

Elektrik/Elektronik-Architekturen im Kraftfahrzeug

Modellierung und Bewertung von Echtzeitsystemen

Bearbeitet von
Thilo Streichert, Matthias Traub

1. Auflage 2012. Buch. xviii, 284 S. Hardcover
ISBN 978 3 642 25477 2
Format (B x L): 15,5 x 23,5 cm
Gewicht: 619 g

[Weitere Fachgebiete > Technik > Elektronik > Elektronische Baugruppen,
Elektronische Materialien](#)

Zu [Inhaltsverzeichnis](#)

schnell und portofrei erhältlich bei


DIE FACHBUCHHANDLUNG

Die Online-Fachbuchhandlung beack-shop.de ist spezialisiert auf Fachbücher, insbesondere Recht, Steuern und Wirtschaft. Im Sortiment finden Sie alle Medien (Bücher, Zeitschriften, CDs, eBooks, etc.) aller Verlage. Ergänzt wird das Programm durch Services wie Neuerscheinungsdienst oder Zusammenstellungen von Büchern zu Sonderpreisen. Der Shop führt mehr als 8 Millionen Produkte.

Tabelle 2.1 Beispiel für die Anwendung von Metriken

	Alternative 1 2 Tür-ECU CAN vernetzt; Sensoren/Aktoren hinten diskret verkabelt	Alternative 2 Sensoren/Aktoren diskret verkabelt	Alternative 3 Master in Fahrertür; andere Türen diskret vernetzt	Alternative 4 4 Tür-ECU CAN vernetzt
Buslast [%]	4	–	–	8
Gewicht [g]	1955	2712	2823	694
Kosten [euro]	2,50	3,26	4	1,88
Montage- aufwand	570	540	525	600
Bündel- durchmesser	12,212	12,39	20,8	2,73
Anzahl Steuergeräte	3	1	1	5

Schalter und Sensoren müssen im Body Controller vorgehalten werden. In der zweiten Alternative wird sämtliche Sensorik und Aktorik direkt an den Body Controller angeschlossen, wodurch einerseits die Türsteuergeräte wegfallen, aber andererseits die Verkabelung für jeden Sensor und Aktor getrennt in die Tür gelegt werden muss. Die dritte Alternative zeigt ein Türsteuergerät in der Fahrertür, an das die Sensorik und Aktorik der anderen Türen diskret mit einzelnen Leitungen angeschlossen ist. In der letzten Alternative sind vier Türsteuergeräte verbaut, die jeweils für die Sensorik und Aktorik in der jeweiligen Tür zuständig sind und über einen CAN-Bus miteinander Daten austauschen.

Wendet man auf diese vier verschiedenen Architekturalternativen die obigen Metriken an, so ergibt sich folgendes Bild, das in Tab. 2.1 dargestellt ist². Auffällig ist hierbei, dass jede Alternative bei bestimmten Kriterien Vorteile mit sich bringt, aber bei anderen Kriterien dominiert wird. Als Entwickler hat man in einem solchen Fall die Aufgabe den Entscheidungsraum weiter einzugrenzen. Hierbei kann die Betrachtung weiterer Baureihen oder Fahrzeugvarianten helfen. Alternativ können auch Argumente helfen, die nicht oder nur schlecht quantifizierbar sind. Zum Beispiel existiert ein Übernahmebauteil aus einem bestehenden Produkt, oder der Reifegrad einer betrachteten Technologie ist höher als bei einer anderen Technologie.

2.2 Einflüsse durch Gesetzgebung und Standardisierung

Die Einflüsse der Gesetzgebung auf eine E/E-Architektur können aus höchst unterschiedlichen Bereichen kommen und sind für die Zulassungsfähigkeit von Fahrzeugen

² Die Werte der Tabelle sind hypothetisch und stellen keinen Bezug zu einem konkreten Produkt dar.

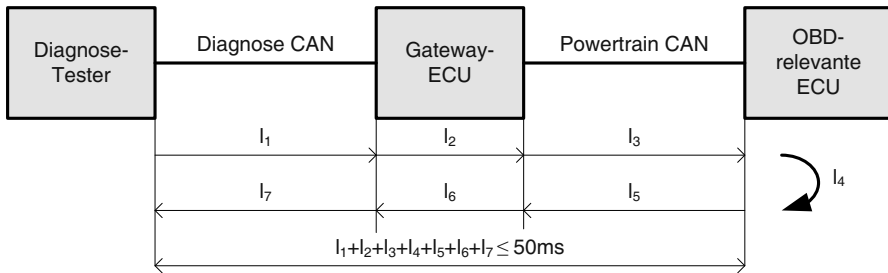


Abb. 2.13 Beispiel für einen Diagnosepfad, welcher die Anforderung der maximalen Latenzzeit von 50 ms erfüllen muss

gen in den Zielmärkten wichtig. Viele dieser länderspezifischen Vorschriften kommen aus dem Bereich der Abgasemissionen und der Unfallsicherheit. Ein Überblick über die gesetzlichen Vorschriften ist in [AG11] gegeben. Um diese vielfältigen, diversen und teilweise komplexen Vorschriften in den Entwicklungsprozessen zu berücksichtigen, bedarf es einer gründlichen Planung während der Entwicklung und Fahrzeugzulassung. Diese Prozedur der Fahrzeugzulassung wird auch als *Homologation* bezeichnet. Im Folgenden soll anhand von drei Beispielen gezeigt werden wie gesetzliche Vorgaben Einfluss auf die E/E-Architektur nehmen.

On-Board Diagnose

Um ein Fahrzeug in den USA auf den Markt bringen zu können, muss dieses den Regeln der CARB-Behörde (California Air Resource Board) genügen. Diese Behörde stellt Anforderungen für die abgasrelevanten Komponenten von Kraftfahrzeugen auf. Durch den Einsatz neuer Antriebstechnologien (Hybrid, E-Antrieb) werden immer mehr E/E-Komponenten von der CARB als OBD-relevant eingestuft. Die Anforderung betrifft auch die Diagnostizierbarkeit von E/E-Komponenten. Beispielsweise müssen die als OBD-relevant eingestuften Steuergeräte, welche die Speicherung von OBD-Fehlern durchführen, innerhalb von 50 ms auf die Anfrage eines Diagnosetesters antworten. In Abb. 2.13 ist ein solcher Pfad dargestellt, der über zwei CAN-Busse und ein Gateway zum diagnostisierten Steuergerät und wieder zurück zum Diagnosetester geht.

Weiterhin wird an einer weltweiten Harmonisierung der On-Board Diagnose gearbeitet, bei der eine einheitliche Diagnoseschnittstelle am Auto definiert werden soll. Dieser Standard [IOFS11, IOFS06] sieht eine Einführung einer Ethernet-Schnittstelle und die Anwendung des Internet Protokolls vor. Zusätzlich kommt eine sogenannte *Diagnostics over IP*-Schnittstelle (DoIP) zum Einsatz. Mit diesen standardisierten Protokollschichten soll nicht nur die Kompatibilität zwischen den Fahrzeugen, sondern auch zwischen Fahrzeug und einem Diagnose-Computer gegeben sein. Somit ergibt sich wiederum ein Einfluss auf die E/E-Architektur. Einerseits muss die Schnittstelle im Fahrzeug vorhanden und technologisch abgesichert sein.

Andererseits müssen die Steuergeräte das Datenaufkommen verteilen und verarbeiten können, das über die Ethernet-Schnittstelle kommuniziert wird.

Elektronisches Stabilitätsprogramm (ESP)

Ein weiteres Beispiel mit Einfluss auf die E/E-Architektur ist die Einführung des elektronischen Stabilitätsprogramms (ESP), das die Anzahl an Schleuderunfällen erheblich reduziert. Während in Premium- und Mittelklassefahrzeugen das System als Serienausstattung verbaut wird, kommt es in kostengünstigen Kleinwagen seltener zum Einsatz. Um langfristig eine flächendeckende Integration in die Fahrzeuge zu erreichen, hat das Europäische Parlament entschieden, dass neu entwickelte Modelle ab dem 1. November 2011 und bereits auf dem Markt befindliche Modelle ab dem 1. November 2014 mit dem elektronischen Stabilitätsprogramm ausgestattet sein müssen [dEU09]. Auch der EuroNCAP-Test wird die Möglichkeiten der Umfelderkennung und aktiven Sicherheit in die Bewertung der Sicherheit eines Fahrzeugs stärker einbeziehen. Ein Fahrzeug, das beispielsweise über radarbasierte Notbremssysteme verfügt, kann Unfälle vermeiden und somit mehr Punkte im Test erreichen. In diesem Fall ist es zwar keine zwingende Vorgabe, dass ein Notbremssystem verbaut ist, es stellt allerdings einen starken Anreiz für Fahrzeughersteller dar solche Systeme zu integrieren.

In beiden Fällen macht es Sinn die Integration der Sicherheitssysteme neu zu bewerten. Bei Systemen, die unter der Annahme einer Sonderausstattung integriert wurden, muss das Fahrzeug mit und ohne dieser Sonderausstattung effizient und funktional sein. Unter der Annahme, dass ein System zur Serienausstattung wird, kann jedoch eine Integration in eine bereits bestehende Komponente sinnvoll sein.

Rechts/Linkslenker

In unterschiedlichen Ländern existieren verschiedene Vorgaben für die Straßenseite, auf der gefahren wird und die Position des Lenkrads. Bei diesen Vorgaben wird im Wesentlichen zwischen vier Kombinationen unterschieden: Bei Rechtsverkehr ist es entweder empfohlen oder verpflichtend das Lenkrad auf der linken Fahrzeugseite zu haben. Bei Linksverkehr ist es entsprechend empfohlen oder verpflichtend das Lenkrad auf der rechten Fahrzeugseite zu haben. Abbildung 2.14 zeigt einen Überblick über diese Vorgaben in den verschiedenen europäischen Ländern. Der Einfluss auf die E/E-Architektur ist an mehreren Stellen gegeben. So müssen einzelne Bedienelemente und Steuergeräte statt auf der linken auf der rechten Fahrzeugseite untergebracht sein und Leitungssätze entsprechend angepasst werden. Teilweise wird auch die Anordnung von Bedienelementen gespiegelt. Während die Anordnung der Pedale und des Schalthebels gleich bleibt, befinden sich teilweise der Scheibenwischer- und Blinkerhebel auf der entgegengesetzten Seite.

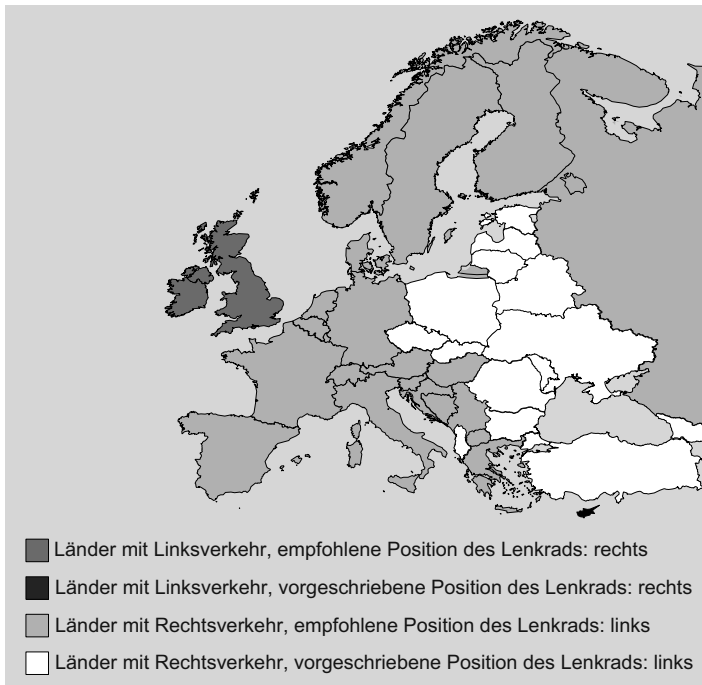


Abb. 2.14 Empfohlene oder vorgeschriebene Position des Lenkrads von europäischen Ländern

Funktionale Sicherheit

Das Thema *funktionale Sicherheit* nimmt bei der Entwicklung von Kraftfahrzeugen einen immer größeren Stellenwert ein. Am Beispiel des Falles von Toyota aus der jüngeren Vergangenheit, bei dem es zu einer Verwechslung des Gas- und des Bremspedals durch den Kunden kam, wird deutlich wie wichtig der Nachweis für den Hersteller von Kraftfahrzeugen ist, dass er nach aktuellem Stand der Technik entwickelt hat, um Risiken für den Kunden und die Umwelt zu minimieren.

Der Einstieg in das Thema soll anhand der eindeutigen Bestimmung der Begrifflichkeiten erfolgen. Im deutschen Sprachgebrauch wird der Begriff *Sicherheit* mit verschiedenen Bedeutungen verwendet. Eine eindeutige Zuordnung kann immer erst durch die Berücksichtigung des Kontextes, in dem der Begriff verwendet wurde erfolgen. Die folgenden beiden Definitionen sind gültig:

- *Sicherheit (engl. Security)* beschreibt den Schutz eines Systems gegenüber äußeren Angreifern, z. B. durch böswillige Manipulation von Daten oder die Beeinträchtigung eines Systems durch unerlaubten Zugriff.
- *Sicherheit (engl. Safety)* beschreibt den Schutz der Umwelt vor einem Objekt.

Anhand eines Beispiels einer *Tür* lassen sich die beiden Begriffsdefinitionen verdeutlichen. Im Fall der Sicherheit – im Sinne der *Security* – hat die Tür die Aufgabe den Zutritt zu einem Raum zu verhindern. Im Fall der Sicherheit – im Sinne

der *Safety* – soll die Türe im Brandfall vor Feuer und Rauch schützen. Im Kontext der funktionalen Sicherheit liegt dem Begriff Sicherheit die *Safety*-Definition zu Grunde.

Die Grundlage für die funktionale Sicherheit bildet die internationale Norm *IEC61508 (Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer Systeme)*, welche von der *International Electrotechnical Commission (IEC)* herausgegeben wird. Für die Anwendung auf Kraftfahrzeuge hat eine Anpassung der Norm stattgefunden, die unter der Bezeichnung *ISO26262* zu finden ist. Die *ISO26262* definiert die funktionale Sicherheit wie folgt: *Absence of unacceptable risk due to hazards caused by malfunctional behavior of E/E systems*. Dies bedeutet übersetzt: Nicht akzeptable Risiken können ausgeschlossen werden, welche aufgrund des Fehlverhaltens von E/E-Systemen eine Gefährdung darstellen.

Die Norm *ISO26262* bildet die Grundlage für die Berücksichtigung und Dokumentation der funktionalen Sicherheit bei der Entwicklung von E/E-Systemen, welche im Kraftfahrzeug zum Einsatz kommen. Die Norm besteht aus zehn Teilen:

- Der erste Teil beinhaltet das Glossar.
- Im zweiten Teil erfolgt die Beschreibung des Managements der funktionalen Sicherheit. Hierfür wird eine Definition der Managementtätigkeiten gegeben, welche während des Sicherheitslebenszykluses eines Systems durchzuführen sind.
- Der dritte Teil beschreibt die Konzeptphase mit zwei Schwerpunkten. Der erste Schwerpunkt liegt auf der Identifikation von potentiell gefährlichen Situationen (engl. hazards), welche in allen Betriebsmodi und Ausfallarten eines Systems auftreten können. Diese können z. B. mittels einer sogenannten *Failure Mode and Effect Analysis (FMEA)* ermittelt werden. Der zweite Schwerpunkt beschreibt die Klassifikation der Sicherheitsanforderungsstufen. Diese sind in fünf Stufen aufgeteilt, den sogenannten *Automotive Safety Integrity Levels (ASIL)*. Sicherheitsrelevante Systeme werden mit den ASIL-Stufen A bis D klassifiziert und Systeme, die nicht sicherheitsrelevant sind, werden als *QM-Thema (Qualitätsmanagement)* eingestuft. Das heißt allerdings nicht, dass von diesen Systemen eine Gefährdung ausgehen darf. Durch die Produkthaftung kann auch eine Komponente, die nach Qualitätsmanagementmethoden entwickelt ist, besondere Mechanismen zur funktionalen Sicherheit beinhalten.
- Im vierten Teil werden das Vorgehen und die Anforderungen bei der Produktentwicklung beschrieben.
- Der fünfte Teil umfasst die sicherheitsrelevanten Themen der Hardware-Ebene.
- Im sechsten Teil wird auf die Software-Ebene der Produktentwicklung eingegangen.
- Der siebte Teil umfasst die Produktion und den Betrieb. Es wird das Vorgehen der Erstellung eines Produktions- und Installationsplans für sicherheitskritische Systeme inklusive deren Wartung und Reparatur beschrieben.
- Die unterstützenden Prozesse werden im achten Teil definiert. Diese gehen z. B. auf das Änderungsmanagement und die Dokumentationsprozesse ein.
- Der neunte Teil beschreibt die ASIL- und sicherheitsorientierte Analyse.
- Im zehnten Teil sind Anhänge zu finden.

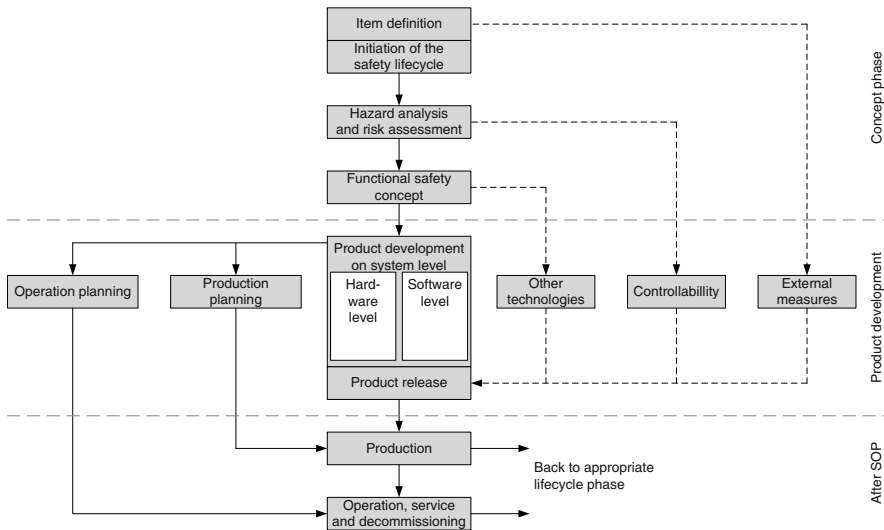


Abb. 2.15 Dargestellt ist der Sicherheitslebenszyklus eines Systems, von der Konzeptphase bis nach dem *Start-of-Production (SOP)*

Der Sicherheitslebenszyklus eines Systems ist in Abb. 2.15 dargestellt. Ein solcher Zyklus umfasst die Konzeptphase, die Entwicklungsphase bis zum *Product Release* sowie die Produktion bis nach dem *Start-of Production (SOP)*. In jeder der einzelnen Phasen sind die drei Managementaktivitäten: Planung, Koordination und Dokumentation durchzuführen.

Innerhalb der Konzeptphase ist eine Gefahren- und Risikoanalyse durchzuführen. Das Risiko R eines Systems kann über folgende Funktion F beschrieben werden:

$$R = F(f, S) \quad (2.5)$$

f steht für die Frequenz, mit der ein kritisches Ereignis auftritt und S für die Ernsthaftigkeit (engl. Severity) des resultierenden Schadens. Die Frequenz f hängt von folgenden Eigenschaften ab:

- Wie oft und wie lange ein System betrieben wird. E steht für *probability of exposure*.
- Wie wahrscheinlich es ist durch menschliches Eingreifen schwerwiegende Folgen abzuwenden. C steht für *Controllability*.

Für die Frequenz f gilt somit:

$$f = C \times E \quad (2.6)$$

Das folgende Beispiel in Tab. 2.2 beschreibt einen Fall für eine Abschätzung der Ernsthaftigkeit (Severity) eines Schadens. Die Klassifizierung der Ernsthaftigkeit geht von S_0 = Keine Verletzungen bis S_3 = lebensgefährliche Verletzungen (Über-

Tabelle 2.2 Beispiel für eine Abschätzung der Ernsthaftigkeit eines Schadens

Klasse	SO	S1	S2	S3
Beschreibung	Keine Verletzungen	Leichte/moderate Verletzungen	Schwere/ lebensgefährliche Verletzungen (Überleben ist wahrscheinlich)	lebensgefährliche Verletzungen (Überleben ist unwahrscheinlich)
Schaden während des Einparkens	trifft zu			
Abkommen von der Straße ohne Überschlag und Kollision	trifft zu			
Kollision vorne/hinten zwischen zwei PKWs		$v < 20 \text{ km/h}$	$20 < v < 40 \text{ km/h}$	$v > 40 \text{ km/h}$
Überschlag		Ohne Kollision (max. ein Überschlag)	Ohne Kollision, mehr als ein Überschlag	Mit Kollision, z. B. mit einem Baum

leben unwahrscheinlich). Anhand der Klassifizierung können verschiedene Fälle, die eintreten können, betrachtet werden. In gleicher Weise lässt sich die Häufigkeit des Auftretens (Exposure) und die Beherrschbarkeit (Controllability) abschätzen.

Die ASIL-Einstufung eines Systems bezieht sich immer auf eine bestimmte Sicherheitsanforderung. Ist ein System mit QM eingestuft, kann es mit den üblichen Qualitätsmanagementmethoden entwickelt und dokumentiert werden. Zu diesen Methoden zählen alle organisierten Maßnahmen, die der Sicherstellung und der Verbesserung eines Systems dienen. Das Qualitätsmanagement ist eine Kernaufgabe des Managements. In Tab. 2.3 sind den einzelnen Schadensklassen anhand ihrer Auftrettsfrequenz f aufgezeigt.

Auf der Basis der Gefahrenanalyse werden Sicherheitsziele als Anforderungen an das System sowie die Entwicklung und Dokumentation abgeleitet. Das Sicherheitskonzept (engl. Functional Safety Concept) beschreibt die hierfür notwendigen

Tabelle 2.3 Einstufung von Gefahrenklassen anhand deren Auftrettsfrequenz

Severity	Frequenz (f) = Exposure $\times$ Controllability					
	$f = 1$	$f = 0.1$	$f = 0.01$	$f = 0.001$	$f = 0.0001$	$f = 0.00001$
S0	QM	QM	QM	QM	QM	QM
S1	ASIL B	ASIL A	QM	QM	QM	QM
S2	ASIL C	ASIL B	ASIL A	QM	QM	QM
S3	ASIL D	ASIL C	ASIL B	ASIL A	QM	QM

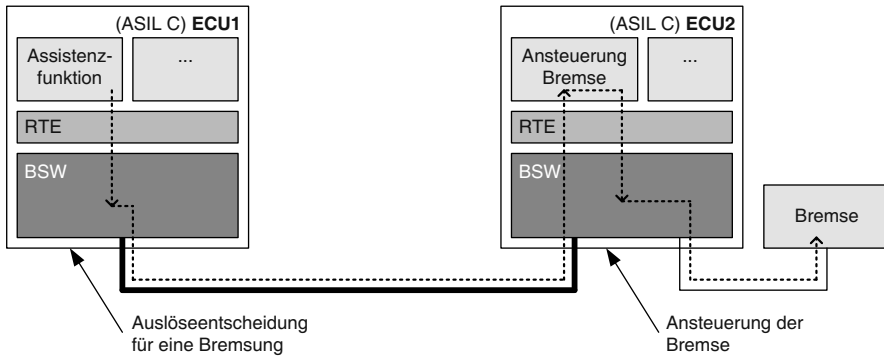


Abb. 2.16 Beispiel für ein Teilsystem, welches einen Bremseneingriff auslösen kann

Schritte. Es umfasst ein Konzept ohne dabei die technische Implementierung vorzuschreiben. So werden zum Beispiel folgende Anforderungen darin beschrieben:

- Fehlererkennungsmechanismen mit Fehlerentschärfung (z. B. durch Übergang in einen sicheren Zustand)
- Fehlertoleranzmechanismen (z. B. durch Redundanz)
- Fehlererkennungsmechanismen mit Warnung (z. B. durch akustische, haptische oder visuelle Warnungen)

Für jede ASIL-Stufe sind Methoden spezifiziert und deren Eignung für die jeweilige Stufe bewertet. Zu den Methoden zählen u. a. Plausibilitätsprüfungen, Redundanz von Daten, Degradationsmechanismen, etc. Weiterhin werden die zulässigen Programmiersprachen sowie deren Eignung für die einzelnen ASIL-Stufen spezifiziert.

Für die Überprüfung eines Systems werden weiterhin Review-Aktivitäten beschrieben. Diese sind je nach Einstufung eines Systems 1.) von einer anderen Person (nicht der Entwickler), 2.) von einem anderen Team, 3.) von einer anderen Abteilung oder 4.) von einer anderen Firma durchzuführen. Dadurch soll eine Unabhängigkeit zwischen den Entwicklern und Überprüfern gewährleistet sein.

Im Folgenden werden einige Einflüsse der Sicherheitsanforderungen auf eine E/E-Architektur anhand eines Beispiels erläutert. Als Beispiel dient eine Fahrerassistenzfunktion (siehe Abb. 2.16), die auf einer ECU1 läuft und von dort über das Bremsensteuergerät ECU2 einen Bremseneingriff auslösen kann.

Eine Gefahrenanalyse des Systems hat ergeben, dass eine Vollbremsung bis zum Stillstand als ASIL C eingestuft werden muss. In dem betrachteten System kann sowohl von ECU1 als auch von ECU2 die Bremse ausgelöst werden. Aus diesem Grund sind beide Steuergeräte mit ASIL C einzustufen. Da die Entwicklung einer Komponente mit hohem ASIL einen höheren Aufwand im Entwicklungsprozess und höhere Materialkosten verursachen kann, ist es wünschenswert den *Safety-Level* gering zu halten. Um für dieses Beispiel die ASIL-Einstufung der ECU1 zu reduzieren, sind folgende Schritte möglich:

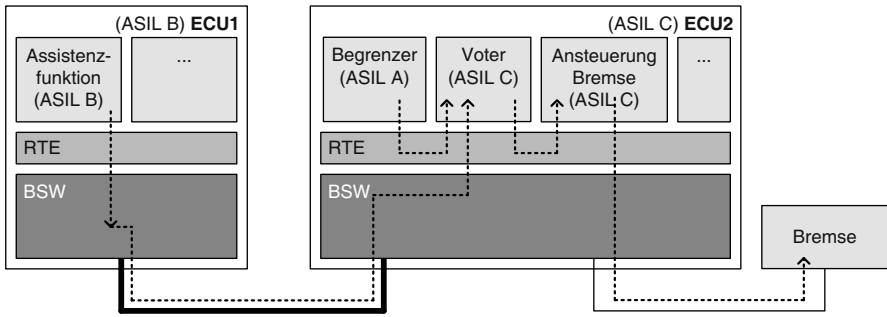


Abb. 2.17 Dargestellt ist das um einen *Begrenzer* und einen *Voter* erweiterte Teilsystem aus Abb. 2.16

- Die Eingriffsdauer der Assistenzfunktion kann zeitlich begrenzt werden (z. B. auf eine Sekunde).
- Es muss dann ein Nachweis erbracht werden, dass Fehleingriffe mit der maximalen Eingriffsdauer vom Fahrer (besser) beherrschbar sind.
- Als weitere technische Maßnahme muss ein *Zeitbegrenzer* auf der ECU2 integriert werden.

Über diese Maßnahmen ist eine Einstufung der ECU1 mit ASIL-B möglich. Die erneute Gefahrenanalyse ergibt nun, dass eine fehlerhafte Vollbremsung durch ECU1 ausgelöst werden kann und diese durch einen Begrenzer in ECU2 entschärft wird. In Abb. 2.17 ist das erweiterte Teilsystem dargestellt. ECU2 enthält nun zusätzlich den zeitlichen Begrenzer und einen Entscheider (Voter). Für die einzelnen Funktionen sind noch jeweils deren ASIL-Einstufung angetragen.

Als Fazit für das Beispiel sind folgende Punkte für den Einfluss auf eine E/E-Architektur von Bedeutung. Eine sinnvolle Funktionseinschränkung hilft in einigen Fällen die ASIL-Einstufung von einzelnen Komponenten zu reduzieren. Weiterhin sollte eine Verteilung von Sicherheitsanforderungen auf die einzelnen Komponenten so stattfinden, dass Funktionen mit hohen ASIL-Einstufungen möglichst auf einem Steuergerät partitioniert werden, welches bereits eine hohe ASIL-Einstufung hat.

2.3 E/E-Architekturkonzepte

Ein wesentlicher Bestandteil bei der Entwicklung von E/E-Architekturen besteht aus dem Aufzeigen und Bewerten von Alternativkonzepten. Wie diese Konzepte im Einzelnen aussehen, ist natürlich abhängig von der Anwendung, den technischen Möglichkeiten und von den existierenden Konzepten. Nichts desto trotz sollen an dieser Stelle grundlegende Architekturkonzepte [EB07] erörtert werden, die verdeutlichen welche Denk- und Argumentationsrichtungen bei der Architekturentwicklung eine Rolle spielen.

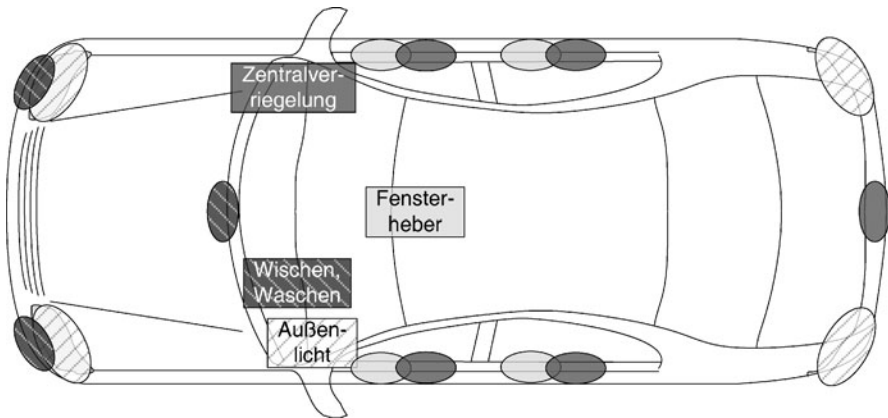


Abb. 2.18 Funktionsorientiertes Konzept: Beim funktionsorientierten Konzept werden für jede Funktion separate Komponenten und Verbindungen vorgesehen

2.3.1 Funktionsorientiertes Konzept

Das funktionsorientierte Konzept basiert auf der Idee, dass für jede Funktion eine separate Komponente mit ihren Sensoren und Aktoren integriert werden muss. In Abb. 2.18 sind vier Funktionen gezeigt, die jeweils getrennte Steuergeräte, Sensorik und Aktorik haben. Die Fensterheber haben in dem Beispiel ein zentrales Steuergerät und in den Türen jeweils Bedienfelder und Motoren. Die Zentralverriegelung hat ebenfalls ein zentrales Steuergerät und in den Türen wiederum die elektrischen Türschlösser als Aktoren. Bei den weiteren Funktionen für Scheibenwischer und Außenlicht verhält es sich analog. Auch hier gibt es jeweils ein zentrales Steuergerät und die zugehörige Sensorik/Aktorik. Die Vorteile, die sich hieraus ergeben sind folgende:

- Geringe Komplexität der einzelnen Komponenten, da ein kleinerer Funktionsumfang mit weniger Schnittstellen unterstützt wird als bei einem Ansatz mit verschiedenen Funktionen auf der gleichen Hardware.
- Geringe Packungsgröße für jede einzelne Komponente, da weniger Schnittstellen nach außen existieren und weniger Bauteile im Steuergerät benötigt werden.
- Vorteilhafte Wärmeentwicklung und angepasste Wärmeableitung, wegen der reduzierten Anzahl an Bauteilen.
- Skalierbarkeit der Fahrzeugarchitektur mit dem Funktionsumfang, da Funktionen und Komponenten äquivalent sind.
- Plattformübergreifende Nutzung der Komponenten möglich

Neben diesen Vorteilen lassen sich folgende Argumente nennen, die gegen einen solchen Ansatz sprechen:

- Eine große Anzahl an Komponenten, da keine Mehrfachnutzung einer Komponente für verschiedene Funktionen in dem Ansatz vorgesehen ist.

- Hoher Verdrahtungsaufwand, da mehr Komponenten miteinander Daten austauschen.
- Keine Mehrfachnutzung von Sensorik und Aktorik, sodass evtl. ein Aktor mehrfach verbaut werden muss. Beispielsweise wird ein Blinker typischerweise für die Diebstahlwarnanlage, den Fahrtrichtungswechsel und die Schließanlage verwendet, was bei einer strengen Auslegung des funktionsorientierten Ansatzes nicht möglich ist.
- Höhere Kosten der Elektrik/Elektronik, da mit steigender Anzahl an Komponenten, Sensoren/Aktoren und Leitungen auch die Kosten zunehmen.

2.3.2 Zentralisiertes Konzept

Das zentralisierte Konzept sieht vor, dass die Funktionalität auf einem Zentralsteuergerät gebündelt wird. Dieser Ansatz ist typisch für kleinere Fahrzeuge oder für standardmäßige Funktionsumfänge, die in den meisten Fahrzeugen vorkommen. In Abb. 2.19 ist ein solcher Ansatz verdeutlicht. Der Funktionsumfang, der gerade noch auf vier Steuergeräte verteilt war, ist ein typischer Funktionsumfang, der in den meisten Fahrzeugen vorkommt. Beim zentralisierten Ansatz übernimmt ein sogenannter *Body Controller* diese Funktionen, wodurch sich die Anzahl an Steuergeräten reduziert. Die Vorteile, die sich hieraus ergeben, sind folgende:

- Alle Funktionen können mit einer Komponente von einem Zulieferer getestet werden.
- Der Aufwand für die Komponentenentwicklung ist reduziert, da keine nebenläufigen Prozesse auf mehreren ECUs berücksichtigt werden müssen.

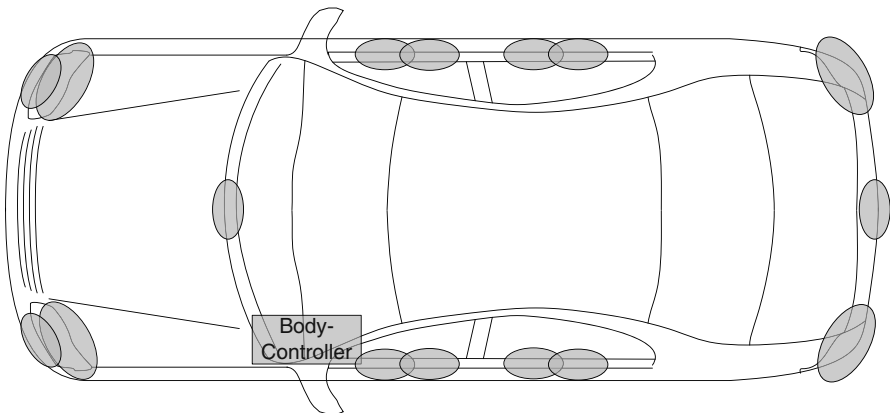


Abb. 2.19 Zentralisiertes Konzept: Beim zentralisierten Konzept wird die Fahrzeugfunktionalität auf einem Zentralrechner zusammengefasst

- Günstigere Kostenstruktur, da u. a. Gehäusekosten nur einmal anfallen und Bauteile wie Mikrocontroller, Speicher und Bus-Interfaces für verschiedene Funktionen verwendet werden.

Umgekehrt ergeben sich folgende Nachteile aus einem zentralisierten Konzept:

- Hoher Verkabelungsaufwand ist möglich, da das zentrale Steuergerät nicht in der Nähe aller Sensoren und Aktoren platziert werden kann, sondern Leitungen immer quer durch das Fahrzeug gelegt werden müssen.
- Ein größerer Bauraum ist für eine solche zentrale Komponente vorzusehen, da mehr Bauteile für die Schnittstellen, größere Stecker und somit mehr Platinenfläche notwendig sind.
- Thermische Probleme können auftreten, da die Wärme von mehr Bauteilen in einem Gehäuse abgeführt werden muss.
- Erschwerter Umgang mit verschiedenen Fahrzeugvarianten, da der Funktionsumfang evtl. nicht zu jedem Fahrzeugtyp passt.
- Eingeschränkte Skalier- und Erweiterbarkeit, da Schnittstellen, Speichergrößen, Rechenleistung, etc. für den Funktionsumfang angepasst sind.

2.3.3 Räumlichorientiertes Master/Slave-Konzept

Beim räumlichorientierten Konzept wird davon ausgegangen, dass der Funktionsumfang aus einem Fahrzeugbereich zusammengefasst wird. Zum Teil werden solche Ansätze auch als Master/Slave-Konzept gesehen, da in jedem Bauraum eine Master-ECU deren Slaves ansteuert und nur die Master untereinander kommunizieren. In Abb. 2.20 ist dieser Ansatz mit vier Bereichen verdeutlicht, in denen jeweils eine ECU vorkommt, die vor Ort die Ansteuerung der Slaves vornimmt. Als Vorteile für diesen Ansatz lassen sich folgende Punkte nennen:

- Geringer Verdrahtungsaufwand, da die Logik zur Ansteuerung in der Nähe der Sensorik und Aktorik sitzt und die Kommunikation zwischen den Master-Steuergeräten über ein Kommunikationssystem erfolgen kann.
- Wenig Bauraum für jede einzelne Komponente, da die benötigte Rechenleistung und Anzahl an Interfaces sich auf die verschiedenen Steuergeräte aufteilt.
- Komponenten sind eventuell plattformübergreifend nutzbar, sofern die Sensorik und Aktorik sich in dem Bauraum ähnelt.
- Geringe Komplexität der Hard- und Software-Slave-Module, da die Funktionen auf den Master-Modulen zusammengefasst sind.

Folgende Nachteile ergeben sich allerdings bei einem solchen Ansatz:

- Netzwerkmanagement notwendig, da Master-Knoten voneinander abhängen und sich gegenseitig wecken müssen.
- Erhöhte Software-Komplexität, da Funktionen aus unterschiedlichen Funktionsgruppen auf der gleichen Komponente laufen und die Kommunikation zwischen den Master-Komponenten geregelt werden muss.

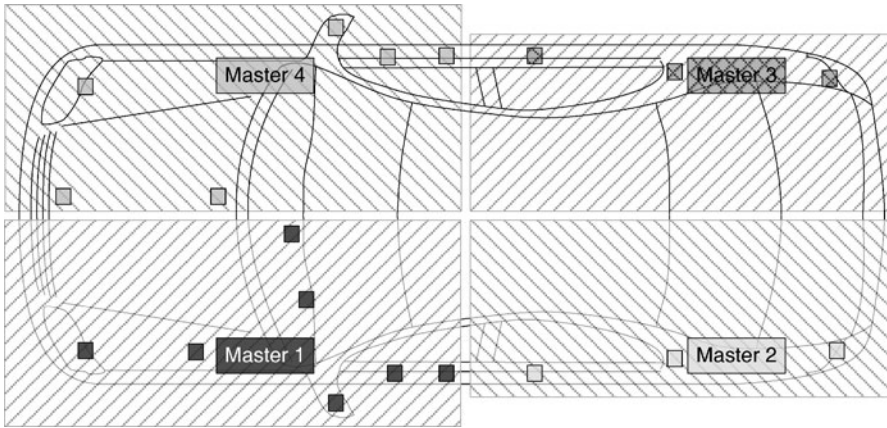


Abb. 2.20 Räumlichorientiertes Master/Slave-Konzept: Dieses Konzept sieht für Bauräume einen Master vor, der die lokale Elektronik steuert. Die Master sind miteinander vernetzt

- Erhöhter Kommunikationsbedarf, da zusammenhängende Funktionen auf mehreren Komponenten verteilt laufen und somit Daten über ein Netzwerk austauschen müssen.
- Erhöhte Testkomplexität, da verteilte Funktionen aus verschiedenen Funktionsgruppen (Safety, Chassis, Comfort, Powertrain) auf den gleichen Ressourcen laufen und um diese konkurrieren.

Baugruppenorientiertes Konzept

Beim baugruppenorientierten Ansatz ist die Fahrzeugfunktionalität mit der zugehörigen Elektronik einer bestimmten Baugruppe zugeteilt. Eine Tür, so wie sie in Abb. 2.21 gezeigt ist, stellt somit eine abgeschlossene Komponente mit den folgenden Vorteilen dar:

- Baugruppen sind getrennt produzier- und testbar, da Mechanik und Elektronik aus einer Baugruppe zusammen verarbeitet werden.
- Geringer Verkabelungsaufwand zwischen den Baugruppen, da Elektronik zum Steuern der Sensorik und Aktorik in der Baugruppe integriert ist und über Bussysteme von extern Daten empfängt. Die Leistungsversorgung der Sensoren und Aktoren geschieht ebenfalls aus einer zentralen Komponente der Baugruppe.

Die Nachteile sind allerdings vergleichbar zum räumlichorientierten Ansatz:

- Abhängig von der Baugruppe steht für die Elektronik ein geringer Bauraum zur Verfügung, dieser ist nicht optimal in Bezug auf Umweltbedingungen wie Temperatur, Feuchtigkeit oder Vibrationen. Die Elektronik muss hierbei an die Baugruppe angepasst sein.
- Erhöhter Kommunikationsbedarf zwischen den verteilten Funktionen, da Funktionen baugruppenübergreifend arbeiten (z. B. Fensterheber, Zentralverriegelung).

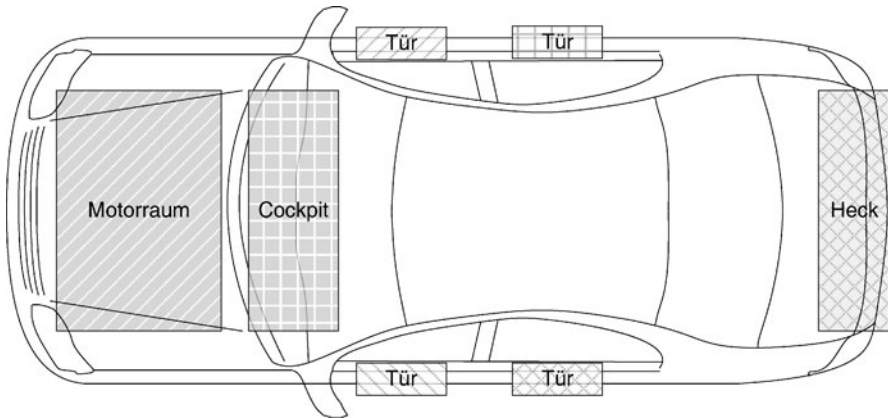


Abb. 2.21 Baugruppenorientiertes Konzept: Hierbei wird die Elektronik möglichst weitgehend in eine Baugruppe integriert

- Netzwerkmanagement notwendig, da die Elektronik aus den einzelnen Baugruppen sich gegenseitig wecken und den Zustand des Fahrzeugs erkennen muss.
- Erhöhte Softwarekomplexität, da verschiedene Funktionen auf der gleichen CPU laufen und ggf. gekapselt werden müssen oder Funktionen auf mehreren CPUs verteilt im Netzwerk laufen.

Eine strenge Auslegung eines Netzwerks entsprechend der vorgestellten Konzepte liegt in der E/E-Architektur heutzutage nicht vor. Stattdessen werden solche Konzepte in einzelnen Bereichen der E/E-Architektur aufgegriffen. In Abb. 2.22 ist

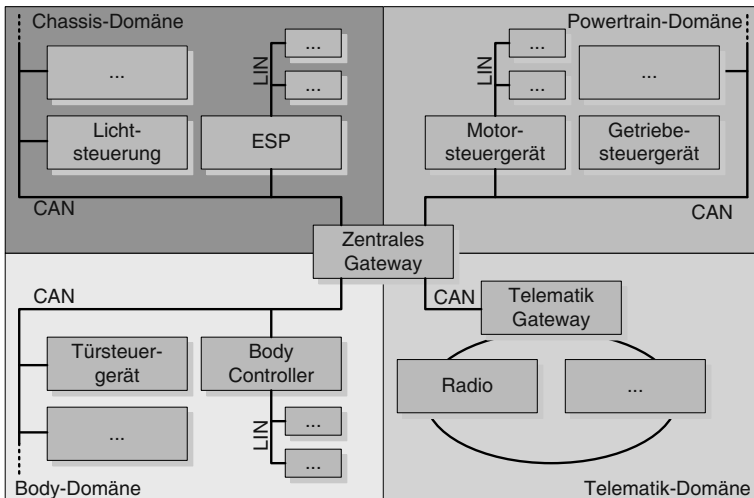


Abb. 2.22 Heutige E/E-Architekturen sind häufig in funktionale Domänen unterteilt und über ein zentrales Gateway miteinander gekoppelt. Innerhalb der Domänen lassen sich wiederum obige Konzepte erkennen

ein typischer Aufbau einer Kommunikationsstruktur dargestellt wie sie in aktuellen Premiumfahrzeugen zu finden ist. Charakteristisch für eine solche Kommunikationsstruktur ist die Gruppierung der Funktionen in die Domänen 1. Antriebsstrang, 2. Fahrerassistenz und Fahrwerk, 3. Innenraum sowie 4. Telematik und Infotainment. Diese Domänen sind durch ein zentrales Gateway miteinander verbunden und können jeweils noch sogenannte Domänen-Gateways beinhalten. Die beschriebenen Ansätze sind teilweise in den einzelnen Domänen wieder zu finden. Beispielsweise ist der räumlichorientierte Ansatz in der Innenraumdomäne zu finden. Hier ist ein Body Controller für vorne und einer für hinten vorgesehen, die jeweils über einen LIN-Bus lokale Slaves ansteuern. Der baugruppenorientierte Ansatz findet sich bei den Türsteuergeräten wieder, bei denen für jede Tür ein separates Steuergerät vorgesehen ist.

2.4 Ebenen der Timing-Bewertung

Bei der Absicherung von Elektrik und Elektronik steht häufig die funktionale Absicherung im Vordergrund. Das System wird hierbei mit verschiedensten Eingabemustern ausgeführt und die Reaktionen des Systems werden mit den erwarteten Reaktionen verglichen. Bei vielen Systemen sind solche Absicherungen völlig ausreichend. Es gibt allerdings auch Systeme, bei denen der Zeitpunkt der Reaktion ausschlaggebend ist. In solchen Echtzeitsystemen hängt die Verwertbarkeit einer Reaktion von dem Zeitpunkt ab, zu dem sie vom System generiert wird. In Abb. 2.23 ist die Verwertbarkeit einer Reaktion über der Zeit dargestellt. Bei Systemen ohne Echtzeitanforderung (oben links) ist die Reaktion immer gleich verwertbar. Unter weicher Echtzeit (oben rechts) versteht man Systeme, bei denen die Verwertbarkeit der Reaktion über der Zeit abnimmt. Sinkt die Verwertbarkeit sofort auf Null, so spricht man von Echtzeit. Bestehen harte Echtzeitanforderungen (unten rechts), so kann die Reaktion eines Systems nach einem bestimmten Zeitpunkt zu verheerenden Folgen führen. Dies ist in der Abbildung mit einer negativen Verwertbarkeit ausgedrückt.

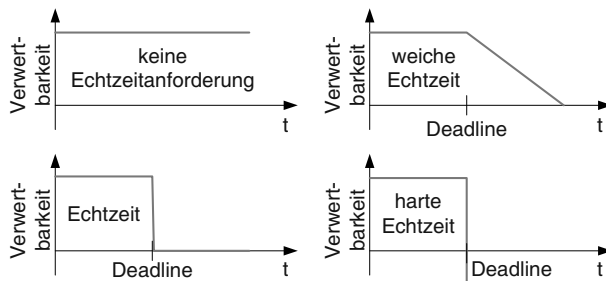
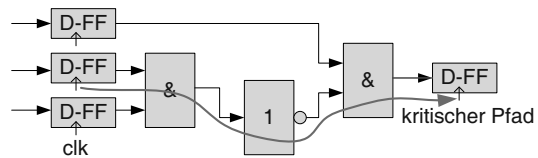


Abb. 2.23 Aufgezeigt ist die Verwertbarkeit einer Reaktion eines Systems bezüglich der Echtzeitanforderungen

Abb. 2.24 Dargestellt ist ein kritischer Pfad am Beispiel der Gatterlaufzeit durch kombinatorische Logik



Diese zeitlichen Eigenschaften beziehen sich auf Systeme und deren Reaktionen. Die Absicherung des zeitlichen Verhaltens einer E/E-Architektur muss allerdings auf verschiedensten Systemebenen erfolgen. Bei Rechnerarchitekturen, Halbleiterbausteinen und der zugehörigen Software unterscheidet man zwischen folgenden Ebenen des zeitlichen Verhaltens:

- **Gatterlaufzeit:** Dieses zeitliche Verhalten bezieht sich auf die spezifische Latenz, die ein Signal vom Eingang durch das Gatter bis zum Ausgang benötigt. Diese Zeit wird auch mit *Propagation-Delay* bezeichnet und kann für logische Pegelwechsel von 1 auf 0 sowie auch umgekehrt variieren. Auf dieser Ebene spielen physikalische Zeiten von Transistoren bzw. der verwendeten Halbleitertechnologie eine Rolle. Somit sind solche Zeitangaben spezifisch für bestimmte Bauteile.
- **Taktfrequenz von integrierten Schaltungen:** Die Länge von kombinatorischen Pfaden bzw. der kritische Pfad in einer integrierten Schaltung bestimmt die Taktfrequenz, mit der eine Schaltung läuft. In Abb. 2.24 ist eine kombinatorische Schaltung zwischen zwei Flip-Flops dargestellt. Der längste Pfad zwischen den Flip-Flops läuft durch ein AND-Gatter, einen Inverter und noch ein AND-Gatter. Die Zeit von den unteren beiden linken Flip-Flops bis zum rechten Flip-Flop wird durch diesen Pfad bestimmt und ist maßgeblich für die Taktfrequenz der Schaltung.
- **Ausführungszeit für einzelne Anwendungen (Task auf Prozessor):** Die Ausführungszeit einer einzelnen Anwendung hängt von der Taktfrequenz des Prozessors, der Prozessorarchitektur sowie der Software-Anwendung ab. Das Zusammenspiel von Prozessorarchitektur und Software muss im Rahmen einer sogenannten *Worst-Case-Execution-Time-Analyse* bestimmt werden. Wie diese Art der Analyse funktioniert ist in Kap. 7 erläutert.
- **Antwortzeit von mehreren Anwendungen auf dem gleichen Prozessor mit Betriebssystem und Scheduling:** Auf dieser Ebene muss neben der Ausführungszeit eines einzigen Tasks auch das Zusammenspiel von mehreren Tasks betrachtet werden (Abb. 2.25). Tasks können sich hierbei gegenseitig unterbrechen oder verzögern, da sie um die gleiche Ressource konkurrieren. Der Einfluss von mehreren Tasks auf die Antwortzeit eines bestimmten Tasks kann analysiert werden, was in Kap. 8 beschrieben ist.

Bei der Absicherung von Kommunikationstechnologien gibt es von der physikalischen bis zur Systemebene ebenfalls verschiedene Ebenen des zeitlichen Verhaltens:

- **Signallaufzeiten auf Leitungen, Ausbreitungsgeschwindigkeit von Wellen:** Die maximale Ausbreitungsgeschwindigkeit im Medium ist kleiner als die Licht-

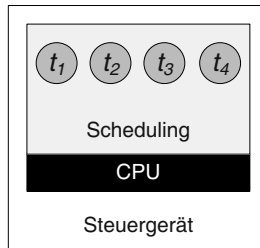


Abb. 2.25 Laufen mehrere Tasks auf einem Prozessor muss das Scheduling bei der Bewertung des zeitlichen Verhaltens berücksichtigt werden

geschwindigkeit mit ca. 3×10^8 m/s. In elektrischen Leitern geht man von einer Ausbreitungsgeschwindigkeit von ca. $2/3$ der Lichtgeschwindigkeit aus. Dieser Wert ist allerdings nicht konstant sondern abhängig von der Frequenz, die übertragen wird. Diese Eigenschaft wird Dispersion genannt. Weiterhin sorgt das Übertragungsmedium für eine Dämpfung des Signals. Die Dämpfung beschreibt hierbei das Verhältnis von Sende- zu Empfangsleistung. Als dritte Einflussgröße muss die Reflexion bei der Übertragung berücksichtigt werden. Hierbei findet eine Überlagerung der ausgehenden Welle mit einer reflektierten Welle statt.

- **Übertragungszeit einer Nachricht über einen Bus (Dauer für N Bits):** Auf dieser Ebene sind das Rahmenformat einer Nachricht und Protokollmechanismen entscheidend. Werden für die Übertragung von N Nutzdatenbits im Rahmenformat noch M weitere Bits für Kopfdaten und Prüfsummen verwendet, so verlängert sich die Übertragungszeit einer Nachricht. Weitere Mechanismen wie *Bitstuffing* oder Datenkodierung können die Nachrichtenübertragung verlängern. Die Analyse solcher Übertragungszeiten ist allerdings sehr stark abhängig von einem Protokoll bzw. von einer Technologie. Deshalb geht Kap. 8 auf die Technologien CAN, LIN, FlexRay und Ethernet separat ein.
- **Antwortzeit von mehreren Nachrichten:** Sofern mehrere Nachrichten über das gleiche Medium übertragen werden sollen, müssen Arbitrierungsmechanismen den Datenverkehr regeln. Diese Arbitrierungsmechanismen haben die gleiche Aufgabe wie Scheduling-Verfahren, auch wenn sie aus algorithmischer Sicht anders sein können (siehe Abb. 2.26). Den Einfluss von Arbitrierungsverfahren

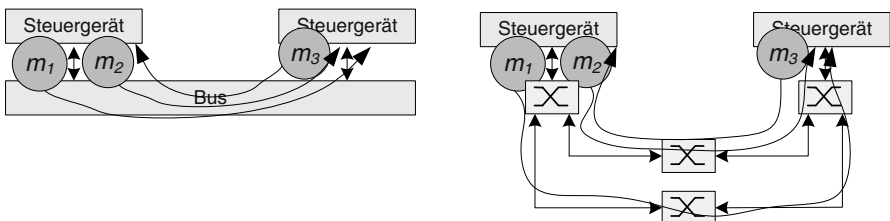


Abb. 2.26 Werden mehrere Nachrichten über einen Bus oder in einem Netzwerk übertragen, so müssen Arbitrierungsmechanismen bei der Bewertung des zeitlichen Verhaltens berücksichtigt werden

und die Auswirkung mehrerer Nachrichten auf die Antwortzeit einer bestimmten Nachricht wird ebenfalls in Kap. 8 erläutert.

- **Scheduling von Tasks und Arbitrierung von Nachrichten:** Auf Systemebene können auf zwei Steuergeräten mehrere Tasks laufen, die miteinander kommunizieren. Auf dieser Ebene wirken sich also sowohl Scheduling-Verfahren, Task-Ausführungszeiten, Arbitrierungsverfahren und Nachrichtenübertragungszeiten auf das Systemverhalten aus.

2.5 Verfahren zu Timing-Bewertung

Der folgende Abschnitt stellt die verschiedenen Verfahren vor, welche eine Bewertung des Timing-Verhaltens ermöglichen. Diese lassen sich wie in Abb. 2.27 dargestellt in zwei Kategorien einteilen:

1. **Experimentelle Verfahren:** Bei diesen Verfahren erfolgt die Timing-Bewertung auf der Basis von Simulationsmodellen oder durch die Verwendung von realer Hardware. Ferner ist eine Kombination der beiden Verfahren möglich.
2. **Analytische Verfahren:** Diese Verfahren bestimmen das Timing-Verhalten auf analytischem Wege anhand von mathematischen Modellen. Die formalen Verfahren lassen sich in zwei Gruppen einteilen: 1.) Die sogenannten holistischen Verfahren erweitern die klassischen Analysemethoden der Schedulingtheorie für verteilte eingebettete Systeme [PWT⁺08]. Das resultierende heterogene Modell, welches die verschiedensten Analysetechniken kombiniert, wird jedoch bei großen Systemen schnell unübersichtlich. 2.) Der modulare Analyseansatz wird oft auch als *Compositional Analysis* referenziert. Bei diesem Ansatz werden die Komponenten eines verteilten Systems parallel und lokal analysiert. Das resultierende Ausgangsereignismodell wird als Eingangsereignismodell für den nächsten Analyseschritt verwendet [RJE03].

Die experimentellen Verfahren befinden sich schon seit vielen Jahren im breiten Serieneinsatz. Sowohl bei der Auslegung von Vernetzungsarchitekturen im Kraftfahrzeug und deren einzelnen Komponenten als auch bei der Absicherung in der Integrationsphase werden Simulations- sowie Testtechniken eingesetzt. Mit diesen Verfahren lassen sich anhand von Testfällen verschiedenste Untersuchungen durch-

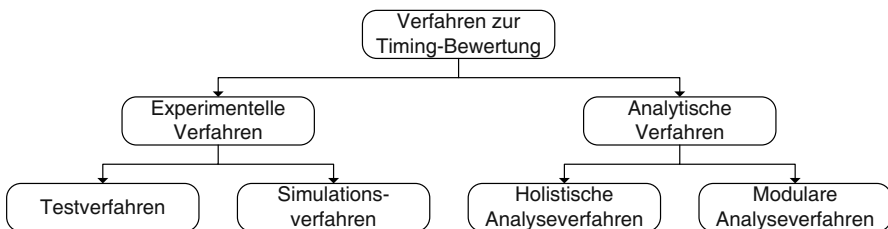


Abb. 2.27 Übersicht möglicher Verfahren zur Timing-Bewertung