erster Linie die einfache, intuitive Bedienung des Fahrzeuges, welche die Sticksteuerung darstellt. Weiters kann das Bedienelement, im Gegensatz zum herkömmlichen Lenkrad, vorteilhafter platziert werden, wobei durchaus Aspekte der Ergonomie entscheidend ins Gewicht fallen können.

Im Jahre 1998 wurde von Mercedes-Benz ein Konzeptcar, der R129 (siehe Abbildung 2.10, vorgestellt. Es handelt sich dort um den Umbau eines serienmäßig gebauten Mercedes SL Roadster, und es war das erste Auto, welches nicht über herkömmliche Bedienelemente (Lenkrad, Pedale) gelenkt wurde, sondern anhand zweier seitlich angebrachter Sidesticks. Die Vorteile dieser Steuertechnik liegen auf der Hand. So können die relativ kompakten Sidesticks in einer ergonomisch vorteilhaften Position angebracht werden. Bringt der Fahrer einen leichten Druck nach vorne auf, so startet das Fahrzeug, bei Intensivierung des Druckes am Stick, wird die Beschleunigung verstärkt. Bleibt der Sidestick nun in der Neutralposition sorgt der Zentralrechner, wie bei heute eingesetzten Tempomaten, für eine konstante Fahrtgeschwindigkeit. Durch eine Rückwärtsbewegung des Steuerhebels veranlasst der Fahrer eine Bremsung, wobei der Zentralrechner Funktionen von ABS usw. integriert und somit, abhängig vom jeweiligen Fahrbahnzustand, für optimale Verzögerungswerte sorgt.

Zum Einlenken des Fahrzeuges in eine Kurvenfahrt, wird der Sidestick



Abbildung 2.10: Steuerung durch Sidesticks, verwendet im umgebauten Mercedes SL der Baureihe R129

einfach nach rechts oder links bewegt, und das Fahrzeug folgt dem Lenkwunsch des Fahrers. Zusätzlich werden durch verschiedene Arten von Rückkopplungsbefehlen direkte Meldungen über aktuelle Zustände an den Fahrer weitergeleitet. So neigt sich der Stick je nach Lenkeinschlag entsprechend stark zur Seite und der an den Rädern gemessene Lenkwiderstand wird durch einen schwergängigeren Stick simuliert. Dadurch kann der Fahrer beispielsweise erkennen, ob er beim Einparken gegen den Bordstein lenkt und ob sich die Räder auf nasser oder eisiger Straße befinden usw. Beim Erreichen des Grenzbereichs kann der Fahrer etwa durch Vibration auf die Gefahrensituation hingewiesen werden.

Mercedes verbaute zwei Sidesticks, einen auf der Mittelkonsole, den anderen auf der Armlehne der Fahrertür. Diese Bauweise bringt gleich mehrere Vorteile mit sich. Zum einen wird der Komfort des Lenkers gesteigert, es kann je nach Belieben mit der rechten oder linken Hand oder sogar mit beiden Händen das Fahrzeug gesteuert werden. Bei gleichzeitiger Verwendung beider Sticks werden die gemessenen Werte vom Bordcomputer addiert und ein einheitliches Gesamtsignal errechnet. Die Arme des Fahrer können hierbei angenehm auf der Mittelkonsole bzw. Seitenlehne ruhen, und werden dadurch, im Gegensatz zu aktuellen Systemen, entspannter platziert. Zudem besteht die Möglichkeit, das Fahrzeug im Bedarfsfall vom Beifahrersitz aus zu steuern, bzw. in einer Notfallsituation korrigierend einzugreifen. Die Ersetzung der sperrigen Bedienelemente durch derartige Sidesticks ermöglicht

neue Innenraumgestaltungen, so kann etwa das Armaturenbrett komplett neu gestaltet oder umfunktioniert werden.

2.2.2 Das Bedienkonzept X-Drive

Das beschriebene Forschungsfahrzeug von Mercedes-Benz ließ die restlichen Automobilhersteller nicht unbeeindruckt und verschiedene Ansätze für eine zukünftige, vorteilhaftere Fahrzeugbedienung entstanden. So realisierte General Motors 2002 ein neues by-Wire-Konzeptcar, welches mit dem vom schwedischen Zulieferer SKF Group entwickelten X-Drive Steuersystem (Abbildung 2.11 ausgerüstet wurde. Dieses neuartige Bedienelement besteht aus zwei Handgriffen, welche an ein ovales Bedienelement befestigt sind und ähnlich dem herkömmlichen Lenkrad platziert werden. Beschleunigt wird, ähnlich wie von den Motorrädern bekannt, durch Drehen an einem der Handgriffe. Die Bremsen sind durch Taster auf der Rückseite ansprechbar. Sie sind auch beidseitig angebracht, wobei die Intensität der Bremsung von der Druckkraft, welche in Summe auf beide Bremstaster aufgebracht wird, abhängig ist. Zum Lenken können die Handgriffe gleich wie bei einem Lenkrad gedreht werden, jedoch insgesamt lediglich um 20 Grad je Richtung. Dies erübrigt das mehrmalige Rotieren des Lenkrades, wie man es aus aktuellen Fahrzeugen gewohnt ist. Die adaptive Lenkung regelt die Lenkübersetzung dermaßen intelligent, dass dieser geringe Lenkeinschlag für die Verkehrssituationen völlig ausreichend ist, und zudem zur Sicherheit beiträgt, indem ein Verreißen des Lenkrades bei hoher Geschwindigkeit ohne großen Folgen bleibt, weil derartige Inputwerte vom Zentralrechner gefiltert werden.

Das Konzeptfahrzeug "Hy-Wire", welches General Motors damals präsentierte, war eine völlige Neuentwicklung, weshalb die Fahrzeugkonstruktion komplett von der heute bekannten abweicht. So wurde die gesamte Technik inklusive des hochmodernen Wasserstoffantriebs in den ca. 30 cm dicken Unterboden des Fahrzeuges integriert. Die Fahrgastzelle wurde direkt darauf positioniert, welche nun aber ein komplett leerer Raum war, den es zu gestalten galt. Die direkt für dieses Forschungsfahrzeug entwickelte X-Drive-Lenkung ist lediglich in der Mittellaufschiene des Fahrzeuges befestigt, und kann dadurch relativ frei im Raum bewegt und wie gewünscht positioniert werden. Somit ist eine Links- bzw Rechtssteuerung ohne Zusatzaufwand zu realisieren. Auch der restlichen Fahrzeuginnengestaltung sind nur wenige Grenzen gesetzt. Es ist hier anzumerken, dass diese Vorteile rein auf den Einsatz eines kompletten by-Wire-Konzeptes zuzuschreiben sind, und nicht von der andersartigen Ausführung des Bedienelementes her stammen.



Abbildung 2.11: Innovative Innenraumgestaltung dank X-by-Wire und X-Drive

2.2.3 Bedienung mit Lenkrad und Pedalen

Natürlich ist in einem by-Wire-Konzept weiterhin eine Steuerung durch herkömmliche Bedienelemente einsetzbar. Die einzelnen Elemente werden dabei durch ähnlich beschaffene Sensor-Aktuator Elemente ausgetauscht. Man erhält dadurch allerdings nur eine geringe Veränderung in der Bedienung und deren Komfort. Allerdings besteht die herkömmliche Steuerung nun seit Einführung des Automobils und unzählige Fahrzeugbenutzer werden es willkommen heißen, diese Art der Bedienung weiterhin zu verwenden. Zumindest von der technischen Seite her soll dem nichts im Wege stehen.

Um die umständlichen und bei Unfällen auch gefährlichen Pedale zu ersetzen kann mit speziellen Trittmatten gearbeitet werden, welche integrierte Sensoren verwenden, um den jeweiligen aufgebrachten Fußdruck zu ermitteln. Dadurch erhält man auch einen größeren Freiraum im Beinbereich und auf die sperrigen Pedale kann verzichtet werden. Allerdings vermittelt die Verwendung von Fußtrittmatten dem Fahrer bedeutend weniger Gefühl, und Rückmeldungen müssten entsprechend simuliert werden. Einsatzfähige Bauformen sind derzeit in Entwicklung.

Neben all diesen unterschiedlichen Bedienkonzepten, welche durch ein x-by-Wire-Fahrzeug ermöglicht werden, können ohne großen Aufwand spezielle, behindertengerechte Steuerungsmöglichkeiten entwickelt und verwendet

werden. Es wäre auch denkbar, diese detailliert auf die jeweilige Individualsituation anzupassen, und Menschen mit Behinderung dadurch die Möglichkeit einer gewissen Mobilität zu geben. Dazu bedarf es einer einheitlichen Schnittstelle zwischen Zentralrechner und dem Bedienelement, wodurch letzteres nachträglich durch eine geeignete Spezialanfertigung realisiert werden kann.

2.3 Wirtschaftlichkeit

Beobachtet man die Zuverlässigkeit von aktuellen Fahrzeugen, so fällt besonders im Segment der Oberklassefahrzeuge, welche mit einer Vielzahl neuer, elektronischer Komponenten ausgestattet sind, eine überdurchschnittliche Anfälligkeit auf. Diese ist in den meisten Fällen darauf zurückzuführen, dass die heute eingesetzten Elektronikkomponenten im Laufe der Zeit entwickelt und eingesetzt wurden, während die Basis der Fahrzeuge ständig an deren Einsatz angepasst werden musste. Die erforderliche, intelligente Kommunikation unter den einzelnen Komponenten wird immer komplizierter und kann mit der aktuellen Architektur nur mehr schwer erreicht werden. Zudem behindert die zugrunde liegende Mechanik teilweise die Funktion und die eigentlichen Vorteile der Elektronik, indem die Aktionen verzerrt oder verzögert ausgeführt werden. Aus diesen Gesichtspunkten ist der Bedarf einer neuen Technologie erkennbar, welche speziell für den Einsatz von Elektronik im Fahrzeug konzipiert worden ist, und deshalb die auftretenden Probleme zu lösen vermag. Hier setzt das Konzept des X-by-Wire an. Eine Vielzahl der heute autonom arbeitenden Subsysteme ließen sich anhand einer zentralen Recheneinheit rein mit entsprechender Software lösen, was bereits die meisten, heute auftretenden Probleme, lösen bzw. abschwächen würde. Einem Einsatz des X-by-Wire würde also aus dieser Sicht nichts mehr im Wege stehen.

Auf der anderen Seite sind die in X-by-Wire-Systemen vorgesehenen Technikkonzepte zur Zeit noch erheblich kostenintensiver, als die bereits seit Jahrzehnten eingesetzten und ständig optimierten Lenk- und Bremssysteme. Wie in diesem Kapitel beschrieben, sind viele Subsysteme heute bereits erhältlich und sie funktionieren auch ohne by-Wire Lösung. Die Fahrzeughersteller gehen deshalb den Weg, dass die aktuellen Systeme laufend verbessert werden, und neue Systeme wie ADR mit Stop and Go oder Lane Keeping Support vorerst als Extraausstattungen in Oberklassefahrzeugen praktische Erfahrung sammeln. Durch diese Einführung als Sonderausstattung werden die Systeme jedoch in einen Bruchteil der Fahrzeuge eingebaut und aufgrund des mangelnden Absatzes wird der mögliche Durchbruch des X-by-Wire Kon-

zeptes erheblich verzögert. Zudem wird die Entwicklung in diesem Bereich deutlich eingebremst, da parallel an den bereits existierenden Konzepten weiterentwickelt werden muss.

Darüber hinaus sind natürlich die Initialkosten für die Automobilhersteller enorm. Bei einem drastischen Umstieg der heutigen Technologie auf by-Wire Systeme müssen einige Fahrzeugkomponenten komplett überarbeitet bzw. neu entwickelt und getestet werden (Energieversorgung, Bedienelemente, sichere elektronische Systemarchitekturen, Aktuatoren). Aus wirtschaftlicher Sicht ist jedoch eine Umlage dieser horrenden Entwicklungskosten, auf eine geringe Stückzahl bei einer vorsichtigen Markteinführung nicht möglich. Dem entgegen steht ein eher höheres Risiko bei Großserieneinführung aufgrund der möglichen Rückrufaktionen.

Um diesem Dilemma zu entgehen und eine erfolgreiche Markteinführung der neuen Technologie zu ermöglichen, bedarf es folgender Bedingungen:

- Zuverlässigkeit der verwendeten Komponenten
- Akzeptanz der Endverbraucher
- Hinreichend große Nachfrage nach Systemen, welche die X-by-Wire Technologie voraussetzen.
- Forcierung der potenziellen Vorteile von by-Wire-Systemen
- Die Bedienung muss kompatibel zur bisherigen Bedientechnik sein oder gegenüber dieser eindeutige Vorteile aufweisen

Teilweise lassen sich diese Bedingungen nicht direkt beeinflussen. Dies gilt vor allem für die Kundennachfrage und deren Interessen. Aus den restlichen Bedingungen lässt sich direkt Forschungs- und Entwicklungsarbeit ableiten. Tragen diese Forschungsarbeiten Früchte, ist auch eine indirekte Beeinflussung der Kundennachfrage möglich, indem diese die Vorteile und Sicherheit der neuen Systeme direkt erleben können. In diesem Moment wird die Vermarktung und Verbreitung von X-by-Wire Systemen auf keinen Widerstand mehr stoßen.

2.4 Fly-by-Wire vs. Drive-by-Wire

Es treten in der Öffentlichkeit immer wieder Fragen auf, warum by-Wire Technologien in Fahrzeugen noch nicht serienreif sind, während derartige Systeme in Flugzeugen seit nunmehr zwei Jahrzehnten erfolgreich eingesetzt

werden. Dabei treten natürlich die Vorteile und der enorme Nutzen der Drive-by-Wire Technologie für die Fahrzeugindustrie in den Vordergrund. Es gibt durchaus Parallelen zwischen Fly-by-Wire und Drive-by-Wire Systemen und deren Entwicklungsprozessen. So wurden sowohl Flugzeuge als auch Automobile anfänglich auf rein mechanische Art gesteuert. Ergänzt wurde diese Art der Lenkanlagen- bzw. Flugsteuerungsbeeinflussung durch (meist hydraulische) Kraftverstärker, teilweise weil es die neu erreichten Eigenschaften verlangten, teilweise um den Komfort für den Fahrer/Piloten zu erhöhen. Dieser Schritt steigerte sich zunehmend in das Bestreben, die mechanischen Komponenten komplett durch Mechatronikbauteile zu ersetzen. Die parallele Entwicklung in Luftfahrt und Kraftfahrzeugtechnik ist lediglich gut 20 Jahre voneinander getrennt. Nun gab es im Luftfahrtbereich jedoch den dringenden Bedarf an größeren und schnelleren (stärkeren) Flugzeugen, welche aus technischer Sicht auch realisiert werden konnten. Problematisch war allerdings die Kontrolle und Beeinflussung der enormen Kräfte, welche am viel größer gewordenen Flugzeugrumpf wirkten. Anhand herkömmlicher Steuermethoden traten vermehrt Probleme auf, das Flugzeug entsprechend zu stabilisieren und zu lenken. Hier bot die by-Wire-Technologie die notwendige Flexibilität und Dynamik an, um die Neukonstruktion des Flugzeuges und deren späteren Flugführung entsprechen zu kontrollieren. Dadurch wurde die Entwicklung und der Einsatz von Fly-by-Wire Systemen enorm vorangetrieben, so dass heute die meisten Flugzeuge auf derartige Technologie angewiesen sind.

Die Technik des Fly-by-Wire hat sich dadurch etabliert und hat, durch ihre Vorteile und Zuverlässigkeit, Anerkennung und Vertrauen gewonnen. Nun wäre es für viele wünschenswert derartige Systeme in den Automobilbereich zu portieren, um dort für ähnliche, vorteilhafte Eigenschaften zu sorgen. So könnte etwa das Fahrzeuggewicht durch den Entfall der sperrigen Mechanik drastisch gesenkt werden, was nicht zuletzt eine revolutionierte Bauweise des Automobils zulassen würde. Zudem könnten Fahrdynamik und Komfort entscheidend verbessert werden, während ein geringerer Verbrauch bzw. eine kleinere Motorisierung ausreichend wäre. Es ist jedoch ein Trugschluss, dass die by-Wire-Technik einfach aus der Luftfahrt übertragen werden kann⁷.

Ein Vergleich einiger technischer Aspekte soll diese Thematik besser hinterleuchten. Beim Ausfall eines Seitenruders in einem Flugzeug, kann das System bzw. die Besatzung anhand dem gegenläufigen Höhenruder, den Bremsklappen und den Triebwerken die Maschine notdürftig manövrieren. Fällt parallel dazu in einem Kraftfahrzeug das Lenksystem aus, bedeutet dies

⁷Ähnliches gilt auch für spurgeführte Fahrzeuge, wo sich durchaus auch ein hoher Automatisierungsgrad etabliert hat, und trotzdem ist eine direkte Überführung der Technologie auf den Kraftfahrzeugbereich nicht machbar.

gleich den Verlust der Steuerungsgewalt. Zudem steht dem Piloten eines Flugzeuges viel mehr Zeit und Raum für erforderliche Korrekturmaßnahmen zur Verfügung, während ein Fahrzeuglenker im dichten Straßenverkehr manchmal nur wenige Augenblicke für eine entsprechende Reaktion hat.

Die redundante Realisierung des Bordnetzes⁸ stellt für den Automobilbau in technischer Sicht kein Problem dar, der Fahrzeuglenker erwartet sich jedoch lange Wartungsintervalle und einfache Handhabung, während die Bordelektronik der Flugzeuge in kurzen, regelmäßigen Abständen gewartet werden können, und das Personal laufend durch Schulungen weitergebildet und für Gefahrensituationen sensibilisiert wird. Zudem beträgt die Lebenserwartung, heute vorzüglich eingesetzter Mikroelektronikbauteile, etwa 7 Jahre, was jedoch nicht mit der Verwendungsdauer eines Fahrzeuges gleich kommt. Es ist auch bekannt, dass die Elektronik auch im ausgeschalteten Zustand altert, was für die langfristige Zuverlässigkeit der Steuerungsgeräte im Automobil momentan ein Problem darstellt.

Vergleicht man also abschließend die Anforderungen im Automobilbereich, so stehen sie jenen aus der Luftfahrt keinesweg nach, während man im automotiven Bereich jedoch ungleich erschwerte Rahmenbedingung vorfindet. Die Komponenten werden in sehr hohen Stückzahlen hergestellt, müssen extrem kostengünstig produziert werden, sollen möglichst lange Wartungsintervalle aufweisen und äußerst benutzerfreundlich realisiert sein. Zudem bedarf es einer Neuentwicklung vieler eingesetzter Komponenten, was enorme Kosten mit sich bringt. Weiters scheint der Einsatz vollelektronischer Systeme im Fahrzeug trotz vieler Vorteile nicht unbedingt als dringend notwendig. Neben der technischen Realisierung muss eine neue Sicherheitsphilosophie eingeführt werden. All diese Anforderungen und Faktoren tragen zur verzögerten Einführung der by-Wire Systeme im Kraftfahrzeugbereich bei. Drive-by-Wire Systeme werden erst dann sinnvoll und deren Einsatz gerechtfertigt, wenn sie klar ersichtliche Vorteile gegenüber den herkömmlichen Systemen aufweisen und diese Vorteile auch quantifizierbar den bestehenden Gefahren und Risiken gegenübergestellt werden können.

⁸In aktuellen Flugsteuerungsrechnern ist eine fünf- bis neunfache Redundanz der sicherheitskritischen Komponenten üblich.

Kapitel 3

Grundlagen und Sicherheitsaspekte

Aus den bisherigen Abschnitten ist zum wiederholten mal hervorgegangen, dass die X-by-Wire Technologie viele Vorteile mit sich bringt und großes Potential in den verschiedensten Bereichen der Kraftfahrzeugindustrie aufweist. Für die dahinterliegende Technik bedeutet dies jedoch hohe Anforderungen, speziell im Bereich der Zuverlässigkeit und Fehlerbehandlung. Im nun folgenden Kapitel werden deshalb Grundlagen der technischen Zuverlässigkeit erklärt und angemessene Lösungswege aufgezeigt. Zudem wird auf einige zu berücksichtigende Randbedingungen im Bezug auf den Einsatz automatisierter Systeme im Kraftfahrzeugbau hingewiesen.

Die Verwendung eines Fahrzeuges ist stets mit einem gewissen Risiko gekoppelt. Die gefahrene Geschwindigkeit stellt, im Falle eines Aufpralles, enorme Kräfte dar und bedeutet ein enormes Verletzungsrisiko für die Fahrzeuginsassen bzw. der sich im Umfeld befindlichen Personen. Die Automobilindustrie forscht bereits seit geraumer Zeit, um das Verletzungsrisiko bei einem Unfall möglichst effektiv zu reduzieren. Das, im Prinzip recht komplexe, Airbagsystem befindet sich seit 1981 auf dem Markt, wurde damals im Mercedes W126 (damalige S-Klasse) erstmals angeboten. Die Zahl der Sicherheitsvorkehrungen hat im Laufe der letzten 20 Jahre rasant zugenommen. Eine ganze Reihe von Sicherheitseinrichtungen wird heute nicht nur in Oberklassefahrzeugen serienmäßig eingesetzt. An diesem Trend der zunehmenden Sicherheit muss sich parallel auch die Technik am Fahrzeug selbst orientieren. So wurde die Häufigkeit der Ausfälle, welche zu gefährlichen Situationen führen können und deshalb ein Risiko für den Menschen darstellen, deutlich gesenkt. In diese Kategorie fallen vor allem Brems- oder Lenkversagen. Teilweise wurden Entwicklungen in diesen Bereichen auch durch gesetzlichen Vorschriften beeinflusst, so ist etwa der Einsatz einer zwei-kreisigen

Bremsanlage, sowie die mechanische Rückfallebene bei Bremse und Lenkung im Automobil verpflichtend vorgeschrieben. Jegliche mechanische Komponenten wurden nach deren maximalen Belastung, inklusive einem definierten Sicherheitsspielraumes konzipiert und eingebaut. Dieser wurde so ausgelegt, dass bei Ausfall einer Komponente, wie etwa eines Bremskreises oder der Lenkmomentunterstützung, die Möglichkeit besteht, das Fahrzeug, auch für nicht speziell darauf geschulte Lenker, weiterhin zu steuern und, respektive der neuen Umstände, relativ sicher zu steuern.

Ein X-by-Wire System ersetzt die grundlegenden Steuerungsmechanismen des herkömmlichen Fahrzeuges mit neuen Komponenten. Die bisher errungenen Standards im Bereich der hydraulischen Bremsen und Lenkung können deshalb nicht weiter verwendet werden, und es müssen von Grund auf neue Systeme entwickelt werden. Die Anforderungen an diese neuen by-Wire-Komponenten sind hoch, da sie mindestens die Eigenschaften und Leistungen der herkömmlichen, bereits etablierten und massenhaft getesteten Systeme erreichen und übertreffen müssen. Zudem werden durch die by-Wire-Technik neue Gesichtspunkte, vor allem im Bereich Komfort und Sicherheit, möglich. Diese müssen jedoch erst ihre Zustimmung bei den Kunden erhalten. Es ist offensichtlich, dass Begriffe wie Zuverlässigkeit, Fehlertoleranz und (Ausfall-) Sicherheit in dem Bereich der Elektronikkomponenten der Automobilindustrie enorme Bedeutung haben. Aus diesem Grund werden die wichtigsten Begriffe hier kurz erklärt und die damit bestehenden Problematiken aufgezeigt.

3.1 Begriffserklärungen

Im Bereich technischer Sicherheitssysteme treten immer wieder Begriffe auf, welche im Alltag oftmals eine nur unscharfe Definition bzw. verschiedene Bedeutungen haben. So hat beispielsweise der Begriff der Sicherheit etwa in verschiedensten Zusammenhängen seine Relevanz. Aus diesem Grund werden hier verschiedene Definitionen, von der technischen Sicherheit bis hin zur Fehlertoleranz, erklärt.

3.1.1 Sicherheit & Zuverlässigkeit

Grundlegend ist zu beobachten, dass technische Leitsysteme vermehrt in sicherheitskritischen Bereichen eingesetzt werden. Der Grund dafür ist oftmals, dass Rechner für komplexe und schnelle Steuerungen besser geeignet sind als der Mensch oder ein analoger Schaltkreis. Entsprechende Einsatzgebiete sind heute in Kernkraftwerken, in verschiedenen hochenergetischen Verfahrens-

techniken, in der Luftfahrtindustrie, spurgeführten Verkehrssystemen und zunehmend in der Kraftfahrzeugindustrie zu finden. In derartigen Systemen spielen die beiden Begriffe Sicherheit und Zuverlässigkeit eine wichtige Rolle und müssen klar definiert und abgegrenzt werden.

Bei der Begriffsbestimmung für Sicherheit begibt man sich jedoch schon in Schwierigkeiten und es stellen sich Fragen wie: „was ist sicher?“ „Gibt es Sicherheit?“ Es ist unumstritten, dass es kein absolut sicheres System gibt, ein gewisses Restrisiko wird in jeder Situation bestehen. Dies liegt in der Natur der Dinge und auf diese Diskussion wird an dieser Stelle nicht weiter eingegangen. Jedoch muss ein Weg gefunden werden, die geforderte Sicherheit in einem System zu umschreiben, diese zu quantifizieren, damit die durchzuführenden Abnahmen im Laufe einer Systementwicklung auch objektiver bewertet werden können. Man findet in der Literatur verschiedenste Ansätze von Begriffsbestimmungen, welche sich jedoch nicht immer abdecken. Ein einprägendes Verfahren der Risikoabwägung ist die Methode der Grenzkrisikoermittlung.

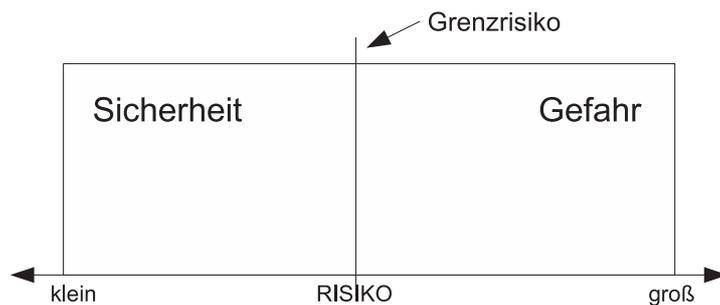


Abbildung 3.1: Grenzkrisiko als Schwelle zwischen Sicherheits- und Gefahrenzone

Entsprechend der Abbildung 3.1, geht von einem sicheren System ein niedriges Risiko aus. Steigt hingegen das Risiko, begibt man sich weiter in den Gefahrenbereich. Eine allgemeine, quantitative Bestimmung der Sicherheit ist nicht möglich, deshalb wird die Grenze zwischen Sicherheits- und Gefahrenzone laut DIN-Norm 40041, als das größte noch vertretbare Risiko eines bestimmten technischen Vorganges oder Zustandes definiert und synonym als Grenzkrisiko bezeichnet. Folglich ist die Sicherheit eine Sachlage, bei der das Risiko kleiner dem Grenzkrisiko ist. Wird das Grenzkrisiko überstiegen, befindet sich das System in der Gefahrenzone und das Risiko der Anwendung ist nicht mehr vertretbar.

Weiters wird in obgenannter DIN-Norm der Begriff der technischen Zuverlässigkeit folgendermaßen definiert: Zuverlässigkeit ist die Beschaffenheit

einer Einheit bezüglich ihrer Eignung, während oder nach vorgegebenen Zeitspannen, bei vorgegebenen Anwendungsbedingungen, die Zuverlässigkeitsanforderung zu erfüllen.

Ähnlich wird der Begriff Zuverlässigkeit in [ntg] definiert: Zuverlässigkeit ist die Fähigkeit einer Komponente oder eines Systems, über einen gegebenen Zeitraum hinweg und unter bestimmten Betriebsbedingungen, korrekt zu funktionieren.

Das System muss sich also innerhalb einer definierten Zeitspanne gemäß der Spezifikation verhalten, unter der Annahme, dass das System vor dieser Zeitspanne auch korrekt funktionierte, und dass während der definierten Betriebszeit keine Wartungsarbeiten notwendig sind, welche die Funktionsweise beeinträchtigen würden. Da die Zeitspanne bei dieser Bewertungsart eine bedeutende Rolle spielt, muss die Länge des zu beobachtenden Intervalls abhängig vom jeweiligen Anwendungsfall möglichst realistisch gewählt werden. Intervalle für schwer zu erreichende, oder nur mit hohem Aufwand zu wartende Systeme wie Satelliten, Forschungsgeräte im Weltraum, Herzschrittmacher, usw.) sind demnach entsprechend hoch anzusetzen. Ein Intervall im Ausmaß von mehreren Jahrzehnten scheint in solchen Fällen durchaus realistisch. Hingegen können Anwendungen auch nur auf einzelne Einsätze ausgelegt werden, so z.B. im militärischen Bereich, wo Wartungsarbeiten nach einer Mission (welche auch nur einige Minuten andauern kann) vorgesehen sind.

Auch die Verfügbarkeit steht, ähnlich wie die Zuverlässigkeit, in engem Zusammenhang mit der Zeit. Sie ist jedoch nicht auf einen Zeitraum bezogen, sondern auf einen bestimmten Zeitpunkt. Laut DIN-Normen wird Verfügbarkeit folgendermaßen definiert:

Die Verfügbarkeit ist die Wahrscheinlichkeit, ein System zu einem gegebenen Zeitpunkt in einem funktionsfähigen Zustand anzutreffen.

Je nach Art der Anwendung wird zusätzlich der Begriff der Wartbarkeit eingeführt. Er beschreibt nach Auftreten eines Fehlers die Wahrscheinlichkeit, dass das System innerhalb einer vorgegebenen Zeit repariert werden kann und erneut einsatzfähig ist. Parallel dazu wird die Kenngröße der mean-time-to-repair (MTTR) eingeführt. Dies ist die Zeit, die ein System während einer Mission im fehlerhaften Zustand verbleibt. Es handelt sich dabei um die Zeitspanne, gemessen vom Auftreten des Fehlers bis zu dessen Beseitigung durch Reparatur oder Erneuerung. Diese Zeit kann als Abschätzung mit

$$MTTR = \lim_{n \rightarrow \infty} \frac{t_1 + t_2 + \dots + t_n}{n} \quad (3.1)$$

berechnet oder analytisch aus der Verteilungsfunktion $G(t)$ der Reparaturzeiten ermittelt werden.

$$MTTR = \int_0^{\infty} (1 - G(t))dt \quad (3.2)$$

Analog dazu wird für die Zuverlässigkeit die mittlere Zeit bis zum Fehler, die mean-time-to-failure (MTTF) definiert. Sie beschreibt bei angenommen konstanter Ausfallsrate λ den Mittelwert der ausfallfreien Arbeitszeit des Systems und lässt sich über deren Kehrwert mathematisch bestimmen. Daraus folgt

$$MTTF = \frac{1}{\lambda} \quad (3.3)$$

Addiert man nun beide Zeiten MTTR und MTTF, so erhält man die Zeit, die zwischen zwei Ausfällen verstreicht. Das Resultat wird mit mean-time-between-failure (MTBF) bezeichnet.

$$MTBF \approx MTTF + MTTR \quad (3.4)$$

Die Verfügbarkeit (V) wird nun quantitativ als das Verhältnis zwischen jener Zeit, wo sich das System im ordnungsgemäßen Zustand befindet, gegenüber der Gesamtlaufzeit (inklusive Ausfallzeiten) ermittelt.

$$V = \frac{MTTF}{(MTTF + MTTR)} \quad (3.5)$$

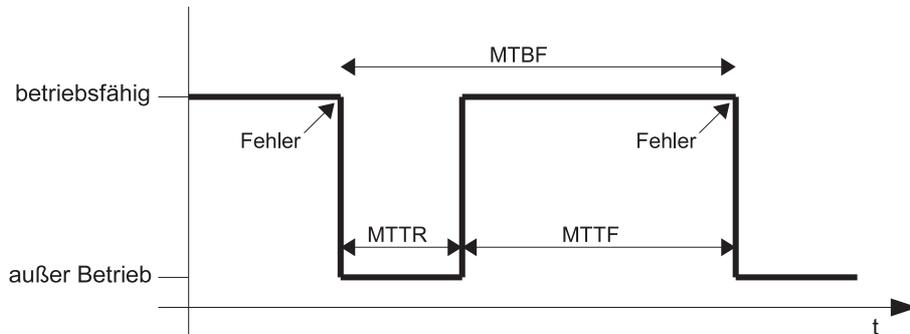


Abbildung 3.2: Abhängigkeit der Kennzahlen MTTR, MTTF, MTBF

Die Verfügbarkeit lässt sich demnach intuitiv erhöhen, indem die Betriebszeit bis zum nächsten Ausfall verlängert wird oder indem die Reparaturzeiten drastisch verkürzt werden. Welche Strategie der Erhöhung der Funktionalität günstiger ist, variiert je nach Anwendungsfall und muss daher in jedem Entwicklungsprozess analysiert werden.

Jedes System wird in erster Linie aufgrund seiner Funktionalität entwickelt und später verwendet. Stellt man jedoch anlehnd an [Mon99] Sicherheit und Funktionalität in sicherheitsrelevanten Anwendungen gegenüber, zeigt sich offenbar erkenntlich, dass sich diese beiden Begriffe gegenseitig beeinflussen und oft sogar konträr zueinander stehen. So stellt sich etwa in einer Gefahrensituation die Frage, ob das gesamte System gestoppt und damit in den sicheren Zustand überführt, oder ob es weitergefahren werden soll. Man kann erkennen, dass die erste Entscheidung zu Gunsten der Sicherheit und zu Lasten der Funktionalität führt, während sich die zweite umgekehrt verhält. Meist wird zu Gunsten der Funktionalität entschieden, denn die ist direkt messbar, während Sicherheit nicht quantitativ bestimmt werden kann und man deren Wert auch erst richtig zu schätzen weiß, wenn man sich in einer Situation befindet, in der Sicherheitsaspekte wichtig wären, sie jedoch nicht vorhanden sind.

Sowohl im Entwicklungsprozess als auch im Entscheidungsprozess während des Betriebes sollte deshalb stets ein vernünftiger Kompromiss zwischen Funktionalität und Sicherheit gefunden werden. Beschreibt man ein sicherheitsrelevantes System, so ist deshalb der Begriff Sicherheit nicht erstrangig, denn naiv betrachtet ist Sicherheit ohne jegliche Funktion nutzlos. Daraus wird erkennbar, dass verschiedene Faktoren berücksichtigt werden müssen, um der Gesamtkomplexität des Systems gerecht zu werden. Aus diesem Grund wird der Oberbegriff der Verlässlichkeit des Systems eingeführt.

Wie aus der Grafik 3.3 ersichtlich, stützt sich die Verlässlichkeit auf folgende Säulen:

- Security. Beschreibt den Zustand, der frei von unvermeidbaren Risiken der Beeinträchtigung ist oder als gefahrenfrei angesehen wird.
- Safety. Bezüglich der Systemzuverlässigkeit, beschreibt safety die interne Ablauf- und Ausfallsicherheit.
- Availability. Die Verfügbarkeit eines Systems ist die Wahrscheinlichkeit, dass das System bestimmte Anforderungen zu bzw. innerhalb eines vereinbarten Zeitrahmens erfüllt.
- Maintainability. Die Maintainability umfasst die Möglichkeit ein System instandzuhalten, dass es seine volle Funktionalität über einen Zeitraum behält.
- Reliability. Die Ausfallsicherheit ist ein Merkmal von Systemen, das den ausfall- und störungsfreien Dauerbetrieb charakterisiert.

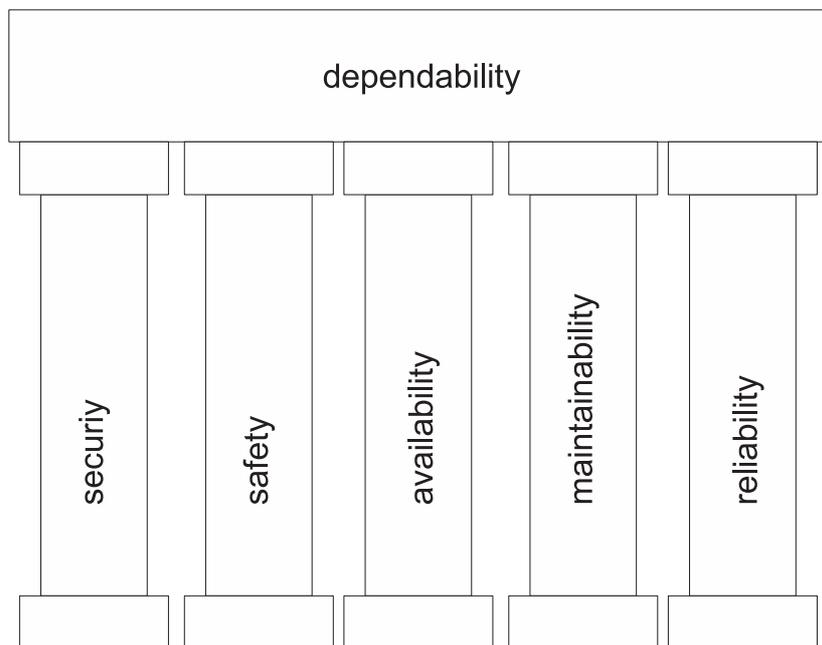


Abbildung 3.3: Die fünf Säulen der Zuverlässigkeit

Weitere, in diesem Zusammenhang jedoch nicht relevante, Faktoren könnten etwa Datenintegrität, Sicherheit im Sinne von Zugriffsrechten und sicherer Authentifizierung, oder Datenvertraulichkeit sein. Erst das Zusammenspiel der einzelnen, für den jeweiligen Anwendungsfall indikativen Faktoren, entscheidet über die Verlässlichkeit der Gesamtanwendung und hat damit eine gewisse Aussagekraft für die Güte des Systems.

3.1.2 Hazards & Risiko

Unerwünschte Systemzustände, welche potenziell zu Unfällen führen, oder dazu beitragen, sich in eine Gefahrensituation zu begeben, werden Hazards genannt. Von Hazards kann man deren Auftrettswahrscheinlichkeit und Folgen ableiten. Die Auftrettswahrscheinlichkeit gibt Aufschluss über die Häufigkeit von gefährlichen Ereignissen. Möglich sind sowohl qualitative als auch quantitative Aussagen. Die Angaben können als Anzahl von entsprechenden Ereignissen pro Zeitraum (Stunde, Jahr, Lebenszeit des Gerätes) gemacht werden. Oft werden jedoch Wahrscheinlichkeitszahlen ohne Einheiten angegeben, was in der Praxis immer wieder zu Verwirrung sorgt, denn ob die Angabe Ausfälle pro Betriebsstunde oder pro Jahr beschreibt, ergibt bei vielen Anwendungen sehr wohl einen signifikanten Unterschied. Eine mögliche qualitative Einteilung der Wahrscheinlichkeiten, wie sie in der Luftfahrt vor-

genommen wird, ist

- Wahrscheinlich
- Unwahrscheinlich
- Extrem unwahrscheinlich

Für die Untergliederung der quantitativen Ausmaße steht die Wahrscheinlichkeit eines Ausfalles pro Betriebsstunde mit etwa 10^{-1} für häufige Ausfälle, 10^{-5} für seltene Ausfälle, bis hin zu extrem unwahrscheinlichen Ausfällen, welche mit einer Wahrscheinlichkeit von 10^{-9} quantifiziert werden.

Das Ausmaß der Folgen beschreibt nichts anderes als die Schwere des aufgetretenen Unfalls und muss auch entsprechend kategorisiert werden. Es gibt hier auch verschiedene Ansätze der möglichen Kategorisierung. Als Beispiel zeigt Tabelle 3.1 eine mögliche Einteilung aus dem Bereich militärischer Systeme:

Kategorie	Definition
Katastrophal	Mehrere Tote
Kritisch	Einzelner Todesfall und/oder mehrere schwere Verletzungen oder Krankheiten der Bewohner des Unfallgebietes
Geringfügig	einzelne schwere Verletzung oder Krankheiten der Bewohner und/oder mehrere Verletzungen oder geringfügige Krankheiten der Bewohner des Unfallgebietes
Unwesentlich	Einzelne geringfügige Verletzungen oder geringfügige Krankheiten von Menschen

Tabelle 3.1: Einteilung der Unfallfolgen für militärische Systeme

Die Aussagekraft beider Teilaspekte für sich ist gering, erst das Produkt der beiden kann als Quantifizierung der Gefahr betrachtet werden und wird Risiko genannt. Das Risiko ist also die Synthese von Auftrittswahrscheinlichkeit und Folgen eines Hazards und kann anhand einer einfachen Multiplikation berechnet werden.

$$Risiko = Wahrscheinlichkeit \times Folgen \quad (3.6)$$

Liegen bereits Daten des entsprechenden Prozesses vor, so gliedert man die Auftrittshäufigkeit nach deren Aufenthaltsdauer in der Gefahrenzone,

nach der Möglichkeit einer Gefahrenabwehr und nach der Wahrscheinlichkeit des Eintritts des unerwünschten Ereignisses. Falls keine Daten des betrachteten Systems oder eines ähnlichen Systems vorliegen, muss die Wahrscheinlichkeit des Eintritts des unerwünschten Ereignisses abgeschätzt werden. Aus ethischer Sicht ist es angebracht, den Faktor der Wahrscheinlichkeit dermaßen zu wählen, dass man sich in Worten ausgedrückt „auf der sicheren Seite“ befindet. Daraus ist jedoch ersichtlich, dass die Aussagekraft des Resultates nicht derart scharf zu bewerten ist, da die einzelnen Faktoren meist nicht gemessen werden können, sondern lediglich grobe, subjektive Abschätzungen sind und somit direkt vom zuständigen Ingenieur beeinflusst werden. Deshalb kann für das Risiko auch keine numerische Grenze, etwa ein akzeptables Risiko oder ein Grenzkrisiko, festgelegt werden, sondern es bedarf der Frage nach deren Vertretbarkeit.

Risikoklassen. Die qualitativen Parameter des Risikos lassen sich kombinieren und daraus Risikoklassen herleiten. Leider sind diese Klassen keiner einheitlichen Norm unterworfen, sondern es existieren eine Reihe verschiedener Klassifizierungen. Die in Tabelle 3.2 aufgezeigte Klassenbildung stammt aus der internationalen Norm IEC 61508. Deren Untergliederung beinhaltet folgende vier Risikoklassen:

- I : Inakzeptables Risiko
- II : Unerwünschtes und nur bei nicht reduzierbarem Risiko oder unverhältnismäßig stark zunehmenden Kosten akzeptabel
- III: Tolerierbares Risiko, wenn die Kosten der Risikoreduzierung überschritten werden
- IV : Unbedeutendes Risiko

	Folgen			
Häufigkeit	Katastrophal	Kritisch	Geringfügig	Unbedeutend
Häufig	I	I	I	II
Wahrscheinlich	I	I	II	III
Gelegentlich	I	II	III	III
Zukünftig	II	III	III	IV
Unwahrscheinlich	III	III	IV	IV
Unglaublich	IV	IV	IV	IV

Tabelle 3.2: Risikoklassifizierung nach IEC 61508

Parallel zu jeder Risikoklasse werden Entwicklungsrichtlinien und -techniken definiert, welche der jeweiligen Klasse entsprechen und deren Gefahrenstufe auch berücksichtigen. Die Klassifizierung der einzelnen Teilbereiche einer zu entwickelnden Anwendung, legt die wichtigsten Rahmenbedingungen fest und entlastet die Arbeit des Entwicklers entscheidend.

Risikograph. Eine andere Möglichkeit der Risikobewertung erhält man anhand eines Risikographen. Dazu werden die in DIN 19250 definierten Risikoparameter dargestellt:

- Schadensausmaß
 - S1: Leichte Verletzung
 - S2: Schwere Verletzung einer oder mehrerer Personen oder Tod
 - S3: Tod mehrere Personen
 - S4: Katastrophale Auswirkung, sehr viele Tote
- Aufenthaltsdauer
 - A1: Selten bis öfter
 - A2: Häufig bis dauernd
- Gefahrenabwendung
 - G1: Möglich unter bestimmten Bedingungen
 - G2: Kaum möglich
- Eintrittswahrscheinlichkeit des unerwünschten Ereignisses
 - W1: Sehr gering
 - W2: Gering
 - W3: Relativ hoch

Daraus ergeben sich 48 mögliche Kombinationen, welche jedoch, aufgrund der Priorisierung einiger Risikoparameter, nicht alle von praktischer Bedeutung sind. So kann von einer weiteren Detaillierung des Parameters S1 abgesehen werden, da die Sicherheitsanforderungen hier sehr gering sind. Ähnliches Verhalten kann auf der anderen Seite beobachtet werden, so spielen bei einem extrem hohen Schadensausmaß die Aufenthaltsdauer und die Möglichkeit, die Gefahr unter Umständen noch abwehren zu können, lediglich nebensächliche Rollen. Deshalb kann auf eine weitere Verfeinerung des Risikoparameters S4 verzichtet werden. Somit erhält man aus der Kombination der obgenannten

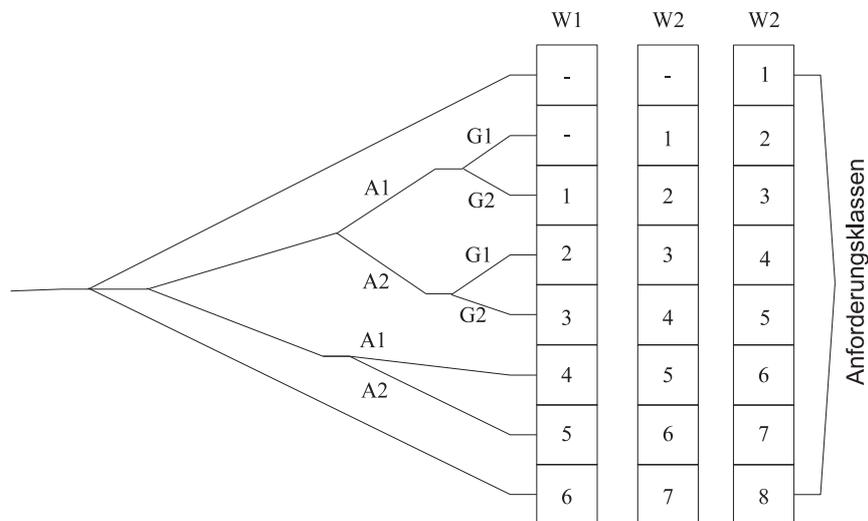


Abbildung 3.4: Risikograph der indikativen Kombinationen

Parameter S, A und G lediglich acht für die Praxis bedeutsame Kombinationen. Nimmt man die Eintrittswahrscheinlichkeit des unerwünschten Ereignisses (Parameter W) in den relevanten Fällen hinzu, resultieren daraus ca. 20 relevante Anforderungsklassen (siehe Abbildung 3.4), für welche jeweils verschiedene Vorgangsweisen und Anforderungen im Bezug auf die System-sensibilität existieren.

3.1.3 Fehler, deren Quellen und Auswirkungen

Bei der Definitionen des Fehlers in sicherheitskritischen Anwendungen findet man in der Literatur unterschiedliche Ansichten und Einteilungen. Die Norm DIN 40041 unterscheidet zwischen Fehler und Ausfall und definiert diese folgendermaßen:

Ein Fehler ist die Nichterfüllung vorgegebener Forderungen durch einen Merkmalswert, während der Ausfall als Aussetzen der Ausführung einer festgelegten Aufgabe und damit als der Übergang vom fehlerfreien in den fehlerhaften Zustand definiert wird.

Der Ausfall ist demnach das Ereignis, welches das System in den fehlerhaften Zustand versetzt. Wenn sich das System in einem fehlerhaften Zustand befindet, liegt nach obiger Definition ein Fehler vor. Für diesen Ansatz sprechen auch die Definitionen aus [Kop02], wo die Thematik in Fehlerursache (Fault), fehlerhaftem Zustand (Error) und Abweichung zwischen beabsichtigter und resultierender Funktion (Failure), weiter verfeinert wird. Diese Kategorien lassen sich jeweils noch mehrfach untergliedern, worauf an dieser

Stelle jedoch verzichtet und auf die entsprechende Literatur [Kop02] verwiesen wird.

Prinzipiell sind alle Komponenten eines Systems fehleranfällig, jedoch nicht auf die gleiche Weise und nicht im gleichen Ausmaß. Statistiken zeigen, dass die meisten Fehler, welche zu katastrophalen Folgen führen, aus Bedien- bzw. Steuerungsfehlern resultieren und meist aus unvorhersehbaren Situationen entstehen. An zweiter Stelle stehen Entwicklungsfehler - meist im Bereich der Software. Dabei stellt sich des öfteren heraus, dass sich die Fehler in der Entwicklungs- bzw. Implementierungsphase einschleichen, trotz einer korrekten und in sich konsistenten Spezifikation. Ein geringerer Anteil an Fehlern ist auf die mechanische Abnutzung und den Ausfall elektronischer Komponenten zurückzuführen.

Als Grundsatz bei der Entwicklung gilt es, die möglichen Fehlerquellen jeder Komponente zu suchen und zu beschreiben, so kann das Wissen über manche Fehlerquellen bereits in die Entwicklung mit einfließen. Dies gilt als eine präventive Maßnahme der Fehlererkennung und trägt, aufgrund des Vorwissens über Möglichkeiten und Wahrscheinlichkeiten der potenziellen Fehlerquellen, dazu bei, das aus der Fehlerwahrscheinlichkeitsanalyse resultierende Fehlermodell, deutlich zu verbessern.

Parallel zur Untersuchung der Fehlerquellen und der daraus resultierenden Fehlern, müssen auch die möglichen Auswirkungen derselben analysiert werden. Der Ausfall einer Komponente kann sich, neben der Nichterfüllung seiner Funktion, auf verschiedene Weise auf das Gesamtsystem auswirken. In sicherheitsrelevanten Anwendungen ist Hauptaugenmerk auf die Fehlerfortpflanzung zu legen, damit ein Fehler in einer Subkomponente nicht den Ausfall des gesamten Moduls oder Systems zur Folge hat. Die entsprechenden Fehlerauswirkungen müssen wiederum klassifiziert und entsprechend behandelt werden.

3.1.4 Fehlertoleranz

Die Eigenschaft eines fehlertoleranten Systems ist, dass es seine Funktion trotz auftretender Fehler, Ausfälle oder Anomalien ausführen kann. Um Fehlertoleranz zu garantieren, bedarf es komplexer und daher auch kostspieliger Lösungen. So müssen in einem fehlertoleranten System jegliche Komponenten mehrfach und voneinander unabhängig vorhanden sein, wodurch der Ausfall eines Funktionskreises überbrückt werden kann. Hier gilt dieselbe Regel wie bei der Sicherheit, und zwar ist es praktisch nicht möglich die 100%-Marke zu erreichen, da die Kosten mit einem immer größeren Gradienten steigen, je näher man sich an diese Grenze begibt. Die zusätzliche Fehlertoleranz wird durch die steigenden redundanten Komponenten erzielt, was eine di-

rekte Steigerung der Komplexität zur Folge hat. Das System wird schlechter überschaubar, wodurch sich zusätzliche Fehler einschleichen können. Zusätzlich steigt mit der Anzahl der verwendeten Komponenten, aus dem Gesichtspunkt des Gesamtsystems, die Ausfallwahrscheinlichkeit einzelner Subkomponenten. Deshalb ist es oftmals nicht rentabel, sich gegen derartige Fehler abzusichern, da sie mit einer äußerst geringen Wahrscheinlichkeit auftreten und nur durch enorme Kosten bewältigt werden können. In der Praxis muss stets ein Kompromiss zwischen Komplexität, Kosten, Leistung und Fehlertoleranzgrad gesucht werden.

Fehlertoleranz wird in vielen Systemen zur Steigerung der Verfügbarkeit eingesetzt. So z.B. bei Serverfarmen oder Satellitensystemen, welche extrem lange Laufzeiten (Jahre) und dem gegenüber kurze Wartungs- bzw. Recoveryzeiten (Sekunden, Minuten) aufweisen. Hat der Ausfall der Funktionalität hingegen schwerwiegende Folgen mit Personen- oder Umweltschäden diverser Schwere, so wird die Fehlertoleranz dazu genutzt, die Sicherheit solcher Systeme zu steigern. Je nach Art der Anwendung kann ein sicherer Zustand existieren, von dem keine Gefahr auf die Umgebung und das System ausgehen kann. Oft ist es ausreichend, bei Erkennung eines aufgetretenen Fehlers das System sicher und schonend (für die Umwelt und sich selbst) in diesen Haltezustand zu überführen. Derartige Systeme werden als fail-safe [SK98] bezeichnet. Falls die Komponente selbst einen sicheren Zustand besitzt und deren Übergang ohne externe Kräfte durchgeführt werden kann, spricht man von einem passiven fail-safe (FS) System. Bedarf es für das Erreichen des sicheren Haltezustandes eine besondere Aktion mit unterstützender, externer Energie, wird dies als aktives fail-safe-System bezeichnet. Existiert hingegen kein sicherer Zustand, wie z.B. bei einem fliegenden Flugzeug, so muss das System seine Grundfunktionalität trotz eines aufgetretenen Fehlers weiterhin erfüllen und wird als fail-operational (FO) bezeichnet. Im Bereich der Fahrzeugtechnik werden derartige Systeme weiters nach deren Anforderungszeitraum in "Langzeit FS" und "Kurzzeit FS" gegliedert.

Eine weitere Möglichkeit der Fehlertoleranz stellen sogenannte fail-silent (FSIL) Systeme dar, welche sich nach Auftreten eines oder mehrerer Fehler selbst ausschalten und somit die Funktionalität des Restsystems nicht beeinflussen.

Für diese Unterscheidung wird der Begriff der echten Fehlertoleranz eingeführt. Dies sind also Systeme, welche sich nicht in einen sicheren Zustand überführen lassen und deren Fehler oder Ausfall katastrophale (finanzielle und/oder menschliche) Verluste verursachen. Es ist hierbei erforderlich, dass die spezifizierte Grundfunktionalität trotz unerwünschter Effekte weiterhin gewährleistet wird und dabei keinerlei Anomalien erkennen lässt. In diesem Fall muss das System die Eigenschaft aufweisen, Fehler während der Ausfüh-

rungszeit sicher zu erkennen und entsprechend zu behandeln. Die Höhe der Fehlertoleranz kann wie folgt klassifiziert werden:

- Keine Fehlertoleranz: Das System hat mindestens einen Schwachpunkt, dessen Versagen den Verlust der Gesamtfunktionalität zur Folge hat (Single point of failure)
- Erhalt der kritischen Funktion: Es existiert kein Punkt, der bei Verlust seiner Funktion die sicherheitskritischen Grundaufgaben des Systems gefährdet. Für nicht kritische Funktionen besteht hingegen keine Gewähr.
- Degradierung: Die kritische Funktion geht durch Ausfall einer beliebigen Komponente nicht verloren, während die nicht kritische Funktion dadurch beschränkt (degradiert) werden kann.
- Temporäre Degradierung: Es existiert eine bestimmte Zeitperiode, wo nicht kritische Funktionen teilweise oder komplett verloren gehen. Nach der Rekonfiguration der verdächtigen Komponenten steht erneut der volle Funktionsumfang zur Verfügung. Ist auch die kritische Funktionalität vom Recovery betroffen, spricht man nicht von einem fehlertoleranten System, sondern von einem hoch verfügbaren System.
- Vollständige Fehlertoleranz: Das Gesamtsystem stellt seine Funktionalität, trotz auftretenden internen sowie externen Fehlern, Ausfällen und Anomalien mindestens bis zur nächsten Wartung oder bis zum Ende der jeweiligen Mission, zur Verfügung. Die gelieferten Ergebnisse sind sowohl im Werte- als auch im Zeitbereich stets korrekt. In einem vollständig fehlertoleranten System existiert kein single point of failure, kein Fehler ist nach außen hin bemerkbar, und Rekonfiguration und Recovery wickeln sich intern dermaßen schnell ab, dass sie sich für die Umwelt nicht bemerkbar machen (Transparenz). Weiters haben redundante Komponenten keinerlei Abhängigkeiten untereinander, damit ausfallende Teile vom System erkannt und deren Funktionalität auf die entsprechenden redundanten Bauteile übertragen werden. Dadurch erhält man ein virtuell fehlerfreies System. Es existieren jedoch Zeitpunkte, wo das System heruntergefahren werden kann und auch Wartungsarbeiten durchgeführt werden können.
- Nonstop: In diese Kategorie fallen Systeme, die ununterbrochene Verwendbarkeit garantieren müssen. Prinzipiell sind Systeme der drei vorangehenden Kategorien denkbar, lediglich muss die erforderliche Reparatur bzw. die Rekonfiguration während dem Betrieb durchgeführt

werden können (hot-plug). Deshalb wird ein sehr hohes Maß an Modularität vorausgesetzt. Beispiele für derartige Systeme sind das Stromnetz, das Telefonnetz, oder solche bei denen eine Wartung nicht bzw. nur durch extrem hohe Kosten möglich ist (Satelliten).

In fehlertoleranten Systemen muss neben dem Auftritt eines einzelnen Fehlers auch die mögliche Situation von mehreren, sogar verketteten Fehlern oder Ausfällen analysiert werden. Der Auftritt eines Fehlers kann in einem zweifach redundanten System einen Kanal ausschalten, so dass das System von nun an gegen einen weiteren, gleichartigen Fehler nicht mehr geschützt ist. Tritt ein solcher Fehler ein, bevor das System einer Wartung bzw. Reparatur unterzogen wurde, ist die Funktionalität gefährdet. Aus diesem Grund müssen permanente, interne Fehler gemeldet und möglichst rasch beseitigt werden. Weitere kritische Fälle einer Fehlerverkettung sind, wenn mehrere Fehler zeitgleich auftreten, und somit der Fehlererkennungsmechanismus überfordert ist und nicht alle Fehler erkennen kann, oder wenn Fehler direkt während der Recoveryphase einer bereits fehlerhaften Komponente auftreten. Die Wahrscheinlichkeit für derartige Fälle ist sehr gering und kann weiter verringert werden, indem Recovery und Fehlererkennungsmechanismen möglichst beschleunigt werden. Die Wahrscheinlichkeit wird dadurch dermaßen gering, dass etwaige Fälle vernachlässigt werden können. Problematisch sind jedoch Folgeausfälle, welche durch Fehlerfortpflanzung entsteht, und systematische Ausfälle, deren Gründe in Konstruktionsfehlern liegen. Beispiele dafür sind Überspannung, thermische Bedingungen, falsche Montage zweier redundanter Komponenten usw.

Aus diesem Grund werden sichere Systeme für mehrere gleichzeitige Fehler ausgelegt, was durch erhöhte Redundanz erreicht werden kann. Eine Kennzahl darüber ist der Robustheitsgrad des Gesamtsystems. Dieser gibt Auskunft darüber, wieviele interne Fehler das System garantiert tolerieren kann. Ein nicht fehlertolerantes System hat einen Robustheitsgrad von 0, während ein 2 von 2 System, welches einen Fehler oder Ausfall tolerieren kann, einen Robustheitsgrad von 1 hat [mon].

3.1.4.1 Redundanz

Mit der Notwendigkeit Systeme für sicherheitskritische Aufgaben einsatzfähig zu gestalten, steigen deren Anforderungen an die Zuverlässigkeit. Um den Eigenschaften derartiger Systeme gerecht zu werden, wird auf eine redundante Auslegung der Subkomponenten (mechanische Teile, Hardware und Software) gesetzt. Gerade im Bereich der sicherheitsrelevanten Anwendungen ist es unerlässlich, Systemmodelle zu verwenden, welche trotz auftretender Anomalien eine korrekte Funktionalität garantieren. Ausweg aus dieser

Problematik bietet die Redundanz. Dabei werden bestimmte Subkomponenten eines Systems zwei- oder mehrfach ausgeführt. Dies erlaubt erst dann von einem Systemausfall zu sprechen, wenn alle redundanten Komponenten zeitgleich ausgefallen sind. Um die Sicherheit zu erhöhen, wäre es demnach sinnvoll die Komponenten möglichst oft zu replizieren. Dies erhöht jedoch die Komplexität des Gesamtsystems und kann in bestimmten Situationen dazu führen, dass das System unbeherrschbar wird, indem sich Fehlererkennung und Fehlerfortpflanzung dermaßen komplex gestalten, dass sie nicht mehr im Verhältnis zur eigentlichen Funktion des Systems stehen. Die Komplexitätsgrenze variiert je nach Art und Bedeutsamkeit des Systems und kann nicht vereinheitlicht werden. Als Designziel gilt es demnach mit einer minimalen Anzahl und Grad an redundanten Bauteilen ein höchstmögliches Niveau an Fehlertoleranz zu erreichen. Dabei muss Redundanz in allen Bereichen adäquat vorhanden sein und nur eine Kombination aus mechanischer, elektronischer, Hardware- und Softwareredundanz kann zum angestrebten Ziel führen. Man unterscheidet folgende drei Arten der Redundanz:

- Heiße (aktive, parallele) Redundanz: Alle Kanäle der redundanten Komponente werden von Beginn an der gleichen Belastung ausgesetzt.
- Warme (leicht belastete) Redundanz: Die redundanten Elemente werden bis zum Ausfall des Arbeitselements lediglich leicht belastet.
- kalte (unbelastete) Redundanz: Die redundanten Elemente sind bis zum Ausfall des Arbeitselementes keiner Belastung ausgesetzt.

Redundanz durch Umschalten: Beim Ausfall der Arbeitseinheit wird auf das Reservesystem umgeschaltet.

Diese Unterteilung findet sich prinzipiell auch in der folgenden Klassifizierung [SK98] wieder:

- Statische Redundanz: In einem redundanten System werden mehrere Kanäle parallel betrieben. Das effektive Ergebnis der redundanten Einheit wird durch einen ausfallsicheren Entscheider [SK98] aufgrund einer Mehrheitsentscheidung ermittelt. Man erkennt eine gewisse Parallelität zur obigen Definition der heißen Redundanz.
- Dynamische Redundanz: In einem Mehrrechnersystem wird ein führender Rechner bestimmt, welcher über einen Multiplexer mit dem Ausgang verbunden wird, während die Ausgänge der restlichen Kanäle keine Verbindung zum Gesamtsystem aufweisen. Diese sind lediglich

einer Sicherheitskomponente zugeführt, welche auftretende Abweichungen des führenden Kanales erkennt und darauf am Multiplexer einen anderen Rechner durchschaltet. Je nach Art des Umschaltemechanismus (manuell oder anhand einer integrierten Komponente) lässt sich diese Kategorie als warme oder kalte Redundanz erkennen.

Betrachtet man die spezielle Situation der Sensoren, so muss hier nicht jede Komponente mehrfach vorhanden sein, sondern es ist möglich, bestimmte Größen von anderen Messwerten abzuleiten oder diese aufgrund physikalischer Eigenschaften, Stellgrößen oder Plausibilitätschecks grob abzuschätzen. Dadurch erhält man eine indirekte oder implizite Redundanz. So unterliegt zum Beispiel der Gradient der Temperaturveränderung im Kühlkreislauf gewissen physikalischen Grenzen und kann diese nicht übersteigen. Werden in einem System Zeitmesser(t), Geschwindigkeitsmesser(v) und Entfernungsmesser(d) eingesetzt, so kann jede der drei Messgrößen durch Kombination der beiden restlichen Werte bestimmt werden:

$$v = \frac{d}{t} \quad (3.7)$$

$$d = v \times t \quad (3.8)$$

$$t = \frac{d}{v} \quad (3.9)$$

Je nach Anwendung besteht die Möglichkeit, dass die Kombination zweier Subsysteme völlig unterschiedlicher Funktionalität zu Redundanz führen kann. So können beispielsweise bei einem Notfall im Flugzeug die Trimming-Stellflächen für die horizontale Stabilisierung eines Flugzeuges durch die Benzinpumpe ersetzt werden, indem der Kraftstoff von einem Flügel in den anderen befördert wird, um durch Gewichtsverlagerung die Horizontallage des Flugzeuges zu beeinflussen. Derartige Redundanzen sind nicht von vorne herein klar erkennbar und müssen in jedem System gezielt gesucht werden. Zudem können solche Techniken nicht verwendet werden, um die Sicherheit eines Systems zu garantieren, können sich in einer Notsituation jedoch als hilfreich erweisen, indem sie deren Auswirkungen gezielt entschärfen.

Um den für den Systemeinsatz geforderten Redundanzgrad¹ zu erreichen, werden die einzelnen Komponenten repliziert, wodurch die sogenannte homogene Redundanz erreicht wird. Hier ist kritisch anzumerken, dass Ent-

¹Redundanzgrad: Wenn von n parallelgeschalteten Elementen k redundant sind (d.h. $n-k$ Elemente können die geforderte Funktion erfüllen), so hat das System einen Redundanzgrad $(n-k)$ aus n [lex]

wicklungsfehler innerhalb einer Komponente auch durch einen beliebig hohen Redundanzgrad nicht kompensiert werden können, da alle (identischen) Module dementsprechendes Fehlverhalten aufweisen. Auf dieses Problem aufbauend wird die Thematik der Diversität (Abschnitt 3.1.4.2), und die dadurch erreichte heterogene Redundanz, interessant.

Eine redundante Bauweise allein ist trotzdem nicht die Lösung für die Realisierung fehlertoleranter Systeme. Es existieren weitere, teilweise noch unbekanntere Ereignisse, welche Auslöser für scheinbar unabhängige Phänomene sein können. Beispielsweise können starke Vibrationen oder Schläge auf den redundant ausgeführten Steuerrechner korrelierte Fehler verursachen. Es ist unter Umständen lebensnotwendig dafür zu sorgen, dass keinerlei Ereignisse alle Komponenten der redundanten Bauweise beeinträchtigen können. Deshalb muss eine weitestgehende Unabhängigkeit der Komponenten untereinander angestrebt werden (unabhängige, physikalisch getrennte Stromkreise, keine physikalisch nahegelegene Montage, möglichst unabhängige Gestaltung der redundanten Kanäle, usw.).

3.1.4.2 Diversität

Um Designfehler in redundanten Komponenten zu vermeiden, wird der Ansatz der Diversität in der Entwicklungsphase eingesetzt. Dabei ist man bestrebt, die einzelnen Komponenten zwar mit derselben Funktionalität auszustatten, jedoch deren Design, Entwicklung sowie die verwendeten Algorithmen und Programmiersprachen, sollen sich in einem möglichst hohen Grad unterscheiden und eine hohe Unabhängigkeit voneinander aufweisen. Die dabei angestrebte Vorgangsweise basiert auf der Annahme, dass verschiedene Entwicklungsteams verschiedene Lösungen finden und dazu verschiedene Denkweisen, Komponenten und Entwicklungsumgebungen verwenden. Dieser theoretische Ansatz ist jedoch nur teilweise korrekt. Ein Grund dafür ist, dass den einzelnen Entwicklungsteams oft ein- und dieselbe Spezifikation zu Grunde liegt, wodurch das Prinzip der Unabhängigkeit bereits verletzt wird. Zusätzlich kann die Spezifikation auch Fehler oder sogar Widersprüche enthalten, und dadurch das zu entwickelnde System signifikant beeinflussen. Werden komplett unabhängig erstellte Spezifikationen verwendet, erschwert dies die anschließende Entwicklung eines Auswertungsalgorithmus, welcher die Ergebnisse der beiden unabhängigen Kanäle vergleichen soll. Zudem sind die einzelnen Lösungswege durch allgemein übliche Vorgangsweisen bei der Modellierung meist nicht komplett verschieden und abhängige Konzeptfehler können sich einschleichen.

Es ist ersichtlich, dass es praktisch unwahrscheinlich ist, eine vollständig unabhängige Entwicklung durchzuführen. Außerdem bedeutet dies enorme

Zusatzkosten für den Entwicklungsprozess. Zum einen werden die sicherheitsrelevanten Subkomponenten zwei- oder mehrfach entwickelt, zusätzlich muss deren Unabhängigkeit bzw. diverse Lösungswege geprüft und beurteilt werden. Außerdem bedarf es geeigneter, fehlertoleranter Vergleichskomponenten, welche die Outputs der einzelnen Kanäle miteinander vergleichen und dadurch auf Fehlverhalten einzelner Komponenten schließt. Aufgrund der Vorteile im Bereich der Fehlererkennung und dessen positiver Beeinflussung der Verfügbarkeit des Gesamtsystems, ist der Einsatz diversitärer Entwicklung in sicherheitskritischen Anwendungen trotzdem unerlässlich. In der Praxis wird deshalb versucht, ein Kompromiss zwischen Sicherheit und Aufwand zu finden.

3.1.4.3 Möglichkeiten für ein Recovery

In fehlertoleranten Systemen übernehmen bei auftretenden Fehlern und Ausfällen einzelner Komponenten deren redundante Teile die Funktionalität. Die fehlerhafte Komponente wird zunächst einem internen Hardwaretest unterzogen. Ist dieser Test erfolgreich, kann mit hoher Wahrscheinlichkeit angenommen werden, dass beim Ausfall lediglich ein temporärer (transienter) Fehler vorlag. Der entsprechende Knoten kann erneut in das System reintegriert werden.

Treten beim Selbsttest erneut Fehler auf, lässt dies auf einen dauerhaften (permanenten) Fehler schließen, und die Komponente muss repariert oder ausgetauscht werden. Nach Behebung des Fehlers in der schadhaften Komponente muss diese wieder ins System eingebunden werden. Je nach Kategorie der Fehlertoleranz muss das Austauschen der Komponenten möglich sein, während sich das System im Betriebszustand befindet. Dabei muss der innere Zustand der reparierten bzw. neuen Komponente dem des laufenden Systems angepasst werden. Dazu existieren zwei Möglichkeiten:

- Backward-Recovery
- Forward-Recovery

Die wesentlich einfachere Methode ist das Backward-Recovery. Dabei werden während des normalen Programmablaufes sichere und stabile Zustände als eventuelle Wiedereinstiegspunkte gespeichert. Bei einer Wiedereinbindung einer Komponente wird das System in den letzten dieser Zustände zurückversetzt und der Zustand der Komponente wird dahingehend adaptiert. Natürlich ist diese Methode nicht in alle Systemen anwendbar, sondern lediglich dort, wo keine direkte Interaktion mit der physikalischen Welt existiert. Mögliche Verwendungsbereiche sind Datenbankserver und Telefonanlagen.

Komplizierter wird die Anwendung der Backward-Recovery-Strategie in einem verteilten System. Dort müssen bereits mehrere Komponenten durch gegenseitige Synchronisation einen gemeinsamen Wiedereinstiegspunkt erreichen. Werden hingegen vor der Wiederintegration nicht alle Komponenten untereinander synchronisiert, entsteht eine noch komplexere Situation, da sämtliche Nachrichten zurückverfolgt werden müssen, welche vom fehlerhaften Subsystem in der Zeit zwischen dem letzten Checkpoint für die Reintegration bis zum Ausfall gesendet wurden. Weiters ist nachzuvollziehen, welche Berechnungen und Aktionen aufgrund dieser Nachrichten inzwischen durchgeführt worden sind. Dies kann schnell zu einer unüberschaubaren Verkettung und deshalb zu einer nicht trivialen Problemstellung führen.

In jenen Fällen, wo die Anwendung einer Backward-Recovery aufgrund der Systemeigenschaften nicht anwendbar ist, wird die sogenannte Forward-Recovery eingesetzt. Als Beispiel hierfür können sämtliche Echtzeitsysteme angeführt werden, bei denen die Zeit eine wesentliche Rolle spielt. Dabei muss die wieder zu integrierende Komponente dem Zustand des Systems angepasst werden, und ohne jegliche Einschnitte bzw. Unterbrechungen für höhere Schichten, transparent eingebunden werden. Man behilft sich hierbei erneut einiger Checkpunkte, die bereits in der Entwicklungsphase mit eingeplant worden sind, und einen minimalen inneren Zustand der jeweiligen Komponente darstellen. Dadurch ist es möglich, die Übertragung des Zustandes auf die reparierte Komponente in einem möglichst kurzen Zeitrahmen durchzuführen, und dabei die Aktivität des Systems nicht zu beeinflussen. Das Recovery der Komponente wird bei Erreichen des nächsten zukünftigen Synchronisationspunktes durchgeführt. In manchen Echtzeitsystemen ist in der geplanten Abfolge von Systemzuständen ein sogenannter „ground state“ [Kop02] vorgesehen, wo keine Tasks aktiv sind, und sich alle Kommunikationskanäle im leeren Zustand befinden. Dieser Zustand eignet sich offensichtlich für einen möglichen Wiedereinstiegspunkt.

Eine andere Vorgangsweise bietet sich in verteilten Systemen mit mehreren Prozessorkernen. Dort wird die Komponente integriert und der Zustand wird einfach von den restlichen, in der Zwischenzeit weiterlaufenden, Prozessen ausgelesen und synchronisieren.

3.2 Der sichere Zustand im KFZ

Wie in den Abschnitten deutlich ersichtlich war, ist es für das Systemdesign entscheidend, ob im zu steuernden Prozessablauf ein sicherer Zustand in Form einer sicheren Halteposition, von der keinerlei Gefahren ausgehen, existiert. Zudem gilt es zu ermitteln, mit welchem Aufwand dieser energie-

niedrige Systemzustand eingenommen werden kann und welche Kosten dies mit sich bringt. Daraufhin kann entschieden werden, ob ein sicherer Zustand für die Verwendung im Gesamtsystem überhaupt geeignet ist und in welchen Situationen dieser eingenommen werden soll.

Überträgt man diese Problematik auf ein mit X-by-Wire ausgestattetes Kraftfahrzeug, stellt sich die Frage, ob es hier wirklich einen sicheren Zustand gibt. In Anlehnung an das Ruhestromprinzip [SK98], ist für den sicheren Zustand eine energiearme Situation zu favorisieren, in der keinerlei Gefahren von hohen Geschwindigkeiten, Spannungskräften oder anliegenden Drehmomenten ausgeht, und die Halteposition, trotz Ausfall der Energieversorgung, wenn möglich ohne Fremdeinwirkung, automatisch erreicht wird (passives Fail-safe System). Ein solcher Zustand ist in einem Kraftfahrzeug unumstritten der Stillstand. Das Problem ist allerdings der Ausfall der Funktionalität vor Erreichen dieser Situation. Zudem muss die Frage gestellt werden, wie der Zustandsübergang bei Erkennen eines ernsthaften Fehlers durchgeführt werden soll. Das Eingreifen der Bremsanlage, um einen schnellstmöglichen Stillstand zu erreichen, ist in Anbetracht einer realen Verkehrssituation nicht zu empfehlen. Zudem müssen Aspekte der Kurvenfahrt weiterhin berücksichtigt werden, so muss das Fahrzeug in jedem Zustand noch durch entsprechende Lenkeingriffe steuerbar sein.

Deshalb wird eine stufenweise Funktionalitätsreduzierung vorgeschlagen. Prinzipiell muss als erster Schritt die Art des Fehlers unterschieden werden. Fällt ein System, welches für übergeordnete Funktionalität (ABS, ESP, usw) zuständig ist, aus, so stellt dies zwar Einbußen im Funktionsumfang dar, die darunterliegenden Basisfunktionen (Bremsen, Beschleunigung, Lenkung) werden jedoch weiterhin ausgeführt. In einem derartigen Fall ist eine Warnung an den Fahrer auszugeben, damit dieser darüber informiert ist, dass elektronische Helfer nicht mehr korrekt funktionieren. Durch die Warnung soll der Fahrer seinen Fahrstil nach eigenem Ermessen adaptieren und das Fahrzeug sollte möglichst rasch zur nächsten Wartung gebracht werden, um den vollen Funktionsumfang wieder herzustellen.

Wird vom System festgestellt, dass ein zusätzlicher Fehler/Ausfall die weitere Funktionalität der Grundfunktionen beeinträchtigt oder diese sogar ausfallen kann, so ist der Übergang in ein Notlaufprogramm mit eingeschränkter Maximalgeschwindigkeit zu empfehlen. Dabei ist es beim Zustandsübergang nicht notwendig, diesen drastisch (etwa durch Einleitung einer Notbremsung) durchzuführen, sondern es soll ein verkehrstypischer Verlauf angestrebt werden, um allenfalls eine gefährliche Situation zu vermeiden. Eine dringende Wartung ist in diesem Fall unumgänglich. Ist zudem ein Totalausfall des Gesamtsystems möglich, so muss ein Shutdown-Prozess eingeleitet werden, der das Fahrzeug anhand aktiv eingeleiteter Bremsung in den Stillstand versetzt.

Übergeordnete Funktionalität durch Steer-by-Wire		
Agilitätsverbesserung	Stabilitätsverbesserung	Automatisierte Querführung
Basisfunktion		
geringer manueller Betätigungsenergiebedarf	keine Beeinträchtigung der Führungsfähigkeit im Normalfahrbereich	
Limp Home		
Lenken unter erschwerten Bedingungen		
Totalausfall		
kein Seitenkraftaufbau möglich	unkontrollierter Seitenkraftaufbau	

Tabelle 3.3: Stufenweise Degradation eines Steer-by-Wire Systems

Dabei ist ein Kompromiss zwischen Intensität der Bremsung und Sicherheit im Verkehr zu wählen, denn eine vom System automatisch eingeleitete Vollbremsung bringt das Fahrzeug in einen labilen Zustand und somit dessen Insassen in Gefahr und das Fahrzeug stellt als Verkehrsteilnehmer eine weitere Gefahrenquelle für Auffahrunfälle dar. Anhand dieser stufenweise Degradation wird das Fahrzeug dem sicheren Zustand immer näher gebracht. Es ist auch keineswegs auszuschließen, dass eine teilweise Degradation nur temporär stattfindet, während das Bordsystem in der Zwischenzeit durch ein eigenständiges Recovery seine volle Funktionalität wiederreicht und erneut voll einsatzfähig ist. Zudem können in einem mit stufenweiser Degradation ausgestatteten X-by-Wire System, Komponenten der obersten Ebene (mit übergeordneten Funktionen) im degradierten Stadium als Standby-Element für eine Basisfunktion dienen. Dadurch wird die Redundanz erhöht und die Erfüllung der Grundfunktionalität kann länger garantiert werden.

Die Stufen einer möglichen Degradation im Bereich der elektronisch gesteuerten Lenkübertragung ist aus Tabelle 3.3 ersichtlich. Dabei wird die Funktionalität der Basiselemente weiter unterteilt und ein sogenannter Limp Home eingeführt. Diese Strategie sieht im Notlaufprogramm eine weitere Degradationsstufe vor, wo die Steuerbefehle zwar umgesetzt werden, jedoch unter erschwerten Bedingungen, indem die Reaktion auf die Lenkbefehle etwa nicht mehr jener der Normalsituation entspricht. Diese Ebene ist der letzte Schritt vor einem Totalausfall, und es muss mit allen Mitteln versucht werden, die hier gewährte Funktionalität zu bewahren.

3.3 Elektromagnetische Verträglichkeit - EMV

Fahrzeuge stellen heute bereits eine Mischung aus analogen und digitalen Bauteilen dar. Durch die drastische Zunahme von Elektronikkomponenten und deren Einsatz in der Regelung bestimmter Grundfunktionen des Automobils (Bremsen, Lenkung), bedarf es einer adäquaten Berücksichtigung der elektromagnetischen Verträglichkeit (EMV). Die EMV ist in allen integrierten Systemen ein nicht zu vernachlässigendes Thema und wird wie folgt definiert:

EMV ist die Fähigkeit eines Systems, bei Anwesenheit von externen Störungen korrekt zu funktionieren und beeinflusst dadurch auch andere Systeme. Die EMV-Anforderungen betreffen alle Phasen des Entwicklungsprozesses und spielen offensichtlich eine große Rolle für die Sicherheit des Gesamtsystems. Deshalb existieren in sicherheitskritischen Anwendungen zudem verschiedene Normen², deren Einhaltung teilweise auch gesetzlich geregelt ist.

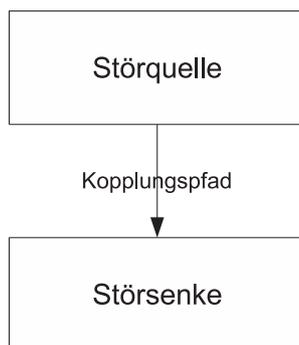


Abbildung 3.5: Zusammenspiel von Störquelle und -senke

Das theoretische Modell der Störkopplung geht von den Begriffen Störquelle, Kopplungspfad und Störsenke aus. Die Störquelle ist jene Komponente, welche die Störungen erzeugt. Die beeinflusste Komponente wird als Störsenke bezeichnet, und der Weg von der Störquelle zur Störsenke ist die Kopplung bzw. der Kopplungspfad. Störquellen und -senken können natürlicher oder technischer Natur sein. Beispielhaft für eine natürliche Störquelle steht der Blitz, während im selben Störkopplungsmodell ein Lebewesen die Senke sein kann. Technische Störquellen sind z.B. Frequenzumrichter, während Funkempfänger typische Störsenken sind.

Als Übertragungsart zwischen Störquelle und Störsenke unterscheidet man folgende Kopplungsmechanismen:

²EN 50082-2, EN 61000-4-2, IEC 1000-4-2, EN 50140 u.a.m.

- Galvanische Kopplung. Die galvanische Kopplung, oder Impedanzkopplung, entsteht an gemeinsamen Impedanzen des Störstromkreises mit dem Stromkreis der Störsenke. Dies können gemeinsame Bauelemente oder Leitungsabschnitte beider Stromkreise sein, worüber Ausgleichsströme fließen, und über die Impedanz des gemeinsamen Leitungsabschnitts Spannungen entkoppeln. Bei Leiterplatten kann eine Impedanzkopplung durch nicht ausreichend dimensionierte Massebahnen und Stützkondensatoren entstehen.
- Induktive Kopplung. Hier wird die Störsenke durch ein Magnetfeld beeinflusst. Dies entsteht üblicherweise in parallelgeführten Leiterschleifen.
- Kapazitive Kopplung. Die Senke wird hier durch ein elektrisches Feld gestört, z.B. hervorgerufen durch Überkopplung auf parallel geführten Leiterbahnen, oder Kabel in einem Kabelkanal.
- Strahlungskopplung. Die Strahlungskopplung wird von einem elektromagnetischen Feld ausgelöst. Als Beispiel können elektrische Leiter auf einer Platine als Antenne wirken und z.B. Radio- oder Funksignale empfangen, was die Übertragung störend beeinflusst.

Eine Störung entsteht dadurch, dass in der Störquelle eine Spannung oder ein Strom variiert wird. Daraus resultieren im Zeitbereich transiente oder periodische Spannungs- bzw. Stromänderungen $U(t)$ bzw. $I(t)$. Diese Signale ergeben, physikalisch bedingt, ein elektromagnetisches Spektrum im Frequenzbereich $U(\omega)$ bzw. $I(\omega)$, welches messbare Störungen in einem unerwünschten Frequenzbereich zur Folge haben, und sich über die zuvor genannten Kopplungsmechanismen weiter ausbreiten kann. Mathematisch gesehen kann dieses Verfahren als Fouriertransformation, welche eine Zeitfunktion $f(t)$ in eine Spektralfunktion $F(\omega)$ transformiert, beschrieben werden.

Um eine elektromagnetische Verträglichkeit, und somit die einwandfreie Funktion der Bauteile, zu gewährleisten, bedarf es einer Funkentstörung an der Störquelle und einer ausreichenden Störfestigkeit der Störsenke.

Im Automobilbau steigt die Tendenz, jegliche Aktuatoren mit eigenen Elektronikbausteinen und sogar Mikroprozessoren anzustatten. Derartige Komponenten müssen in den verschiedensten Umgebungen platziert werden. So muss sich ein Modul der Motorsteuerung beispielsweise im Bereich des Motorraumes befinden, wo natürlich extrem rauhe Bedingungen herrschen. Neben Schmutz und extremen Temperaturen sind die Komponenten Vibrationen und vor allem elektrischen, magnetischen oder elektromagnetischen Feldern ausgesetzt. Die Anforderungen an das verwendete Schutzgehäuse

sind dementsprechend hoch anzusetzen, um eine korrekte Funktionalität der Komponenten dauerhaft zu gewährleisten. Auf der anderen Seite steigt die Anzahl der Module mit hoher Bauteildichte und die Geschwindigkeit der Prozessoren. Zudem besteht der Bedarf, analoge und digitale Schaltkreise in ein und dem selben Gehäuse unterzubringen. Dies sind die größten Einflussfaktoren für elektromagnetische (EMI³) und hochfrequente (RFI⁴) Störungen. Weiters zeichnet sich in der Fahrzeugspezifikation der Trend zu einem höherfrequenten Bordnetz ab. Auch diese Eigenschaft wirkt sich entsprechend auf die EMV der jeweiligen Komponenten aus und muss im Designprozess berücksichtigt werden.

Um sich gegen derartige Störungen und Beeinflussungen aus dem Umfeld des Moduls zu schützen, werden diese in entsprechende Gehäuse gepackt. Dabei bedarf es eines Gehäuses mit physikalischem Schutz der Elektronik um vor allem Schmutz und Vibrationen zu widerstehen. Zusätzlich steht die Vermeidung von Emission und der Schutz vor Beschädigung durch EMI/RFI im Hauptaugenmerk einer gewünschten Schutzverkleidung. Für diese Anforderungen am besten geeignet sind metallische Abschirmungen. Die Herstellung derartiger metallischer Gehäuse erfolgt durch Gießen oder Pressen, was sich beim Bau integrierter Komponenten nicht immer als Vorteil erweist. Anhand eines Gießverfahrens können komplexe, verschachtelte Strukturen mit ausgezeichneten Schutzeigenschaften erreicht werden. Als nachteilig stellt sich das relativ hohe Gewicht, sowie die hohen Produktionskosten heraus. Das Pressverfahren stellt eine kostengünstigere Methode dar, erweist sich jedoch in der Robustheit und Flexibilität als unterlegen. Deshalb werden auch bereits Abschirmungsstrukturen aus Kunststoff gefertigt, welche anschließend mit einer metallischen Schicht überzogen werden. Der Strahlenschutz ist jedoch um ein Vielfaches geringer als in vollmetallischen Ausführungen und ist zudem an den Ecken stärker als an glatten Flächen.

Mit der zunehmenden Wichtigkeit der elektromagnetischen Abschirmung in den weitläufigsten Gebieten wird nach einer geeigneteren Materie für Abschirmungen gesucht. Forschern ist es bereits gelungen einen leitfähigen Kunststoff herzustellen, welcher hervorragende Eigenschaften, wie maximale und konstante Abschirmung, Reflexions- und Absorptionsfähigkeit und ei-

³Die elektromagnetische Beeinflussung (electromagnetic interference) ist eine durch magnetische und elektrische Felder verursachte Beeinflussung der Funktionalität anderer Geräte. Alle elektronischen Geräte geben, in Folge elektromagnetischer Aktivitäten, Emissionen ab und stören sich somit gegenseitig.

⁴Unter Hochfrequenzstörung (radio frequency interference) versteht man Störungen, die im hochfrequenten Bereich generiert werden und andere Geräte in ihrer Funktionalität beeinträchtigen.

ne zusätzlich hohe Oberflächenleitfähigkeit, aufweist⁵. Die Teile werden im derartigen Verfahren durch eine Spritzgusstechnik gefertigt. Dadurch lassen sich, vergleichbar mit dem Metallgussverfahren, komplexe Strukturen erzeugen. Das geringe Gewicht und die hohe Schutzwirkung versprechen eine noch kompaktere und leichtere Bauweise und machen die Technik interessant für die künftige Entwicklung.

3.4 Gefahr durch NEMP und HPM

Ein nuklearer elektromagnetischer Puls (NEMP) entsteht bei einer exoatmosphärischen, nuklearen Explosion, wobei auf der Erdoberfläche ein elektromagnetischer Puls mit steilem Anstieg zu verzeichnen ist. Diese Auswirkungen können je nach Höhe der Explosion ein riesiges Gebiet betreffen. Der starke Puls verursacht eine Einkopplung in Antennen und elektrischen Leitungen, welche neben Störungen auch zu Beschädigungen der einzelnen Bauteile und somit zu deren Ausfall führen kann. Untersuchungen und Forschung in diesem Bereich wurde bisher auf militärischer Ebene vollzogen [Sch06].

Ein weiterer Begriff ist jener der Hochleistungs-Mikrowellen (HPM). Durch Bestrahlung elektrischer Bauteile mit leistungsfähigen, gepulsten Mikrowellen wird deren Funktionalität, aufgrund der intensiven Störung der Strahlung, beeinträchtigt. Im militärischen Bereich wurde an Bedrohungsszenarien derartiger Angriffe gearbeitet und versucht die entwickelten Systeme entsprechend dagegen abzuschirmen.

Werden zukünftige Fahrzeuge mit X-by-Wire ausgestattet, wo die Grundfunktionalitäten der Fahrdynamik rein elektronisch angesteuert und beeinflusst werden, so stellen derartige, bisher rein militärisch interessante Szenarien, eine mögliche Gefahrenquelle dar. Durch Bestrahlung mit HPM oder durch Auslösen eines NEMP könnten damit nicht auszudenkende Verkehrssituationen entstehen. Neben einer enormen Anzahl an Verletzten würde der Personenverkehr zusammenbrechen, deren weitere Auswirkungen hier nicht weiter ausgeführt werden. Offensichtlich schafft man mit der Einführung zusätzlicher Innovation und Technik in den Alltag Möglichkeiten für neue Bedrohungen. Es ist eine Frage der Kosten und folglich der Rentabilität, ob es sinnvoll ist, die sicherheitsrelevanten Komponenten dermaßen zu schützen, damit sie etwaige Umstände überleben. Im militärischen Bereich ist diese Entscheidung trivial, dort spielen die Kosten in dem Sinne auch eine relativ geringe Rolle. Im Fahrzeugbau würde eine dermaßen hohe Abschirmung für

⁵Leitfähige Kunststoffe werden im Bereich der Polymerelektronik erforscht. Einer, für Entwicklungen in diesem Bereich ausgezeichneten Forscher, ist Prof. Dr. Alan J. Heeger von der University of California, Santa Barbara. [pol]

die Serienfertigung nicht tragbare Zusatzkosten mit sich bringen.

Im militärischen Bereich behilft man sich neben verstärkter Abschirmung, zusätzlich mit der Integration mechanischer Notlösungen, welche die elementarsten Funktionen eines Systems im Falle eines plötzlichen Totalverlustes des Bordnetzes, bewerkstelligen lassen. Die Übertragung derartiger Lösungsansätze auf das Fahrzeug wäre technisch natürlich denkbar, die Vorteile des eingesetzten X-by-Wire Systems können dadurch aber nicht voll ausgeschöpft werden. Die zusätzlichen Komponenten erschweren erneut den Einbau und stellen eine zusätzliche Gewichtsbelastung dar.

Zur Lösung der Problematik wird deshalb der Ansatz eines energiearmen sicheren Zustandes (Abschnitt 3.2) vorgeschlagen. Es ist ein System anzustreben, welches sich bei einem Komplettausfall der Elektronik eigenständig und möglichst ohne zusätzlicher Energie in den sicheren Zustand überführt. Dabei müsste in einer derartigen Situation eine Bremsung eingeleitet werden, sowie der aktuelle Lenkeinschlag beibehalten werden bzw. kontinuierlich und mit einer gewissen Verzögerung einer Geradeausfahrt angenähert werden. Wichtig ist natürlich die Einleitung der Bremsung, welche jedoch immer eine gewisse Energie benötigt. Wenn man davon ausgeht, dass keinerlei elektrische Energie und keine Befehle der Steuereinheit zur Verfügung stehen, muss auf eine geeignete gespeicherte Energie⁶ zurückgegriffen werden können, welche das Fahrzeug möglichst schnell, jedoch adäquat abbremst. Das Verhalten des Lenkeinschlages ist ein nächstes Diskussionsthema. Im massiven Fall, wo wiederum keinerlei Energie bzw. Steuerbefehle zur Verfügung stehen, ist es am einfachsten, den aktuellen Lenkeinschlag beizubehalten. Inwiefern eine derartige Lösung in allen Verkehrssituationen akzeptabel ist, bedarf es aus einer genaueren Untersuchung festzustellen. Die erforderlichen Zusatzkomponenten und deren Entwicklungsaufwand müssen jedenfalls einigen Rahmenbedingungen entsprechen. Man muss sich zudem immer die äußerst geringe Wahrscheinlichkeit einer solchen Situation vor Augen halten, welche derartige Maßnahmen erforderlich machen.

⁶Denkbar ist die Energie aus einer Feder, welche im Bremssattel sitzt. Bremsdruck aus einem Hochleistungsspeicher wäre eine weitere Lösungsmöglichkeit, jedoch bedarf es wiederum hydraulischer bzw. pneumatischer Leitungen, deren Einsatz in X-by-Wire Systemen jedoch vermieden werden soll.

Kapitel 4

Systemarchitektur

Die zukünftigen X-by-Wire Systeme müssen äußerst sicherheitskritische Funktionalitäten, deren Ausfall zu katastrophalen Folgen mit Menschenverlusten führen kann, erfüllen. Deshalb muss bei der Entwicklung besondere Sorgfalt auf die Korrektheit und das Auftreten von Fehlern, sowie deren Erkennung und Behandlung gelegt werden. Es bedarf einer eigenen Architektur des Gesamtsystems, welche den Verzicht auf die mechanische Rückfallebene erst ermöglicht. Eine solche Architektur umfasst, neben genereller Designprinzipien, die Festlegung der Strategie zur Erreichung des angestrebten Fehlertoleranzniveaus (Abschnitt 3.1.4). Darauf aufbauend beschreibt eine sicherheitsrelevante Architektur die enthaltenen Rechnersysteme, welche den Kern der Elektronik des Bordnetzes darstellen und legt, neben den Anforderungen und Eigenschaften der verwendeten Algorithmen und Software, die Grundlagen für die Systemkommunikation samt Eigenheiten fest. Über das Kommunikationssystem werden später die einzelnen Module und deren Sensorik und Aktuatorik untereinander kommunizieren. Weiters bedarf es auch einiger grundlegender Rahmenbedingungen im Entwicklungsprozess, welche eine fehlerfreie Systementwicklung überhaupt erst ermöglichen.

In diesem Kapitel wird versucht eine mögliche Gesamtarchitektur, geeignet für den Einsatz in X-by-Wire Projekten, zu beschreiben. Die Untergliederung hält sich dabei an die physikalischen Subkomponenten der Gesamtarchitektur, während einleitend einige grundlegende Architekturprinzipien und Definitionen im Bereich der fehlertoleranten Echtzeitsysteme abgehandelt werden.

4.1 Grundlegende Elemente der X-by-Wire Architektur

Einem X-by-Wire System muss aufgrund seiner hohen Anforderungen im Bereich der Sicherheit und seinem geforderten Echtzeitverhalten ein verteiltes und fehlertolerantes System zugrunde liegen. Aus der Praxis lässt sich in erster Linie der Bedarf an Zusammensetzbarkeit verschiedener Bauteile ableiten. Das Grundsystem muss trotz verschiedener Variationen der Ausführungen und damit mit den verschiedensten Komponenten und deren Konfigurationen kompatibel sein. Die Differenzen in den einzelnen Modulvariationen dürfen keineswegs Auswirkungen auf das Gesamtsystem und deren Funktionalität haben, genauso wenig soll ein Modul ein anderes Element in der Systemarchitektur beeinflussen. Diese Eigenschaften müssen auf jede Komponente im Gesamtsystem zutreffen, damit deren Funktionalität auch unter erschwerten Umständen garantiert werden kann.

Um diesen Voraussetzungen gerecht zu werden, bedarf es einer geplanten und konsequenten Vorgangsweise vom Entwurf bis hin zur Fertigstellung und Integration jedes Bauteiles. Jede noch so kleine Nuance muss genauestens analysiert und auf mögliche Fehlerursachen hin durchleuchtet werden. Komplexe Anwendungen werden in mehrere, simple Teilprozesse zerlegt, welche stets überschaubar bleiben und möglichst einfach auf Korrektheit geprüft werden können. Die so entstehenden Module werden über genau spezifizierte Schnittstellen aneinanderggeführt. Die Systemarchitektur darf in keinem Punkt Spielraum für Interpretationen offen lassen, sondern muss jegliche Aspekte vollständig - auch im Bezug auf Vorwissen und Kausalität - beschreiben. Nur so kann die Qualität des Gesamtsystems garantiert werden.

Es ist zu erwarten, dass ein einsatzfähiges X-by-Wire System aus mehreren fehlertoleranten Knoten bestehen wird, welchen es ermöglicht wird über einen geeigneten Kommunikationskanal Daten auszutauschen. Ein grundlegender Prinzipaufbau wird in Abbildung 4.1 dargestellt. Jede der Komponenten muss auf deren sicherheitskritischen Eigenschaften hin untersucht und entsprechend klassifiziert (siehe Abschnitt 3.1.2) werden. Dadurch kann die jeweilige Komponente ihren Sicherheitsanforderungen entsprechend entwickelt werden und dementsprechenden Sicherheitsmaßnahmen unterworfen werden, um im späteren Gesamtsystem die kritische Grundfunktionalität garantieren zu können. Zudem muss der eingesetzte Kommunikationskanal und die -methode sicherheitskritische Aspekte berücksichtigen und all den Anforderungen eines harten Echtzeitsystemes¹ gegenüber kompatibel sein. Näheres

¹Ein System ist dann ein hartes Echtzeitsystem, wenn es mindestens eine harte Deadline einzuhalten hat. Eine Deadline wird als hart eingestuft, wenn deren Nichteinhalten zu

zu den Eigenschaften, sowie ein Vergleich bestehender Kommunikationsprotokolle wird im Abschnitt 4.4 detailliert erläutert.

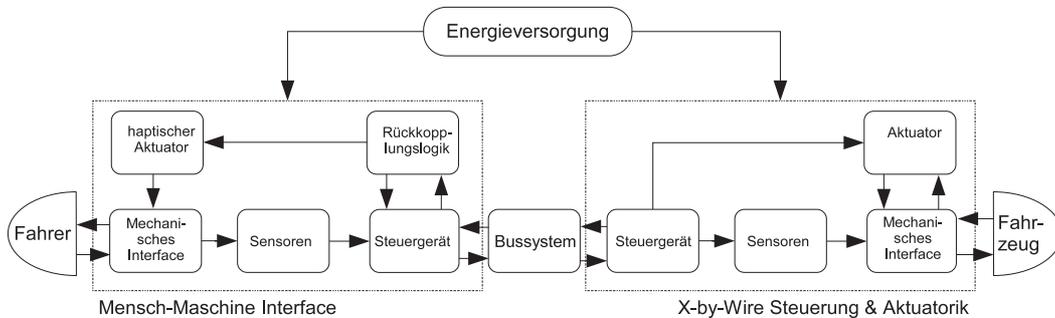


Abbildung 4.1: Grundaufbau eines X-by-Wire Systems

Bei der Entwicklung von X-by-Wire Systemen ist demnach ein zugrundeliegendes verteiltes System unabdingbar. Diese Art der Architektur bringt enorme Vorteile mit sich und hat sich gerade im Bereich der sicherheitskritischen Echtzeitsysteme weitestgehend durchgesetzt. Zum einen ist es angebracht, die Architektur des zu entwerfenden Systems an die gegebene physikalische Form der Maschine bzw. des Fahrzeuges anzupassen, was für ein vernetztes System spricht. Dabei können mehrere Hardwarekomponenten derselben Bauart integriert werden, welche an verschiedenen Positionen durch entsprechende Programmierung für unterschiedliche Funktionalität dienen. Dies ermöglicht wiederum eine kostengünstige Massenproduktion der verwendeten Hardwarekomponenten. Aufgrund der vorhandenen Kommunikationsbasis müssen die Hardwareknoten nicht in unmittelbarer Nähe der jeweiligen Sensoren bzw. Aktuatoren positioniert werden, sondern können zu Gunsten besserer Umgebungsbedingungen an einem dafür geeigneten Ort² montiert werden.

Ein weiterer, wichtiger Aspekt ist die Möglichkeit der Reparatur bzw. des Austausches fehlerhafter Komponenten. Durch den modularen Aufbau wird die Lokalisierung des Fehlers sowie eventuell erforderliche Reparaturmaßnahmen erst ermöglicht und kann durch vorhandene, redundant ausgelegte Knoten sogar, ohne einen Ausfall der Funktionalität und ohne Durchdringen an höhere Schichten, transparent durchgeführt werden. Das Gesamtsystem kann aus einem abstrakten Blickwinkel als ein Netzwerk ähnlicher Subkomponenten gesehen werden. Wichtig ist das Zusammenspiel der Knoten mit der darunter liegenden Kommunikationsebene. Die Anforderungen

katastrophalen Folgen führen kann.

²Günstige Montageorte für Steuerrechner sind etwa im Armaturenbrett oder im Kofferraum

der einzelnen Komponenten können stark variieren, vor allem deren Echtzeitbedingungen unterscheiden sich enorm. Das Prinzip der Modularität ist hier weiterzuführen, deshalb ist mit der Bereitstellung der Daten für den jeweiligen Knoten sein Task beendet. Im weiteren muss das Kommunikationsnetz für eine zeitgerechte und korrekte Übermittlung derselben sorgen. Es bestehen offensichtlich höhere Anforderungen an den Kommunikationskanal als in herkömmlichen Datenübertragungsverfahren, so müssen etwa die Daten zuverlässig und innerhalb einer gewissen Zeitspanne korrekt übermittelt werden. Zudem können Aspekte wie Steuerungsmechanismen, Fehlererkennung und globale Synchronisation von einem geeigneten Datenübertragungsverfahren zur Verfügung gestellt werden.

Wie bereits in der Einleitung angemerkt, muss bei der Entwicklung stets auf die Kompatibilität der verschiedenen Komponenten geachtet werden. In der Praxis wird nicht ein Gesamtsystem entwickelt, welches allgemein eingesetzt wird, denn jeder Automobilhersteller hat seine eigenen Zulieferer, von welchen die verschiedensten Bauteile bezogen werden. Um den Einsatz und das Zusammenspiel unterschiedlicher Bauelemente zu ermöglichen, bedarf es detailliert spezifizierter Schnittstellen. Dabei existieren bereits einige Verfahren, nennenswert ist die Interface Definition Language oder Interface Description Language (IDL). Es werden dabei lediglich die zur Verfügung stehenden Strukturen und Algorithmen des jeweiligen Modells beschrieben, nicht jedoch deren interne Realisierung. Bezüglich Echtzeitsystemen müssen neben Eigenschaften der übertragenen Daten und Funktionen auch Aspekte der Prozesssteuerung und die vorkommenden Kontrollsignale des Gesamtsystems umfassend in der Schnittstellendefinition vorhanden sein. Im System findet man deshalb eine Vielzahl an Schnittstellendefinitionen, ein Teil davon sind Schnittstellen zur Außenwelt, d.h. zwischen System und Benutzer, oder zu anderen Systemen. Der Rest sind systeminterne Schnittstellen, welche das Zusammenspiel der Komponenten untereinander ermöglichen. Jede dieser Schnittstellenkategorien weist erheblich unterschiedliche Anforderungen und Rahmenbedingungen auf. Beispielsweise unterscheiden sie sich in der Zeitanforderung, indem Benutzereingaben eine viel geringere Frequenz aufweisen als etwa ABS-Steuersignale vom Rechenknoten zum entsprechenden Aktuatormodul. Aufgrund der überaus großen Bedeutung der Schnittstellendefinitionen und der Bedarf einer konsequenten und genauen Umsetzung wurden diesbezüglich einige Standards verfasst. Beispielhaft kann in diesem Zusammenhang die Spezifikation J1708/1587 der Society of Automotive Engineers (SAE) angeführt werden, welche eine Fülle relevanter Nachrichten und Parameter im Bereich der Schwerfahrzeuge beschreibt.

Anhand der bisher beschriebenen Komponenten lässt sich bereits das Grundmodell einer möglichen Systemarchitektur für X-by-Wire Systeme be-

schreiben. Ergänzt werden muss dieses Modell durch die Eigenschaften der Erweiterbarkeit. Es muss die Möglichkeit bestehen, in einem bestehenden Netzwerk zusätzliche Knoten einzufügen oder ein weiteres Netzwerk anzubinden. Der Bedarf entsteht bei der Realisierung der verschiedensten Ausführungsvarianten, welche der Kunde im Automobilbereich heute bereits gewohnt ist. So muss ein einfacher Weg gefunden werden, die unterschiedlichen Komponenten der einzelnen Sonderausstattungen an das bestehende Bordnetz anzufügen. Zudem muss es möglich sein, zukünftig entwickelte Systeme möglichst einfach in das bestehende Netzwerk zu integrieren, ohne eine Umrüstung oder sogar eine Neuentwicklung der bestehenden Architektur vornehmen zu müssen. Davon betroffen ist vor allem das zu Grunde liegende Kommunikationssystem. Die Anzahl der Knoten kann theoretisch durch den Einsatz von Gateways, welche ein zusätzliches Netz an das bereits bestehende anbinden, erweitert werden. Zudem entsteht durch den Einsatz eines Gateways ein zweigeteiltes Netzwerk, welches in Summe höhere Kapazitäten zur Verfügung stellt. Ein dabei auftretendes Problem ist der Flaschenhals des Gateways zwischen den beiden Netzwerkteilen, weshalb dieser entsprechend dimensioniert und fehlertolerant sein muss.

In jedem Schritt der Entwicklung müssen die einzelnen Komponenten auf deren Abhängigkeiten hin untersucht werden. Diese sind weiter im System zu verfolgen, um auf diesem Weg bereits in der Entwicklungsphase zu einer späteren Fehlerrobustheit zu gelangen. Dabei werden die abhängigen Bereiche klar gekennzeichnet und über Schnittstellen mit weiteren abhängigen Bereichen verbunden. Durch Einplanung einer Fehlererkennungslogik (siehe Kapitel 3.1.3) in den jeweiligen Bereichen, können in einer Komponente auftretende Fehler bereits vor deren Ausbreitung auf andere Bereiche erkannt und korrigiert oder zumindest maskiert werden. So gelangen über die Schnittstelle keinerlei Fehler zu den anderen abgeschlossenen Bereichen, weshalb man sinngemäß auch von *error-containment-regions* sprechen kann. Diese Art der Fehlererkennung, eingesetzt in allen Stufen des Gesamtsystems, angefangen mit der Hardware bis hinauf zu den laufenden Applikationen, trägt wesentlich zur Zuverlässigkeit des Systems bei. Zudem wird durch die verstärkte Modularisierung in allen Bereichen des Systemaufbaues die Möglichkeit der Wartung und Reparatur wesentlich erleichtert.

4.1.1 Zeitbasis

Die Zeitmessung ist die Angabe von Messgrößen der Zeit in eindeutigen Maßeinheiten und umfasst die Bestimmung eines Zeitpunktes oder die Messung von Zeitintervallen auf einer Zeitskala. Aufgrund von Messfehlern entstehen Unterschiede in der Zeitmessung parallel laufender Systeme. Diese haben im

Alltag meist nur geringe Folgen und können somit vernachlässigt werden. In genauen mathematischen Modellen, oder in präzisen Algorithmen genügt eine allgemeine Zeitmessung jedoch nicht mehr. Bereits in der speziellen Relativitätstheorie von A. Einstein wurden Zeit und Raum aus einem nicht herkömmlichen Blickwinkel analysiert und es wurde gezeigt, dass diese beiden Größen stets in Relation, beispielsweise zu einer anderen Größe, stehen müssen, um klare und detaillierte Aussagen bzw. Messungen durchführen zu können und die Messergebnisse auch vergleichen und weiterverwenden zu können [ein].

Da der Aspekt der Zeit speziell in Echtzeitsystemen eine durchaus primäre Rolle spielt, muss innerhalb des Systems eine einheitliche Zeitbasis geschaffen werden, welche als Referenzzeit für alle internen Daten und Steuerungsbefehle gilt und damit die Zeitenstempel der einzelnen Knoten zueinander für Vergleiche relevant erscheinen lässt. In jedem Knoten des Netzwerkes läuft ein Oszillator, welcher aufgrund des Kostendrucks keine hohe Qualitäten aufweisen kann und deshalb relativ ungenau ist. Genauer betrachtet haben derartige Oszillatoren eine Driftrate im Bereich $10^{-4} \dots 10^{-6}$ s/s, während durch Einsatz hochwertiger Quarze, sowie dem Entgegenwirken von Temperaturunterschieden anhand eines Quarzofens, die Driftrate weiter gesenkt werden kann. Die Genauigkeit der herkömmlichen Oszillatoren und daher auch der in den einzelnen Knoten vorhandenen lokalen Uhren ist in einem verteilten System dieser Art aber keinesfalls akzeptabel. Zudem laufen die Uhren ohne entsprechende Synchronisation zunehmend auseinander, wodurch sich der Zeitunterschied im andauernden Betriebs immer vergrößern würde. Bei Messwerten beispielsweise, ist der Zeitpunkt der Messung für deren Gültigkeit ausschlaggebend. Denkt man hier an Messungen der Umlaufgeschwindigkeiten an den Rädern, welche als Inputdaten für das ABS-System dienen oder gar an die Position der Kurbelwelle im Motorblock, so wird deutlich, dass eine äußerst präzise und synchrone Zeit innerhalb des Systems dringend notwendig ist. Man behilft sich dabei durch verschiedene Algorithmen, welche die internen Uhren immer wieder angleichen und somit das gesamte Uhrenensemble einen gewissen absoluten Zeitunterschied nicht überschreitet. Das Abgleichen der einzelnen Uhren kann anhand einer Zustandskorrektur des internen Zählers erreicht werden, oder indem die Geschwindigkeit des Oszillators entsprechend adaptiert wird. Die Zustandskorrektur erfolgt durch Addition bzw. Subtraktion der ermittelten Zeitdifferenz und stellt somit einen nicht kontinuierlichen Verlauf auf der Zeitachse dar. Dies kann unvorhersehbare Probleme im System auslösen, weshalb für die Zeitanpassung eine Adaptierung der Oszillatorgeschwindigkeit, gegensätzlich dem lokalen Drift, zu bevorzugen ist. Für weitere Ausführungen zum Thema der globalen Zeit, sowie deren Grenzen und Algorithmen wird auf die Literatur [Kop02] ver-

wiesen. Durch Anwendung dort beschriebener Vorgangsweisen kann unter bestimmten Voraussetzungen und Abstraktionen eine globale Zeit eingeführt werden, anhand welcher alle auftretenden Ereignisse eindeutig klassifiziert werden können. Zudem erweist es sich als sinnvoll, das intern synchronisierte System in gewissen Zeitabständen an die internationalen Zeitstandards anzupassen. Besonders bei lange autonom laufenden Systemen zeigt sich diese Vorgangsweise erforderlichlich.

4.1.2 Zeitgesteuert - Ereignisgesteuert

Im Vorfeld des Designentwurfes stellt sich nun auch die Frage, nach welchem Prinzip das Gesamtsystem bzw. deren Kommunikation gesteuert werden soll. Es sind zwei verschiedene Ansätze denkbar - Zeitsteuerung oder Ereignissteuerung. Ein ereignisgesteuertes Modell bildet das Umfeld des Rechnersystems direkter ab, als es beim zeitgesteuerten System der Fall ist. Beim ereignisgesteuerten Ansatz wartet das System auf den Vorfall bestimmter Ereignisse, erst nach deren Auftreten wird der Rechenprozess gestartet oder wird eine entsprechende Information übertragen. So reagiert die Elektronik z.B. auf die Betätigung eines Bedienelementes, oder auf das Eintreffen von Messwerten eines Fahrwerksensors. Hardwaretechnisch lässt sich diese Strategie mit einer Interruptverarbeitung vergleichen. Es bietet die Vorteile, dass wenig Overhead erzeugt und abgearbeitet werden muss, indem lediglich jene Situationen verarbeitet werden, wo auch signifikante Ereignisse aufgetreten sind. Dadurch lässt sich im Normalfall ein ressourcenschonendes Design realisieren. Dieser Überlegung gegenüber steht das Problem, dass hochpriorere Ereignisse gegenüber anderen Tasks im System Vorrang haben müssen. Um dies zu implementieren, muss eine Prozesssteuerung realisiert werden, welche die laufenden Tasks vorzeitig unterbricht und dem hochprioreren Task die notwendigen Ressourcen zur Verfügung stellt. Nach Abarbeitung des hochprioreren Ereignisses wird wieder am ursprünglichen Punkt weitergearbeitet. Problematisch wird dieser Ansatz im Belastungsfall, falls etwa eine Kettenreaktion von wichtigen Ereignissen aufgrund eines Alarmes oder Fehlers ausgelöst wird. Die effektive Rechenleistung verringert sich mit zunehmenden hochprioreren Ereignissen. Da ein sicherheitskritisches System gerade in derartigen Situationen seine Vorzüge unter Beweis stellen muss, ist es unabdingbar, die Stabilität und Korrektheit des Systems in solch einem Fall zu bewahren. Aufgrund der einzeln zu bearbeitenden Ereignisse steigt die Anforderung an das System linear mit der Anzahl an auftretenden Ereignissen. Dies ist ein Indiz gegen die Stabilität und die korrekte Abarbeitung in einem Hochlastfall. Es kann hier nur durch eine deutliche Überdimensionierung der Ressourcen eine gewisse Art an Sicherheit gewährleistet werden, was aber deutlich gegen

die angestrebte, kostengünstige Produktion spricht.

Das zeitgesteuerte Modell ist im Vergleich zum ereignisgesteuerten System äußerst starr und unflexibel. In einem rein zeitgesteuerten System bewirken auftretende Ereignisse keinerlei direkte Auswirkungen, sondern das Verhalten bzw. der Zyklus wird bereits im Vorfeld bestimmt und bleibt in jeder Situation unverändert. Der Ablauf und das Verhalten wird im Prinzip nur durch das Fortschreiten der Zeit gesteuert. In einem vernetzten, verteilten System kann die Steuerlogik deshalb an die Komponente des Kommunikationskanales weitergegeben werden. Das heißt, die einzelnen Knoten signalisieren, dass sie Nachrichten zu versenden hätten, der Zeitpunkt der effektiven Übertragung ist jedoch von vorne herein bestimmt und kann nicht von den Komponenten oder von äußeren Ereignissen beeinflusst werden. Erst sobald ein Nachrichtenversand im definierten Zyklus vorgesehen ist, wird diese auch weitergeleitet. Das System läuft stets mit konstanter Belastung und weist keinerlei Spitzen auf. Diese Eigenschaft wird mit einem Mehraufwand im Leerlauf des Systems erkaufte, da der Zyklus, trotz keiner oder weniger abzuarbeitender Ereignisse, auf die gleiche Weise abgearbeitet wird. Für sicherheitskritische und echtzeitrelevante Systeme sind die Eigenschaften, welche ein zeitgesteuertes Design aufweist, offensichtlich wünschenswert, während der Mehraufwand bei niedriger Belastung keine weiteren Auswirkungen oder Nachteile mit sich bringt. Im Umfeld eines Fahrzeuges wird der Zustand der jeweiligen Bedienelemente zyklisch abgefragt, genauso wie die Werte an den Sensoren ständig abgefragt werden. Natürlich muss das zugrunde liegende System dementsprechend dimensioniert werden, damit keine relevanten Informationen aufgrund eines zu langsamen Zyklus verloren gehen können.

Eine weitere Variante ergibt sich daraus, dass in einer auch noch so hohen Abstraktionsebene nicht gänzlich auf die Ereignissteuerung verzichtet werden kann. Deshalb behilft man sich damit, dass die auftretenden Ereignisse limitiert werden, und gleichzeitig in der Periode des zeitgesteuerten Modells eine Bearbeitungs- und Kommunikationszeit des Systems für etwaige, unvorhersehbare Ereignisse reserviert wird. Durch die Einschränkungen an der Auftrittshäufigkeit der Rechen- und Kommunikationbeanspruchung haben derartige Events meist keine sicherheitskritische Bedeutung.

4.2 Sensoren

Der Einsatz von Sensoren in der Automobilherstellung hat, speziell seit dem Einzug der Mechatronik, stark zugenommen. Bereits die Überwachung der grundlegenden Funktionalitäten eines Fahrzeuges bedarf einer Vielzahl an Sensoren. Erweiterte Funktionalität und zusätzliche technische Lösungen er-

höhen die Anzahl der notwendigen Sensoren zudem. Im Folgenden werden im Automobil verwendete Sensoren nach deren Einsatzgebiet klassifiziert:

- **Antriebsstrang:** Hier findet man vor allem Sensoren zur Überwachung der Motorfunktion (Drucksensoren, Drehzahlsensoren), aber verstärkt auch Sensoren, welche Inputwerte für die eingesetzte elektronische Steuerung liefern (Ladedrucksensor, Umgebungsdrucksensor, Luftmassensensor usw.). Wird die elektronische Steuerung weiter ausgedehnt und die mechanische Verbindung vom Lenkstrang bzw. Bremssystem entfernt, so bedarf es zusätzlicher Sensoren wie Pedalwertgeber und Winkelgeber.
- **Komfort:** Diese Klasse der Sensoren liefert Werte an Navigationssystem, Klimatronic, Zentralverriegelung, Einparkhilfen usw. Es bedarf dabei Drehratensensoren, Luftgüte-, Feuchte- und Temperatursensoren, Drucksensoren und Abstandsensoren.
- **Sicherheit:** Auch im Bereich der Sicherheit haben sich zahlreiche mechatronische Systeme etabliert, einige davon sind ABS, ESP und Airbag. Um diverse Systeme im Bereich der Sicherheit bereitzustellen, bedarf es einer Menge von Sensoren, wie Abstandsradar, Neigungssensor, Drehmomentsensor, Lenkradwinkelsensor, Beschleunigungssensor, Gierratensensor, Neigungssensor usw.

Die erforderliche Präzision und Priorität der einzelnen Sensoren ist im Kraftfahrzeugbereich weit gestreut. In der Tabelle 4.1 wird ein Vergleich der Sensordaten im Motorbereich angeführt. Stellt man die daraus errechneten Gültigkeitsintervalle verschiedener Bereiche gegenüber, so ist eine Differenz von einigen Größenordnungen ersichtlich. Dies ist ein Maßstab für die erforderliche Flexibilität des darunter liegenden Steuersystems. Es wird zudem offensichtlich, dass die Granularität und Präzision der zuvor eingeführten globalen Zeit, hohen Anforderungen entsprechen muss, denn jegliche Messwerte sind nur in Kombination eines Zeitstempels relevant und weisen je nach Einsatzgebiet eine unterschiedlich lange Gültigkeit auf.

Messwert	max. Veränderung	Genauigkeit	Intervall
Position Kurbelwelle	6000 U/min	0,1°	3,6 μ s
Position Gaspedal	100%/s	1%	10 ms
Motorkraft	50%/s	1%	20 ms
Öl- und Wassertemperatur	10%/min	1%	6 s

Tabelle 4.1: Messwerte und Gültigkeitsintervalle in der Motorsteuerung

Anlehnend an [Kop02] stellt Tabelle 4.1 die unterschiedlichen Genauigkeiten und daraus resultierende Gültigkeitsdauer in verschiedenen Bereichen des Automobils dar. Im Bereich der Kolbenposition liegt die relevante Zeitspanne, mit angenommener Höchstdrehzahl von 6000 U/min und einer geforderten Genauigkeit von $0,1^\circ$, rechnerisch bei $3\mu\text{s}$. Es muss angenommen werden, dass der gemessene Wert nach dieser Zeitspanne nicht mehr gültig ist und deshalb nicht mehr verwendet werden darf. Deshalb muss der Sensor dermaßen ausgelegt werden, dass innerhalb der geforderten Intervalle immer wieder neue Messungen durchgeführt werden, die Messwerte entsprechend aufbereitet und an den jeweiligen Steuerknoten übertragen werden. Dieser berechnet die Steuersignale, welche wiederum an den entsprechenden Aktuator geschickt werden (in diesem Fall an die Einspritzanlage des Motors). Zudem ist dieser Task kritisch, denn ein falscher Einspritzzeitpunkt kann zu kapitalen Motorschäden führen, wodurch eine der Grundfunktionalitäten des Fahrzeuges verloren ginge. All diese Schritte innerhalb der geforderten $3\mu\text{s}$ verlässlich durchzuführen, liegt sogar oberhalb der Möglichkeiten aktueller Motorsteuerungssysteme. Deshalb behilft man sich in einer derartigen Situation mit der sogenannten state-estimation. Dabei fließen a-priori Kenntnisse des zu steuernden Prozesses und deren physikalische Eigenschaften in die Berechnung mit ein, sowie die konstanten Verzögerungswerte, welche für Kommunikation und Berechnung innerhalb des Steuerkreises benötigt werden. Dadurch wird der erwartete Zustand zu dem Zeitpunkt, wo das Steuersignal den Aktuator erreicht, vorausberechnet und entsprechende Steuerungsmaßnahmen eingeleitet.

Die bereits in Massen vorhandenen Sensoren werden in diesem Kontext vor allem durch zusätzliche Sensoren im Bereich der neuen Bedienelemente ergänzt, welche die Umstellung auf ein X-by-Wire System erst ermöglicht. Die restlichen Sensoren sind bereits aus heute eingesetzter Mechatronik wie ABS oder ESP bekannt. Interessant sind also Sensoren, welche den Fahrerwunsch bezüglich der Längs- und Querbewegung des Fahrzeuges messen und entsprechend darstellen. Wie bereits erwähnt, stellen diese Funktionen sicherheitskritische Aspekte im Automobil dar und die Messdatenerfassung muss deshalb äußerst zuverlässig sein. Es ist hier nicht von Bedeutung, welche Art der Bedienelemente effektiv eingesetzt wird, sondern es sollen zunächst die grundlegenden Anforderungen erörtert werden, welche später durch Einsatz verschiedener Komponenten realisiert werden können.

Das Designziel besteht darin, möglichst platzsparende, einfache und günstige Sensoren zu verwenden, damit die Steuerbefehle genau zu erfassen und anhand geeigneter Maßnahmen das geforderte Sicherheitsniveau zu erreichen. Zudem sollten die Sensoren möglichst geringen Verschleiß aufweisen, damit die Wartungsintervalle hoch angesetzt werden können und die Reparaturkos-

ten nicht derart ins Gewicht fallen. Die Art des jeweiligen Sensors ist natürlich stark von der zu messenden physikalischen Größe abhängig und in jedem Bereich kann die gewünschte Größe anhand verschiedener Meßverfahren ermittelt werden. Bei Dreh- und Bewegungssensoren werden vorwiegend Potentiometerlösungen, welche durch ihre niedrigen Preise, der einfachen Struktur und das durch langjährige Erfahrung gesammelte Know-How den Einzug in den Fahrzeugbereich gefunden haben. Allerdings weist das Potentiometermessverfahren prinzipbedingt Nachteile bei rauen Bedingungen, wie Temperaturschwankungen, Vibrationen und Verschmutzung auf. Zudem haben derartige Sensoren einen recht geringen Messumfang. Von diesen Problemen motiviert, wurde nach neuen Möglichkeiten und Messtechniken gesucht. In diesem Zuge wurden kontaktlose Sensoren [KG03] entwickelt, welche zur Zuverlässigkeit und Präzision zukünftiger X-by-Wire Systemen entscheidend beitragen sollen. Diese, auf einer induktiven Messmethode basierende Größenerfassung wurde bereits von namhaften Herstellern in Serienproduktionen umgesetzt und ist heute in großen Stückzahlen im Umlauf. Der bedeutendste Vorteil ist, dass durch die neuartige induktive Methode keinerlei mechanische Verschleißteile vorhanden sind. Zudem kann diese Bauweise durchaus in rauen Umgebungen eingesetzt werden, ohne eine negative Beeinflussung der Messwerte zu erhalten. Letzterer Aspekt ist in der Integration von Bedienelementen weniger von Bedeutung, da diese im Fahrzeuginnenraum platziert sind und daher lediglich moderaten Umgebungsbedingungen ausgesetzt sind. Jedoch wird dadurch der Einsatz derartiger Technologie für Systemteile im Bereich des Motorraumes äußerst interessant. Zudem stellt die verschleißlose Technologie in jeglichen Anwendungsbereichen Vorteile dar und trägt zur Zuverlässigkeit des Gesamtsystems bei.

Um die Funktionalität auch bei auftretenden Fehlern zu garantieren, muss auch im Sensorikbereich eine gewisse Redundanz vorhanden sein. Dies kann dadurch erreicht werden, dass mehrere baugleiche Sensoren verwendet werden und durch Mehrheitsentscheidung ein gemeinsamer Wert ermittelt wird. Mit k -facher heißer Redundanz können somit $\frac{k-1}{2}$ Fehler maskiert werden. Zusätzlich können Plausibilitätschecks, aufgrund bestimmtem Vorwissen bezüglich der gemessenen Größe, eingeführt werden. Stark verfälschte Messwerte können dadurch erkannt und vom weiteren Steuerungsprozess ausgeschlossen werden. Ein weiterer, vorteilhafter Aspekt kann durch das Prinzip der indirekten Redundanz erreicht werden. Anhand der Messung zweier verschiedener physikalischer Größen kann dabei auf eine dritte Größe geschlossen werden. Als klassisches Beispiel kann der Zusammenhang zwischen Beschleunigung, Geschwindigkeit und Zeit angeführt werden. Wenn am Bedienelement diese Größen für alle Freiheitsgrade bestimmt werden, so kann der Ausfall eines Sensors durch Berechnung des ausgefallenen Wertes kompensiert werden

bzw. Messfehler und Störeinflüsse in einzelnen Sensoren werden durch die laufende gegenseitige Kontrolle erkannt und ausmaskiert. Zudem verschafft man sich den Vorteil, dass Konzeptfehler bzw. prinzipielle Messfehler einer Messtechnik nicht an die darüberliegenden Schichten durchgereicht werden.

Die Tendenz geht zunehmend dahin, dass die Sensoren verstärkt mit Logikelementen kombiniert werden. Der entscheidende Vorteil liegt dabei in der Signalvorverarbeitung. Bestimmte Ausreißer der ermittelten Messwerte werden anhand der Aufzeichnung der letzten Historie in Kombination mit Informationen über den a-priori bekannten Verlauf entdeckt und entsprechend korrigiert. Zudem besteht die Anforderung, die meist analogen Messwerte zu digitalisieren. Auch dieser, inzwischen weit erforschte und bekannte Aspekt, wird im „intelligenten“ Sensor vorgenommen, damit die übergeordnete Logik einen reinen und verlässlichen Inputwert erhält und von der Messung vollkommen entkoppelt wird. Diese kontextbezogene Verlagerung einiger grundlegender Funktionen ist zudem für spätere Diagnoseverfahren interessant, da sich der Messwert andernfalls vom Sensor ausgehend über weitere Module erstrecken würde, bis er als reiner Inputwert bereitstehen würde, und eine Fehlerverfolgung bzw. Fehlerlokation sich nur erschwert durchführen ließe.

Adäquate Sensorik ist zudem auch für die Kontrolle der Aktuatoren erforderlich. Bereits beim Entwurf sollte darauf Rücksicht genommen werden, denn verschiedene Sensoren können dadurch mit doppeltem Nutzen eingesetzt werden. Somit bedarf es nicht unbedingt eigener Sensoren, welche die korrekte Funktionalität prüfen, sondern in den meisten Fällen kann der Aktuator durch indirekte Kontrolle überwacht werden. Innerhalb einer gewissen Zeitspanne nach Ausgang eines Bremsbefehles sollte beispielsweise eine messbare Verzögerung am Rad eintreten. Dadurch könnte ein Sensor am Schließmechanismus des Aktuators eingesetzt werden, der die korrekte Arbeitsweise kontrolliert. Durch Beobachtung der Sensorwerte direkt am jeweiligen Rad erhält man dieselbe Wirkung, zusätzlich wird die Funktionalität des gesamten Bremskreises bestätigt, und nicht lediglich die Aktivität eines einzelnen Stellteiles.

Mit den - teilweise negativen - Erfahrungen des Mechatronikeinsatzes in der Praxis lässt sich zunehmend der Bedarf eines hochgradigen Diagnose-systems feststellen. Dazu muss ein Konzept entwickelt werden, welches die Fehlersuche bzw. Fehlereingrenzung tatkräftig unterstützt und somit Reparatur und Wartungskosten einspart. Alle Verschleißteile und Problembereiche müssen, falls keine indirekte Messung möglich ist, durch aktive Sensoren überwacht werden. Damit lässt sich ein Fehler auf einen speziellen Problembereich zurückführen und gezielt lokalisieren.

4.3 Rechnersysteme

Die zentrale Rolle in allen elektronisch geregelten Anlagen stellen unumstritten die Steuereinheiten dar. Abstrahiert als Black-box erhält diese, durch verschiedene Inputwerte von den Sensoren, Informationen über den Zustand der Umwelt. Daraus werden die optimalen Steuersignale berechnet und an die Aktuatoren weiterleitet, welche gezielt in die Fahrdynamik des Fahrzeuges eingreifen. Für derartige Berechnungen sind komplexe Operationen notwendig, zudem soll es ermöglicht werden, Programme auf einer entsprechenden Abstraktionsebene für solch ein System zu erstellen. Die hohe Performance der Mikroprozessoren, neben deren zunehmender Miniaturisierung und sinkenden Kosten, lässt für deren Einsatz keine Alternativen offen. Der allgemein starke Absatz von Mikroprozessoren sorgt, neben Preisvorteilen, auch für steigende Zuverlässigkeit und ausgiebige Testerfahrungen. Deshalb weisen sie eine relativ geringe Fehlerhäufigkeit auf und haben somit bereits Einzug in den Bereich der Mechatronik gefunden.

Das große Problem der Mikroprozessoren im Einsatzgebiet von sicherheitskritischen Prozessen ist jedoch deren hoher Komplexitätsgrad. Dank der stark zugenommenen Miniaturisierung werden auf heute aktuellen Chips bereits Milliarden von Transistoren, und somit eine unüberschaubare Vielzahl an Gattern und Verbindungen, verbaut. Erst dadurch wird die heute erreichte Performance ermöglicht. Parallel zur Miniaturisierung werden jedoch auch die Verbindungen und Isolationsschichten immer feiner und dünner, zusätzlich wird eine höhere Leistungsdichte erreicht. Damit steigen allerdings auch die Fehlerquellen schlagartig an. Problematiken wie Elektromigration³ und Gate-Oxid wear-out⁴ werden durch die steigende Integration zusätzlich verschärft und stellen Sicherheitslücken beim Einsatz derartiger Hardware dar. Allerdings treten Fehler, deren Ursprung auf solche Probleme zurückzuführen sind, erst nach langem Betrieb oder überdurchschnittlicher Belastung der Hardwarekomponente auf und fallen somit in die Phase des allgemeinen Alterungsprozesses. Als Ergebnis verkürzt sich somit die Lebenserwartung des Chips. Es ist offensichtlich, dass sich, aufgrund eingeschlichener Fehlerquellen im Designprozess, welche durchaus aus der physikalischen Natur der Elemente stammen und sich nicht gänzlich vermeiden lassen, keine 100%ig zuverlässige Hardware herstellen lässt. So können etwa kleinste Verunreini-

³Eine hohe Stromdichte hat zur Folge, dass eine Vielzahl an rasch bewegten Elektronen entsteht, welche die Atome der leitenden Materie verschieben. Durch diese Verlagerung verengen sich die Verbindungsleitungen und an den Enden bilden sich unerwünschte Anlagerungen (Hillocks)

⁴Mikroskopische Verunreinigungen im Isolator bilden Störstellen und erhöhen die ungewünschten Tunnelströme (Leakage)

gungen bei der Prozessorherstellung bereits zu enormen Fehlerquellen führen. Um schlechte Teile bereits vor Auslieferung auszuschneiden, werden die Teile streng getestet und einem so genannten Burn-in unterzogen. Dabei werden die Teile überdurchschnittlich hoch beansprucht, in zudem rauen Umgebungsbedingungen (hohen Temperaturen), damit Schwachstellen sofort erkennbar werden und die auftretenden „Kinderkrankheiten“ damit frühzeitig erkannt, und die fehlerhaften Elemente ausgesondert werden können.

Einzig im militärischen Bereich entwickelt man an höchst sicheren Lösungen und geht dabei den Weg, für den jeweiligen Zweck gezielt Prozessoren zu fertigen, welche nur mit den für den jeweiligen Verwendungszweck notwendigen Komponenten ausgestattet werden. Damit wird eine weitaus geringere Komplexität erreicht, der Überblick ist einfacher zu bewahren und formale Korrektheitsbeweise sind machbar. Fehler sind hier zwar unwahrscheinlicher, aber trotzdem nicht auszuschließen. Eine spezielle Chipentwicklung für den zivilen Einsatz ist wirtschaftlich jedoch nicht tragbar.

Eine weitere Auswirkung des hohen Komplexitätsniveaus eingesetzter Mikroprozessoren ist, dass deren Funktionalität lediglich durch Tests erprobt werden kann, es aber nicht möglich ist, einen kompletten und formalen Korrektheitsbeweis zu erbringen. Trotz den aufgezeigten ungelösten Problemen, werden derartige Prozessoren in allen verschiedensten Bereichen eingesetzt. Laut Statistiken erreicht man durch den Einsatz geeigneter Fehlererkennungsmechanismen eine Fehlererkennungswahrscheinlichkeit von bis zu 95%. Dieses Niveau reicht für die meisten Anwendungen aus. Derartige Tests beziehen sich jedoch immer auf die begrenzte Anzahl der Testdaten und können, wiederum aufgrund der zu hohen Komplexität der Bausteine, nicht allumfassend sein.

Wie in allen sicherheitskritischen Prozessen, so ist auch bei der Realisierung der Grundfunktionalitäten im X-by-Wire System der Einsatz derartiger Komponenten ohne zusätzlichen Vorsorgemaßnahmen, abzuraten. Dadurch würde sich der Fahrer durch die Benutzung des Fahrzeuges, neben der unerwünschten Verkürzung der Wartungsintervalle und Steigerung deren Kosten, auf ein erhöhtes Risiko einlassen. Deshalb ist eine angemessene Hardwareredundanz, wie beispielsweise eine TMR⁵ im Hinblick auf die geforderte Sicherheit bzw. Zuverlässigkeit unumgänglich, um einen gewissen Grad an Verlässlichkeit trotz auftretender Fehler zu gewähren. Zudem muss das Thema der Hardwarediversität betrachtet werden. Durch den Einsatz verschiedener Architekturen in den einzelnen Redundanzkanälen sinkt die Wahrscheinlichkeit eines parallelen Desinfelers sprunghaft. Die extrem hohen Kosten, welche

⁵Triple-Modular-Redundancy - Dreifach heiße Redundanz mit ausfallsicherem Mehrheitsentscheider

durch doppelte und unabhängige Entwicklung der einzelnen Kanäle entstehen, sind jedoch meist für das Scheitern dieses Designprinzips ausschlaggebend.

Der vielversprechendste Ansatz ist demnach der Einsatz verschiedener Techniken, um Fehler im Designprozess der Steuereinheit zu vermeiden bzw. diese frühzeitig zu erkennen und entsprechend zu behandeln. Ein unter solchen Bedingungen hergestellter Mikroprozessor kann somit in verschiedensten sicherheitskritischen Anlagen eingesetzt werden und erzielt zudem Preisvorteile aufgrund seines hohen Absatzes. Dazu muss in der Vielzahl an zur Verfügung stehenden Mikroprozessoren nach einem für die jeweilige Situation geeigneten Prozessor gesucht werden. Durch Vergleich der Eigenschaften und Architekturmerkmale und der dazu kompatiblen Zusatzmodule, lässt sich ein Sortiment der engeren Wahl finden. Zu berücksichtigende Eigenschaften könnte der Umgang mit ungültigen Operationscodes (bei auftretenden Fehlern), die Integritätsanforderung sowie natürlich der Leistungsumfang sein. Es haben sich auch bereits einige Modelle verschiedener Hersteller herauskristallisiert, welche verstärkt in sicherheitskritischen Applikationen eingesetzt werden und durchaus ihren Erwartungen gerecht werden.

Das Rechnersystem beinhaltet neben dem Mikroprozessor natürlich noch weitere Komponenten, deren sicherheitstechnische Relevanz im folgenden kurz angeführt wird:

- Widerstände, Widerstandsarrays und Potentiometer: Bei allen diesen Komponenten wird ein Betrieb deutlich unter deren Belastungsgrenze vorausgesetzt. Somit lässt sich bis auf einen gewissen Drift (in digitalen Schaltungen jedoch nicht weiter störend) und einem eher unwahrscheinlichen Bruch bzw. Kurzschluss, keinerlei sicherheitskritische Merkmale erkennen.
- Kondensatoren: Fehlerannahmen sind hier Unterbrechung oder Kurzschluss sowie ein begrenzter Drift.
- Dioden: Kurzschluss und Unterbrechung gelten als Fehlerannahmen. In einem Fehlerfall sind Veränderungen der Kennlinie und der Frequenzcharakteristik zu erwarten.
- Transistoren und Operationsverstärker: Unterbrechung, Kurzschluss sowie Abnahme der Verstärkung sind in einem Fehlerfall zu verzeichnen. Zusätzlich besteht die Möglichkeit eines fehlerhaften Schwingens.
- Optokoppler: Unterbrechungen einzelner Anschlüsse, sowie Kurzschlüsse zwischen den beiden Ein- oder Ausgängen sind relevante Fehlerannahmen.

- Schwingquarze: Problematisch ist vor allem die umgebungsabhängige Driftrate des erzeugten Taktes. Wird in Echtzeitsysteme durch die Definition der globalen Zeit kompensiert.
- A/D und D/A Wandler: Kurzschlüsse und Stuck-at-faults⁶ sowie Übersprechen der Ausgänge werden hier als Fehlerannahmen getätigt.
- digitale Bauelemente: Inverter, Latch, Bustreiber, Speicher: Als Fehlermöglichkeiten sind Unterbrechungen, Kurzschlüsse und Übersprechen an beliebigen Stellen, sowie der Stuck-at-Fault zu erwähnen.

Es ist zunächst erschreckend, welche Anzahl an Fehlern in einem Rechnersystem auftreten können, durch deren Berücksichtigung im Designprozess können die meisten dieser Gefahren jedoch erfolgreich maskiert und damit beseitigt werden. Zusätzlich ist die Architektur einiger obgenannter Komponenten, wie der Optokoppler und der Widerstand, durch DIN-Normen geregelt, welche ein gewisses Qualitätsniveau vorschreibt. Auch die Verwendung bestimmter Materialien wird durch diese Normen geregelt. Kombiniert mit der bereits jahrzehntelangen Erfahrung mit analogen Bauteilen ist deren Sicherheitsrisiko rückläufig. Die Berechenbarkeit des Restrisikos ist jedoch aufgrund der Komplexität des Gesamtsystems nicht trivial und die Sicherheit nur durch Redundanz erreichbar.

Die bisher stattgefundene Entwicklung kann als eine immer wiederkehrende und verstärkte Aufrüstung einer mechanischen Fahrzeugbasis mit elektronischen Zusatzkomponenten gesehen werden. Diesem Entwicklungsprozess entstammen zwar lauffähige Systeme, welche jedoch kennbare Defizite im Bereich der Benutzerfreundlichkeit, Zuverlässigkeit und Wartbarkeit aufweisen. Ein zentraler Punkt ist dabei die hohe Anzahl an verschiedenen Steuerrechnern, welche in aktuellen Fahrzeugen verbaut wird. Momentan besteht die Philosophie, dass jede Zusatzfunktion sein eigenes Modul benötigt, welche den Kundenwünschen entsprechend eingebaut werden. Somit erreichen heutige Fahrzeuge, besonders jene der Oberklasse, eine derartige Vielzahl an heterogenen Steuergeräten, welche selbst für den Fachmann schwierig zu überblicken ist. Dies stellt zudem Nachteile bei der Fehlerdiagnose, Reparatur und Wartung dar. Zusätzlich ergeben sich vermehrt korrelierte Fehler, welche zu „unerklärlichen“ Fehlern führen und die elektronischen Systeme in der Öffentlichkeit in ein schlechtes Licht rücken.

Ein Verbesserungsvorschlag in dieser Hinsicht ist das Zusammenführen mehrerer Steuerrechner, getrennt nach logischen Bereichen, zu einem zentra-

⁶Bei einem Stuck-at-Fault klemmt der Ausgang eines logischen Bauteiles auf logisch „0“ bzw. „1“ fest.

len Steuergerät. Dieses müsste intern die nötigen Redundanzen und durchgängige Unabhängigkeiten aufweisen, nach außen sind sie jedoch als abgeschlossene fehlertolerante Einheit zu sehen. Wird dieses Konzept auf X-by-Wire Fahrzeuge übertragen, bedarf es dort einer Steuereinheit, welche im Hinblick der zuvor beschriebenen Eigenschaften höchste Sicherheit aufweist und für die Basisfunktionen zuständig ist. Diese steuert somit die Brems- und Lenkungsaktuatoren, je nach Vorgaben der Steuerbefehle an dem Bedienelement. Diese unterste Recheneinheit muss in höchstem Maß fehlertolerant ausgelegt sein, damit ein Verlust dieser Funktion auch in Extremsituationen ausgeschlossen werden kann.

Ähnlich einem Layerprinzip befinden sich, diesem System überlagert und dessen Funktionalität nutzend, weitere Steuereinheiten, welche für die Bereitstellung höherer Funktionen verantwortlich sind. Auch diese müssen verstärkt nach logischen Zusammenhängen gegliedert werden.

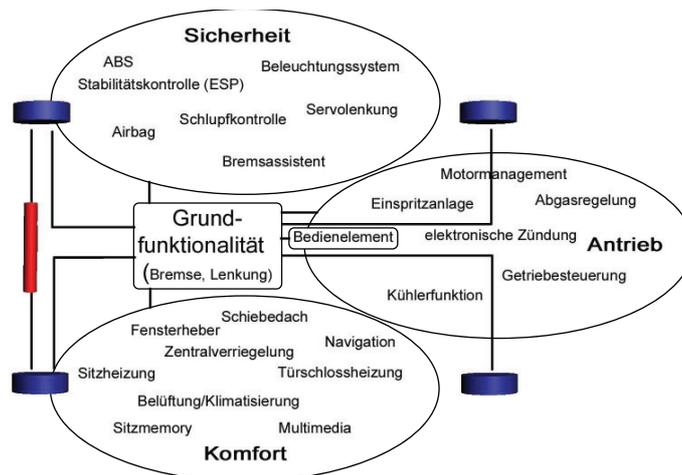


Abbildung 4.2: Mögliche Architektur mit Funktionsklassen

Durch die aus Abbildung 4.2 ersichtliche Strukturierung erhält man eine logische Klassifizierung der einzelnen Steuergeräte, und auftretende Fehler können eindeutiger der jeweiligen Komponente zugeordnet werden. Darüber hinaus ist es in einem gewissen Maße ressourcenschonend, wenn ähnliche Aufgaben in einer gemeinsamen Komponente durchgeführt werden. Mehrere überlagerte Sicherheits- bzw. Komfortsteuerungen können in einem fehlertoleranten Zentralrechner zusammengefasst werden, nicht wie bisher für ABS ein eigenes Steuergerät verbauen, für ASR ein weiteres usw. Gegen dieses Design spricht allerdings, wenn auch nur in einem gewissen Maße, die heute angewandte Individualisierung des Fahrzeuges durch selbst kombinierbare Extraausstattung. So wird eine ESP-Komponente zum Beispiel erst dann

eingebaut, wenn diese auch vom Kunden bestellt wird. Besteht diese in der Fertigung eindeutig zu Kostensteigerung führende Politik der Autohersteller weiterhin, so kann dies auch mit der neuen Architektur, durch verschiedene Softwareausführungen im jeweiligen Steuerknoten realisiert werden. Die Zusatzkosten der überdimensionierten Steuereinheit werden durch die Ersparnissen aus den vereinfachten Einbau und vor allem der Vorteile in der Zuverlässigkeit, Flexibilität und Wartung kompensiert.

Eine zentrale Steuereinrichtung, welche für sicherheitskritische Systeme entsprechend konzipiert wurde, vereinfacht zudem die Konfiguration des Systems, indem eine einheitliche Schnittstelle zum jeweiligen Subsystem besteht. Der Einbau kann genauso an dafür geeigneten Positionen erfolgen, denn der Verkabelungsaufwand ist aufgrund der verwendeten Busstruktur akzeptabel.

Der Prinzipaufbau ist somit der Funktion des Gesamtsystems angepasst und stellt keine ständige Erweiterung eines bestehenden Systems dar. Eine Vielzahl an heute auftretenden Problemen kann durch eine, von Grund auf neu konzipierte und den neuen Anforderungen und Möglichkeit entsprechend durchdachte Architektur, bereits vor deren Entstehung beseitigt werden. So sind etwa grundlegend neue Raumkonzepte, eine revolutionäre Bedienung sowie bis heute nicht vorstellbare Sicherheits- und Komfortaspekte realisierbar. Ein erster Schritt in diese Richtung ist die Neukonzeption der zugrundeliegenden Basis, denn letztendlich baut das gesamte Fahrzeug darauf auf.

4.4 Kommunikation

Die Datenkommunikation gewinnt im Automobilbereich zunehmend an Bedeutung. Die ersten eingesetzten Sensoren wurden durch Punkt-zu-Punkt Verbindungen mit den jeweiligen Elektronikbauteilen fest verdrahtet, was im Laufe der Zeit einen Kabelbaum im wahrsten Sinne des Wortes entstehen ließ. Mit der steigenden Anzahl an elektronischen Sensoren und zusätzlichen Bedienelementen, vor allem im Bereich der Komfortsteuerung, stieg der Aufwand der Verkabelung, deren hohe Anfälligkeit und schlechte Handhabung weiter und forderten Einsatz eines Datenbusses. Der Einsatz von flexiblen und schnellen Datenbussen im Fahrzeug wird durch folgende Aspekte bestätigt:

- Gewicht- und Kosteneinsparung bei der Verkabelung
- Flexibilität bei Integration zusätzlicher Komponenten
- Hohe Geschwindigkeit in bestimmten Steuerkreisen (z.B. Motorsteuerung)

- Hohe Zuverlässigkeit im Zeit- und Wertebereich in sicherheitskritischen Bereichen
- Interne Kommunikation und Mehrfachverwendung von Informationen
- Steigende Anforderungen im Multimediabereich
- Bedarf an Diagnosesystemen und Zugang für eine einfache Rekonfiguration des Systems
- Die rasante Entwicklung im Elektronikbereich ermöglicht den Einsatz neuer Konzepte, welche zur Sicherheit und zum Fahrkomfort beitragen. Diese erfordern eine in zunehmenden Maße adäquate und flexible Kommunikationsstruktur.

Schon bald wurden erste Bussysteme für die Steuerleitungen im Kraftfahrzeug eingesetzt. In einem herkömmlichen Automobil konnten dadurch bis zu 1 km Kabel eingespart werden, was klar für die Kosten- und Gewichtsreduktion spricht. Die Hersteller entwickelten jeweils verschiedene, konzerninterne Lösungen und setzten diese auch ein. Jedoch stieg immer mehr der Wunsch nach genormten Standards, denn die Zulieferer der Autohersteller wechselten mit der Zeit, und zudem stieg der Kostendruck im Automobilbau. Aus diesem Grund wurden einheitliche Bussysteme, welche gewissen Standards unterliegen, entwickelt. Trotzdem existiert eine Fülle an verschiedenen Bussystemen, diese Entwicklung ist jedoch auf die verschiedenen Anforderungen in den einzelnen Bereichen eines Fahrzeuges zurückzuführen. So fordert beispielsweise ein modernes Multimediasystem hohe Durchsatzraten neben moderater Echtzeitfähigkeit. Das Motormanagement, hingegen erfordert, wie im vorhergehenden Abschnitt (4.2) beschrieben, bei kurzen Nachrichten eine sehr hohe Übertragungsgeschwindigkeit, sowie äußerste Präzision. Im Bereich der sicherheitsrelevanten Applikationen wird höchste Ausfallsicherheit und hohe Echtzeitfähigkeit vorausgesetzt, während im Bereich der Bordelektronik (Fensterheber, Klimaautomatik) wieder geringe Anforderungen bezüglich Geschwindigkeit und Echtzeit bestehen.

Daraus ergibt sich eine Reihe von Eigenschaften, welche beim Einsatz eines bestimmten Busses berücksichtigt werden müssen. Es treffen kommunikationstechnische, modellspezifische und wirtschaftliche Überlegungen aufeinander, welche hier kurz angegeben werden:

- Kommunikationsspezifisch:
 - Länge des Kommunikationskanales (physikalische Ausbreitung)
 - Maximalanzahl der Knoten

Möglicher und durchschnittlicher Durchsatz

Echtzeitfähigkeit

Störsicherheit

- Modellspezifisch:

Netzwerktopologie

Vorhandene Stromversorgung

Umgebungsparameter (EMV, Temperatur, usw.)

- Wirtschaftlich:

Kosten für den Datenbus

Kosten für kompatible Komponenten

Wartungsintervalle, Anfälligkeit

Den Umfang der verschiedenen Bewertungskriterien betrachtend, kann nachvollzogen werden, dass es nicht möglich ist, einen Einheitsbus einzusetzen und damit allen verschiedenen Aspekten gerecht zu werden. Eine derartige Vorgangsweise würde den Einsatz eines schnellen und höchst sicherheits- und echtzeitfähigen Busses für alle Bereiche erfordern, was jedoch, zumindest aus wirtschaftlichen Gründen, untragbar wäre. Im konträren Beispiel, durch globalen Einsatz eines low-cost Systems, könnten sicherheitsrelevante Aspekte nicht abgehandelt werden. Der parallele Einsatz verschiedener Bussysteme, verbunden durch spezielle Gateways, ist der daraus resultierende Lösungsansatz, welcher heute bereits teilweise in die Realität umgesetzt worden ist. Aus der Tabelle 4.2 sind heute vielfach eingesetzte Bussysteme ersichtlich.

Bussystem	Einsatzgebiet
LIN	Subbus
MOST	Multimedia
CAN	allgemeiner Einsatz
TTCAN	Echtzeitanwendungen
TTP/A	allgemeiner Einsatz
TTP/C	Echtzeitanwendungen
ByteFlight	Echtzeitanwendungen
FlexRay	Echtzeitanwendungen
Bluetooth	Wireless - Kommunikation

Tabelle 4.2: Überblick aktueller Bussysteme im Fahrzeugbau

Das erste serienmäßig eingesetzte Bussystem war das CAN-Netzwerk, welches im Jahre 1991 erstmals in der S-Klasse von Mercedes verbaut wurde. Dieser Bus etablierte sich im europäischen Raum der Autoindustrie zunehmend zum eingesetzten Standard. Im folgenden Abschnitt wird dessen Aufbau und Funktionsweise näher beschrieben.

4.4.1 CAN - TTCAN

Das Controller Area Network (CAN) wurde von der Firma Bosch gezielt für den Einsatz im Fahrzeug entwickelt. Aufgrund der Erfolge hat sich der Einsatz inzwischen sogar auf die Anlagenautomatisierung ausgeweitet und wird auch in diesem Bereich erfolgreich eingesetzt. Im Automobilbereich sind heute bereits Fahrzeuge der Mittelklasse mit CAN-Netzwerken ausgestattet, was für deren weite Verbreitung spricht. Prinzipiell stellt der CAN-Bus eine serielle Datenübertragung für die angeschlossenen Komponenten zur Verfügung. Die Netzwerktopologie des Busses erwies sich im Automobilbereich als vorteilhaft, da durch diese Art der Verkabelung, Gewichtersparnisse erzielt werden konnten und auch der Ausfall einer Komponenten am Bus erfolgt für die restlichen Komponenten transparent und stört die Kommunikation nicht. Zudem können Erweiterungen anhand einfacher Steckverbindungen realisiert werden, was für die Flexibilität im Fahrzeugbereich spricht. Das System wurde ursprünglich für nicht sicherheitsrelevante Bereiche entwickelt, wird aber inzwischen auch für ABS, ESP, Motorsteuerung usw. eingesetzt. Da die heute verwendeten Mechatroniksysteme lediglich eine übergeordnete Funktionalität haben, und die Übertragungsraten des CAN-Busses mit inzwischen 1 MBit/sek reichlich dimensioniert sind, rechtfertigt dies in gewissem Maße den Einsatz eines im Prinzip für nicht sicherheitsrelevante Bereiche konzipiertes System. Es kam jedoch immer mehr der Wunsch nach einem Kommunikationssystem auf, welches die Bedürfnisse eines harten Echtzeitsystems befriedigt, was später zu zeitgesteuerten Bussystemen führte.

Nachrichten-ID (Arbitration) 11 Bit	RTR 1Bit	Kontrollfeld 6 Bit	Datenfeld 0 .. 64 Bit	CRC-Feld 16 Bit	ACK 2 Bit	End-of-Frame 7 Bit
--	-------------	-----------------------	--------------------------	--------------------	--------------	-----------------------

Abbildung 4.3: Nachrichtenformat am CAN-Bussystem

Das CAN-System ist ereignisgesteuert und die Kommunikation wird deshalb von den einzelnen Steuerrechnern geregelt. Dabei wird zunächst geprüft, ob der Kanal nicht belegt ist, worauf die Nachricht über die dafür vorgesehene Kommunikationsschnittstelle (CNI) auf den Bus geführt wird

und vom entsprechenden Empfänger gelesen werden kann. CAN unterstützt dabei vier verschiedene Nachrichten-Frames: data-, error-, remote- und overload frames. Das Datenframe besteht wie aus Abbildung 4.3 ersichtlich, aus 7 Feldern. Neben verschiedenen Steuerfeldern setzt sich die Nachricht aus dem Arbitrierungsfeld, Datenfeld und einer CRC-Sequenz zusammen. Das Feld der Busarbitrierung beinhaltet die eindeutig codierten Namen der jeweiligen Nachricht, und dient gleichzeitig als Arbitrierung für den gemeinsamen Kommunikationskanal, indem der kleinste Wert die höchste Priorität hat. Aus diesem Grund besitzt in einem CAN-Netzwerk jede Nachricht eine eigene ID-Nummer, welche zugleich über deren Priorisierung am Datenbus entscheidet. Anhand der eindeutigen Nummerierung ist die Busarbitrierung einfach durchführbar, der Bus hat daher einen dominanten (in dem Fall logisch 0) und rezessiven Status. Bei einem Senderversuch eines Knotens muss der sendende Knoten selbst den Kanal abhören und darf die Nachricht nur dann vollständig versenden, wenn das Arbitrierungsfeld komplett auf den Bus gelegt werden konnte, ohne von einem gleichzeitigen, höherprioreren Knoten gestört worden zu sein. Andernfalls wird der Senderversuch abgebrochen und nach einer erkannten Leerlaufzeit des Kanals wiederholt.

Gewinnt ein Knoten die Phase der Busarbitrierung, gelangt die Nachricht zum Empfänger. Dieser erkennt den Inhalt der Nachricht bereits durch Registrieren der Nachrichten-ID und speichert diese gegebenenfalls in der CNI. Bei erfolgreichem CRC-Check, wird in der Originalnachricht am Bus direkt das zweite Bit des Ack-Feldes auf dominant gesetzt. Dadurch wird dem Sender ohne zusätzlichem Kommunikationsaufwand signalisiert, dass zumindest ein Knoten die Nachricht korrekt empfangen hat.

Remoteframes werden für Anfragen gewisser Informationen von anderen Knoten verwendet und findet deshalb in Diagnoseverfahren häufig Verwendung, um zu prüfen, ob gewisse Knoten korrekt funktionieren. Der Typ der Fehlernachricht unterscheidet sich von den anderen, indem mindestens fünf aufeinanderfolgende dominante Bits auf den Bus gelegt werden. Diese Nachricht gewinnt gegenüber den Datenbits immer die Arbitrierung des Übertragungskanales und signalisiert somit allen andern Knoten den Fehler. Das Overloadframe wird vom überlasteten Empfangsknoten gesendet, damit der Sender die Übertragung der nächsten Nachricht verzögert, und somit dem Kommunikationsprinzip „das langsamste Glied bestimmt über die Geschwindigkeit“ gerecht wird.

Durch die implementierte Ereignissteuerung muss das CAN-System im Bereich echtzeit- und sicherheitskritischer Anwendungen einige Abstriche verzeichnen, da anhand dieser Technologie die geforderte Fehlertoleranz, Zusammensetzbarkeit und vor allem das Echtzeitverhalten nicht gewährt werden kann. Zum Beispiel sind Vorhersagen für bestimmte Ereignisse nicht mach-

bar, da der Zeitpunkt der Kommunikation vom Eintreten eines Ereignisses im Knoten bestimmt wird. Deshalb ist das CAN-Netzwerk nicht deterministisch. Für den Bereich der X-by-Wire Systeme wurden deshalb zeitgesteuerte Kommunikationsprinzipien entwickelt.

Referenznachricht	Exklusives Zeitfenster	Exklusives Zeitfenster	Arbitriertes Zeitfenster	Freies Zeitfenster	Referenznachricht	Exklusives Zeitfenster
-------------------	------------------------	------------------------	--------------------------	--------------------	-------------------	------------------------

Abbildung 4.4: Überlagerte Zeitsteuerung im TTCAN

Um den neuen Anforderungen gerecht zu werden, wurde das CAN-Netzwerk weiterentwickelt und ein zeitgesteuertes Protokoll darübergestellt. Dabei können die Verwendung der einzelnen Zeitfenster vom Entwicklungsingenieur äußerst flexibel bestimmt werden. Sie können entweder an hochpriorie Aufgaben vergeben, oder für die herkömmliche Arbitrierung des darunter arbeitenden, ereignisgesteuerten Systems (siehe Abbildung 4.4) eingesetzt werden. Der Grad zwischen Echtzeitfähigkeit und maximalen Datendurchsatz kann dadurch der entsprechenden Anwendung angepasst werden.

4.4.2 TTP

Beim Time-Triggered-Protokoll (TTP), entwickelt von der TU Wien, handelt es sich um ein zeitgesteuertes Kommunikationssystem. Der Zugang zum Kommunikationskanal muss nicht durch einen eigenen Algorithmus geregelt werden, sondern ist durch die zugewiesenen TDMA-Runden⁷ geregelt. Nach erfolgter Festlegung dieser Einteilung ist eindeutig bestimmt, zu welchem Zeitpunkt die einzelnen Komponenten den Datenkanal beanspruchen können, was es ermöglicht, das zeitliche Verhalten bestimmter Bauteile vorherzusagen. Dadurch wird zunehmend ein höherer Unabhängigkeitsgrad der einzelnen Bauteile erzielt und es wird erleichtert, Subkomponenten unabhängig voneinander zu entwickeln.

Jeder am Bus befindliche Rechenknoten enthält eine so genannte Message Descriptor List (MEDL), welche Informationen darüber enthält, zu welchem Zeitpunkt ein Knoten berechtigt ist, den gemeinsamen Kanal zu beanspruchen. Die MEDL ist einfach aufgebaut und besteht aus drei Feldern, welche den genauen Zeitpunkt der Kommunikation, die Speicheradresse im CNI, wo die zu versendende Nachricht abzuholen bzw. die empfangene Nachricht

⁷Time Division Multiple Access - Dabei wird der Kommunikationskanal in verschiedene Zeitschlitze (time-slots) unterteilt, welche dem jeweiligen Prozess für die Datenübertragung zugeordnet werden.

gespeichert wird, und einem Feld mit Attributen für Richtung, Nachrichtenlänge und weitere Optionen, enthält. Diese Liste ist statisch und kann von den Steuergeräten nicht verändert werden. Weiters verfügt das CNI über einen Mitgliedsvektor (membership vector), welcher als ein Bitfeld realisiert wird. Jede Position im Feld entspricht einem Knoten im Netzwerk, und falls der jeweilige Knoten in der letzten Runde korrekt funktioniert hat, steht dessen Wert auf logisch 1.

Typ I/N	Mode Bit1	Mode Bit2	Mode Bit3	Daten max 16 Byte	CRC-Prüfsumme 16 Bit
------------	--------------	--------------	--------------	----------------------	-------------------------

Abbildung 4.5: Aufbau einer TTP/C-Nachricht

Es sind zwei verschiedene Nachrichtenformate definiert: N-frames, welche im Normalbetrieb für Datenaustausch sorgen und I-frames, die in der Initialisierungsphase bzw. zur Resynchronisation bei neu hinzu gekommenen oder wieder eingebundenen Knoten eingesetzt werden. Wie aus Abbildung 4.5 ersichtlich, beginnt die Nachricht mit einem Header, dessen erstes Bit den Nachrichtentyp definiert. Der Header besteht weiters aus drei Modebits, welche einen Modechange aller Komponenten durchführen können. Im Normalbetrieb sind diese drei Bits nicht gesetzt. Nun folgt der Nachrichtenteil, welcher maximal 16 Bytes umfassen kann. Abgeschlossen wird die Nachricht von einem 16 Bit CRC-Feld. Anzumerken ist die Berechnung des CRC-Wertes. Im CNI des Senders wird der zu versendenden Nachricht, bestehend aus Header und Datenfeld, der CNI-interne Zustand (C-State)⁸ angehängt und darüber der CRC-Wert errechnet. Der Empfänger stellt seinen C-State an das Ende des Nachrichtenfeldes und berechnet auf seine Weise den CRC-Wert. Ist der resultierende Wert nicht übereinstimmend mit jenem aus dem empfangenen CRC-Feld, so liegt entweder ein Fehler in der Nachricht selbst vor, oder die Zustände der beiden CNI's unterscheiden sich. Auf jeden Fall muss die Nachricht verworfen werden. Dadurch wird durch geringstem Mehraufwand eine ständige Statusvereinbarung durchgeführt.

I-Nachrichten bestehen neben dem Header aus dem C-State, und ermöglichen die einfache Integration bzw. Resynchronisierung der Knoten. Im Betrieb des Kommunikationssystems wird der Zeitpunkt der Kommunikation nur von der fortlaufenden Zeit bestimmt, indem die Nachrichten dann versendet werden, wenn der in der MEDL eingetragene Zeitpunkt erreicht wurde.

⁸C-State ist der aktuelle Zustand des Kommunikationskontrollers. Er umfasst Informationen über die globale Zeit, die aktuelle Position in der MEDL und den membership-vector.

Der physische Datenkanal ist aufgrund der Fehlertoleranz redundant ausgeführt, und die Nachricht wird auf beide Kanäle gelegt. Wird zumindest eine Nachricht am Sender korrekt empfangen, setzt dieser das entsprechende Bit des Senders auf logisch 1. Im Fehlerfall wird dieser somit innerhalb einer TDMA-Runde erkannt.

Um das Problem eines permanent falsch sendenden Knotens (Bubbling Idiot) zu unterbinden, werden in der Schnittstelle zu den redundanten Datenkanälen ausfallsichere Bus-Guardians eingesetzt, welche den Bus nur in der dafür bestimmten Zeitspanne zugänglich machen. Realisiert wird diese Komponente durch eine einfache AND-Verknüpfung, wobei das Datensignal mit einem weiteren Signal verknüpft wird, welches lediglich in den dafür vorgesehenen Zeitintervallen auf logisch „1“ steht und somit eine Durchschaltung des Datensignales ermöglicht.

Die Bereitstellung einer präzisen, synchronisierten Zeitbasis innerhalb der einzelnen Knoten ist in einem derartigen Prinzipaufbau unabdingbar. Dank des zeitgesteuerten Kommunikationskanales und den a-priori bekannten Sende- bzw. Empfangszeitpunkten kann anhand dieser die Uhrsynchronisation durchgeführt werden. Mit jeder empfangenen Nachricht erhält der Knoten indirekt auch die interne Zeit des Senders und kann die eigene Uhr dementsprechend korrigieren. Ein weiterer Vorteil der zeitgesteuerten Kommunikation ist, dass auch die Art der Nachrichten zu jedem Zeitpunkt a-priori bekannt sind, und eine sonst übliche Namensgebung in der Nachricht dadurch hinfällig wird. Dies steigert zusätzlich die Effizienz des Protokolls.

Das hier beschriebene TTP-Protokoll wurde für die Anforderungen der Klasse C der SAE (Society of Automotive Engineering) entwickelt. Diese Klasse fordert höchste Übertragungsgeschwindigkeiten (über 100 kBit/s) und geeignetes Echtzeitverhalten für sicherheitskritische Anwendungen. Aus diesem Grund ist der Einsatz dieses Netzwerkes, im Vergleich zu einfacheren Bussystemen, mit höheren Kosten verbunden, da bereits die einzelnen Komponenten teurer sind. Deshalb wurde eine nach unten skalierte Version des TTP Protokolls entworfen, welche für die Klasse A konzipiert wurde und synonym mit TTP/A bezeichnet wird. Es ist ein Master/Slave Protokoll, mit einem oder mehreren Backupmastern. Der Master teilt den einzelnen Prozessen die Zeitschlitz des TDMA-Verfahren zu und sorgt zugleich für eine adäquate Zeitsynchronisation. Auf physikalischer Ebene wird ein Standard Universal Asynchronous Receiver Transmitter (UART) eingesetzt, wodurch der Einsatz von low-cost Komponenten in den einzelnen Rechnerknoten ermöglicht wird. Durch das a-priori-Wissen über die Nachrichtenfolge entfällt auch hier die Notwendigkeit einer Bezeichnung, was den effektiven Datendurchsatz steigert.

In der Tabelle 4.3 werden die hier besprochenen Kommunikationsprinzi-

pien gegenübergestellt und in einigen prägnanten Punkten verglichen.

Eigenschaft	CAN	TTP/A	TTCAN	TTP/C
Einsatzbereich	nicht sicherheitskritische Anwendungen mit geforderter Flexibilität	nicht sicherheitskritische Anwendungen	harte Echtzeitsysteme	harte Echtzeitsysteme
Steuerungsprinzip	Ereignisgesteuert	Zeitgesteuert	Zeitgesteuert	Zeitgesteuert
Busarbitrierung	CSMA/CD mit Priorisierung	Master/Slave	überlagertes TDMA	TDMA
Uhrsynchrisation	nicht vorgesehen	Synchronisation durch den Master	durch Einführung eines Synchronisationsframes	durch bekannte Kommunikationszeitpunkte
Bitrate	10 kbit/s ... 1 MBit/s	20 kBit/s	10 kBit/s ... 1 MBit/s	2 MBit/s
Anzahl Knoten	flexibel	256 inkl. Master	flexibel	64
Overhead pro Nachricht	31 Bit ideltime + 11 Bit Arbitrierung + 15 Bit CRC	Startbit, Stopbit, Paritybit	31 Bit ideltime + 11 Bit Arbitrierung + 15 Bit CRC	4 Bit (Header) + 2 bzw. 3 Byte CRC

Tabelle 4.3: Vergleich von Bussystemen

Die verschiedenen Anforderungen der einzelnen Bereiche im Fahrzeug erfordern den Einsatz dafür abgestimmter Systeme. Deshalb empfiehlt es sich auch das Kommunikationssystem auf verschiedene Stufen abzustimmen. Der Bereich der Grundfunktionalität und der sicherheitsrelevanten Anwendungen muss demgemäß durch ein entsprechend leistungsfähiges und zuverlässiges System abgedeckt werden. Der Einsatz einer zeitgesteuerten Architektur (TTP bzw. TTCAN) ist in diesem Bereich unbedingt erforderlich, damit die Funktionalität des Basissystems auch mit einer gewissen Fehlertoleranz gewährleistet werden kann. Die Anbindung der weiteren Bereiche kann durch

dafür entwickelte Gateways bewerkstelligt werden. Aufgrund der hohen Flexibilität und der geringen Anforderungen im Bezug auf Geschwindigkeit kann im Bereich der Bordelektronik bzw. des Komforts ein low-cost Kommunikationssystem verwendet werden. LIN⁹ bzw. CAN oder TTP/A entsprechen diesen Voraussetzungen. Im Multimediabereich wurden weitere Kommunikationssysteme, wie MOST, USB, FIREWIRE, DVI, GIGASTAR, usw. entwickelt, welche vor allem Vorteile durch eine hohe Datenübertragung bringen, welche bei Telefon, Fernsehen und Navigation erforderlich ist.

Zu beachten ist, dass die Struktur der Gateways keine Fehlerfortpflanzung bzw. keine Störeinflüsse von einem Netzwerksegment in ein anderes zulassen dürfen, denn dadurch würde das Prinzip der fault-containment-regions verletzt und die Zuverlässigkeit des Systems könnte nicht garantiert werden. Ein einfacher Fehler in einem Multimodul könnte durch eine nicht berücksichtigte Fehlerfortpflanzung unter Umständen Auswirkungen auf die Basisfunktionalität des Fahrzeuges haben, was für das Gesamtkonzept keineswegs tragbar ist.

4.5 Aktuatoren

Aktuatoren stellen im Bereich der Steuer- und Regelungstechnik ein wandlerbezogenes Gegenstück zum Sensor und bilden das Stellglied im Regelungsprozess, indem sie die Steuersignale in meist mechanische Arbeit bzw. Bewegung umsetzen. In den aktuellen Ausführungen der Fahrzeugtechnik beschränken sich elektrisch gesteuerte Aktuatoren im sicherheitskritischen Bereich zunächst auf Ventile, da die effektive Grunddynamik des Fahrzeuges noch durch hydraulische bzw. mechanische Teile beeinflusst wird. Mit dem Einzug der X-by-Wire Technik werden diese jedoch durch neu entwickelte Aktuatoren ersetzt, welche zumindest die Zuverlässigkeit der ersetzten Systeme aufweisen müssen.

Die Aktuatoren stehen direkt im Kontakt zur Umwelt des Regelsystems und beeinflussen diese auch aktiv. Das fehlertolerante Prinzip, welches in allen bisher diskutierten Bereichen berücksichtigt wurde, muss nun auch in der effektiven Umsetzung fortgeführt werden, um eine Gefahrenstelle im Gesamtsystem (single point of failure) zu vermeiden. Technisch sind dabei verschiedene Ansätze mit unterschiedlichen Eigenschaften und sicherheitsrelevantem Verhalten möglich. So kann, wie auch in den meisten anderen Bereichen, durch Redundanz eine geforderte Fehlertoleranz erreicht werden. Es werden dabei Systeme mit stand-by Modulen und mit aktiven Modulen unterschied-

⁹Das Local Interconnect Network wurde speziell für eine low-cost-Kommunikation von Sensoren und Aktuatoren in Kraftfahrzeugen entwickelt [lin].

den. Im ersten Fall hat jeder der Aktuatoren die nötige Performance, um allein die geforderte Leistung aufzubringen, während das redundant ausgeführte Modul erst dann aktiv wird, sobald ein Fehler in der Primärkomponente auftritt. Dieses Prinzip ist vom wirtschaftlichen Standpunkt nur schlecht vertretbar, da das Gesamtsystem durch die kalte Reserve überdimensioniert ist. In zweiten Fall arbeiten alle Aktuatoren parallel, der Ausfall einer Komponente führt allerdings zu Performanceeinbußen im Regelkreis, indem weniger Leistung zur Verfügung steht. Die verminderte Leistung kann inzwischen dennoch für weitere Steuermaßnahmen genutzt werden, und überbrückt die Zeitspanne bis zur Reparatur. Das System befindet sich allerdings in einem latenten Zustand und kann das Auftreten eines weiteren Fehlers nicht mehr maskieren, d.h. die Funktionalität geht verloren, was in sicherheitsrelevanten Bereichen nicht akzeptiert werden kann. Aus diesem Grund muss das System in einer derartigen Situation adäquate Sicherheitsmaßnahmen treffen, indem etwa ein Notlaufprogramm eingeleitet und die mögliche Höchstgeschwindigkeit entsprechend gedrosselt wird.

Beide Systeme setzen allerdings ein fail-silent Verhalten (siehe Abschnitt 3.1.4) der fehlerhaften Aktuatoren voraus. Ist dies nicht der Fall, könnte das ausgefallene Modul den anderen entgegenwirken, oder in einer Position festklemmen, wodurch die Leistung der weiterhin korrekt arbeitenden Bauteile zusätzlich vermindert wird, oder aufgrund der Überlast sogar zu deren Beschädigung führen kann. Um die Eigenschaft einer fail-silent-Komponente zu erreichen, muss jede Komponente durch eine geeignete Methode überwacht werden und im erkannten Fehlerfall sofort, etwa durch Ausschalten oder Auskuppeln, aus dem Regelkreis entfernt werden. Zu Gunsten der schnelleren Fehlererkennung bzw. -lokalisierung muss jeder Knoten direkt oder indirekt durch Sensoren überwacht werden. Ohne diese aktive Beobachtung wird der Ausfall wesentlich später erkennbar, wenn sich die Auswirkungen bereits auf die Funktionalität des Gesamtsystems ausgebreitet haben.

Eine weitere Möglichkeit ist der Einsatz eines triple-modular-redundant Aktuators. Diese Bauweise besteht aus drei Aktuatoren, wobei die Leistung zweier Bauelemente jene des dritten übersteigt und zudem in der Lage ist, die geforderte Arbeit am Stellteil zu verrichten. Somit kann der Ausfall eines Aktuators ohne spezielle Fehlererkennungsmechanismen maskiert werden. Die Anwendung dieses Designs ist jedoch aufgrund der hohen Redundanz kostenaufwendig und weist zudem Nachteile bezüglich der Bauweise (Gewicht und Ausmaße) auf.

Das Design variiert für die unterschiedlichen Einsatzgebiete, so wurde bisher ein Aktuator zur Bewegung eines Stellgliedes, wie sie etwa im Bereich einer Lenkung eingesetzt werden beschrieben. Betrachtet man Ventile, welche den Durchfluss in einer Leitung regeln, so trifft man auf grundlegend neue

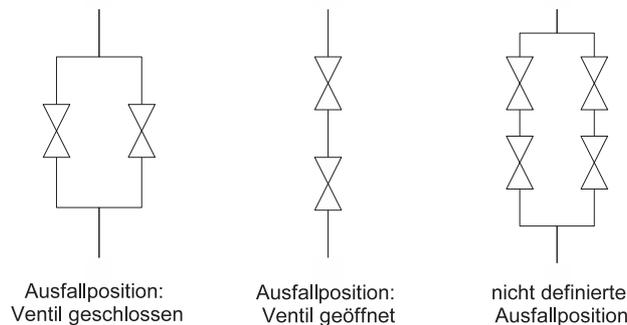


Abbildung 4.6: Verschiedenen Anordnungsmöglichkeiten der Aktuatoren

Eigenschaften und Bauweisen. Wie in Abbildung 4.6 ersichtlich, entscheidet neben dem Redundanzgrad auch die Anordnung der Ventile für deren Eigenschaften und sie können hinsichtlich dem im Fehlerfall günstigeren Zustand positioniert werden. Zusätzlich besteht die Möglichkeit, die Aktuatoren in einen definierten Ausfallzustand zu bringen. Dabei behilft man sich meist mechanischer Konstruktionen, wie etwa Federn, damit z.B. das Ventil im Fehlerfall in den geschlossenen bzw. offenen Zustand überführt wird.

In momentan erhältlichen Serienfahrzeugen sind die Hauptsysteme, welche die grundlegende Fahrzeugdynamik steuern, bekanntlich auf mechanische bzw. hydraulische Weise realisiert. Durch die Ersetzung dieser Komponenten mit neuer, elektromechanischer Technologie können Vorteile in der Dynamik, Sicherheit und Komfort erreicht werden. Voraussetzung dazu ist allerdings der Einsatz entsprechend fehlertoleranter und robuster Techniken, welche die Grundfunktionalität auch im Fehlerfall garantieren.

4.5.1 Aktuatoren für die Bremsanlage

Die weit verbreitete hydraulische Bremse wird, dank der laufenden Verbesserungen und Neuerungen, stets robuster und hat inzwischen eine hohe Zuverlässigkeit erreicht. Demnach werden die neuen elektromechanischen Systeme nahe am bestehenden Konzept ansetzen, damit möglichst viele der positiven Errungenschaften direkt in die neue Technologie einfließen können. Andererseits sind die Freiheitsgrade bei der Entwicklung des Bremsaktuators groß. Es muss ein möglichst leichtes, platzsparendes Modul gebaut werden, welches die hohen Ansprüche für die Bremswirkung abdecken kann, in den recht kleinen Raum innerhalb der Radfelge montiert werden kann und zudem die

nötige Flexibilität für übergeordnete Stabilitätsprogramme liefert. Die von den verschiedenen Herstellern gefertigten Bremsmodule für Brake-by-Wire, sind den herkömmlichen Systemen in gewissem Maße ähnlich. Der Verzicht auf die hydraulischen Leitungen lässt die Komponenten jedoch einfacher erscheinen. Die Kraft der Elektromotoren wird dabei über ein Schneckengetriebe auf einen axial platzierten Bolzen übertragen, welcher sich in die Richtung des inneren Bremsbelages bewegt. Die dadurch entstehende Spannkraft wird, wie bereits in hydraulischen Bremsen üblich, über den Schwimmrahmen gleichmäßig auf den äußeren und inneren Bremsbelag verteilt. Die exakte Ansteuerung des Elektromotors erfordert einen Positiongeber. Durch Kombination mit der im Modul befindlichen Steuerlogik, kann somit auch der Belüftungspielraum zwischen Bremsscheibe und Bremsklötze automatisch geregelt werden, was einem automatischen Nachstellen der Bremsen gleichkommt.

Es wird an verschiedenen Nuancen experimentiert, so entwickelt man z.B. an Bremsmechanismen, welche die kinetische Energie des Elektromotors nach Ende der Bestromung abfangen soll, und an Kupplungssystemen, welche beim Öffnen der Bremsen die Elektromotoren auskoppelt, um damit die vorhandene Bremsdynamik weiter zu steigern. Dieses Verfahren würde deutliche Vorteile für die Schlupfregelung und die restliche Fahrdynamik bedeuten, denn der Elektromotor kann konstant angetrieben werden, während mit der Kupplung die gewünschte Bremskraft mit geringsten Verzögerungswerten, entsprechend schnell angepasst werden kann. Im Falle einer Notbremsung könnte das „Bremsgetriebe“ ausgekuppelt werden, während die Elektromotoren, nun im Leerlauf befindlich, auf die Höchstdrehzahl beschleunigen. Dies kann in dem Zeitbereich geschehen, wenn der Fahrer mit hoher Geschwindigkeit das Gaspedal verlässt (Pre-crash Maßnahmen). Bei der folgenden Bremsung wird ein steilerer Anstieg der Bremswirkung erzielt, d.h. die maximale Bremswirkung steht schneller zur Verfügung. Zudem könnte noch im Voraus das Lüftspiel bis auf ein Minimum reduziert werden.

Die Bremsanlage unterliegt offensichtlich den höchst sicherheitskritischen Bereichen im Fahrzeug und muss äußerst zuverlässig arbeiten. Im Fahrzeug wird deshalb der Einsatz von zwei Bremskreisen, wie er bei hydraulischen Anlagen auch üblich und sogar gesetzlich vorgeschrieben ist, vorgesehen. Fällt einer der Bremskreise aus, so arbeitet der zweite davon unbeeinflusst weiter. Da die Bremsleistung aus elektrischer Energie stammt, muss auch die Stromversorgung (siehe Abschnitt 4.6) entsprechende sicherheitskritische Eigenschaften aufweisen. Es ist nicht erforderlich, den Ausfall eines Bremsmodules durch redundante Montage zu tolerieren. Es genügt durch entsprechende Maßnahmen ein fail-silent Verhalten der ausgefallenen Komponente anzustreben. Die restlichen drei Radbremsen arbeiten weiter und werden

von der fehlerhaften Komponente nicht gestört. Die Warnung an den Fahrer, anhand eines entsprechenden Signals im Fahrzeuginnenraum, soll diesen zu einer rascher Reparatur bewegen.

4.5.2 Aktuatoren für das Lenksystem

Bei der Lenkung entfällt durch den Einzug der by-Wire Technologie das gesamte Lenkgestänge, welches von der Achse bis zum Lenkrad führt und einige bedeutende Nachteile mit sich bringt (Lenksäulenintrusion, Package). Der vom zentralen Steuergerät erteilte Lenkbefehl wird über das Kommunikationssystem an den Aktuator an der Radachse geleitet. Dieser ist für die Umsetzung des jeweiligen Lenkbefehles zuständig. Dabei werden anhand von Elektromotoren und geeigneten Übersetzungen, bevorzugt durch Schneckengetriebe, der Radeinschlag an der Fahrzeugvorderachse beeinflusst. Zusätzlich ist auch im Lenkbereich der Einsatz von Kupplungen und bestimmten Bremsmechanismen möglich, welche unerwünschte Nebenwirkungen des Elektromotors, wie das baulich bedingte Nachlaufen, entgegenwirken und somit die Dynamik der Lenkung zusätzlich positiv beeinflussen.

Da das Lenksystem die einzige Vorrichtung für die Bestimmung der Querdynamik im Fahrzeug darstellt und keinerlei Backupsysteme für den Notfall bestehen, bedarf es in diesem Bereich der höchsten Sicherheitsvorkehrungen in Bezug auf Systemfehler bzw. Ausfälle am Aktuator. An dieser Stelle ist deshalb der Einsatz redundanter Aktuatorik notwendig. Dabei ist die Verwendung einer zweifachen fail-silent Redundanz oder eines TMR-Aktuators möglich. Da beide Bauarten lediglich einen Fehler im System tolerieren, ist die zweifache Redundanz mit Fehlererkennung aufgrund seiner Kosten- und Gewichtsvorteile vorzuziehen. Beim Ausfall eines Aktuators oder bei einem permanenten Fehler im Regelkreis der Lenkung muss dieser Verlust unverzüglich erkannt werden und das Fahrzeug sofort in ein Notlaufprogramm wechseln, indem die Geschwindigkeit begrenzt wird. Denn ein weiterer Ausfall, wenn dieser auch unwahrscheinlich erscheinen mag, würde zu einem nicht mehr lenkbaren Fahrzeug führen. An den jeweiligen Aktuatoren muss zu deren Überwachung entsprechende Sensorik angebracht werden. Die daraus gewonnenen Daten sind rücklaufend mit dem Steuerrechner und der Fehlererkennungslogik verbunden, welche in erkennbaren Gefahrensituationen die notwendigen Schritte einleiten.

Die hier beschriebenen Aktuatoren beeinflussen die Grunddynamik des Automobils und sind deshalb als zeitgesteuerte Architektur mit den zugehörigen Steuer- und Bedienelemente über kompatiblen Kommunikationstechnik

(TTP/C bzw. TTCAN) zu vernetzen. Diese Ebene tritt an die Stelle der heute noch mechanisch realisierte Rückfallebene, und spezielle Designprinzipien müssen eingehalten werden, um die Funktionalität unter allen Umständen zu gewährleisten.

Im modernen Fahrzeug findet man natürlich eine ganze Palette weiterer Aktuatoren. Die meisten davon sind bereits seit längerem im Einsatz und können trotz zugrundeliegender by-Wire Technologie weiterverwendet werden. Die Anbindung an das Basisnetz erfolgt, wie im vorigen Abschnitt beschrieben, anhand geeigneter Netzwerkkomponenten. Diese Vorgangsweise erfordert keine Neuentwicklung des gesamten Automobils, sondern viele, bereits vertraute Technologien können eingesetzt werden, und die Forschung kann ihr Hauptaugenmerk auf die Umstellungen in den Basisfunktionen legen.

4.6 Stromversorgung

Durch den Entfall der mechanischen Verbindungen und Servomotoren treten im X-by-Wire Design eine Vielzahl von Elektronikkomponenten an deren Stelle, welche auf eine konstante und in allen Situationen zuverlässige Stromzufuhr angewiesen sind. Deshalb ändert sich die Rolle der elektrischen Energieverteilung im Kraftfahrzeug und fällt, spätestens mit dem Einsatz eines konzipierten X-by-Wire Systems, sogar in den sicherheitskritischen Bereich.

In heutigen Fahrzeugen hat sich zunehmend die 12 V Bordspannung etabliert, worauf auch sämtliche Systeme angepasst wurden. Eingesetzt wird in den meisten Fällen ein hierarchisches Stromnetz mit Sternstruktur, abgesichert durch thermische Sicherungen. Diese Eigenschaften erweisen sich bei der Fehlersuche als hinderlich und geben auch keinerlei Sicherheit bei dem Ausfall einzelner Komponenten bzw. Leitungsabschnitten. Auf dieses Problem aufmerksam geworden, wurde bereits im Jahre 2000 das 2-Batterien Konzept eingeführt, welches anhand der redundanten Stromkreise eine hohe Verfügbarkeit der Motorsteuerung, inklusive dem Kaltstart, vorsieht. Die Batterien werden mit Bordnetzatterie und Startatterie, entsprechen ihren Einsatzgebieten, bezeichnet. Die Startatterie speist lediglich den Starterkreis, und versorgt dabei prinzipiell Starter und startrelevante Verbraucher. Die gesamten Ruhestromverbraucher, welche auch im Stillstand des Fahrzeuges laufend Energie verbrauchen, sind an die zweite Batterie angeschlossen. Je nach Ladezustand der Batterien ist zudem ein Parallelschalten beider Stromversorger möglich, um das Kaltstartverhalten, speziell nach langen Standzeiten, zu verbessern. Zudem wurden mit der verstärkten Beanspruchung des Energienetzes strukturelle Bereiche gebildet und Verteilungsknoten für die

verschiedenen Bereiche, wie Motorraum, Innenbereich, Tür, Heck, Beleuchtung usw. errichtet. In diesen Verteilungsknoten werden zusätzlich logische Komponenten integriert, welche eine Diagnose des Energienetzes erleichtern und im Stande sind, eine dynamische Lastenaufteilung durchzuführen.

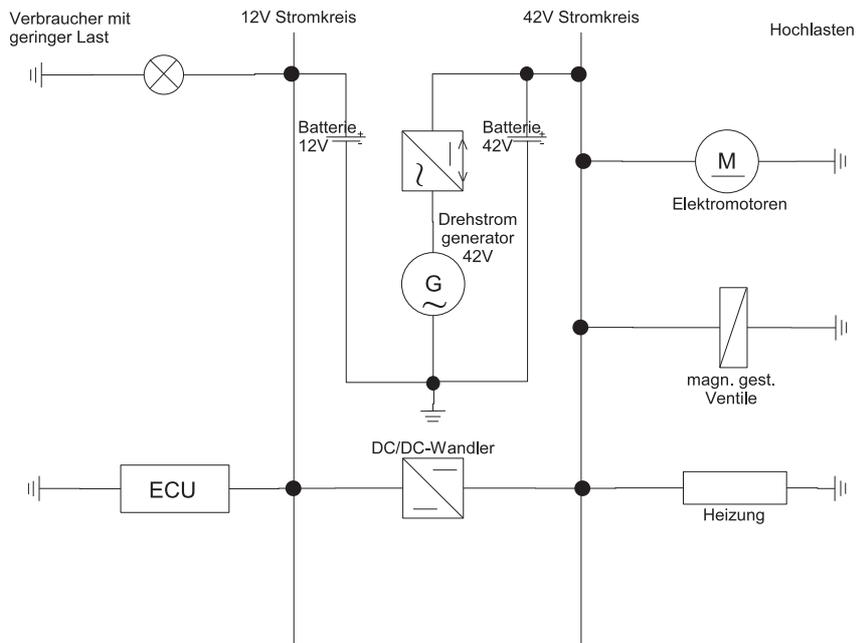


Abbildung 4.7: 12V/42V Stromkreis

Um die Grundfunktionalitäten des X-by-Wire Konzeptes zu bewerkstelligen bedarf es jedoch zusätzlicher Neuerungen im Energieversorgungsbereich. Zum einen muss für die Komponenten der Basisfunktionen eine vollständig redundante und voneinander unabhängige Stromversorgung gewährleistet werden, damit ein Ausfall in einem der Stromkreise das Fahrzeug und dessen Steuerung nicht beeinflusst. Zudem reicht die bisher eingesetzte Spannung in Höhe von 12 V für die Hochstromverbraucher der by-Wire Aktuatoren (Brems- und Lenkmodule) nicht aus, und der Einsatz eines 42 V-Netzes wird erforderlich. Bei dem Umstieg auf ein 42 V-Bordnetz, muss die Umrüstung bzw. Neuentwicklung aller im Kraftfahrzeug eingesetzten Elektrokomponeenten durchgeführt werden, was natürlich vermieden werden soll. Deshalb empfiehlt sich hier die Verwendung eines hybriden Bordnetzes, welches eine gestaffelte Umstellung von 12 V auf 42 V, anhand eines zusätzlichen Drehstromgenerators und einer zweiten Batterie, erlaubt. Wird im Stromkreis zudem ein DC/DC-Wandler für Netzkopplungen eingesetzt, so erhält man wie in Abbildung 4.7 ersichtlich, eine angestrebte Elektroarchitektur. Die starken Stromverbraucher, wie by-Wire Aktuatoren oder Heizelemente

können mit dem 42 V-Netz betrieben werden, während die restlichen Elektrokomponenten mit der herkömmlichen Spannung von 12 V gespeist werden und einer Weiterverwendung dieser daher nichts im Wege steht.

Die Energieversorgung muss nun zusätzlich sicherheitskritische Funktionen erfüllen und darf in keiner Hinsicht einen Schwachpunkt der Gesamtarchitektur darstellen. Den Komponenten, welche ausdrücklich als sicherheitsrelevant eingestuft werden, muss eine entsprechende Energieversorgung gewährt werden, auch in Ausnahmezuständen und Fehlersituationen. Zumindest die Energie, welche für den Übergang in einen sicheren Zustand, in diesem Kontext der sicher eingeleitete Stillstand des Fahrzeuges, muss für die dafür notwendigen Bauteile sichergestellt werden. Daraus wird ersichtlich, dass auch das Energieversorgungskonzept mit Redundanz ausgerüstet werden muss. Diesen Anforderungen kann man durch zwei Grundstrukturen gerecht werden:

4.6.1 Lokale Reserven

Beim Ausfall der primären Energieversorgung stehen für die sicherheitsrelevanten Teilkomponenten des X-by-Wire Systems lokale Energiereserven in entsprechender Dimensionierung bereit. Dabei wird meist auf räumlich naheliegende Batterien zurückgegriffen, welche rein für den Notfall vorgesehen sind.

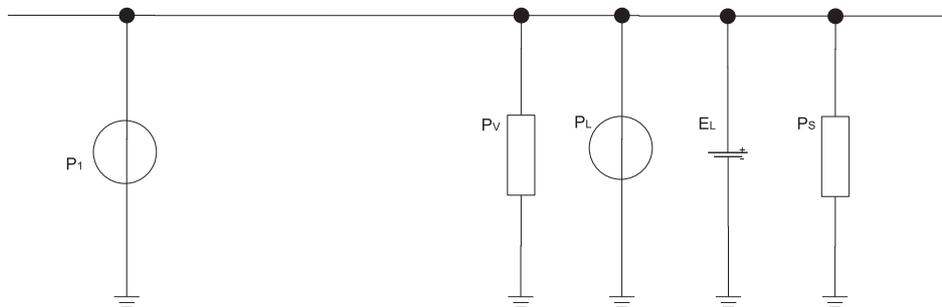


Abbildung 4.8: Stromkreis mit lokalen Reserven [Leo04]

Angelehnt an die Abbildungen 4.8 und 4.9, sei P_S die Leistungsaufnahme der sicherheitskritischen Verbraucher, t_S die maximale Ausführungszeit der sicherheitskritischen Funktion, P_i die verfügbaren Leistungsquellen im Normalbetrieb und P_V die Leistungsaufnahme aller restlichen Komponenten des Versorgungszweiges. Daraus ergibt sich rechnerisch die (idealisierte) Leistungs- (4.1) und Energiebedingung (4.2):

$$P_L > P_S + P_V \quad (4.1)$$

$$E_L > P_S * t_S + P_V * t_S - P_L * t_S \quad (4.2)$$

4.6.2 Redundante Energiekreise

Mit dieser Energiestruktur wird die Ausfallwahrscheinlichkeit der Stromversorgung durch die mehrkanalige Ausführung des Bordnetzes reduziert. Dazu müssen alle Komponenten des Stromkreises redundant und unabhängig voneinander ausgeführt werden. Entsprechend der Abbildung 4.9 ergibt sich folgende Leistungs- und Energiebedingungen:

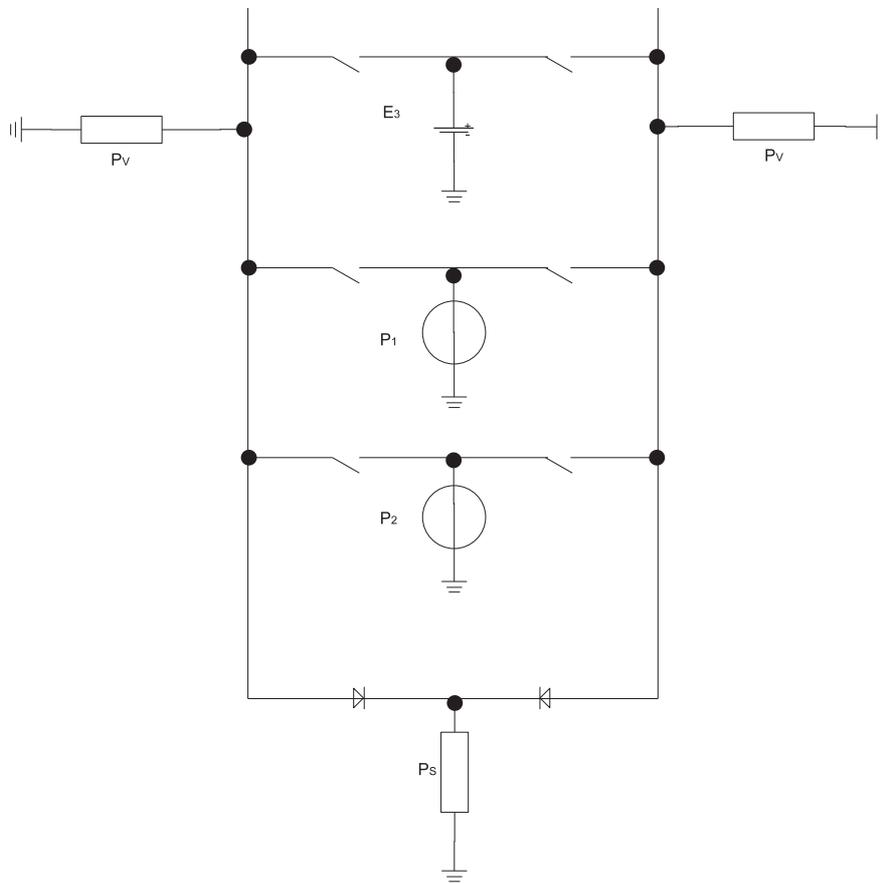


Abbildung 4.9: Redundante Stromkreise [Leo04]

$$P_S < P_1 + \frac{E_3}{t_S} - P_V \text{ und } P_S < P_2 + \frac{E_3}{t_S} - P_V \quad (4.3)$$

Zusätzlich bedarf es mit dieser Konstruktionsweise einer ausfallsicheren Einheit, welche die einzelnen Stromkreise überwacht und im Bedarfsfall eine

Umschaltung auf den redundanten Stromkreis vornimmt.

Die redundante Ausführung des gesamten Stromkreises ist gemäß dem Prinzip der Mehrkanaligkeit, welches bisher in allen sicherheitsrelevanten Ebenen eingesetzt worden ist. Die Nachteile dieser Architektur liegen jedoch auf der Hand und verzeichnen in den Bereichen Gewichts-, Kosten- und Vernetzungsaufwand Nachteile. Anders als in der Luftfahrt, wo das Redundanzprinzip angewandt wird, fallen diese Faktoren in der Automobilindustrie enorm ins Gewicht, was den Einsatz in Frage stellt. In dieser Hinsicht ist das Design mit den lokalen Reserven angemessener, muss allerdings bezüglich der Energiereserven entsprechend dimensioniert werden. Dabei besteht hier das Problem, dass das Fahrzeug bei einem Ausfall des Bordnetzes nicht beliebig weiterverwendet werden kann, sondern es funktionieren lediglich die Grundfunktionen, und selbst deren Reserven sind zeitlich begrenzt. Dies bedeutet, dass das Fahrzeug nach einer gewissen Zeit nicht mehr betriebsfähig sein wird. Mit dem Ausfall der Primärversorgung beginnt somit für das Fahrzeug die Phase der Degradation. Nach Erkennung eines ernsthaften Problems in der Energieversorgung wird als erste Reaktion die Erhöhung der Energieproduktion angestrebt, indem die Leerlaufdrehzahl des Motors erhöht wird. Anschließend müssen entsprechend der vordefinierten Priorisierung Leistungsreduktionen bei den Verbrauchern, bis hin zu deren kompletten Abtrennung vom Energienetz vorgenommen werden. Damit fällt das System langsam in den Zustand, in dem lediglich die hochprioren Systeme versorgt werden. Fällt das Energieniveau weiter, so fällt das Fahrzeugsystem in ein Notlaufprogramm bzw. wird sicher in den Stillstand gebracht.

Unabhängig von der eingesetzten Architektur muss im Bereich der Energieversorgung darauf hingearbeitet werden, dass auftretende Probleme unverzüglich gemeldet werden, um dadurch eine möglichst präventive Wartungsarbeit zu erzielen. Zudem muss im Bereich der Stromverteilungstechnik die Energie- und Leistungsverteilung dahingehend optimiert werden, dass kritische Zustände vermieden werden. Das Energieversorgungsnetz spielte bisher im Automobil eine eher sekundäre Rolle, was sich nun, mit dem Einsatz von by-Wire Elementen, ändert. Im Bereich der Lastzustandserfassung müssen neue Systeme eingesetzt werden, welche die gesamten im Netzwerk befindlichen Lasten genauestens ermitteln und an die Verteilerlogik weiterleitet. Die eingesetzten Energiespeicher müssen überprüft und deren Ladezustand zuverlässig erfasst werden. Die dadurch gewonnenen Daten fließen in eine Steuerregelung ein, welche abhängig von den aktuellen Last- und Ladezuständen, die Einspeisung der Verbraucher regelt. Offensichtlich ist etwa die Priorisierung der Bremsmodule gegenüber der Heizung, welche beide starke

Stromverbraucher darstellen. Die Regelung soll jedoch Verbraucher im gesamten Fahrzeug betreffen, wodurch eine gewisse Transparenz erreicht wird, und der Fahrer von der erfolgten Regelung möglichst wenig bemerkt.

Die variablen Lasten und Leistungen aller Verbraucher und Quellen im Bordnetz und der schwierig einzuschätzende Zustand der Bleibatterie¹⁰ machen aus der zuvor beschriebenen Regelung ein komplexes Steuerverfahren, wo zahlreiche Hersteller bemüht sind, Ansätze und Lösungsvorschläge zu finden.

4.7 Sichere Software

Bei der bisher beschriebenen Systemarchitektur wurde stets auf die mögliche Anpassung des Gesamtsystems für den sicherheitskritischen Einsatz hingearbeitet. Die eingesetzte Hardware und deren interne Kommunikation wurden dabei durch geeignete Maßnahmen für den Notfall ausgerüstet und in allen Bereichen sind adäquate Ressourcen vorhanden. Allerdings wurde in der bisherigen Diskussion ein immer relevanter werdender Systemteil vernachlässigt. Darauf wird nun in diesem Abschnitt eingegangen.

Die bekanntlich rasante Entwicklung der Technologie ermöglicht heute den Einzug komplexester Systeme in allen möglichen Einsatzgebieten. Aktuell eingesetzte Steuergeräte, wie sie vor allem aus der Oberklasse der Fahrzeuge bekannt sind, verfügen im Vergleich zu anfänglichen Desktoprechnern vor 10 Jahren, um Größenordnungen mehr Rechenleistung und Speicherkapazität. Die Verdoppelung der Integrationsdichte innerhalb 18 Monaten¹¹ hielt nun über eine Zeitspanne von etwa 30 Jahren an und hat die Entwicklung im gesamten Bereich der Mikroelektronik vergleichsweise überdimensional vorangetrieben. Deshalb besteht heute die Möglichkeit, aufwändige Rechenverfahren in allen möglichen Subkomponenten einzusetzen. Parallel beeinflusste die steigende Performance auch den Bereich der Softwareentwicklung. Es entstanden immer komplexere Programme mit einer unüberschaubaren Datenfülle. Dieser Trend beeinflusste auch immer mehr die Bereiche der Automobilindustrie, da die möglichen Resultate jenen der herkömmlichen, meist analogen bzw. mechanischen Methoden, weit überlegen waren. Etwas zeitverzögert fanden automatische Regelungen auch Einzug in sicherheitsrelevante Bereichen und erzielten auch hier überragende Ergebnisse. Allerdings wurde

¹⁰Das Spannungsverhalten der herkömmlichen Bleibatterie ist von verschiedenen chemischen Veränderungen, dem Alter der Batterie und deren Umgebungsbedingungen abhängig. Deshalb ist die Abschätzung des Funktionsstatus lediglich mit einer gewissen Ungenauigkeit machbar.

¹¹It. Moore'sches Gesetz

nicht erkannt, dass mit der steigenden Komplexität die Überschaubarkeit der Funktionalität keinesweg gewährleistet war, und sich in das Gesamtsystem zunehmend Entwicklungsfehler eingeschlichen haben. Diese Mängel haben bereits zu verschiedenen katastrophalen Folgen geführt und machten dadurch auf sich aufmerksam. Im Bereich der Hardware konnte dem entgegengewirkt werden, indem relevante Bereiche redundant bzw. mit verschiedenen Technologien ausgerüstet wurden.

Die Software unterliegt keinem physikalischen Alterungsprozess, wodurch angenommen werden kann, dass sich mit zunehmender Betriebsdauer keine altersbedingten Fehler einschleichen. Die redundante Ausführung wirkt aus diesem Grund nicht den Fehlern in der Software entgegen, es können damit lediglich Fehler der Hardware erkannt werden. Als Grundregel gilt bei der Entwicklung sicherheitskritischer Software, genauso wie im restlichen Entwicklungsprozess, die konsequente Anwendung konstruktiver Maßnahmen, um Entwicklungsfehler in jeder Phase zu vermeiden. Systematische Testläufe und weitere analytische Maßnahmen werden angewandt, um die Teilstrukturen auf deren Korrektheit hin zu prüfen. Trotzdem muss im erstellten System mit Fehlern gerechnet werden, da ein vollständiger Korrektheitsbeweis für den Komplexitätsgrad heutiger Software nicht möglich ist. Dies stellt für das sicherheitsrelevante Einsatzgebiet ein Problem dar, und es müssen weitere Maßnahmen ergriffen werden, damit trotz auftretender Fehler, eine kritische Situationen im Bezug auf die Grundfunktionalität der Gesamtarchitektur vermieden wird.

Um den Konzeptfehlern bei der Softwareentwicklung entgegenzuwirken, setzt man neben entsprechend fehlervermeidenden Methoden auf die Konzepte der Softwarediversität und Programmüberwachung.

4.7.1 Softwarediversität

Da in jeder Implementierung grundsätzlich Fehler nicht auszuschließen sind, behilft man sich anhand diversitärer Entwicklungen, wodurch Fehler der Software erkannt werden können. Dabei werden möglichst unabhängig voneinander verschiedene Programmversionen entwickelt, welche anschließend sequentiell oder parallel auf verschiedenen Redundanzkanälen ausgeführt und deren Ergebnisse gegenübergestellt werden. Es wird angenommen, dass die Wahrscheinlichkeit eines korrelierten Fehlers bei unabhängigen Programmentwicklungen relativ gering ist¹². Die Unabhängigkeit der diversitären Lösungen muss bevorzugt durch verschiedene Messverfahren, Algorithmen und

¹²Laut Statistiken wurden jedoch typische Denk- und Vorgangsweisen unterschiedlicher Entwicklungsteams festgestellt, welche sogar zu ähnlichen Programmabläufen führten.

zugrundeliegende Architektur unterstützt werden. Man unterscheidet hierbei Entwurfsdiversität und systematisch erzeugte Diversität.

Die Entwurfsdiversität zeichnet sich durch verschiedene Entwürfe je Entwicklungsteam aus, welche in verschiedenen Implementierungen desselben Problembereiches führen soll. Es wird dabei ein gegensätzlicher Entwurf erstellt, wobei die beiden Entwicklungsteams in der Entwurfsphase Absprachen treffen und gezielt unterschiedliche Lösungsansätze und -methoden verwenden. Als Alternative steht die komplett unabhängige Entwurfsphase zur Auswahl, wo die Teams ohne jeglichen Kontakt zueinander eine Problemlösung suchen. Ein Nachteil ist, dass die zu Grunde liegende Spezifikation meist dieselbe ist. Darin enthaltene Unvollständigkeiten können auch durch Diversität nicht mehr aufgedeckt werden. Auch ist die Unabhängigkeit zwischen den mehrfachen Kanälen nur schwer nachweisbar.

Eine systematisch erzeugte Diversität erhält man durch Modifikation des Programm- und Datenflusses, was auch automatisch durchgeführt werden kann. Der angewandte Algorithmus wird dadurch nicht verändert. Eine systematische Diversität kann durch verschiedene Maßnahmen erreicht werden:

- Vertauschung der Register: Bei der redundanten Programmausführung werden die verwendeten Register vertauscht. Damit wirken sich Stuck-at-Faults auf verschiedene Berechnungszweige in der Software aus, wodurch die Fehlererkennungswahrscheinlichkeit ansteigt.
- Vertauschen parallelisierbarer Befehlssequenzen: Im Programmcode wird nach parallelisierbaren Codesequenzen gesucht. Existieren diese, werden die Reihenfolgen der Ausführung vertauscht. Datenabhängige Fehler, welche vom Inhalt der umliegenden Speicherbereiche abhängen, können damit leichter erkannt werden.
- Änderung sich wiederholender Sequenzen: Besteht ein Programm aus sich wiederholenden Befehlssequenzen, werden dafür diversitäre Programmteile entworfen. Diese werden anstelle der ursprünglichen Codesequenzen eingesetzt. Dadurch entstehen mehrere unterschiedliche Programmvarianten.
- Verwendung diversitärer Datentypen: Die Originaldatentypen werden auf eine neue Art abgebildet und anhand dieser Repräsentation werden die verwendeten Befehle entsprechend angepasst, damit das erforderliche Resultat mit den veränderten Datentypen korrekt berechnet wird. Dadurch erhält man eine diversitäre Programmvariante, ohne den dahinter liegenden Algorithmus zu verändern.

Die hier angeführten Verfahren zur Einführung systematischer Diversität können durch einen dafür geeigneten Precompiler automatisiert durchgeführt werden. Es ist anzumerken, dass die Diversität in dem Fall vor allem behilflich ist, um Betriebs- und Hardwarefehler zu erkennen, und weniger für eine Vermeidung der Entwicklungsfehler im Softwareblock beiträgt.

Um effektive Maßnahmen gegen Designfehler zu erlangen, ist somit eine Entwurfsdiversität unabdingbar. Durch den Einsatz zwei diversitärer Programme wird eine Sicherung des Arbeitsprozesses erzielt, indem Softwarefehler erkannt und das System somit in den definierten sicheren Zustand überführt werden kann. Diese Arbeitsweise führt allerdings zu einer eingeschränkten Verfügbarkeit der Anlage, was speziell bei einem Einsatz im Fahrzeug nicht wünschenswert ist. Um keine Einschränkungen der Verfügbarkeit zu erlangen, werden mindestens $k=3$ diversitäre Programme, welche parallel oder sequentiell ausgeführt werden, benötigt. Anhand einer Mehrheitsentscheidung werden $\frac{k-1}{2}$ Abweichungen maskiert, während die korrekte Funktionalität trotzdem gewahrt wird.

Bei der letzteren Vorgangsweise werden jedoch mindestens drei redundante Hardwarekanäle für die parallele Berechnung benötigt. Die sequentielle Ausführung scheint aufgrund der stark angestiegenen Ausführzeit nur für wenige Einsatzbereiche geeignet, und ist speziell in Echtzeitberechnungen meist nicht anwendbar. Weiters ist anzumerken, dass der Entscheider aufgrund seiner Fehlertoleranz und der diversitären Berechnungskanäle komplex aufgebaut ist und nicht-planbare Wartezeit aufweist. Um diese Problematiken zu umgehen, werden die verschiedenen Programmversionen in einem ausführlichen Testlauf gegenübergestellt. Treten dabei bei einer ausreichend großen Anzahl von Testdatensätzen keine unterschiedlichen Verhaltensweisen auf, werden die einzelnen Programme als fehlerfrei angesehen und somit im Automatisierungsprozess eingesetzt. Als weitere Alternative lässt sich speziell in zyklischen Regelungsprozessen die eingesetzte Software periodisch tauschen. Die Fehler in einem Programm wirken sich dadurch vermindert auf die Funktionalität aus. Generell entstehen durch die Diversitäre Entwicklung immer hohe Entwicklungskosten.

4.7.2 Programmablaufüberwachung

Aufgrund der Schwierigkeiten beim Einsatz diversitärer Software (bedingte Unabhängigkeit, Kosten, Effektivität), wird in sicherheitskritischen Systemen oftmals eine Programmablaufüberwachung während des Betriebs eingesetzt. Diese ist während der gesamten Laufzeit des Prozesses aktiv in Betrieb, und wird dadurch zu den online Testverfahren gezählt. Man unterscheidet zeitliche und logische Ablaufüberwachungen, welche meist in kombinierter Form

auftreten.

4.7.2.1 Zeitliche Programmablaufüberwachung

Durch die zeitliche Überwachung werden Fehler erkannt, welche den Programmablauf auf unvorhergesehener Weise verlängern. Es werden nicht ausschließlich Softwarefehler erkannt, sondern der Kontrollpunkt liegt tiefer, weshalb das korrekte Zusammenspiel von Hard- und Software geprüft wird. D.h. es werden Programmzähler, Programmlogik, Stack, Takterzeugung, Arbeitsweise des Prozessors, sowie auf die Laufzeit auswirkende Softwarefehler erkannt.

Realisiert wird dieses Testverfahren auf einfache, hardwaretechnische Art, indem ein Timer (Watchdog WD) die Ablaufzeit mitverfolgt, welcher an definierten Punkten im Ablaufprozess rückgesetzt wird. Übersteigt der Timer aufgrund einer Verzögerung im Programmablauf einen gewissen Wert T_{WD} , so wird ein Fehler angenommen und ein Alarm wird ausgelöst. Anzumerken ist, dass die Taktgenerierung des zu kontrollierenden Prozesses nicht mit jener des Timers zusammenhängen darf, zudem sollte das Rücksetzen des Timers nicht anhand eines einzigen Befehls erfolgen, sondern eine Verwendung einer Befehlsabfolge ist zu favorisieren. Damit lassen sich unbeabsichtigte Rücksetzaktionen aufgrund eines Systemfehlers vermeiden. Die Konfiguration des Timers und dessen Zeitschwellen kann je nach Bedarf und Art des Anwendungsbereichs variieren. So erfordert eine rasche Fehlererkennung die Auslösung des Alarms bereits bei geringfügiger Abweichung der Ausführungszeit, was allerdings zu einer hohen Alarmdichte führen wird. Grundlegend gilt, dass die Zykluszeit des Programms T_{Zyk} kleiner als die der Watchdogzeit sein muss. Weiters müssen Fehlertoleranzzeit T_{FT} und die Auslösezeit der abzuschaltenden Elemente im Alarmfall T_{Aus} berücksichtigt werden. Diese Beziehungen werden wie folgt dargestellt:

$$T_{Zyk} < T_{WD} < 2 * T_{Zyk} \quad (4.4)$$

$$T_{WD} < T_{FT} - T_{Aus} \quad (4.5)$$

Die Programmüberprüfung kann zudem verfeinert werden, indem innerhalb des Programmzyklus zusätzliche Prüfpunkte eingerichtet werden. Eine eindeutige Kennzeichnung dieser Punkte und das a-priori Wissen über deren Vorgänger und Nachfolger lässt zudem die korrekte Verzweigung des laufenden Programms feststellen. Bisher wurde lediglich die Überschreitung der Ausführzeit geprüft, ein Überspringen eines relevanten Programmzweiges bliebe allerdings unerkannt. Deshalb muss die Timerzeit durch Hinzunahme

der minimalen Ausführzeit weiter verfeinert werden. Es gilt folglich:

$$T_{WDmin} > \frac{1}{2} * T_{Zyk} \quad (4.6)$$

$$T_{WDmax} < 2 * T_{Zyk} \quad (4.7)$$

Theoretisch kann dieses Prüfverfahren dahingehend verfeinert werden, dass für jede relevante Programmsequenz durch einen eigenen Timer überwacht wird. Der Aufwand in der Konfiguration und Wartung steigen dadurch erheblich und bei jeder Codeänderung müssen die Grenzwerte neu berechnet werden.

4.7.2.2 Logische Überwachung

Die logische Überwachung basiert auf einer in der Software ausgeführten Kontrolle des Programmflusses. Prinzipiell wird der Ablauf des Programms anhand a-priori Wissen geprüft und überwacht. Dazu benötigt es meist Erweiterungen an der Hardware, damit die aktuellen internen Zustände ausgelesen werden können. Dies kann einerseits durch eine Erweiterung des Befehls- und Datenbusses bewerkstelligt werden. Die zusätzlichen Datenleitungen beinhalten zu jedem auf dem Bus befindlichen Datenpaket Kontrollinformationen, welche zu einer speziellen Auswertelogik führt und dort entsprechend geprüft werden. Dadurch kann die Ausführung und Reihenfolge der Befehle verfolgt und kontrolliert werden. Der Aufwand dieser Methode ist allerdings hoch, weshalb diese Methode selten eingesetzt wird.

Ein anderes Prinzip der logischen Programmüberwachung wird durch ein spezielles Zählverfahren dargestellt. Das Programm wird in Zweige unterteilt, und jedem dieser Teilstücke wird eine eindeutige Signatur zugewiesen. Beim Durchlaufen des Programms werden diese Signaturen aufsummiert. Diese Signatursumme wird an bestimmten Punkten mit einem im voraus berechneten Sollwert abgeglichen, und somit auf einen eventuell fehlerhaften Programmablauf hin getestet. Die Wahl der Testpunkte beeinflusst die Effektivität der Fehlererkennung und deren Lokalisierung. Offensichtlich wird auch durch diese Methode zusätzliche Rechenleistung sowie Speicherbedarf notwendig.

Als weitere logische Ablaufüberwachung gilt die Rücksprungkontrolle, welche die Rücksprungadresse nach Ausführung eines Unterprogramms oder Funktion mit der Stackadresse vor Abzweigung vergleicht und einen hier vorliegenden Fehler erkennt.

Für jedes Anwendungsgebiet muss eine dafür vorgesehene Abstimmung zwischen den einzelnen Programmablaufkontrollen gefunden werden. Die zeit-

	Externer Timer mit unabhängigem Takt	Externer Timer mit abhängigem Takt	Interner Timer mit abhängigem Takt
Einfacher Watchdog, ein Triggerpunkt	< 0,7 %	< 0,6 %	< 0,4 %
Einfacher Watchdog, mehrere Triggerpunkte	< 0,8 %	< 0,7 %	< 0,5 %
Watchdog mit Zeitfenster	< 0,8 %	< 0,6 %	< 0,4 %
Watchdog mit variablem Zeitfenster	< 0,95 %	< 0,75 %	< 0,55 %

Tabelle 4.4: Fehlererkennungswahrscheinlichkeit mit zeitlicher Programmablaufüberwachung

liche Ablaufüberwachung trägt zum Aufdecken der Fehler, welche eine Programmverzögerung bewirken, bei. Die Ursache hierfür können in fehlerhaften Programmzählern, Endlosschleifen, Veränderungen der Taktfrequenz, Ausfall der Stromversorgung oder des Prozessors sein. Unter der Annahme einer gleichen Auftretenswahrscheinlichkeit dieser Fehlerursachen, kann eine typische Fehlererkennungswahrscheinlichkeit gemäß Tabelle 4.4 bestimmt werden.

Es ist erkennbar, dass mit gesteigertem Aufwand eine sehr hohe Fehlererkennungswahrscheinlichkeit erreicht werden kann. Derartige Kontrollstrukturen können aufgrund der Kostenintensität jedoch nur in höchst sicherheitskritischen Anwendungen implementiert werden. Die logische Programmprüfung erkennt weiterführend Fehler im internen Programmablauf und ist bei Fehlern im Programmcounter der zeitlichen Überwachung sogar überlegen. Allgemein spielt die Art der auftretenden Fehler und deren Wahrscheinlichkeit eine wichtige Rolle und ist je nach Anwendungsbereich unterschiedlich zu bewerten. All diese Aspekte müssen für jedes Konzept separat und im Zusammenhang mit der geforderten Performance und den vertretbaren Kosten abgewogen werden, bevor eine Entscheidung über die Art der Programmkontrolle gefällt werden kann.

Theoretisch können mit den nötigen Mitteln die Probleme der Softwarefehler bis auf ein minimales Restrisiko gesenkt werden. Die nötigen Auf-

wendungen übersteigen aber meist den Rahmen des jeweiligen Projektes und einfache Komponenten, ausgestattet mit derartiger Softwareredundanz, sind im hart umworbenen Konkurrenzkampf nicht mehr wettbewerbsfähig. Speziell die diversitäre Softwareentwicklung fällt mit enormen Kosten ins Gewicht, und aufgrund der nicht vollständig zu vermeidenden Abhängigkeiten im Entwicklungsprozess wird deren Nutzen von verschiedenen Kritikern skeptisch betrachtet. Zudem bestehen Probleme bei der Durchführung des anschließenden Vergleiches. Die diversitären Softwarelösungen haben unterschiedliche Durchlaufzeiten, welche zudem in den einzelnen Situationen variieren [SK98]. Hinzu kommen die auftretenden Rundungsfehler, welche nicht von Konzeptfehlern unterschieden werden können. Es wird also ersichtlich, dass der Einsatz diversitärer Softwarepakete nicht dermaßen problemlos erfolgt und man deshalb nach einer gerechtfertigten Alternative bzw. Kombinationsmöglichkeit sucht.

Die Ursache für die hohe Entwicklungsfehlerrate im Softwarebereich liegt in erster Linie in deren Komplexität und Umfang. Durch gezielte Entwicklungsmaßnahmen kann die Fehlerrate beachtlich gesenkt werden. Ähnlich wie im Bereich der Systemarchitektur muss das Softwaresystem in möglichst kleine und überschaubare Module aufgeteilt werden. Die Anbindung an das Gesamtsystem erfolgt ausschließlich über definierte Schnittstellen. Der daraus resultierende Vorteil ergibt sich durch das überschaubare Design der einzelnen Module, sowie die Möglichkeit einer formalen Überprüfung der Korrektheit. Diese Maßnahmen müssen durch eine robuste, defensive Programmierung unterstützt werden, indem speziell auf Fehlerbehandlungen großer Wert gelegt wird. Zudem müssen modulinternen Prüfungen durchgeführt werden, und die effektiven Daten mit Annahmen, Erwartungen sowie Plausibilitätschecks abgeglichen werden. Eine stetige Kontrolle der Integrität für bearbeitete bzw. übertragene Daten hilft auch bei der Fehlervermeidung. Auch die Dokumentation im Quellcode stellt eine nicht zu unterschätzende Maßnahme gegen eingeschlichenen Fehlern dar. Durch diese Maßnahmen und zusätzlichen, projektspezifischen Codierungsrichtlinien, kann das Qualitätsniveau der erstellten Software deutlich gesteigert werden. Grundsätzlich muss neben der effektiven Programmierung bereits bei der Konzipierung ein Datenfluss- und Kontrollflussdiagramm angefertigt werden, welche in Kombination mit semantischen Analysen die Korrektheit des Entwurfes noch vor dessen Implementierung prüfen lässt. Die Abnahme der einzelnen Codemodule erfolgt durch mehrere Reviews, Meilensteinanalysen und ständige Walktroughs.

Anhand dieser Vorgangsweise werden die einzelnen Programmteile auf eine konsequente und robuste Art implementiert, und später durch den Systemintegrator anhand der klar definierten Schnittstellen zu einem Programm zusammengeführt. Natürlich können damit nicht alle Fehler im Entwicklungs-

prozess der Software beseitigt werden, sie werden jedoch auf ein geringeres Ausmaß minimiert. Die große Bedeutung dieser Errungenschaft ist, dass die Fehler gar nicht erst ins System kommen, sondern sie werden bereits vor deren Entstehung eliminiert. Eine spätere Programmablaufprüfung oder eine zweifache Diversität dient lediglich zur Fehlererkennung, die Funktionalität des Gesamtsystems wird jedoch unter Umständen eingeschränkt. Trotzdem muss eine Gesamtsicherheit der Software durch Kombination der hier erwähnten Methoden angestrebt werden, welche den sicherheitstechnischen und finanziellen Aspekten des Projektes entspricht.

Kapitel 5

Zusammenfassung & Ausblick

5.1 Zusammenfassung

Der Einzug der elektronischen Komponenten im Automobil wird immer stärker. Heute erhältliche Fahrzeuge werden vermehrt den Bedürfnissen der neuen, hochmodernen Systeme angepasst. Durch diese schrittweise Einführung immer neuer Extraausstattungen entstand ein komplexes und schwer zu überschaubares Gebilde. Zusätzlich blieb die alt bewährte Grundstruktur, welche für die Basisfunktionen des Fahrzeuges zuständig ist, bestehen und wurde lediglich den neuen Anforderungen entsprechend modifiziert. Die Vorteile elektronisch gesteuerter Elemente liegen auf der Hand, weshalb elektrische Komponenten auch in allen Bereichen des Fahrzeuges, wenn oftmals auch nur unterstützend, eingesetzt werden. Jegliche Multimedia- und Komfortfunktionen werden heute bereits ausschließlich durch elektronische Steuergeräte gehandhabt. Dadurch erhält man neue Möglichkeiten in der Funktionalität des jeweiligen Systems sowie eine höhere Flexibilität auf Gesamtebene.

Eine Vielzahl an hochmodernen, elektronischen Helfern ist auch im Bezug der aktiven sowie passiven Sicherheit zu verzeichnen. In diesem Bereich ist der Einsatz meist als überlagerte Funktionalität realisiert, welche auf die bereits ausgereiften und daher als relativ sicher und zuverlässig geltenden Basiskomponenten zurückgreifen. Diese Mehrschichtigkeit stellt im Zusammenhang mit der inzwischen erreichten Performance der Steuergeräte, ein immer gravierender werdendes Problem dar. Die Anpassung der Basiskomponenten, welche im sicherheitsrelevanten Bereich ausschließlich mechanisch realisiert sind, wird immer aufwändiger und die Eigenschaften bezüglich Flexibilität, Dynamik und Leistung entsprechen in manchen Bereichen nicht den Erwartungen bzw. Möglichkeiten der überlagerten modernen Technologie. Deshalb können die elektronischen Regelungen teilweise nicht voll ausgenutzt wer-

den, was im Prinzip ein Hindernis in der Forschung und Entwicklung der Automobilindustrie darstellt.

Um dieses Problem zu umgehen, wird an verschiedenen Studien gearbeitet, welche X-by-Wire Technologie einsetzen. Dabei wird speziell die zuvor beschriebene Problematik aufgearbeitet, und ein von Grund auf neues Design der Basisfunktionen im Automobil erstellt. Ausschlaggebend ist dabei die Ersetzung der mechanischen und hydraulischen Bauteile, welche für das Lenken und Bremsen des Fahrzeuges dienen. An deren Stelle wird die Grunddynamik des Fahrzeuges mit Hilfe elektronischer Steuereinheiten, entsprechenden Bedienelementen und Stellgliedern kontrolliert. Aus diesem Abstraktionslevel ist bereits erkennbar, dass durch den Einsatz der X-by-Wire Technologie, die gesamte Fahrzeugarchitektur homogen ist, womit das Zusammenspiel der einzelnen Komponenten reibungsloser stattfinden kann. Dadurch kann das Potential der heute bereits verwendeten elektronischen Komponenten weiter ausgeschöpft werden, bzw. durch deren geeignete Strukturierung, eine Menge an vorteilhaften Eigenschaften erzielt werden. Das durch alle Schichten konsequent umgesetzte by-Wire Prinzip bringt massive Neuerungen für die Kraftfahrzeugindustrie mit sich. Eine komplette Umstrukturierung des Fahrzeuginnenraumes, mit Schwerpunkten in den Bereichen Sicherheit, Ergonomie und Komfort ist lediglich eine der vielen Vorteile. Die relativ freizügige Gestaltung der Bedienelemente ermöglicht es spezielle Konzepte zu entwickeln, welche auch für eine behindertengerechte Steuerung geeignet sind. Zudem wird das Fahrwerk des Fahrzeuges je nach Benutzerwunsch und aktueller Straßensituation optimal abgestimmt. Die hochmoderne Motorsteuerung erlaubt die jeweils bestmögliche Abstimmung der Motordynamik, was durch verbesserte Verbrennung und optimierte Drehzahlen eine sparsamere Fahrt und zudem mehr Leistung bringt. Die Ersetzung einiger robuster, mechanischer Bauteile durch by-Wire Technologie führt zu Gewichtseinsparungen und führt indirekt zu besserer Balance und umweltfreundlicherem Auftreten, sowie zu einer gesteigerten Dynamik in den verschiedensten Bereichen der elektronischen Regelung. Die Interaktion der einzelnen Sensoren und Aktuatoren, kombiniert mit der vorhandenen Rechenleistung im Automobil, eröffnen neue Möglichkeiten, welche bisher völlig unvorstellbar waren. Die Relevanz sowie der Nutzen solcher Systeme muss jedoch abgewogen werden, dies wird über einen zukünftigen Einsatz im Kraftfahrzeug entscheiden.

In der heutigen Situation, mit einer Vielzahl an Mechatroniksysteme, welche im Hintergrund aber auf die mechanischen Systeme aufbauen, tauchen zunehmend gravierende Probleme auf. Die Unzuverlässigkeit und die andauernden Schwierigkeiten bei gehobenen Fahrzeugklassen, zudem kombiniert mit einer schlechten Fehlerdiagnose, kratzt inzwischen merklich am Image der großen Automobilhersteller. Das Hauptproblem bei diesen Auto-

modellen ist die mehrschichtige Ausführung der Grundfunktionen. Enorme Technik wird auf eine alte, und nicht dafür geeignete Fahrzeugbasis aufgebaut, während ein von Grund auf einheitliches und homogenes Konzept, welches in der Lage wäre, die überlagerte Mechatronik zu bedienen, fehlt.

Dieses Problem aufgreifend, forscht man an Komponenten, welche die Grundfunktionalitäten des Autos anhand elektronischer Steuerelemente steuert. Es stellt sich dabei immer wieder die Frage, ob elektronische Steuerelemente auch sicher und zuverlässig sind, und sie für den Einsatz in sicherheitsrelevanten Bereichen überhaupt geeignet sind. Auf diese Frage kann getrost mit ja geantwortet werden, denn die Ausfallwahrscheinlichkeit kann durch entsprechende Architektur und Designrichtlinien je nach Bedarf angepasst werden. Rechnerisch kann mit elektronischen Komponenten und einer geeigneten Struktur eine höhere Zuverlässigkeit erzielt werden, als mit herkömmlichen mechanischen Systemen. Eine überdimensionierte Ausfallsicherheit bringt allerdings hohe Kosten und eine gesteigerte Komplexität mit sich, weshalb ein wirtschaftlicher Kompromiss zwischen Aufwand und Zuverlässigkeit gefunden werden muss. Wie die Ausführungen in den vorangehenden Kapiteln im Detail beschreiben, muss bei der Systemarchitektur, neben einem entsprechenden Entwurfsdesign, gezieltes Augenmerk auf die Fehlertoleranz und die logische Verschachtelung der modularen Teilkomponenten gelegt werden. Somit ist man durchaus in der Lage eine Basis zu entwickeln, welche die Grunddynamik des Fahrzeuges zuverlässig steuert und dafür ausgelegt ist, mit zusätzlichen mechatronischen Komponenten zu interagieren. Dabei ist hervorzuheben, dass die beschriebene Architektur die Verwendung verschiedener Teilnetze vorsieht, was eine Weiterverwendung heute bereits eingesetzter Technologien im Automobil ermöglicht. Ohne diese Eigenschaft wäre eine komplette Neuentwicklung sämtlicher Bauteile notwendig, was aus wirtschaftlichen Gründen nur äußerst schwer machbar wäre.

Die neu strukturierte Systemarchitektur bietet, aufgrund der logischen Kapselung und die Eingrenzung in error-containment-regions, beste Voraussetzungen für einen modularen Aufbau, was der Verkaufsphilosophie der Automobilhersteller, sowie der harten Preispolitik entgegenkommt. Zusätzlich ermöglicht dieses Designprinzip eine verbesserte Diagnosefähigkeit der Elektronikkomponenten und punktet deshalb im Bereich der Wartbarkeit.

Neben dem bisher beschriebenen Teil der Hardware, darf die Software keinesfalls vernachlässigt werden. Erst das Zusammenspiel von Software und zugrundeliegendem Rechnerystem ermöglicht die Funktionalität der gesamten Architektur. Deshalb müssen Fehler und Gefahren in der Software genauso vermieden werden wie in den restlichen Komponenten. Entsprechende Entwicklungs- und Codierungsrichtlinien, Softwarediversität, Programmprüfung und -überwachung sind daher unerlässlich und erst eine geeignete

Kombination dieser Methoden führt, wie in Kapitel 4.7 beschrieben, zum gewünschten Ziel.

5.2 Ausblick

Der aktuelle Entwicklungsprozess auf mechanisch funktionierenden Grundfunktionen läuft langsam aber sicher gegen eine Grenze, was den Umstieg auf eine neuartige Basis erforderlich macht. Bereits laufende Projekte forschen an dieser neuartigen Fahrzeugstruktur, welche inzwischen bereits Ergebnisse liefern. Die Realisierung eines kompletten by-Wire Automobils ist aus technischer Sicht machbar, es fehlen lediglich Testdaten sowie praktische Erfahrung. Weiters gilt es die adäquate Auslegung und Konfiguration des Gesamtsystems zu finden. Der Umstieg der aktuellen Fahrzeuge auf X-by-Wire Technik stellt eine nicht triviale Herausforderung dar. Wie bereits im Kapitel 2.3 beschrieben, müssen bei der Einführung der neuen Technologie einige wirtschaftliche Grundprinzipien beachtet werden. Zudem muss das Klientel sowohl von der Zuverlässigkeit, als auch von den Vorteilen einer vollkommen elektronischen Steuerung überzeugt werden.

Indirekt hat mit dem „Ausstattungsboom“ der Fahrzeuge ein Schritt in die richtige Richtung stattgefunden. Die neuesten Mechatroniksysteme werden, wie bereits aus der langjährigen Geschichte des Kraftfahrzeuges bekannt, in den Oberklassemodellen eingeführt und dort als der Stand der Technik präsentiert. In den letzten Jahren verfolgten die Automobilhersteller zudem verstärkt die Strategie, derartige Systeme auch für Modelle der Mittel- und Kompaktklasse zu adaptieren und dort anzubieten. Dadurch ist es gelungen, die modernen Elektroniksysteme einer breiten Benutzerschicht zugänglich zu machen. Der gesteigerte Absatz ermöglichte zudem eine interessante Preispolitik. Als Resultat dieser Entwicklung verwendet heute ein großer Anteil der Fahrzeuglenker verschiedene Mechatroniksysteme, kann sich von deren Vorteile überzeugen und wird gleichzeitig mit der neuen Technologie vertraut. Die Kehrseite der Medaille ist jedoch die relativ hohe Ausfallrate der im Automobil eingesetzten Elektronikkomponenten, sowie deren schlechte Wartbarkeit. Die starke Forschung und Entwicklung in diese Richtung bringt jedoch schon Besserung, was auch jüngste Statistiken belegen.

Die konsequente Entwicklung des Fahrzeuges führt also klar in Richtung der X-by-Wire Systeme, welche die Leistung moderner Rechensysteme auszunutzen vermag, und deshalb für revolutionäre Neuerungen im Automobilbereich sorgen wird. Die Vorteile liegen vor allem in der Flexibilität des zugrundeliegenden Konzeptes, welches eine einfache Erweiterbarkeit bietet. Dadurch besteht auch die Möglichkeit der zukünftigen Weiterentwicklung

in jeglichen Bereichen des Fahrzeuges, ohne auf Kompatibilitätsprobleme zu stoßen.

Ist der Umstieg auf by-Wire Technologie erst einmal erfolgt, so kann an weitere, systemübergreifende Konzepte gedacht werden. So wären Möglichkeiten einer Schnittstelle nach außen denkbar, welche über Großrechner oder mit anderen Fahrzeugen kommunizieren. Dabei könnte beispielsweise ein gesicherter Kolonnenverkehr auf Autobahnen organisiert werden, und sogar eine Diagnose der Fahrzeugkomponenten per Fernwartung wäre möglich. Durch Kommunikation mit anderen Fahrzeugen kann zudem für reibungsloses Verkehrsaufkommen gesorgt werden, indem eine eingeleitete Bremsung an das Folgefahrzeug mitgeteilt wird, welches seine Geschwindigkeit, um die Reaktionszeit des Fahreres eher, verringern kann. Die Überwachung der Fahrzeuge im Bezug auf Geschwindigkeitsübertretungen und anderen Verkehrsdelikten könnte je nach Wunsch auch erleichtert bzw. automatisiert werden. Eine komplette Fernsteuerung des Fahrzeuges über einen Leitrechner wäre ein weiteres Konzept, was ein X-by-Wire Fahrzeug mit entsprechender Schnittstelle bereitstellen könnte. Viele dieser, keineswegs als vollständig anzusehenden Möglichkeiten, sind bereits heute Teil der Forschung und Entwicklung, und könnten theoretisch auch mit aktuellen Fahrzeugen, wenn auch mit einigen Abstrichen, umgesetzt werden. Dabei muss jedoch auf eine höhere Dynamik und Flexibilität verzichtet werden. Zudem spricht die Fehleranfälligkeit heute entwickelter, heterogener Systeme klar gegen ein derartiges Konzept.

In der Literatur wird oft die Notwendigkeit der X-by-Wire Systeme in modernen Kraftfahrzeugen in Frage gestellt, da anhand verstärkter Mechatroniksysteme im heutigen Kontext auch bliebig Funktionen erreicht werden können. Will man dem aktuellen Dilemma der überhöhten Probleme, zu geringen Wartbarkeit und Flexibilität entkommen, führt der Weg nur über die beschriebene by-Wire Technologie. Auch eine mehrstufige Systemarchitektur, mit mechanischer Rückfallebene als Notsystem, schränkt die Möglichkeiten der neuen Plattform ein und verringert die Effektivität derselben in den verschiedensten Bereichen.

Es besteht noch genügend Entwicklung- und Testsaufwand, insbesondere im Bereich der ausfallsicheren Aktuatoren, langlebigen Prozessoren und der sicheren Software. Fahrzeuge mit X-by-Wire Basis sind aber keine "Zukunftsmusik" mehr, sondern werden in nächster Zukunft bereits Einzug in den Markt finden.

Abkürzungsverzeichnis

ABS	...	Anti-Blockier-System
ADR	...	Automatische Distanzregelung
AMK	...	Aufmerksamkeitskontrollen
ASR	...	Antriebs-Schlupf-Regelung
BAS	...	Bremsassistent
CAN	...	Controller Area Network
CRC	...	Cyclic Redundancy Check
EBV	...	Elektronische Bremskraftverteilung
EHB	...	Elektrohydraulische Bremse
EMI	...	Electromagnetic Interference
EMV	...	Elektromagnetische Verträglichkeit
ENV	...	Enhanced Night Vision
ESP	...	Elektronisches Stabilitätsprogramm
FCAS	...	Full Collision Avoidance
FDR	...	Fahrdynamikregelung
FO	...	Fail Operational
FS	...	Fail Safe
FSIL	...	Fail Silent
HPM	...	High-Power Microwave
IDL	...	Interface Description Language
LIN	...	Local Interconnect Network
MSR	...	Motorschleppmomentregelung
MTBF	...	Mean Time Between Failure
MTTF	...	Mean Time To Failure
MTTR	...	Mean Time To Repair
NEMP	...	Nuklearer elektromagnetischer Puls
RFI	...	Radio Frequency Interference
TDMA	...	Time Division Multiple Access
TMR	...	Triple Modular Redundancy
TSR	...	Traffic Sign Recognition
TTP	...	Time Triggered Protocol

Abbildungsverzeichnis

2.1	Aufbau eines ABS-Gerätes	7
2.2	Eingriff des ABS-Systems	8
2.3	Aufbau einer ASR-Steuerung	10
2.4	Aufbau eines Bremsassistenten	12
2.5	Aufbau einer ESP-Steuerung	13
2.6	Entwicklung der Informationsgewinnung und Assistenzsysteme im Fahrzeug	17
2.7	Prinzipaufbau des Brake-by-wire-Systems	20
2.8	Diagramm eines Steer-by-wire-Systems	24
2.9	Assistenzsysteme vom Normalzustand bis zum Unfall	29
2.10	Steuerung durch Sidesticks, verwendet im umgebauten Mercedes SL der Baureihe R129	33
2.11	Innovative Innenraumgestaltung dank X-by-Wire und X-Drive	35
3.1	Grenzzisiko als Schwelle zwischen Sicherheit und Gefahrenzone	42
3.2	Abhängigkeit der Kennzahlen MTTR, MTTF, MTBF	44
3.3	Die fünf Säulen der Zuverlässigkeit	46
3.4	Risikograph der indikativen Kombinationen	50
3.5	Zusammenspiel von Störquelle und -senke	62
4.1	Grundaufbau eines X-by-Wire Systems	69
4.2	Mögliche Architektur mit Funktionsklassen	83
4.3	Nachrichtenformat am CAN-Bussystem	87
4.4	Überlagerte Zeitsteuerung im TTCAN	89
4.5	Aufbau einer TTP/C-Nachricht	90
4.6	Verschiedenen Anordnungsmöglichkeiten der Aktuatoren	95
4.7	12V/42V Stromkreis	99
4.8	Stromkreis mit lokalen Reserven [Leo04]	100
4.9	Redundante Stromkreise [Leo04]	101

Tabellenverzeichnis

3.1	Einteilung der Unfallfolgen für militärische Systeme	47
3.2	Risikoklassifizierung nach IEC 61508	48
3.3	Stufenweise Degradation eines Steer-by-Wire Systems	61
4.1	Messwerte und Gültigkeitsintervalle in der Motorsteuerung . .	75
4.2	Überblick aktueller Bussysteme im Fahrzeugbau	86
4.3	Vergleich von Bussystemen	92
4.4	Fehlererkennungswahrscheinlichkeit mit zeitlicher Programm- blaufüberwachung	109

Literaturverzeichnis

- [BBW] Automotive braking method and device for carrying out said method. <http://www.wipo.int/pctdb/en/wo.jsp?IA=EP2000010796&-DISPLAY=DESC>.
- [Bör04] J. Börcsök. *Elektronische Sicherheitssysteme - Hardwarekonzepte, Modelle und Berechnung*. Hüthig Verlag Heidelberg, 2004.
- [DFM⁺97] E. Dilger, T. Führer, B. Müller, S. Poedna, und T. Thurner. X-by-Wire: Design von verteilten, fehlertoleranten und sicherheitskritischen Anwendungen in modernen Kraftfahrzeugen. *Brite-EuRam III-Projekt*, 1997.
- [Düc93] H. Dücker. Ergebnisvalidierung und nebenläufige Hardwarefehlererkennung mittels systematisch erzeugter Diversität. In *Verlässliche Informationssysteme*, pages 135–162. G.Weck, Braunschweig, 1993. Universität Karlsruhe, Institut für Rechnerentwurf und Fehlertoleranz.
- [ein] Die Relativität von Raum und Zeit. <http://www.einstein-online.info/de/einsteiger/spezRT/RTRaumZeit/index.html>.
- [ENV] Enhanced visibility in the dark Siemens VDO integrated Night Vision in the head-up display. <http://www.mrunix.de/forums/archive/index.php/t-37408.html>.
- [FHK⁺01] H. Friedrich, J. Hoffmann, J. Kreft, C. Semmler, und B. Witte. Auf dem Weg zum intelligenten Auto - Steer-by-Wire als Basis zukünftiger Assistenzfunktionen. In *VDI-Berichte 1613*, 2001.
- [HB98] B. Hedenetz und R. Belschner. Brake-by-Wire without mechanical Backup by Using a TTP-Communication Network. *SAE Technical Paper*, 1998.

- [ISS02] R. Isermann, R. Schwarz, und S. Stölzl. Fault-Tolerant Drive-by-Wire Systems. *IEEE Control Systems Magazine*, Okt 2002.
- [KG03] Hella KG. Elektronik-Kontaktlose Sensoren für X-by-Wire Systeme. Technical report, Hella KG, 2003.
- [Kop94] H. Kopetz. A Solution to an Automotive Control System Benchmark. In *IEEE 1994*, 1994.
- [Kop98] H. Kopetz. A Comparison of CAN and TTP. *Consumer Electronics, IEEE Transaction on*, 1998.
- [Kop02] H. Kopetz. *Real-Time Systems - Design Principles for Distributed Embedded Applications*, volume 6. Kluwer Academic Publishers, 2002.
- [KWG⁺04] C.R. Kelber, D. Webber, G.K. Gomes, M.A. Lohmann, M.S. Rodrigues, und D.Ledur. Active Steering Unit with integrated ACC for X-by-Wire vehicles using a joystick as H.M.I. In *2004 IEEE Intelligent Vehicles Symposium*, June 2004.
- [Leo04] J. Lehold. Die elektrische Infrastruktur für zukünftige Fahrerassistenzsysteme. In *Automatisierungs- und Assistenzsysteme für Transportmittel - Möglichkeiten, Grenzen, Risiken*. Braunschweiger Symposium - Gesamtzentrum für Verkehr Braunschweig, Feb. 2004.
- [lex] USV Lexikon. <http://www.errepi.de/de/usvlexi.htm>.
- [lin] LIN Subbus. <http://www.lin-subbus.org>.
- [Mah00] R. Mahmoud. *Sicherheits- und Verfügbarkeitsanalyse komplexer KfZ-Systeme*. PhD thesis, Universität Siegen, 2000.
- [Maj04] M. Majuntke. Fly-by-Wire Anwendungen im Automobil, 2004.
- [Mar01] R. Marstaller. Fahrerhaltensänderung bei der fahrerassistierenden KfZ-Steuerung mit aktiven Bedienelementen gegenüber dem konventionellen Bedienkonzept. In *VDI-Berichte 1613*, 2001.
- [mon] Prinzipien der Fehlertoleranz. http://sergio.montenegros.de/public/ft_einf.html.

- [Mon99] S. Montenegro. *Sichere und fehlertolerante Steuerungen*. Carl Hanser Verlag München Wien, 1999.
- [ntg] Zuverlässigkeitsbegriffe im Hinblick auf komplexe Software und Hardware. NTG-Empfehlung 3004.
- [pol] Leitfähige Kunststoffe.
- [Rei03] H.R. Reichel. *Elektronische Bremssysteme - Vom ABS zum Brake-by-Wire*, volume 2. Expert Verlag, 2003.
- [RTT00] C. Rossi, A. Tilli, und A. Tonielli. Robust Control of a Throttle Body for Drive by Wire Operation of Automotive Engines. In *IEEE transactions on control systems technology*, volume 8, 2000.
- [Sch80] G.H. Schildt. Grundlagen für Vergleiche mit Sicherheitsverantwortung. In *Siemens Forsch.- u. Entwickl.-Ber*, volume 9. Springer Verlag, 1980.
- [Sch06] G.H. Schildt. *Impulstechnik*. LYK Informationstechnik, 2006.
- [SK98] G.H. Schildt und W. Kastner. *Prozessautomatisierung*. Springer Wien - New York, 1998.
- [Sto04] U. Stock. Fehlertolerante Netzwerke für Drive-by-Wire Anwendungen im KFZ. Technical report, OKI Electric Europe GmbH, 2004.
- [The01] I. Theis. *Das Steer-by-Wire System im Fahrzeug - Analyse der menschlichen Zuverlässigkeit*. PhD thesis, Universität München, 2001.
- [Wei] G.K. Weitbrecht. Elektromechanische Bremse. Bosch.