26

Karlsruher Schriftenreihe Fahrzeugsystemtechnik

David Schmitz

Entwurf eines fehlertoleranten Lenkventils für Steer-by-Wire Anwendungen bei Traktoren

KIT Scientific Publishing

David Schmitz

Entwurf eines fehlertoleranten Lenkventils für Steer-by-Wire Anwendungen bei Traktoren

Karlsruher Schriftenreihe Fahrzeugsystemtechnik
Band 26

Herausgeber
FAST Institut für Fahrzeugsystemtechnik
Prof. Dr. rer. nat. Frank Gauterin
Prof. Dr.-Ing. Marcus Geimer
Prof. Dr.-Ing. Peter Gratzfeld
Prof. Dr.-Ing. Frank Henning

Das Institut für Fahrzeugsystemtechnik besteht aus den eigenständigen Lehrstühlen für Bahnsystemtechnik, Fahrzeugtechnik, Leichtbautechnologie und Mobile Arbeitsmaschinen

Eine Übersicht aller bisher in dieser Schriftenreihe erschienenen Bände finden Sie am Ende des Buchs.

Entwurf eines fehlertoleranten Lenkventils für Steer-by-Wire Anwendungen bei Traktoren

von
David Schmitz

KIT Scientific Publishing

Dissertation, Karlsruher Institut für Technologie (KIT)
Fakultät für Maschinenbau, 2014

Impressum

Karlsruher Institut für Technologie (KIT)
KIT Scientific Publishing
Straße am Forum 2
D-76131 Karlsruhe

www.ksp.kit.edu

Print on Demand 2014

ISSN 1869-6058
ISBN 978-3-7315-0264-7
DOI: 10.5445/KSP/1000043068

Vorwort des Herausgebers

Steer-by-Wire Systeme bieten sowohl ein hohes Maß an konstruktiver Freiheit für die Fahrzeugintegration als auch die Chance zum autonomen Lenken. In Traktoren lassen sich beispielsweise durch solche Systeme sehr einfach Rückfahreinrichtungen umsetzen, bei denen der Fahrersitz um 180° gedreht werden kann. Zudem kann auf ein zusätzliches Lenkventil zur automatischen Spurführung verzichtet werden. Da Steer-by-Wire Systeme keine mechanische oder hydrostatische Rückfallebene zwischen Lenkrad und Lenkzylinder besitzen, muss ein besonderes Augenmerk auf deren Sicherheit gelegt werden. Derartige Systeme müssen ein sicheres Lenken auch bei jedem beliebigen Fehler ermöglichen und Fehler selbstständig erkennen.

Die Karlsruher Schriftenreihe Fahrzeugsystemtechnik will einen Beitrag leisten, durch neue Technologien Fahrzeuge sicherer und einfach beherrschbar zu machen. Für die Fahrzeuggattungen Pkw, Nfz, mobile Arbeitsmaschinen und Bahnfahrzeuge werden Forschungsarbeiten vorgestellt, die Fahrzeugtechnik auf vier Ebenen beleuchten: das Fahrzeug als komplexes mechatronisches System, die Fahrer-Fahrzeug-Interaktion, das Fahrzeug in Verkehr und Infrastruktur sowie das Fahrzeug in Gesellschaft und Umwelt.

In **Band 26** wird ein Steer-by-Wire System für Traktoren vorgestellt. Der Fokus der Arbeit liegt auf dem sicheren Lenkventil, das aufgelöste Steuerkanten besitzt und durch den Einsatz von acht 2/2-Wegeventilen redundant aufgebaut ist. Für andere Teilsysteme, wie z.B. die Druckversorgung oder die elektronische Steuerung, werden heute bekannte, redundante Systeme vorgeschlagen. Für die Lenkventilarchitektur mit aufgelösten Steuerkanten konnte nachgewiesen werden, dass bei Vorliegen eines beliebigen Fehlers ein sicheres Lenken möglich ist. Zudem können durch den Einsatz einer modellbasierten Fehlererkennung Fehlfunktionen erkannt und der Fahrer gewarnt

sowie das Fahrzeug in einen sicheren Zustand gebracht werden. Die sichere Funktion des Lenksystems wurde an einem Prüfstand nachgewiesen und das sicherheitsunkritische Fahrverhalten mit einem validierten Simulationsmodell bestätigt.

Karlsruhe, im August 2014 *Prof. Dr.-Ing. Marcus Geimer*

Entwurf eines fehlertoleranten Lenkventils
für Steer-by-Wire Anwendungen bei Traktoren

Zur Erlangung des akademischen Grades
Doktor der Ingenieurwissenschaften
der Fakultät für Maschinenbau
Karlsruher Institut für Technologie (KIT)

genehmigte
Dissertation
von

Dipl.-Ing. David Schmitz

Tag der mündlichen Prüfung: 06. August 2014

Hauptreferent: Prof. Dr.-Ing. Marcus Geimer
Korreferent: Prof. Dr.-Ing. Hubertus Murrenhoff

Kurzfassung

An das Lenksystem eines Traktors werden immer höhere Anforderungen gestellt, um produktivitätssteigernde Funktionen, wie beispielsweise eine automatische Spurführung, realisieren zu können. Darüber hinaus gewinnen Aspekte wie die Ergonomie der Fahrerkabine oder die Fahrsicherheit eines schweren Gespanns auf öffentlichen Straßen an Bedeutung. Steer-by-Wire Systeme ohne mechanischen oder hydraulischen Durchgriff zwischen Lenkrad und gelenkten Rädern bieten sehr große Freiheiten und Möglichkeiten für die Umsetzung dieser Anforderungen. Durch die hohe Sicherheitsrelevanz des Lenksystems in einem Fahrzeug besteht die Herausforderung, ein fehlertolerantes und damit sicheres System mit einer möglichst geringen Komplexität zu realisieren und dadurch wettbewerbsfähig gegenüber konventionellen Lenksystemen zu sein. In der vorliegenden Arbeit wird ein hydrostatisches Steer-by-Wire System mit einem Lenkventil mit unabhängigen Steuerkanten vorgeschlagen und bezüglich der Eignung für die Nutzung in sicherheitskritischen Anwendungen, wie der Fahrt auf öffentlichen Straßen, bewertet. Durch experimentelle Untersuchungen wird nachgewiesen, dass Ventilfehler durch die gewählte Ventilarchitektur inhärent kompensiert werden können und die Anforderung der Lenkbarkeit auch im Fehlerfall erfüllt ist. Die Fehlererkennung erfolgt dabei sowohl durch einen aktiven Selbsttest als auch modellbasiert unter Verwendung von Sensorsignalen, die auch für andere Teilsysteme notwendig sind. Der Verzicht auf eine strikt zweikanalige Struktur des Lenkventils mit unabhängigen Abschaltpfaden und eine sensorische Überwachung aller Ventile sorgt dabei für eine niedrige Systemkomplexität, führt jedoch auch zu einer Beeinträchtigung der Lenkperformance im Fehlerfall. Eine simulative Abschätzung zeigt, dass diese Beeinträchtigung in den relevanten Fahrmanövern durch den Fahrer ausgeglichen werden kann und so die sichere Lenkbarkeit des Fahrzeugs nicht gefährdet.

Abstract

Nowadays the field of agriculture is driven by a rising demand regarding productivity and turnover, but also regarding driver's comfort, driver assistance and driving safety. One component, which contributes to these requirements, is the steering system. Within these, steer-by-wire systems without a direct energy transmission from the steering wheel to the steered wheels offer the most freedom to realize new functionalities and fulfill additional requirements, such as a variable steering ratio for on-road use. Because of the high safety requirements for steering systems during on-road use and the high cost pressure, the main challenge is to design a safe system with a low overall complexity. In this thesis, a hydrostatic steering system with a steering valve architecture using independent metering edges is proposed and analyzed regarding functionality and safety. Experimental results show that, using this valve architecture, hydraulic faults can be compensated inherently by the controller without a time-critical fault detection and reconfiguration. Furthermore, these faults can be detected without measuring the position of each valve spool by means of an active self-test and a model-based fault-detection algorithm. As shut-off valves and spool position sensors are not necessary, the overall complexity is low, but with the drawback that faults influence the closed-loop control performance. Model-based investigations indicate, however, that the reduced control performance can be safely compensated by the driver during the relevant driving maneuvers.

Danksagung

Die vorliegende Arbeit entstand während meiner Tätigkeit als Doktorand der Bosch Rexroth AG in Lohr am Main sowie als wissenschaftlicher Mitarbeiter am Lehrstuhl für Mobile Arbeitsmaschinen (MOBIMA) des Karlsruher Instituts für Technologie (KIT). Dem Leiter des Lehrstuhls und meinem Doktorvater, Herrn Professor Geimer, gilt mein besonderer Dank für die langjährige Betreuung, die stets vorhandene Diskussionsbereitschaft und die guten Anregungen zu dieser Arbeit. Ebenfalls danken möchte ich Professor Murrenhoff (IFAS, RWTH Aachen) für die Übernahme des Korreferats und Professor Koch (IFKM, KIT) für den Vorsitz bei meiner Doktorprüfung. Neben der wissenschaftlichen Betreuung am Institut möchte ich an dieser Stelle auch Bosch Rexroth für die industrielle Betreuung danken, insbesondere Uwe Neumann, Olaf Cochoy und Karin Tischler.

Ein wesentlicher Erfolgsfaktor für das Gelingen einer Dissertation sind aber auch die tiefen technischen Diskussionen mit Arbeitskollegen und Gleichgesinnten sowie deren Aufmunterungen. Mein Dank gilt insbesondere Björn Müller, Christoph Sturm, Ingo Schepers und Daniel Weiler. Ich danke euch herzlich für die angenehme Zeit und euer offenes Ohr. Darüber hinaus danke ich allen Kollegen, Mitarbeitern und Studenten, die mich insbesondere beim experimentellen Nachweis am Prüfstand entlastet haben.

Diese Arbeit wäre ohne die Rückendeckung meiner Eltern und meiner Freunde nicht möglich gewesen. Ich möchte mich bei euch bedanken, dass ihr mich in meiner Entscheidung zur Dissertation stets unterstützt und ermutigt habt. Meiner wunderbaren Frau Anja Schmitz danke ich für die moralische Unterstützung auf den letzten Metern und für das Korrekturlesen.

Mundelsheim, im Oktober 2014 *David Schmitz*

Inhaltsverzeichnis

Symbolverzeichnis

Zeichen	Einheit	Bedeutung
α_D	–	Durchflusszahl
δ	°	Winkel
λ	1/h	Ausfallrate / Übergangsrate
μ	1/h	Reparaturrate
μ	-	Reibungskoeffizient
ρ	kg/m^3	Dichte
$\dot{\varphi}$	rad/s	Gierrate
a	m/s^2	Beschleunigung
A	m^2	Fläche
e	-	Regelabweichung
f	1/s	Frequenz
F	N	Kraft
g	-	Tastgrad
I	A	Strom
l	m	Länge
P	-	Zustandswahrscheinlichkeit
p	bar	Druck
$\dot{p}$	bar/s	Druckgradient
Q	l/min	Volumenstrom
$\mathbf{Q}$	-	Generatormatrix
r	-	Residuum
s	m	Weg
t	s	Zeit
u	-	Stellgröße / Ansteuersignal
V	m^3	Volumen
v	m/s	Geschwindigkeit

Zeichen	Einheit	Bedeutung
x	m	Position
$\dot{x}$	m/s	Geschwindigkeit
y	m	Position

Index	Bedeutung
av	Average
C	Cylinder
d	Dangerous
F	Fehlerhaft
ff	Fehlerfrei
ist	Ist-Wert
L	Links
LS	Load-Sensing
LV	Lenkventil
max	Maximal-Wert
modell	Modell-Wert
nom	Nominal-Wert
P	Pumpe
R	Rechts
ref	Referenz-Wert
soll	Soll-Wert
T	Tank / Test
V	Ventil
y	Y-Richtung

Abkürzungsverzeichnis

Abkürzung	Bedeutung
A	Aktor
ABS	Antiblockiersystem
AgPL	Agricultural Performance Level
ASIL	Automotive Safety-Integrity Level
CCF	Common Cause Failure
DC	Diagnostic Coverage
ECU	Electronic Control Unit
EPS	Electric Power Steering
ESP	Elektronisches Stabilitäts-Programm
EV	Energieversorgung
FMEA	Fehlermöglichkeits- und Einflussanalyse
FO	Fail-Operational
FS	Fail-Safe
FSIL	Fail-Silent
FSU	Fail-Silent Unit
FTU	Fault-Tolerant Unit
G	Generator
GPS	Global Positioning System
HIL	Hardware in the Loop
KFZ	Kraftfahrzeug
LE	Leistungselektronik
MTTF	Mean time to failure
MTTR	Mean time to repair
MTTT	Mean time to test
NFZ	Nutzfahrzeug

Abkürzung	Bedeutung
PKW	Personenkraftwagen
PL	Performance Level
PWM	Pulsweitenmodulation
QM	Qualitätssichernde Maßnahmen
S	Sensor
SbW	Steer-by-Wire
SIL	Safety-Integrity Level
StVZO	Straßenverkehrszulassungsordnung
V	Verbraucher

1 Einleitung

Durch die Abschaltung der künstlichen Verschlechterung der Signalqualität der GPS-Ortung für zivile Zwecke im Jahre 2000 hat nach der *3-Felder-Wirtschaft* und der *Mechanisierung* eine weitere Revolution im Ackerbau begonnen: *Precision Farming*. Unter diesem Oberbegriff werden alle Maßnahmen und Innovationen im Bereich der Landwirtschaft zusammengefasst, die durch den Einsatz von modernster Computertechnologie zu einer effizienteren, schnelleren und besseren Bewirtschaftung von Ackerland führen. Technologien, wie beispielsweise automatische Spurführungssysteme, ermöglichen die autonome Feldbearbeitung unter gleichbleibender Prozessqualität bei unterschiedlichen Umgebungsbedingungen am Tag und bei Nacht. Sie führen damit zu einer enormen Steigerung der Produktivität durch Einsparung von Betriebsmitteln und Zeit, aber auch zu einer Entlastung des Fahrers von anstrengenden Routinetätigkeiten. Darüber hinaus werden landwirtschaftliche Traktoren neben der Feldbearbeitung zunehmend für Transportfahrten auf öffentlichen Straßen bei einer kontinuierlich steigenden Masse des Gesamtgespanns und zunehmend höheren Transportgeschwindigkeiten eingesetzt. Daraus ergeben sich höhere Anforderungen im Hinblick auf den Fahrkomfort, vor allem jedoch an die Fahrsicherheit des gesamten Gespanns. Ein weiterer Trend, der im Bereich der mobilen Arbeitsmaschinen erkennbar ist, ist die immer stärkere Berücksichtigung von ergonomischen Aspekten während der Entwicklung. Dies zeigt sich vor allem bei der Entwicklung von modularen und flexiblen Fahrerkabinen, die optimal auf die Bedienung durch den Fahrer abgestimmt sind [53].

Neben anderen wichtigen Komponenten eines Traktors leistet das Lenksystem einen entscheidenden Beitrag zur Erreichung der zuvor genannten Ziele wie höhere *Produktivität*, *Fahrkomfort*, *Fahrsicherheit* und *Ergonomie* [73]. Im Unterschied zu den Lenksystemen von Kraft- und Nutzfahrzeugen sind

nahezu alle Lenkungen im Bereich der Traktoren rein hydrostatische Lenkungen ohne ein mechanisches Lenkgestänge zwischen dem Lenkrad und den gelenkten Rädern, wie es schematisch in Abbildung 1.1 dargestellt ist[1]. Derartige Systeme zeichnen sich vor allem durch eine hohe Kraftübersetzung und eine flexible Verschlauchung zwischen Lenkventil und Lenkzylinder bei vergleichsweise niedrigen Kosten aus. Bei dieser Mehrzahl der nicht-elektronifizierten Lenksysteme stellt die Komponentenauslegung stets ein Kompromiss zwischen unterschiedlichen Optimierungszielen dar, wie beispielsweise guter Geradeauslauf bei hohen Fahrgeschwindigkeiten und geringe Betätigungskräfte beim Rangieren im Stand.

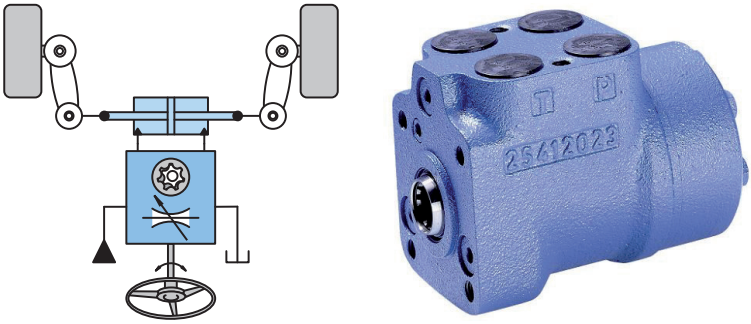


Abb. 1.1: Schematische Darstellung eines hydrostatischen Lenksystems und Foto einer hydrostatischen Lenkeinheit aus [9]

Zur Ermöglichung einer automatischen Spurführung, aber auch zur Erhöhung des Fahrkomforts, werden derartige Systeme heutzutage durch elektrohydraulische Ventile ergänzt, um einen elektronischen Stelleingriff und damit nahezu beliebige Adaptionen am Lenksystem zu ermöglichen. Dabei ist zu beachten, dass das Lenksystem eines der sicherheitskritischsten Teilsysteme eines Traktors ist, für das sehr hohe Sicherheitsanforderungen gelten. Bisher am Markt befindliche Systeme wurden für die Verwendung während der Feld-

[1] Statt der Hydraulikpumpe ist das allgemeine Symbol für eine hydraulische Energiequelle dargestellt [17].

arbeit konzipiert und müssen durch den Fahrer abgeschaltet werden, bevor eine öffentliche Straße befahren wird. Eine Verbesserung des Fahrkomforts und der Fahrsicherheit während Transportfahrten kann durch diese Systeme daher nicht erreicht werden.

Erste Entwicklungen elektrohydraulischer *Steer-by-Wire (SbW)*[2] Systeme für Traktoren mit Straßenzulassung [83, 81] zeigen jedoch, dass es sinnvoll ist, das elektrohydraulische Lenksystem als sicherheitsrelevantes Gesamtsystem zu betrachten, welches einen entscheidenden Mehrwert bietet. Die elektrischen Zusatzfunktionalitäten sind in einem derartigen Lenksystem nicht auf die Feldbearbeitung limitiert und dem Fahrer wird nicht die Verantwortung übertragen, die Komfort-Funktionen während der Straßenfahrt zu deaktivieren. Einhergehend mit der Erfüllung der Sicherheitsanforderungen für eine Straßenzulassung solcher Systeme ist jedoch häufig ein starker Anstieg der Systemkomplexität und damit der Systemkosten, unter anderem durch den zunehmenden Anteil komplexer Elektronikbauteile. Die Entwicklung eines sicheren Steer-by-Wire Systems für Traktoren stellt daher eine komplexe Herausforderung dar, bei der nicht zu selten die Kunden-, die Sicherheits- und die Kostenanforderungen stark divergieren [14], siehe Abbildung 1.2. Eine Lösung dieser Herausforderung ist jedoch erforderlich, um das Verhältnis von Aufwand zu Nutzen von fehlertoleranten Steer-by-Wire Systemen zu verbessern und so zu einer größeren Marktdurchdringung solcher Systeme zu kommen.

Die vorliegende Arbeit beschäftigt sich mit der Fragestellung, wie durch die Wahl einer geeigneten Gesamtsystemstruktur bei Erfüllung der geforderten Sicherheits- und Kundenanforderungen die Systemkomplexität gering gehalten werden kann. Der Fokus der Untersuchung liegt dabei auf dem hydraulischen Teilsystem der Aktuatorik, dem Lenkventil, das den wesentlichsten Unterschied zu Steer-by-Wire Systemen im Kraft- und Nutzfahrzeugbereich

[2] Ein Steer-by-Wire (SbW) System ist ein Lenksystem, bei dem der Fahrerwunsch rein elektrisch erfasst und übertragen wird. Bei derartigen Lenksystemen kann der Fahrer seine Muskelkraft nicht zum Lenken der Räder verwenden.

darstellt. Für das fehlertolerante hydrostatische Lenkventil wird dazu eine Ventilarchitektur vorgeschlagen und analysiert, die eine niedrigere Komponentenkomplexität aufweist und dabei auch geringere Anforderungen an die Überwachung der verwendeten Ventile stellt als bestehende Lösungen des Stands der Technik.

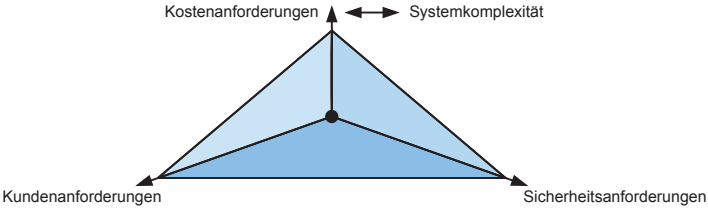


Abb. 1.2: Spannungsdreieck zwischen den Anforderungen *»Kosten«*, *»Kunde«* und *»Sicherheit«*

In Kapitel 2 werden dazu die Grundlagen und der Stand der Technik aus den Bereichen *»Lenkanlage«*, *»funktionale Sicherheit«* und *»Fehlertoleranz«* vermittelt, die für das Verständnis der Arbeit notwendig sind. Dabei wird unter anderem eine Klassierungsweise der Kraftfahrzeug-Lenksysteme auf Traktoren übertragen und beispielhaft einige der am Markt befindlichen Systeme darin eingeordnet und erläutert. Kapitel 3 befasst sich anschließend mit der Synthese und dem Vergleich verschiedener elektrohydraulischer Lenksystem-Architekturen. Dazu wird der wesentliche Zusammenhang zwischen den Anforderungen und der Systemarchitektur abgeleitet, sowie das Gefahrenpotential von elektrohydraulischen Lenksystemen bewertet. Zur Lösung des scheinbaren Widerspruchs von ausreichender Sicherheit und geringer Systemkomplexität wird in Kapitel 4 ein Ventilkonzept mit unabhängigen Steuerkanten vorgeschlagen und sicherheitstechnisch bewertet. Wie aus Abbildung 1.3 erkennbar ist, basiert Kapitel 4 auf den Ergebnissen von Kapitel 3. Die Anforderungen an die Lenkwinkelregelung und die Fehlererkennung werden anschließend in Kapitel 5 analysiert, umgesetzt und in Kapitel 6.1 experimentell an einem Prüfstand nachgewiesen. Um die erzielten Ergebnisse

auf Fahrzeugebene bewerten zu können, wird in Kapitel 6.2 das Fahrverhalten des Traktors modellbasiert bewertet. Kapitel 6.3 endet mit einer Bewertung des untersuchten Lenksystems auf Systemebene und schließt damit den Kreis zu Kapitel 3. Ein Überblick der erzielten Ergebnisse und einen Ausblick auf die nächsten Schritte liefert die Zusammenfassung in Kapitel 7.

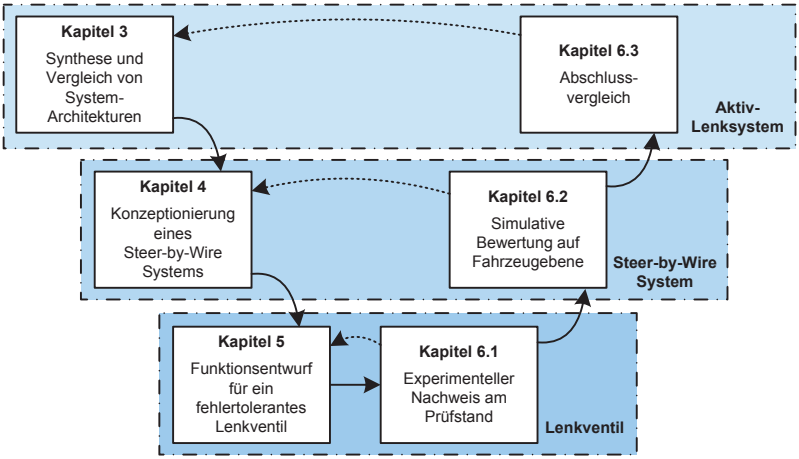


Abb. 1.3: Gewähltes Vorgehen für den Entwurf und Nachweis eines fehlertoleranten Steer-by-Wire Lenkventils

2 Grundlagen und Stand der Technik

Ziel des folgenden Kapitels ist die Einführung von Begrifflichkeiten und die Darstellung des Stands der Technik, die für das Verständnis der Arbeit wichtig sind. Darüber hinaus wird für die Lenkung von Traktoren eine Klassifikation vorgestellt, die als Basis für die Generierung der Systemarchitekturen in Kapitel 3 dient.

2.1 Lenkanlagen von Traktoren

Die ECE-Richtlinie 79 [22] beschreibt für Straßenfahrzeuge wichtige Anforderungen an die Gestaltung, Auslegung und Prüfung der Lenkanlage. Viele dieser Aspekte wurden in die Norm für Traktorlenkanlagen ISO 10998 [40] übernommen und teilweise konkretisiert.

Bei Fahrzeugen gibt es verschiedene Arten, wie eine Lenkbewegung ermöglicht wird. Abbildung 2.1 stellt die drei wichtigsten Arten für mobile Arbeitsmaschinen schematisch dar. Bei der Achsschenkellenkung sind die Räder einer oder mehrerer Achsen um die Hochachse drehbar gelagert, um eine Kurvenfahrt einzuleiten. Bei Fahrzeugen mit Knicklenkung wird dies durch die gegenseitige Verdrehung zweier Fahrzeugteile um die Hochachse erreicht, ohne dass einzelne Räder eine Lenkbewegung ausführen. Demgegenüber wird bei der Radseiten- beziehungsweise Panzerlenkung eine Kursänderung des Fahrzeugs durch unterschiedliche Rad- beziehungsweise Kettendrehzahlen auf beiden Seiten des Fahrzeugs realisiert. Fahrzeuge dieser Art besitzen die Fähigkeit, auf der Stelle zu drehen und benötigen daher wenig Platz zum Wenden. Neben den hier vorgestellten Grundformen gibt es auch Kombinationen dieser, wie beispielsweise bei Radladern mit Knick- und Achsschenkellenkung [21], sowie Sonderformen wie die Einzelradlenkung [69].

Während Panzer- und Knicklenkungen üblicherweise bei Raupenbaggern und Radladern verwendet werden, sind Traktoren bis auf wenige Ausnahmen mit einer Achsschenkellenkung an der Vorderachse ausgestattet. Traktoren mit Allrad-Lenkung sind selten und werden in dieser Arbeit nicht explizit betrachtet.

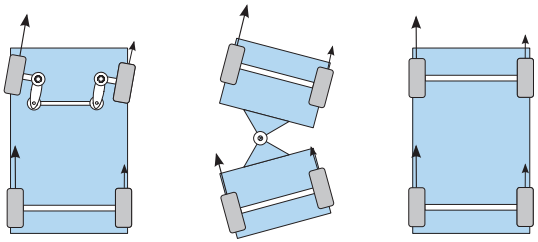


Abb. 2.1: Schematische Darstellung verschiedener Arten von Lenkanlagen (v.l.n.r.: Achsschenkellenkung, Knicklenkung, Radseitenlenkung)

2.1.1 Begriffsdefinitionen

Die Zusammenhänge der in [22] und [40] enthaltenen Begriffsdefinitionen zur Lenkanlage von Fahrzeugen sind in Abbildung 2.2 grafisch dargestellt. Demnach besteht die **Hauptlenkanlage** eines Fahrzeugs aus den gelenkten Rädern, der Übertragungseinrichtung für Signal und Energie, der Betätigungseinrichtung und der Energieversorgungseinrichtung. Darüber hinaus kann das Fahrzeug eine **Fahrassistenz-Lenkanlage** enthalten, innerhalb derer zwischen einer automatischen und einer korrigierenden Lenkfunktion unterschieden wird. Bei der automatischen Lenkfunktion trägt der Fahrer die Hauptverantwortung über die Fahrzeugführung, auch wenn das Fahrzeug bei der automatischen Spurführung selbstständig lenkt. Bei korrigierenden Lenkfunktionen wird der Fahrerwunsch ereignis- und situationsabhängig verändert, um beispielsweise elektronische Stabilisierungssysteme mit Lenkeingriff zu realisieren. Werden Lenkbefehle außerhalb des Fahrzeugs generiert

und an dieses übertragen, wie dies beispielsweise bei der Elektronischen Deichsel [106, 34] der Fall ist, so fällt dies unter den Begriff der **autonomen Lenkanlage**. Die dunkelblau markierten Teilsysteme bilden den Fokus der vorliegenden Arbeit und werden im Folgenden mit den Begriffen *»Lenkanlage«*, *»Lenksysteme«* oder *»Lenkung«* synonym zusammengefasst.

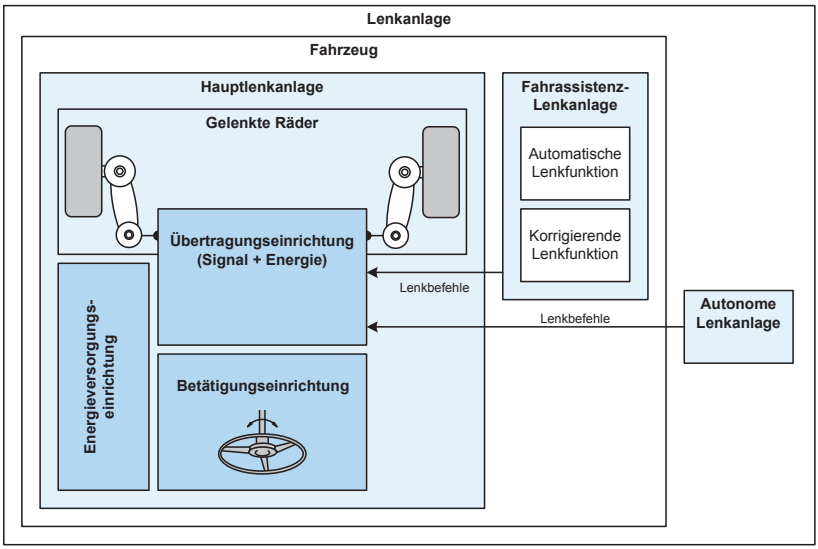


Abb. 2.2: Grafische Darstellung des Zusammenhangs wichtiger Begriffsdefinitionen [22, 40]

Entsprechend der **Erzeugung der Lenkkräfte** wird in den zuvor genannten Normen folgende Unterscheidung gemacht: Bei der Muskelkraftlenkung wird die komplette zum Lenken benötige Energie durch den Fahrer aufgebracht. Demgegenüber wird der Fahrer bei einer Hilfskraftlenkung durch eine Fremdkraftquelle unterstützt. Lenksysteme werden nur dann als Hilfskraftlenkung bezeichnet, wenn im Falle des Ausfalls der Fremdkraftquelle eine Lenkung des Fahrzeugs mit Muskelkraft möglich ist, ohne die vorgeschriebenen Grenzwerte für die Betätigungskräfte zu überschreiten. Andernfalls und

im Falle der ausschließlichen Verwendung einer Fremdkraftquelle bezeichnet man eine solche Lenkung als Fremdkraftlenkung.

Bezüglich der **Übertragung der Lenkkräfte** werden rein mechanische, rein hydraulische, rein elektrische und rein pneumatische Übertragungseinrichtungen sowie Kombinationen daraus (Hybridübertragungseinrichtungen) unterschieden. Während bei rein mechanischen Lenksystemen die Lenkkräfte *ausschließlich* mechanisch übertragen werden, erfolgt bei rein hydraulischen, rein elektrischen und rein pneumatischen Lenksystemen die Übertragung der Lenkkräfte an *irgendeinem* Punkt innerhalb des Energieübertragungssystems auf eine dieser Arten. Hydromechanische und elektromechanische Hybridübertragungseinrichtungen sind bei Servolenkungen im PKW-Bereich weit verbreitet, Lenksysteme von Traktoren haben in der Regel rein hydrostatische Übertragungseinrichtungen (siehe Kapitel 2.1.2). Nach [40] kann die Übertragungseinrichtung nochmals in die Energie- und die Signalübertragungseinrichtung unterteilt werden. Daraus resultiert beispielsweise die Bezeichnung *»elektrohydraulische Lenkung«* für eine Traktor-Lenkung mit rein hydraulischer Übertragung der Lenkkräfte (Energie-Übertragungseinrichtung) und der Möglichkeit der elektrischen Übertragung beziehungsweise Beeinflussung der Lenksignale (Signal-Übertragungseinrichtung).

In [71] wird ein weiteres Unterscheidungsmerkmal für die **Charakteristik** der Übertragung vom Lenkrad zu den gelenkten Rädern eingeführt: Demnach werden Lenksysteme als passiv bezeichnet, wenn ein fester Zusammenhang zwischen dem Lenkradwinkel und dem Radlenkwinkel sowie zwischen dem Betätigungsmoment am Lenkrad und dem Unterstützungsmoment besteht, der während der Fahrt nicht elektronisch beeinflusst werden kann. Ist der erstgenannte Zusammenhang fest, aber der Zusammenhang zwischen dem Betätigungsmoment und dem Unterstützungsmoment variabel, so spricht man von einem semi-aktiven System. Bei aktiven Systemen besteht die Möglichkeit, beide Zusammenhänge situationsabhängig während der Fahrt zu verändern.

Alle aktiven Lenksysteme lassen sich nach [71] in **Überlagerungslenkungen** und **Steer-by-Wire** Systeme unterteilen. Während bei Überlagerungslenkungen an einer bestimmten Stelle zwischen dem Lenkrad und den gelenkten Rädern eine Winkel- beziehungsweise Volumenstrom-Überlagerung einer Fremdkraftquelle möglich ist, wird bei Steer-by-Wire Systemen der konventionelle Durchgriff aufgetrennt. Nach [11] haben Steer-by-Wire Systeme keine direkte mechanische oder hydraulische Verbindung zwischen der Betätigungseinrichtung und den gelenkten Rädern im nominalen Betrieb, der Lenkwunsch des Fahrers wird also rein elektrisch übertragen und in einem mechatronischen Aktor in eine Lenkbewegung umgesetzt. In der Regel sind Steer-by-Wire Systeme Fremdkraftlenkanlagen, je nach Sicherheitskonzept kann die Rückfallebene jedoch auch eine Hilfskraft- oder Muskelkraftlenkung sein. Systeme mit einer Hilfskraft- oder Muskelkraftlenkung als Rückfallebene zeichnen sich gegenüber reinen Steer-by-Wire Systemen häufig durch eine höhere Komplexität aus. Sie können jedoch als technologische Übergangslösung betrachtet werden, um Feld-Daten über das Ausfallverhalten der Komponenten zu sammeln und damit das Vertrauen in die Sicherheit von Steer-by-Wire Systemen in der Bevölkerung zu steigern. Im PKW-Bereich werden Steer-by-Wire Systeme häufig mit Lenkanlagen mit rein elektrischer Energieübertragung gleichgesetzt. In diesem Anwendungsbereich eignen sich quasi ausschließlich derartige Lenkungen zur Realisierung eines Steer-by-Wire Systems, weil in diesen *trockenen* Systemen die wartungsintensive Lenkhydraulik überflüssig wird. Gegenüber bereits am Markt verfügbaren trockenen elektromechanischen Lenksystemen wären hydrostatische Steer-by-Wire Systeme für PKW ein technologischer Rückschritt. Daher eignen sich Steer-by-Wire Systeme mit rein hydrostatischer Energieübertragung vor allem für schwere Fahrzeuge, wie mobile Arbeitsmaschinen, bei denen hohe Lenkkräfte erforderlich sind und die derzeit mit einer rein hydrostatischen Hilfskraftlenkanlage und einer Arbeitshydraulik ausgestattet sind.

2.1.2 Klassifikation und Stand der Technik

Entsprechend der zuvor eingeführten Begriffe und Unterscheidungsmerkmale lässt sich eine Klassifikation für Traktorlenksysteme mit Achsschenkellenkung an der Vorderachse einführen, siehe Abbildung 2.3. Bei der Klassifikation bleiben die elektrischen und pneumatischen Übertragungseinrichtungen unberücksichtigt. Während pneumatische Systeme nicht von den Normen abgedeckt werden [22, 40], sind rein elektrische Lenkungen mit aktuellen 12V-Bordnetzen [90] auf Grund des Leistungsbedarfs zur Erreichung hoher Lenkkräfte für den Einsatz in Fahrzeugen mit hohen Vorderachslasten wie Traktoren und Nutzfahrzeuge ungeeignet [97][1]. Muskelkraftlenkungen haben bei landwirtschaftlichen Traktoren keinerlei Bedeutung, da durch die gesetzliche Begrenzung der maximalen Betätigungskraft[2] (siehe Kapitel 3.1) solche Lenksysteme allenfalls für Kleinsttraktoren im Kommunalbereich einsetzbar sind. In Abbildung 2.3 sind die rein mechanischen Hilfskraft- und Fremdkraftlenkungen eingeklammert, weil im Fahrzeug keine mechanische Fremdkraftquelle vorhanden ist, die in geeigneter Weise zum Lenken verwendet werden kann.

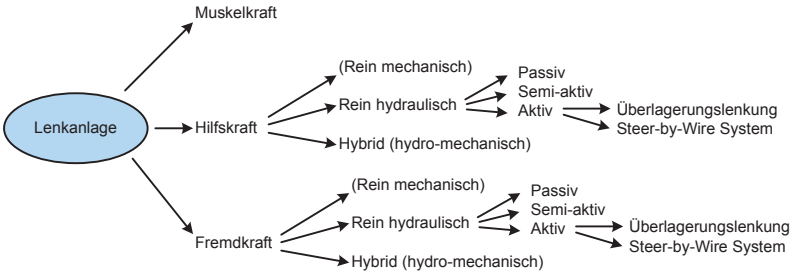


Abb. 2.3: Klassifikation der Lenkanlagen von Traktoren mit Vorderachslenkung in Anlehnung an [40, 71]

[1] Rein elektrische Servolenkungen werden derzeit in Oberklasse-PKW mit Zahnstangenkräften von bis zu 15 kN eingesetzt [71]. In Traktoren treten höhere Kräfte bis über 50 kN auf.

[2] Die Betätigungskraft ist die Kraft, die der Fahrer am Lenkrad einprägt. Demgegenüber ist die Lenkkraft die Kraft, die zum Verstellen der Räder benötigt wird.

Hydromechanische Hybrid-Übertragungseinrichtungen nehmen eine Sonderrolle bei den Lenksystemen von landwirtschaftlichen Traktoren ein und werden in dieser Arbeit nicht näher betrachtet. Durch den Einsatz dieser Lenksysteme aus dem Nutzfahrzeugbereich sind zulässige Höchstgeschwindigkeiten über 60 km/h und damit Transportfahrten auf Autobahnen mit solchen Traktoren möglich [46]. Nachteilig ist jedoch die Notwendigkeit eines mechanischen Lenkgestänges zwischen dem Lenkrad und den gelenkten Rädern und der zusätzliche konstruktive Aufwand für die Realisierung einer automatischen Spurführung, die beispielsweise durch einen zusätzlichen am Achsschenkel angebrachten konventionellen Lenkzylinder realisiert wird.

Die Mehrzahl der am Markt befindlichen Traktor-Lenksysteme sind rein hydrostatische Hilfskraftlenkanlagen, bei denen die Unterstützungwirkung konstruktiv festgelegt ist (passives Lenksystem). Abbildung 2.4 zeigt den Schaltplan und ein Foto eines solchen Lenkventils. Im Vergleich zu elektro- oder hydromechanischen Lenksystemen eines PKW haben diese Lenksysteme keinen mechanischen Durchgriff zwischen dem Lenkrad und den gelenkten Rädern, da die zum Lenken benötigte Energie und Ölmenge über flexibel verlegbare Hydraulikschläuche zum Lenkzylinder übertragen und in eine Lenkbewegung umgewandelt werden. Da Traktoren für die Arbeitsfunktionen bereits mit einem Hydrauliksystem ausgerüstet sind, kann solch eine Lenkung mit vergleichsweise niedrigen Kosten integriert werden.

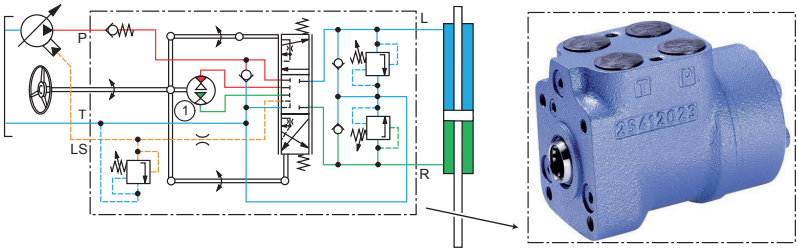


Abb. 2.4: Hydraulischer Schaltplan und Foto einer hydrostatischen Lenkeinheit für mobile Arbeitsmaschinen aus [9]

Nachteilig ist jedoch die Notwendigkeit, das Lenkventil in oder an der Kabine zu platzieren, um den Wunsch nach Modularität bei der Kabinengestaltung und einer geringen Geräuschentwicklung zu erfüllen. Damit die Lenkfähigkeit auch bei einem Ausfall der Hydraulikpumpe gewährleistet ist, wird in das Lenkventil eine vom Fahrer angetriebene Konstantstrompumpe ① integriert. Im nominalen Fall wird diese saugseitig von der zentralen Hydraulikpumpe versorgt und dient lediglich der Dosierung des Hydrauliköls zu dem Lenkzylinder. Im Fehlerfall hat der Fahrer jedoch die Möglichkeit, mittels Muskelkraft den Lenkzylinder zu verstellen. In diesem als Notlenkbetrieb bezeichneten Betriebsmodus ist die zum Lenken benötigte Kraft um ein vielfaches höher als im nominalen Betriebszustand. Um ein Überschreiten der zulässigen Betätigungskräfte zu verhindern, setzen manche Hersteller bei großen Traktoren zusätzliche Notlenkpumpen ein [49]. Derartige Lenksysteme zählen dann zu den rein hydrostatischen Fremdkraftlenkanlagen, da das Fahrzeug nicht mehr durch Muskelkraft gelenkt werden kann.

Wird ein derartiges Lenksystem durch ein zusätzliches elektrohydraulisches Lenkventil (*Bypass-Ventil*) erweitert, so kann eine aktive Überlagerungslenkung realisiert werden, bei der die Lenkübersetzung zwischen dem Lenkrad und den gelenkten Rädern situationsabhängig angepasst und eine automatische Spurführung realisiert werden kann [79]. Bei Verwendung eines zum Bypass-Ventil in Reihe geschalteten Absperrventils besteht ein redundanter Abschaltpfad für den Fall eines hydraulischen Fehlers. In diesem hydraulisch sicheren Zustand ist nur noch das konventionelle Lenkventil aktiviert und damit die Lenkbarkeit des Traktors gewährleistet, falls auch die Ansteuerung der Magnetventile im Bypass-Ventil entsprechend sicher ist. Die derzeit am Markt befindlichen Überlagerungslenkungen sind nur für off-road Anwendungen konzipiert und müssen während der Straßenfahrt vom Fahrer elektrisch deaktiviert werden, um die Lenkbarkeit sicher zu gewährleisten [79, 13]. Ist in solchen Systemen mit aktiver Überlagerungslenkung nur eine Fremdkraftquelle vorhanden, so steigt bei einem Ausfall dieser die zum

Lenken benötigte Kraft stark an. Schon sehr früh wurde erkannt, dass elektrohydraulische Lenksysteme unabhängig von der automatischen Spurführung auch für Fahrzeuge mit mehreren gelenkten Achsen sehr gut geeignet sind, weil mit diesen verschiedene, auf die jeweilige Arbeitsaufgabe angepasste, Lenkprogramme und Lenkmanöver dargestellt werden können [94].

Während rein elektrische Steer-by-Wire Systeme bei langsam fahrenden Arbeitsmaschinen wie Flurförderfahrzeugen weit verbreitet und Stand der Technik sind [50], waren rein hydrostatische Steer-by-Wire Systeme bis vor kurzem kaum nennenswert am Markt vertreten. WROBLEWSKI [100] untersucht und entwickelt ein solches System für Anwendungen im Bereich der Flurförderfahrzeuge. WROBLEWSKI kombiniert dazu die bewährten hydraulischen Komponenten des rein hydrostatischen Lenkventils mit zwei unabhängigen elektrischen Antrieben, die in einem einzigen Statorgehäuse untergebracht sind, zu einer elektrohydraulischen Stelleinheit. Auf Grund der deutlich höheren Anforderungen gegenüber langsam fahrenden Arbeitsmaschinen ist dieses Konzept jedoch nicht für Traktoren mit Straßenzulassung geeignet [100].

Im Jahre 2009 wurde erstmals ein rein hydrostatisches Steer-by-Wire System für den Serieneinsatz in landwirtschaftlichen Traktoren vorgestellt und später auf den Markt gebracht, das die erforderlichen Sicherheitsanforderungen für eine Fahrt im öffentlichen Straßenverkehr erfüllt [52, 34, 83, 81]. Neben einer geschwindigkeitsabhängigen variablen Lenkübersetzung bietet dieses Lenksystem auch eine elektronische Stabilisierung des Fahrverhaltens durch Lenkeingriffe (Fahrassistenz-Lenkanlage) [74]. Abbildung 2.5 zeigt den zentralen Teil des hydrostatischen Lenkventils. Dieses besteht aus zwei identischen Kanälen mit jeweils einem Proportionalventil für Lenkbewegungen nach links ① und jeweils einem für Lenkbewegungen nach rechts ②. Die Schieber-Position dieser Ventile wird sensorisch überwacht, um im Falle eines Fehlers den jeweils defekten Kanal über ein Abschaltventil ③ hydraulisch abzutrennen. In Kombination mit einer zweikanaligen Struktur im

Bereich Sensorik, Energieversorgung und Steuergerätearchitektur kann auf diese Weise ein sicheres und fehlertolerantes Lenksystem realisiert werden. Die redundante Druckversorgung wird durch eine elektrisch angetriebene Notlenkpumpe realisiert, die einen Maximaldruck von 70 bar aufbringen kann [81]. Im Gegensatz zu Hilfskraftlenkanlagen führt bei fehlertoleranten Fremdkraftlenkanlagen der Ausfall einer Fremdkraftquelle zu keinem Anstieg der Betätigungskraft, was sich positiv auf die Lenkbarkeit des Fahrzeugs in kritischen Situationen auswirkt.

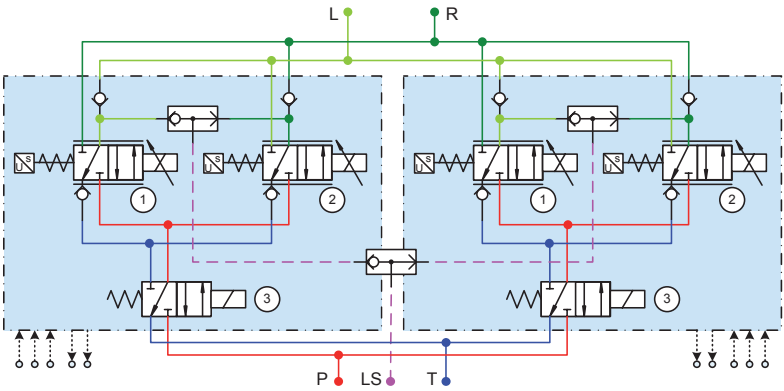


Abb. 2.5: Schaltplan eines hydrostatischen Steer-by-Wire Ventils nach [83]

Es ist offensichtlich, dass bei der Entwicklung eines sicheren Lenksystems neben dem technischen Verhalten des Lenksystems während und nach dem Eintritt eines Fehlers auch der Einfluss dieses Fehlers auf den Fahrer betrachtet werden muss. NEUKUM [63] untersucht in diesem Zusammenhang vielfältige Fehlerfälle und Szenarien für aktive PKW-Überlagerungslenkungen, bei denen ein Fehler im Überlagerungsgetriebe haptisch auf den Fahrer zurückwirkt. THEIS [91] betrachtet dieses Thema auf eine andere Weise und untersucht die menschliche Zuverlässigkeit im Zusammenhang mit einem Steer-by-Wire System im Kraftfahrzeug. THEIS arbeitet heraus, dass der Fahrer bei komplexen elektronischen Systemen während der Entwicklung

des Sicherheitskonzepts berücksichtigt werden muss, weil diesem eine sicherheitsrelevante Aufgabe zukommt. Dies gilt insbesondere für die Entwicklung von Warnszenarien, da in solchen Fällen durch das Warnsignal eine bestimmte Fahrerreaktion ausgelöst werden soll, um gefährliche Situationen zu vermeiden oder zu entschärfen. BARTHENHEIER [5] untersucht das Potential einer fahrertyp- und fahrsituationsabhängigen Lenkradmomentengestaltung und zeigt damit die Wichtigkeit einer haptischen Rückmeldung für den Fahrer auf. In Steer-by-Wire Systemen wird diese Rückmeldung synthetisch durch einen Handkraftaktor generiert. KRAUTSTRUNK [54] bewertet ein fehlerhaftes Lenkradmoment eines solchen Handkraftaktors als sicherheitskritisch und entwickelt eine fehlertolerante Architektur und eine dazugehörige Regelung zur Realisierung eines sicheren Handkraftaktors.

2.2 Funktionale Sicherheit

Das Thema *»Sicherheit«* ist für das Lenksystem eines Fahrzeugs mit Straßenzulassung von zentraler Bedeutung. Im folgenden Abschnitt werden wichtige Begriffe definiert und zentrale Normen aufgelistet, die im Entwicklungsprozess berücksichtigt werden müssen. Das Praxisbeispiel eines elektromechanischen PKW-Lenksystems sowie weitere Forschungsarbeiten runden das Kapitel ab.

2.2.1 Begriffsdefinitionen

Die **Sicherheit** ist nach DIN EN 61508-4 [16] die „Freiheit von unvertretbaren Risiken“. Dabei ist das **Risiko** die Kombination aus der Wahrscheinlichkeit des Eintritts eines Schadens und dessen Ausmaßes [39]. Bei der Beurteilung des Schadens wird üblicherweise der materielle Schaden vernachlässigt und lediglich der Schaden für Leib und Leben betrachtet. Ist ein nicht vertretbar hohes Risiko vorhanden, so liegt eine **Gefahr** vor [93].

Es ist technisch nicht möglich und wirtschaftlich nicht sinnvoll, das Risiko beliebig weit zu reduzieren, so dass stets ein Restrisiko vorliegt und von der Gesellschaft toleriert werden muss.

Die **funktionale Sicherheit** ist der Teil der Gesamtsicherheit, der von der korrekten Funktion eines sicherheitsbezogenen Teilsystems (Sicherheitssystem) abhängig ist. Abbildung 2.6 stellt verschiedene Aspekte der Gesamtsicherheit und den Zusammenhang zur funktionalen Sicherheit grafisch dar. Der wichtigste Aspekt zur Erreichung eines sicheren Systems ist die unmittelbare Sicherheit innerhalb der konstruktiven Sicherheit. Gefährdungen sollten stets durch eine geeignete Konstruktion und Gestaltung soweit wie möglich vermieden werden. Ist dies nicht möglich, so sollte der Bediener einer Maschine und andere Personen in der Umgebung durch Schutzeinrichtungen, wie beispielsweise einer Abdeckung, vor Gefahren geschützt werden (mittelbare Sicherheit). In vielen Systemen ist dieser Schutz nicht für alle Gefahren möglich, so dass spezielle Sicherheitssysteme entwickelt werden müssen, um das Risiko auf ein akzeptables Maß zu reduzieren (funktionale Sicherheit). Sicherheitsmaßnahmen aus dem Bereich der mittelbaren und funktionalen Sicherheit führen gelegentlich dazu, dass die Verwendung einer Maschine oder eines Systems für den Endanwender umständlicher wird, wie beispielsweise bei der Zweihandbedienung von Pressen oder bei Schutztüren für die Bestückung einer Drehmaschine. In solchen Systemen muss durch eine geeignete Auslegung dieser Sicherheitsmaßnahmen dafür gesorgt werden, dass diese nicht ohne Weiteres übergangen werden können. Neben der konstruktiven Sicherheit ist auch die hinweisende Sicherheit wichtig, bei der durch Warnungen an der Maschine oder in dessen Handbuch auf Restrisiken hingewiesen wird und Vorschriften zur Gefährdungsreduktion festgelegt werden.

Ein wichtiger Aspekt für die Beurteilung des von einer Maschine ausgehenden Risikos ist die Kenntnis über dessen **sicheren Zustand**. Nach [93] ist dieser ein Zustand der Betrachtungseinheit, der auf Grund der getroffe-

nen Schutzmaßnahmen selbst unter der Annahme von sicherheitsbezogenen Fehlfunktionen ein vertretbar niedriges Restrisiko aufweist. In sehr vielen Systemen ist der deaktivierte Zustand, in dem die Betrachtungseinheit im Stillstand ist, der sichere Zustand.

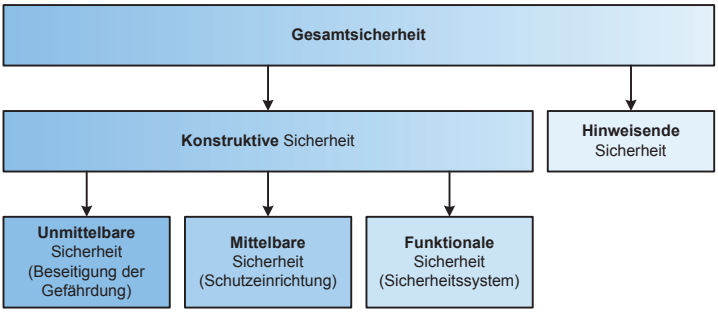


Abb. 2.6: Darstellung verschiedener Aspekte der Gesamtsicherheit nach [58]

Ein **Ausfall** ist die Beendigung der Fähigkeit einer Einheit, eine geforderte Funktion zu erfüllen. Der Ausfall wird als gefahrbringend bezeichnet, wenn er das Potential hat, das System in einen gefährlichen Zustand oder in eine Fehlfunktion zu überführen.

Demgegenüber ist ein **Fehler** der *Zustand* einer Einheit, der dadurch charakterisiert ist, dass diese eine geforderte Funktion nicht mehr ausführen kann. Das Verhalten der Betrachtungseinheit weicht in diesem Zustand von dem normalen Verhalten ab [31]. Ein Fehler ist häufig das Resultat eines Ausfalls, kann aber auch ohne vorherigen Ausfall bestehen, wie beispielsweise bei Fertigungsfehlern. Fehler haben häufig eine Ursache und eine oder mehrere Auswirkungen, wobei beide von der jeweiligen Betrachtungstiefe abhängig sind.

2.2.2 Normen und deren Anwendungsbereich

Zentraler Ankerpunkt aller Normen rund um das Thema Produkt- und Maschinensicherheit bildet die Maschinenrichtlinie. Wie aus Abbildung 2.7 ersichtlich ist, sind unter der Maschinenrichtlinie verschiedene Hierarchien an unterschiedlichen Sicherheitsnormen zusammengefasst. A-Normen (Grundnormen) beschreiben allgemeine Zusammenhänge und Definitionen wie Gestaltungsleitsätze oder Vorschriften zur Risikobeurteilung. Demgegenüber beziehen sich B-Normen (Fachgrundnormen) auf spezielle Anwendungsgebiete wie hydraulische Systeme, Maschinensteuerungen oder elektrische Antriebe. Je nach Anwendung existieren darunter noch detailliertere maschinenspezifische C-Normen (Produktnormen) mit weiterführenden Informationen und Vorschriften. Normen des Typs C haben für Maschinenhersteller die höchste Priorität [78].

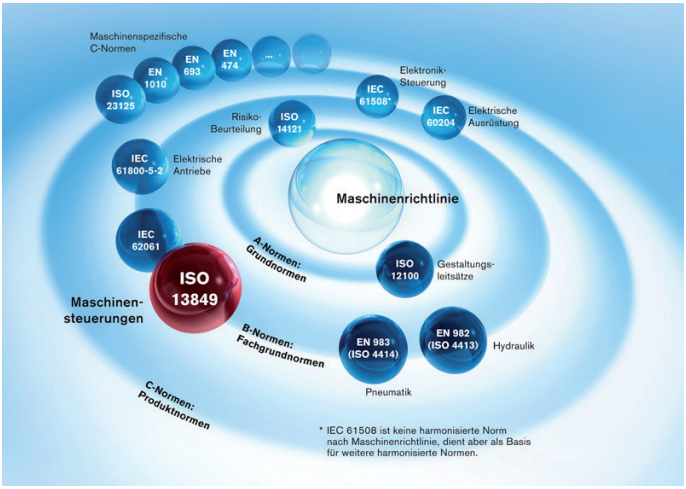


Abb. 2.7: Darstellung der Hierarchie einzelner durch die Maschinenrichtlinie harmonisierter Sicherheitsnormen aus [10]

Von sehr großer Bedeutung für die funktionale Sicherheit von Maschinen ist die ISO-Norm 13849 [18]. Im Unterschied zu vielen anderen Normen zum Thema funktionale Sicherheit lassen sich mit dieser Norm auch nicht-elektrische Systeme mit hydraulischen oder mechanischen Komponenten beschreiben und erfassen. In [18] sind verschiedene Grund-Architekturen für sicherheitsrelevante Steuerungen vorgegeben, die je nach Risikobeurteilung angewendet und deren Wirksamkeit nachgewiesen werden muss. Die Risikobeurteilung erfolgt dabei in fünf Stufen von *»PL e«* (*Performance Level e*) bis zur niedrigsten Einstufung *»PL a«*.

Zum Nachweis der funktionalen Sicherheit von elektrischen Steuerungen im Kraftfahrzeugbereich bis 3,5 Tonnen zulässige Gesamtmasse existiert seit 2011 die ISO-Norm 26262 [43]. Diese Norm ist speziell auf die KFZ-Industrie zugeschnitten und beinhaltet sowohl quantitative als auch qualitative Anforderungen. Neben der eigentlichen Produktentwicklung werden durch diese Norm auch alle anderen Produktlebensphasen abgedeckt. Die Risikobewertung erfolgt in vier verschiedenen Stufen von der schärfsten Anforderung *»ASIL D«* (*Automotive Safety Integrity Level D*) bis zur niedrigsten Einstufung *»ASIL A«*. Funktionen oder Systeme, die eine Einstufung niedriger als *»ASIL A«* aufweisen, können über qualitätssichernde Maßnahmen (QM) ausreichend abgesichert werden.

Für Traktoren sowie land- und forstwirtschaftliche Maschinen existiert die ISO-Norm 25119 [42]. Diese C-Norm beinhaltet einzelne Aspekte sowohl aus der ISO 13849 (z.B. Sicherheits-Kategorien und Sicherheitseinstufung) als auch aus der ISO 26262 (z.B. Risikograph), deckt jedoch ebenfalls nur elektrische, elektronische und programmierbare elektronische Systeme ab. In der ISO 25119 wird statt der Risikoeinstufung mittels *»PL«* die Bezeichnung *»AgPL«* (*Agricultural Performance Level*) verwendet.

Da alle diese Normen auf den vollständigen Produktentwicklungsprozess zugeschnitten sind, können nicht alle darin enthaltenen Verfahrensschritte und

Anforderungen bei einer Konzeptentwicklung beziehungsweise einem Systementwurf berücksichtigt werden. Dazu zählen Schritte wie die Hardware- und Softwareentwicklung sowie deren Integration und Test, die Produktfreigabe sowie die Überwachungen aller folgenden Produktlebenszyklen wie Produktion, Betrieb, Wartung und Außerbetriebnahme. Das Fehlen insbesondere der Schritte Hard- und Softwareentwicklung hat zur Folge, dass ein formaler sicherheitstechnischer Gesamtnachweis nicht erfolgen kann. Basierend auf den Verfahrensschritten der drei zuvor genannten Sicherheitsnormen lassen sich im Rahmen einer Konzeptentwicklung jedoch stets die folgenden fünf Schritte systematisch bearbeiten:

1. **Beschreibung der Betrachtungseinheit:** In diesem Schritt wird die Betrachtungseinheit auf Systemebene beschrieben. Neben der Beschreibung der Betrachtungseinheit selbst werden die Schnittstellen zu anderen Systemen definiert und spezielle Anforderungen an das System aufgelistet.

2. **Gefahrenanalyse und Risikobewertung:** Durch eine systematische Analyse werden die von der Betrachtungseinheit in verschiedenen Situationen ausgehenden Gefahren identifiziert und mit Hilfe eines Risikographen bewertet. Dabei ist auch eine vorhersehbare Fehlbedienung oder Fehlverwendung der Betrachtungseinheit zu berücksichtigen. Die Gefahrenanalyse und Risikobewertung erfolgt ohne die Berücksichtigung von geplanten, aber noch nicht umgesetzten Sicherheitsmaßnahmen [71]. Bei der Bewertung des Risikos werden die folgenden drei Aspekte berücksichtigt [42]:

    - **Schwere der Verletzungen**: Welche Verletzungen sind für die beteiligten Personen in der jeweiligen Gefahrensituation zu erwarten?

    - **Exposition in Szenario**: Wie hoch ist die Wahrscheinlichkeit oder die Häufigkeit, dass beteiligte Personen sich in einer Situa-

tion befinden, in der die Gefahrensituation prinzipiell auftreten kann?[3]

- **Kontrollierbarkeit der Situation**: Welche Möglichkeiten und Chancen haben die beteiligten Personen nach Eintreten der Gefahrensituation einen Schaden abzuwenden oder abzumildern?

Je nach Bewertung der zuvor genannten Kriterien erfolgt eine Sicherheitseinstufung in eines der zuvor genannten Sicherheitslevel. Die Einstufung erfolgt entsprechend des Schemas aus Anhang A.1. Für alle ermittelten Risiken werden anschließend Sicherheitsziele für die Betrachtungseinheit definiert die darauf abzielen, die jeweiligen Gefahren zu vermeiden. Manche C-Normen, wie beispielsweise die EN ISO 23135 für Drehmaschinen, schreiben die maschinenspezifischen Sicherheitsfunktionen und die dazugehörigen erforderlichen Performancelevel bereits vor [78].

3. **Sicherheitskonzept:** Für die zuvor definierten Sicherheitsziele wird ein Konzept entwickelt, mit dessen Hilfe das Risiko auf ein tolerierbares Niveau reduziert werden kann. In diesem Konzept werden unter anderem Degradations- und Warnszenarien, sowie für die einzelnen Sicherheitsfunktionen der sichere Zustand und dessen Erreichung festgelegt.

4. **Systemkonzipierung für Hardware und Software:** Im folgenden Schritt wird die Hard- und Software definiert beziehungsweise entwickelt, mit der das Sicherheitskonzept umgesetzt werden kann. Bei einer Konzeptentwicklung muss in diesem Schritt eine angemessene Betrachtungstiefe gewählt werden. Die Betrachtungstiefe sollte auch an den Detailgrad der vorliegenden Informationen über die spätere Hard- und Software angepasst werden.

[3] Dieser Aspekt berücksichtigt nicht die Wahrscheinlichkeit, mit der eine gefahrbringende Situation tatsächlich eintritt.

5. **Sicherheitstechnische Bewertung:** Abhängig von der im vorherigen Schritt gewählten Betrachtungstiefe und der jeweiligen Sicherheitseinstufung der Betrachtungseinheit erfolgt eine angemessene sicherheitstechnische Bewertung. Dieser Nachweis sollte sowohl qualitativ als auch quantitativ erfolgen. In den jeweiligen Normen ist je nach Sicherheitseinstufung vorgeschlagen, welche formalen Methoden für die Bewertung und den Nachweis angewendet werden sollten [42]. Die zwei wesentlichen Elemente sind Sicherheitsanalysen wie beispielsweise eine *Fehlermöglichskeits- und Einflussanalyse* (*FMEA*) und Sicherheitsaudits sowie -reviews, die mit steigendem Performancelevel unter Teilnahme von Mitgliedern anderer Entwicklungsteams beziehungsweise anderer Abteilungen durchgeführt werden sollten.

2.2.3 Stand der Technik

Einzelne der oben genannten Schritte werden im folgenden Abschnitt am Beispiel einer elektromechanischen PKW-Lenkung aus [71] veranschaulicht. Bei der EPS (Electric Power Steering) handelt es sich um eine elektromechanische Servolenkung, bei der die Unterstützungswirkung bedarfsgerecht rein elektrisch ohne den Einsatz von hydraulischer Energie erfolgt, siehe Abbildung 2.8. Dies wird dadurch realisiert, dass ein über ein Getriebe mit dem mechanischen Lenkgestänge verbundener Elektromotor ein Moment in das System einleitet. Derartige Systeme sind bis zu einer Leistung von 1000 W und einer Zahnstangenkraft von 15 kN verfügbar und damit auch in Oberklassefahrzeugen einsetzbar [71]. Mit solch einem *semi-aktiven* Lenksystem lassen sich im PKW Zusatzfunktionen wie Einpark- oder Spurhalteassistenten realisieren.

Aus der Gefahrenanalyse und Risikoeinstufung entsprechend der ISO 26262 ergeben sich für ein solches EPS-System die folgenden Gefahren und Sicherheitsziele [71]:

- **Unerwünschte Ansteuerung des Servomotors (ASIL D):** Das Lenksystem muss Fehler, die zu einer unerwünschten Aktuatorfunktionalität führen, erkennen und in einen sicheren Zustand wechseln.
- **Schwergängigkeit des Lenksystems durch Fehlansteuerung des Servomotors (ASIL D):** Das Lenksystem muss Fehler, die zu einer Schwergängigkeit des Lenksystems führen, erkennen und in einen sicheren Zustand wechseln.
- **Plötzliches Einsetzen der Lenkunterstützung (ASIL A):** Das Lenksystem muss das ungewollte Einschalten der Unterstützung verhindern.

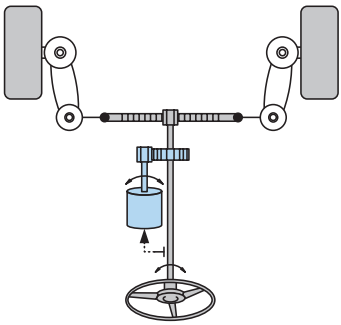


Abb. 2.8: Schematische Darstellung einer elektromechanischen Servolenkung

Für mechanische Komponenten muss durch geeignete Entwicklungsprozesse sichergestellt werden, dass sowohl der Verlust des Durchgriffs zwischen Lenkrad und Rädern als auch eine mechanische Schwergängigkeit ausgeschlossen werden können.

Für dieses Lenksystem ist der sichere Zustand derart definiert, dass die Lenkunterstützung deaktiviert und die mechanische Lenkfähigkeit nach ECE-R 79 gewährleistet ist. Um diesen sicheren Zustand zu erreichen, ist ein sicherer Abschaltpfad in der Leistungselektronik der Motoransteuerung vorgesehen, der bei jedem Start des Systems auf Funktionsfähigkeit überprüft wird. Dieser Abschaltpfad kann sowohl von dem eigentlichen Mikroprozessor als auch

von einem separaten Sicherheitsrechner ausgelöst werden. Für Systemfehler, die während der Fahrt auftreten und erkannt werden, gibt es je nach Schwere ein mehrstufiges Degradations- und Abschaltkonzept, damit nicht jeder Fehler zu einem kompletten Ausfall der Lenkunterstützung führt.

MARTINUS [58] untersucht den Aspekt der funktionalen Sicherheit für das mechatronische System *»mobile Arbeitsmaschine«* in allgemeiner Weise. Dazu entwickelt MARTINUS auf Basis einer Analyse ein sicherheitsgerichtetes Entwicklungskonzept, das aus einem an das V-Modell angelehnte Vorgehensmodell und dazugehörigen Methoden sowie Werkzeugen besteht. Ziel ist es dabei, den für mechatronische Systeme komplexen quantitativen Sicherheitsnachweis der Hard- und Software durch einen sicherheitsgerichteten Systementwicklungsprozess zu substituieren, der an die jeweilige Risikoeinstufung angepasst werden kann [58].

Während im Bereich der elektrischen Antriebe bereits Lösungen am Markt verfügbar sind, bei denen die Sicherheitsfunktionen direkt in die Steuerung integriert sind, werden solche sicheren Gesamtlösungen entsprechend der ISO 13849 im Bereich der hydraulischen Steuerungssysteme derzeit in Forschungsprojekten untersucht. RICHTER [77, 78] untersucht am Beispiel eines Vorschubantriebs für eine Werkzeugmaschine insbesondere die Sicherheitsfunktion *»sicher begrenzte Geschwindigkeit«* und *»sicherer Stopp«*. Elektrohydraulische Stetig-Ventile mit Sicherheitsverantwortung werden auch von GORGS [32] untersucht. Der schlimmste Fehler in dem betrachteten Proportionalventil ist laut RICHTER ein klemmender Ventilschieber, der vor allem durch erhöhte Reibung infolge eingelagerter Partikel (*»Silting«*) oder durch die Verklemmung eines großen Fremdkörpers entstehen kann. Sollen die zuvor genannten Sicherheitsfunktionen ohne ein zusätzliches Absperrventil realisiert werden, so muss der Aktor des Ventilschiebers in der Lage sein, so hohe Kräfte aufzubringen, dass in das Ventil eingedrungene Fremdkörper abgeschert sowie die erhöhte Reibung durch eingelagerte Partikel überwunden werden kann.

2.3 Fehlertolerante Systeme

Zur Beurteilung der Sicherheit eines Systems ist die Kenntnis über dessen Ausfallverhalten essentiell. Der folgende Abschnitt beginnt ebenfalls mit wichtigen Begriffsdefinitionen. Anschließend werden Beispiele des Stands der Technik aus dem Gebiet der Hydraulik vorgestellt, die verschiedene Ausprägungen des Ausfallverhaltens repräsentieren.

2.3.1 Begriffsdefinitionen

Die **Zuverlässigkeit** ist die Eigenschaft einer Betrachtungseinheit, seine vorgesehene Funktion zu erfüllen. Für alle sicherheitsrelevanten Systeme gilt die Aussage, dass die Zuverlässigkeit um so höher sein muss, je höher das von einer Fehlfunktion ausgehende Risiko ist. Zur Erhöhung der Zuverlässigkeit sollte stets und zuerst eine Verbesserung der Einzelkomponenten, und damit eine Fehlervermeidung angestrebt werden. Ist durch diese Maßnahme eine ausreichende Steigerung der Zuverlässigkeit unter wirtschaftlichen Randbedingungen nicht mehr möglich, so muss durch eine **fehlertolerante** Systemauslegung dafür gesorgt werden, dass ein Fehler kurzfristig oder dauerhaft keine gefährlichen Situationen hervorrufen kann. Dabei ist die **Fehlertoleranzzeit** das Zeitintervall, in dem Fehler zu keinem gefährlichen Zustand führen. Fehlertoleranz kann durch **Redundanz** erreicht werden. Dabei wird zur Vermeidung einer Fehlfunktion des Systems im Fehlerfall auf zusätzliche Hard- oder Software zurückgegriffen, die im fehlerfreien Zustand prinzipiell nicht benötigt wird [45]. Entscheidend ist dabei die Sicherstellung, dass das jeweils redundante Modul nicht in gleicher Weise von diesem Fehler oder der Fehlerursache betroffen ist, da andernfalls die Fehlertoleranz nicht gegeben ist, weil die Redundanz unwirksam ist.

Im Zusammenhang mit Redundanz werden unter anderem die folgenden Ausprägungen unterschieden:

- **Strukturell oder analytisch:** Liegt die Redundanz als zusätzliche Hardware oder als Softwarekomponente vor?
- **Diversitär oder nicht-diversitär:** Besitzt die redundante Komponente einen anderen oder identischen Aufbau beziehungsweise ist die redundante Komponente anders oder identisch realisiert?
- **Statisch oder dynamisch:** Ist die redundante Komponente ständig aktiv, an der Funktionserfüllung beteiligt und ist die Fehlertoleranz ohne Rekonfiguration gewährleistet, oder wird die jeweilige Komponente erst im Fehlerfall aus einem Ruhezustand oder dem komplett deaktivierten Zustand aktiviert?

ISERMANN [45] unterscheidet zudem verschiedene Degradationsstufen beziehungsweise Ausprägungen des Ausfallverhaltens:

- **Fail-operational (FO):** Ein Fehler wird toleriert. Das System erfüllt nach einem Fehler weiterhin seine Funktion. Diese Ausprägung ist erforderlich, wenn unmittelbar nach einem Komponentenausfall kein sicherer Zustand erreicht werden kann.
- **Fail-safe (FS):** Das System befindet sich nach einem Komponentenausfall im sicheren Zustand oder wird in diesen überführt. Der sichere Zustand wird passiv ohne externe Energie oder aktiv mit externer Energie erreicht.
- **Fail-silent (FSIL):** Das System verhält sich nach einem Komponentenausfall an seinen äußeren Schnittstellen *»still«* und beeinflusst andere Systeme nicht in negativer Weise.

Neben der Fähigkeit einer Betrachtungseinheit tolerant gegenüber bestimmten Komponentenfehlern zu sein, ist auch die Fähigkeit der Betrachtungseinheit wichtig, Komponentenfehler zu erkennen und je nach Situation darauf zu reagieren. JOHANNSEN [48] fasst dies unabhängig von technischen Systemen mit dem Begriff **Fehlermanagement** zusammen und unterscheidet die folgenden Phasen:

- **Fehlererkennung**: Die Feststellung, dass ein oder mehrere Teile einer Betrachtungseinheit vom gewünschten Verhalten abweichen.
- **Fehlerdiagnose**: Die Feststellung, welche Teile der Betrachtungseinheit aus welchem Grund, auf welche Art und in welchem Ausmaß vom gewünschten Verhalten abweichen.
- **Fehlerkorrektur** beziehungsweise **-kompensation**: Die Rückführung der Betrachtungseinheit in den ordnungsgemäßen Zustand (z.B. durch Reparatur) beziehungsweise die vorübergehende Änderung der Betrachtungseinheit mit dem Ziel der Annäherung an den ordnungsgemäßen Zustand.

Zur Fehlererkennung und -diagnose existieren viele Verfahren und Methoden [45]. Im Wesentlichen lassen sich diese in signal- und in modellbasierte Methoden unterteilen. Signalbasierte Methoden, wie die Extremwert- oder Trendüberprüfung, nutzen dazu die Kenntnisse über den Wertebereich oder den Signalverlauf eines einzelnen Signals. Modellbasierte Methoden nutzen ein oder mehrere Signale in Kombination mit einem Signal- oder Prozessmodell, um auf ein Fehlverhalten rückschließen zu können. Innerhalb der modellbasierten Methoden werden hauptsächlich die folgenden drei Methoden unterschieden:

- Fehlererkennung mit **Paritätsgleichungen**: Bei dieser Methode wird das reale Eingangs-/Ausgangsverhalten mit einem fest parametrierten Modell abgebildet. Die Differenz zwischen den realen Messgrößen und

den Modellgrößen bilden die Paritätsgleichungen, die zur Fehlererkennung verwendet werden.

- Fehlererkennung mit **Parameterschätzverfahren**: Durch eine Parameterschätzung werden Modellparameter bestimmt, die zu einer bestmöglichen Übereinstimmung zwischen dem Eingangs-/Ausgangsverhalten des Modells und der Realität führen. Aus der Abweichung der Modellparameter von der nominalen zur aktuellen Situation wird anschließend auf Fehler geschlossen.
- Fehlererkennung mit **Zustandsbeobachtern**: Für das reale System wird ein Zustandsbeobachter entworfen, der fortlaufend die Zustände des realen Systems schätzt. Deren Kenntnis ermöglicht, eine Aussage über die Anwesenheit von Fehlern zu machen.

Nach [2] lässt sich die Fehlererkennung und -diagnose in on- und off-board sowie on- und off-duty unterteilen. Während bei der on-board Diagnose die Diagnose vom Fahrzeug selbst durchgeführt wird, kommen bei der off-board Diagnose externe Testgeräte zum Einsatz. Demgegenüber arbeiten on-duty Methoden während dem Einsatz des Fahrzeugs und off-duty Methoden beispielsweise während dem Start des Fahrzeugs oder im ausgeschalteten Zustand.

Findet während dem Betrieb einer Maschine eine ständige Überprüfung und Auswertung von Mess- und Systemgrößen mit dem Ziel statt, einen Komponentenausfall frühzeitig zu erkennen beziehungsweise rechtzeitig vorherzusagen, so fällt dies in den Bereich des **Condition Monitorings** (Zustandsüberwachung) [8]. Durch Condition Monitoring ist es möglich, die Systemkomponenten zustandsabhängig zu warten oder zu wechseln und damit im Vergleich zur reaktiven und präventiven Instandhaltung die Verfügbarkeit zu steigern sowie schadensfallbedingte Ausfälle zu reduzieren. Besonders für den Einsatz in mobilen Arbeitsmaschinen wird durch BOOG [8] eine belastungsabhängige Instandhaltung in Verbindung mit einem *»Load Cycle*

Monitoring« vorgeschlagen und untersucht, bei der aus den realen Lastkollektiven auf die potentielle Restlebensdauer geschlossen wird.

Im Bereich der Regelungstechnik werden nach BLANKE [7] aktiv und passiv fehlertolerante Regler beziehungsweise Systeme mit aktiver und passiver Fehlertoleranz unterschieden. Bei passiv fehlertoleranten Reglern können durch die geeignete Wahl des Reglers ein beziehungsweise mehrere Fehler toleriert werden, ohne die geforderten Anforderungen zu verletzen. Demgegenüber sind aktiv fehlertolerante Regler auf eine Rekonfiguration (Fehlerkompensation) im Fehlerfall innerhalb der Fehlertoleranzzeit angewiesen. Um diese Rekonfiguration durchführen zu können, muss das System in der Lage sein, den jeweiligen Fehler zu erkennen und zu diagnostizieren, damit die jeweils angemessene Maßnahme eingeleitet werden beziehungsweise die Reglerstrategie geändert werden kann. Durch die separate Auslegung des aktiv fehlertoleranten Reglers auf den fehlerfreien und den fehlerbehafteten Zustand weisen Systeme mit aktiver Fehlertoleranz in der Regel eine bessere Regelgüte auf als Systeme mit einem passiv fehlertoleranten Regler [7].

2.3.2 Stand der Technik

Um das Risiko eines gefahrbringenden Ausfalls eines Systems zu mindern, ist der wichtigste Schritt die Verwendung von bewährten Bauteilen und Sicherheitsprinzipien [18]. Dies kann bei mechanischen Systemen relativ zuverlässig über eine ausreichende Dimensionierung und Materialwahl der Komponenten gewährleistet werden. Komplexe mechatronische Systeme bestehen häufig aus einer bewährten Basisarchitektur (fail-operational) in Kombination mit weiteren Zusatzkomponenten. Die Zusatzkomponenten sind dabei in der Lage, Fehler zu erkennen und in einen sicheren Zustand überzugehen (fail-safe). Die Basisfunktionalität wird dann von der bewährten Rückfallebene übernommen. Bekannte Beispiele für solch eine Systemarchitektur sind Systeme wie das Antiblockiersystem oder die Servolenkung im PKW.

Das Antiblockiersystem ist eine Erweiterung des Zweikreisbremssystems um die Funktionalität, die Blockierneigung einzelner Räder frühzeitig zu erkennen und das Blockieren durch eine Modulation der Radbremsdrücke zu verhindern. Im Falle eines Fehlers schaltet sich diese Zusatzfunktionalität ab, ohne dass der Fahrer die Bremsfähigkeit verliert. Eine ähnliche Struktur weisen Servolenkungen im PKW und die in Kapitel 2.1.2 beschriebene hydrostatische Überlagerungslenkung für Traktoren auf. Tritt bei letztgenannter Lenkung ein Fehler in dem elektrohydraulischen Ventil auf, so wird dieser erkannt und infolge dessen unmittelbar eine sichere Abschaltung eingeleitet. Nach erfolgter Abschaltung ist die Lenkfähigkeit über die bewährte Rückfallebene (hydrostatisches Lenkventil) gewährleistet. Bei derartigen Systemen ist zu beachten, dass eine bewährte Rückfallebene nur dann einen Übergang in den sicheren Zustand garantiert, wenn der Ausfall und die Abschaltung des fail-silent Systems keine derart großen Lenkwinkelfehler in das System einleiten, die den Fahrer vor unlösbare Probleme bei der Spurhaltung stellen würden [29].

Je nach Problemstellung ist die Wahl einer Systemstruktur mit bewährter Rückfallebene nicht möglich oder sinnvoll, wie beispielsweise bei Steer-by-Wire Systemen. Zwar ist die Realisierung eines Steer-by-Wire Systems entsprechend der vorgestellten Klassifikation als hydrostatische Hilfskraftlenkung mit konventioneller Rückfallebene vorstellbar, allerdings unter Verlust der Vorteile der Steer-by-Wire Architektur hinsichtlich Einbauflexibilität [36]. In [81, 83] wird daher ein hydrostatisches Lenkventil für ein Steer-by-Wire System mit nicht-diversitärer Redundanz vorgeschlagen, das aus zwei identischen Kanälen mit fail-safe Verhalten besteht: Die zur Gewährleistung der Fehlertoleranz und damit der Lenkfähigkeit benötigten Ventile sind in identischer Ausprägung doppelt vorhanden, siehe Abbildung 2.5. Im fehlerfreien Zustand werden beide Kanäle gleichermaßen zur Verstellung des Lenkzylinders verwendet. Nach Eintritt und erfolgreicher Erkennung eines Komponentenausfalls wird der jeweils defekte Kanal durch ein Absperrventil

in den sicheren Zustand überführt und die Lenkfähigkeit über den anderen Kanal sichergestellt.

Die Fehlertoleranz eines anderen Hydrauliksystems zur Regelung eines hydraulischen Verbrauchers untersucht SIIVONEN [87, 89]. Die zugrunde liegende Steuerungsarchitektur zeichnet sich zum Einen dadurch aus, dass alle Steuerkanten unabhängig voneinander angesteuert werden können und zum Anderen dadurch, dass jede Steuerkante durch eine Kombination mehrerer unterschiedlich großer Schaltventile realisiert ist, siehe Abbildung 2.9. In anderen Anwendungen wird diese Ventilarchitektur durch ein weiteres Ventil ergänzt, das die beiden Verbraucheranschlüsse A und B miteinander verbindet. Dadurch kann eine Eilgangschaltung für Differentialzylinder sowie eine Schwimmstellung für Gleichgangzylinder realisiert werden. Systeme mit unabhängigen Steuerkanten weisen die Eigenschaft auf, dass eine sichere Unterbrechung des Volumenstroms in der Regel ohne zusätzliche Absperrventile gewährleistet werden kann, da im Falle eines beliebigen Einzelfehlers in einem der Ventile eine gefahrbringende Zylinderbewegung durch Abschaltung der restlichen Ventile gewährleistet werden kann [4]. Bei der quantitativen Bestimmung der Ausfallrate und damit der erreichbaren Sicherheitslevel muss jedoch die hohe Komponentenanzahl und je nach Ansteuerungsverfahren deren Schalthäufigkeit berücksichtigt werden. Zur Erreichung der Zuverlässigkeit eines proportionalen Schieberventils muss die Ausfallrate jedes einzelnen Schaltventils sehr niedrig sein [4].

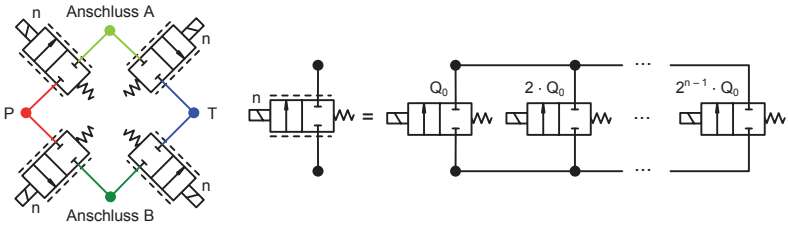


Abb. 2.9: Digitalhydraulische Ventilarchitektur nach [87]

SIIVONEN weist für ein solches System nach, dass durch die Vielzahl der Komponenten und Freiheitsgrade ein fehlertolerantes Verhalten des Gesamtsystems gewährleistet werden kann, ohne dass zusätzliche Komponenten benötigt werden. Zudem entwickelt SIIVONEN Methoden zur on-duty Fehlererkennung und -diagnose in der Ansteuerelektronik mit Hilfe einer Spannungsmessung [87] und durch den Einsatz von Drucksensoren in einem aktiven off-duty Selbst-Test [88]. SIIVONEN weist nach, dass die Fehlertoleranz durch eine Rekonfiguration der Ansteuerungsstrategie im Fehlerfall verbessert werden kann.

Fehlertoleranzstrategien für mechatronische Systeme werden in [6] durch BECK beschrieben. Dabei geht es vor allem um die praxisnahe Darstellung und Anwendungen von verschiedenen Methoden zur Fehlererkennung, -diagnose und -toleranz. Darüber hinaus werden Hardware-Redundanz und analytische Redundanz miteinander verglichen und verschiedene Möglichkeiten zur Reglerumschaltung während der Rekonfiguration vorgeschlagen. MÜNCHOF [61] entwickelt und vergleicht ebenfalls modellbasierte Methoden zur Fehlererkennung und -diagnose für eine hydraulische Servoachse. Dabei untersucht MÜNCHOF auch den Einfluss von veränderlichen Systemparametern wie der Öltemperatur und der Ventilkennlinie auf die Fehlererkennung. Eine wesentliche Herausforderung bei der Fehlererkennung ist laut MÜNCHHOF die unbekannte Größe der auf den hydraulischen Verbraucher angreifenden Kraft, die durch Verwendung von Drucksensoren in den Zylinderkammern abgeschätzt werden kann.

Zur Modellierung und quantitativen Bewertung der Zuverlässigkeit komplexer fehlertoleranter Systeme entwickelt ABELE [1] am Beispiel einer hochzuverlässigen Energiebordnetz-Architektur für sicherheitsrelevante Verbraucher in Kraftfahrzeugen eine systematische Methodik. Für die Modellierung derartiger Systeme eignet sich vor allem der *Markov-Prozess*, da damit vielfältige Systemeigenschaften auf vergleichsweise einfache Weise abgebildet und in angemessener Art dargestellt und dokumentiert werden können. Zur Model-

lerstellung greift ABELE auf die bewährte Methode der *Fehlermöglichkeits- und Einflussanalyse* (*FMEA*) zurück und erweitert diese zur Berücksichtigung der Fehlerauswirkung auf unterschiedlichen Abstraktionsebenen des Systems. Mehrfachfehler, die bei fehlertoleranten Systemen während der quantitativen Bewertung stets betrachtet werden müssen, können bei dieser modifizierten FMEA mit Hilfe einer Fehlerkorrelationstabelle auch über mehrere Ebenen hinweg abgebildet werden.

3 Synthese und Vergleich von System-Architekturen

Im folgenden Kapitel werden verschiedene System-Architekturen für fehlertolerante Aktiv-Lenksysteme generiert und miteinander verglichen. Basis für deren Generierung bildet eine Zusammenfassung aller relevanten Anforderungen seitens der Gesetzgebung und des Kunden sowie eine grundlegende Gefahrenanalyse und Risikobewertung. Dies entspricht auf Systemebene den Schritten 1 bis 4 der in Kapitel 2.2.2 vorgestellten Vorgehensweise. Die Ergebnisse bilden die Basis für die Konzeptionierung eines Steer-by-Wire Systems in Kapitel 4 und die sicherheitstechnische Bewertung dessen (Schritt 5).

3.1 Anforderungen an Aktiv-Lenksysteme

Die Anforderungen, die beim Systementwurf eines Lenksystems berücksichtigt werden müssen, resultieren zum Einen aus der Gesetzgebung und aus Normen sowie zum Anderen von Seiten des Markts. Während in der Gesetzgebung und in den Normen vor allem die Basisanforderungen festgelegt sind, damit das Fahrzeug sicher gelenkt werden kann und von dem Lenksystem keine Gefahr ausgeht, beziehen sich die Marktanforderungen vor allem auf die Zusatzfunktionalitäten und die Zusatzeigenschaften, die von einer Lenkung erfüllt werden müssen. In diesem Zusammenhang kommt dem Begriff *»Sicherheit«* eine doppelte Bedeutung zu: Während es eine Grundvoraussetzung ist, dass das Lenksystem sicher ist und dass von diesem keine Gefahr ausgeht, so ist es trotzdem optional möglich die (Fahr-)Sicherheit des Traktors durch die Einführung von Funktionen wie einer variablen Lenkübersetzung oder Fahrstabilisierungssystemen mit Lenkeingriff zu erhöhen und sich bezüglich der Sicherheit von anderen Systemen abzuheben. Die nächsten Abschnitte

fassen die wesentlichsten Anforderungen für ein rein hydrostatisches Traktor-Lenksystem zusammen.

3.1.1 Gesetzgebung

Neben den bereits in Kapitel 2 genannten Normen und Richtlinien ISO 10998 und ECE-R 79 gibt es noch weitere europäische und nationale Dokumente, wie die Richtlinie 70/311/EWG oder der §38 der Straßenverkehrszulassungsordnung StVZO, die Anforderungen an ein Lenksystem stellen. Der Zusammenhang verschiedener nationaler und internationaler Zulassungsvorschriften ist in Abbildung 3.1 dargestellt. Seit der zweiten Revision der ECE-R 79 in 2005 werden auch Lenksysteme ohne mechanischen oder hydraulischen Durchgriff, wie beispielsweise rein elektrische Steer-by-Wire Systeme, von dieser Richtlinie abgedeckt [22]. In Ergänzung dazu wurde auch ein weiterer Anhang aufgenommen, der spezielle Vorschriften für die Sicherheitsaspekte komplexer elektronischer Fahrzeugsteuerungssysteme enthält. Die darin vorgeschriebenen Dokumente sind jedoch im Wesentlichen bereits in der Dokumentation enthalten, die durch die ISO 25119 hinsichtlich funktionaler Sicherheit vorgeschrieben ist.

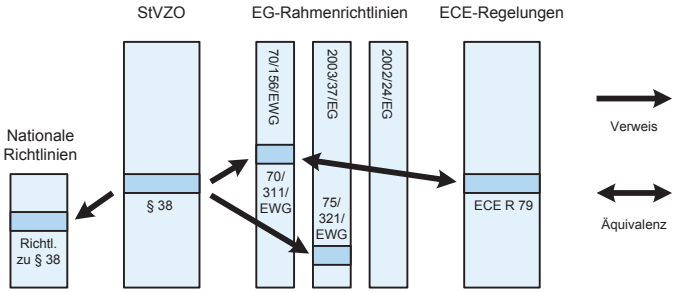


Abb. 3.1: Schematische Darstellung des Zusammenhangs verschiedener nationaler und internationaler Zulassungsvorschriften nach [20]

Für das Lenksystem eines Traktors ergeben sich aus den zuvor genannten Vorschriften für den Nominalfall die folgenden Basisanforderungen:

- Einfaches und sicheres Lenken: Bis zur bauartbedingten Höchstgeschwindigkeit muss das Fahrzeug sicher gelenkt werden können, ohne dass außergewöhnliche Vibrationen am Lenkrad auftreten. Eine Geradeausfahrt muss möglich sein, ohne dass außergewöhnlich große Korrekturbewegungen nötig sind.
- Geringe Betätigungskräfte: Das Lenken des Fahrzeugs entlang einer vorgegebenen Trajektorie muss möglich sein, ohne dass festgelegte Grenzwerte für die maximalen Betätigungskräfte am Lenkrad überschritten werden.
- Weg- und Zeitsynchronisation: Zwischen der Bewegung des Betätigungselements und den gelenkten Rädern muss Weg- und Zeitsynchronisation bestehen[1]. Aus diesem Grund sind Lenkanlagen, bei denen die Position des Betätigungselements proportional zur Geschwindigkeit der Lenkbewegung ist, nicht für die Straßenfahrt zugelassen. Derartige Lenksysteme werden häufig bei Radladern eingesetzt, die mit einem Joystick gelenkt und nicht auf öffentlichen Straßen verwendet werden.
- Lenkgeschwindigkeit: Die Einfahrt in eine stationäre Kreisfahrt mit einem festgelegten Radius muss auch bei geringster Motordrehzahl und maximal zulässiger Beladung des Fahrzeug innerhalb einer festgelegten Zeitdauer möglich sein.
- Rückstellverhalten: Nach dem Loslassen des Eingabegeräts während der stationären Kreisfahrt darf sich der Kreisradius nicht verkleinern. Im Idealfall sollten sich die Räder zurückstellen und der Kreisradius sollte sich dadurch vergrößern.

[1] Diese Anforderung muss bei Lenkanlagen mit einer korrigierenden Lenkfunktion nicht erfüllt werden.

Hinsichtlich der Sicherheit des Lenksystems werden darüber hinaus die folgenden Anforderungen gestellt:

- Absicherung gegen hohe Drücke: Hydrostatische Lenksysteme müssen durch Druckbegrenzungsventile gegen zu hohe Drücke abgesichert sein, die in der Hydraulikpumpe entstehen oder durch externe Lasten hervorgerufen werden können. Zudem müssen alle hydraulischen Schläuche und Leitungen auf das Vierfache des maximalen Nenndrucks ausgelegt sein.
- Störanfälligkeit: Die gelenkten Räder, die Betätigungseinrichtung sowie alle mechanischen Teile der Übertragungseinrichtung gelten als nicht störanfällig, wenn bestimmte Bedingungen wie ausreichende Dimensionierung und geeignete Materialwahl erfüllt werden.
- Definiertes Ausfallverhalten: Im Fehlerfall ist eine plötzliche Änderung des Lenkwinkels nicht zugelassen, Änderungen in der Lenkübersetzung jedoch schon.
- Fehlererkennung und Fahrerwarnung: Sämtliche Fehler in nicht-mechanischen Komponenten müssen durch das Lenksystem erkannt werden und dem Fahrer in geeigneter Weise angezeigt werden. Ein Anstieg der Betätigungskräfte als Fahrerwarnung ist ausreichend, wenn gewährleistet ist, dass die Betätigungskräfte den vorgegebenen Grenzwert nicht überschreiten. Eine Selbstdiagnose bei Systemstart ist erforderlich. Erst nach erfolgreicher Prüfung dürfen die Warnlampen erlöschen. Elektrisch angetriebene Notlenkpumpen müssen beim Starten der Maschine auf Funktionsfähigkeit überprüft werden.
- Fehlertoleranz: Das Lenksystem muss *einfehlersicher* sein, so dass die Lenkbarkeit auch nach Eintritt eines beliebigen Einzelfehlers gewährleistet ist. Dies gilt auch bei einem Ausfall des Verbrennungsmotors. Die Lenkbarkeit des Fahrzeugs muss aufrecht erhalten werden, solange sich das Fahrzeug bewegt.

- Priorisierung der Energieversorgung: Falls an der Energiequelle der Lenkanlage auch weitere Verbraucher angeschlossen sind, so muss gewährleistet sein, dass die Lenkanlage priorisiert mit Öl versorgt wird und eine dauerhaft vorliegende Undichtigkeit in einem Nebenverbraucher nicht zu einem Verlust der Lenkfähigkeit führen kann. Bei gemeinsam genutzter hydraulischer Energieversorgung muss angezeigt werden, wenn der Ölstand im Reservoir unter ein kritisches Level sinkt.

Handelt es sich bei dem Lenksystem um eine Fremdkraftlenkung entsprechend der Definition aus Kapitel 2, so gelten die folgenden Zusatzanforderungen:

- Fremdkraftquelle: Bei Fahrzeugen mit einer bauartbedingten Höchstgeschwindigkeit über 25 km/h muss eine weitere Fremdkraftquelle vorhanden sein, die bei einem Ausfall der ersten Fremdkraftquelle die Lenkbarkeit aufrecht erhält. Bei der Art der Energiequelle sind sowohl Druckspeicher als auch Hydraulikpumpen zulässig, falls die zweite Hydraulikpumpe ihre Energie von einer anderen Energieerzeugungsanlage als die erste bezieht.
- Sicherheitskonzept: Die Lenkanlage muss so beschaffen sein, dass nach Eintritt einer sicherheitsrelevanten Störung eine dauerhafte Weiterfahrt mit einer Geschwindigkeit über 10 km/h unterbunden wird. Nach einem Ausfall einer Energiequelle muss das Fahrzeug bei einer Geschwindigkeit von 10 km/h mindestens 25 *Achten* mit einem festgelegten Bahndurchmesser von 40 m fahren können.

3.1.2 Markt

Die Statistik der Einsatzverteilung eines Traktors in Abbildung 3.2 zeigt, dass ein Traktor zum größten Teil für Arbeiten auf dem Feld eingesetzt wird. Auf der anderen Seite ist jedoch auch der durchschnittliche Anteil

von mehr als 15 %, der auf Transportfahren mit Anhängern entfällt, nicht zu vernachlässigen und motiviert die Entwicklung von Komfort- und Sicherheitsfunktion für die Straßenfahrt. Im folgenden werden Funktionen und Eigenschaften aufgelistet, die seitens der Maschinenhersteller und Endkunden an ein Lenksystem gestellt werden, siehe unter anderem [14, 81, 96]. Selbstverständlich hängen sowohl die Funktionen als auch die Eigenschaften vom jeweiligen Maschinentyp und dem jeweiligen Einsatzgebiet ab und nicht alle der hier genannten Funktionen und Eigenschaften werden von heutigen Lenksystemen gleichermaßen erfüllt.

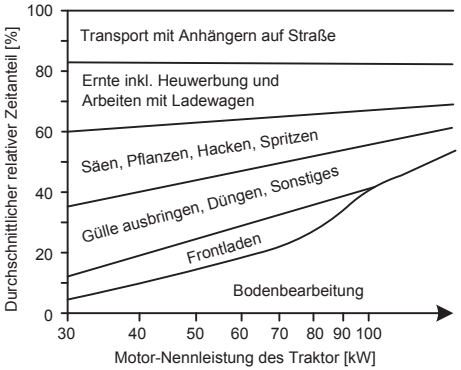


Abb. 3.2: Durchschnittliche Verteilung der Traktoreinsätze in West-Deutschland, geschätzt für Betriebsgrößen von 50-100 ha, ausgenommen Lohnunternehmer und Betriebe mit hohem permanenten Grünlandanteil nach [75]

Funktionen:

- Automatische Lenkfunktion: Durch eine automatische Lenkfunktion ist es möglich, den Kurs des Fahrzeugs unabhängig von der Fahrervorgabe verändern zu können und damit eine automatische Spurführung zu realisieren.
- Rückfahrbetrieb: Bei Fahrzeugen mit drehbarem Fahrersitz oder drehbarer Kabine muss die Betätigungseinrichtung auch im Rückfahrbetrieb komfortabel erreichbar sein.

- Variable Lenkübersetzung: Durch eine Anpassung der Lenkübersetzung an die jeweilige Fahrgeschwindigkeit und Arbeitsaufgabe kann erreicht werden, dass sowohl ein Rangieren und Wenden ohne große Betätigungswege als auch ein komfortables und feinfühliges Fahren bei hohen Geschwindigkeiten möglich ist.
- Alternative Eingabegeräte: Je nach Art und Gestaltung des Fahrzeugs und der Kabine ist es vorteilhaft, wenn das Fahrzeug auch über alternative Eingabegeräte, wie einen Joystick, gelenkt werden kann. Dies gilt in besonderem Maße, wenn der Fahrersitz drehbar ist.
- Fahrstabilisierung: Durch ein Fahrassistenzsystem (korrigierende Lenkfunktion) kann die Fahrsicherheit erhöht werden, indem eine Unter- oder Übersteuerneigung des Traktors durch Sensorik erkannt und durch entsprechende Lenkkorrekturen kompensiert wird.
- Autonome Lenkfunktion: Für Anwendungen, bei denen ein Traktor einem Führungsfahrzeug fahrerlos folgen soll, muss im Lenksystem eine Schnittstelle existieren, über die außerhalb des Fahrzeugs generierte Lenkbefehle aufgenommen und in eine Lenkbewegung umgewandelt werden können.

Eigenschaften:

- Lenkgeschwindigkeit: Für das schnelle Wenden und Rangieren am Feldende ist eine gewisse Lenkgeschwindigkeit erforderlich. Für konventionelle Lenksysteme gilt die Anzahl der notwendigen Lenkraddrehungen von einem bis zum anderen Anschlag als Maß dafür, wie schnell am Feldende rangiert werden kann.
- Feinsteuerbarkeit: Zur Erreichung der notwendigen Feinfühligkeit der Lenkung, vor allem bei hohen Fahrgeschwindigkeiten, ist eine gewisse Feinsteuerbarkeit des Volumenstroms notwendig. Durch die Feinsteuerbarkeit wird das sichere Lenken des Fahrzeugs gewährleistet.

- Dynamisches Verhalten: Bei schnellen Änderungen am Betätigungselement ist ein gutes Ansprechverhalten ohne Ansprechverzögerung oder Nachlauf gewünscht.
- Geradeauslauf: Das Erreichen eines optimalen Geradeauslaufs, vergleichbar mit dem von Kraftfahrzeugen, ist bei hydrostatischen Lenksystemen erschwert, da keine mechanische Verbindung zwischen dem Lenkrad und den gelenkten Rädern existiert und die Auslenkung der Räder durch Leckage, Ölkompressibilität und externe Lasten gestört wird.
- Kraft- und Positionsrückmeldung: Eine optimale Rückmeldung der Lenkkräfte und des Lenkwinkels an den Fahrer führt zu einem hohen Fahrkomfort und bei hohen Fahrgeschwindigkeiten zu mehr Fahrsicherheit.

Sonstige Anforderungen:

- Bauraumbedarf und Platzierbarkeit der Komponenten: Durch den Wegfall der mechanischen Verbindung zwischen Lenkrad und gelenkten Rädern bei rein hydrostatischen Lenksystemen hat der Maschinenhersteller viele Gestaltungsfreiheiten. Für die Komponenten der hydrostatischen Lenkung ist es entscheidend, wie viel Bauraum diese in Anspruch nehmen und wo diese platziert werden müssen.
- Kompatibilität zur Arbeitshydraulik: Wenn das hydrostatische Lenksystem kompatibel zum bestehenden Hydrauliksystem ist, können Komponenten und damit Bauraum und Kosten gespart werden. Hat das Aktiv-Lenksystem die gleichen Schnittstellen wie das konventionelle Lenksystem, dann kann dieses zudem als Option angeboten werden.
- Komplexität und Kosten: Eine geringe Komplexität des Lenksystems reduziert den Komponentenaufwand und damit die Kosten. Zudem reduziert sich in vielen Fällen gleichermaßen die Fehleranfälligkeit.

3.1.3 Fazit

Die Zusammenstellung der Anforderungen verdeutlicht, dass die Anforderungen an Lenksysteme für Traktoren anders sind als die Anforderungen an das Lenksystem eines Kraft- oder Nutzfahrzeugs. Vor allem der große und spezielle Funktionsumfang sowie die starke Verzahnung mit den Arbeitsfunktionen des Traktors über die zentrale Hydraulikversorgung führen zu anderen Architekturen und Lösungen als im Automobilbereich. Bei der Realisierung der Zusatzfunktionen ist darauf zu achten, dass die Systemkomplexität und damit auch die Fehleranfälligkeit nicht unnötig stark ansteigt.

3.2 Analyse der Betrachtungseinheit

Vor der Durchführung der Gefahrenanalyse und Risikobewertung ist eine möglichst präzise Beschreibung und Abgrenzung der Betrachtungseinheit notwendig (Schritt 1[2]). Anschließend können die Gefahren systematisch aus den Funktionen des Lenksystems abgeleitet werden (Schritt 2). Die Risikobewertung erfolgt auf Basis des Risikographen der ISO 25119 und durch modellbasierte Untersuchungen an einem Simulationsmodell, das die Fahrdynamik eines Traktors abbildet. Die in diesem Abschnitt vorgestellten Ergebnisse bewerten die Gefahren eines Aktiv-Lenksystems auf Maschinenebene und gelten gleichermaßen sowohl für Überlagerungslenkungen als auch für Steer-by-Wire Systeme. Die Schritte 3 und 4 werden in Kapitel 3.3.2 bearbeitet.

3.2.1 Beschreibung der Betrachtungseinheit

Um die Systemkomplexität handhabbar zu halten und eine Risikobewertung durchführen zu können, erfolgt in diesem Schritt eine Zusammenfassung beziehungsweise Relativierung und Vernachlässigung einiger Funktionen.

[2] Siehe Vorgehensweise in Kapitel 2.2.2.

Die automatische, die autonome und die korrigierende Lenkfunktion werden zusammengefasst und als Schnittstellengröße *»Lenkbefehle«* betrachtet. Die für die variable Lenkübersetzung benötigte Fahrzeuggeschwindigkeit sowie die für den Rückfahrbetrieb nötige Information über die Orientierung von Sitz oder Kabine ist ebenfalls eine Schnittstellengröße. Alternative Eingabegeräte können ohne eine genaue Kenntnis über deren Gestaltung, Anordnung und Funktionalität im Rahmen einer Gefahrenanalyse auf Konzeptebene nicht berücksichtigt werden. Dies ist dadurch begründet, dass es beispielsweise von der Position und Art der Aktivierung eines Joysticks abhängt, welche Fehlbedienungen und daraus resultierende Gefahren auftreten können. Darüber hinaus können auch Gefahren durch die Verwendung des Joysticks an sich entstehen, wenn beispielsweise der Fahrer nicht an die Fahrt mit einem derartigen Eingabegerät gewöhnt ist. Insgesamt führt ein zweites Eingabegerät zu einem deutlichen Anstieg der Systemkomplexität und damit auch der Anfälligkeit für Fehler und Fehlbedienungen, da die möglichen Übergangsszenarien zwischen dem Lenkrad und dem alternativen Eingabegerät unter Annahme eines gewissen Fahrerverhaltens in Normal- und Schrecksituationen festgelegt werden müssen.

Das in Abbildung 3.3 dargestellte Lenksystem stellt die Betrachtungseinheit für die folgende Gefahrenanalyse und Risikobewertung dar. Betrachtet wird ein rein hydrostatisches Aktiv-Lenksystem mit einem Lenkrad als Betätigungseinrichtung. Der vom Fahrer vorgegebene Lenkradwinkel (Schnittstelle zum Fahrer) wird je nach Fahrsituation durch das Lenksystem in einen gewünschten Radlenkwinkel umgerechnet und durch einen Regler am Rad eingestellt. Die Räder lassen sich für die Realisierung einer automatischen Lenkfunktion auch unabhängig von der Fahrervorgabe verstellen. Durch die Regelung des Radlenkwinkels werden viele Störungen, die auf das Lenksystem an der Schnittstelle zur Umgebung einwirken, ausgeregelt und der Geradeauslauf entscheidend verbessert [72]. An der Schnittstelle zum Fahrzeug werden neben Energie und Stoff vor allem Informationen ausgetauscht.

Während die Signale der korrigierenden Lenkfunktion additiv dem Fahrerwunsch überlagert werden, werden die Signale der automatischen und autonomen Lenkfunktion nur ausgewertet, wenn der Fahrer aktiv in den jeweiligen Betriebsmodus wechselt. Die Information über den Zustand der Lenkung (fehlerfrei oder gestörter Betrieb) ist eine Information, die vom Lenksystem an das Fahrzeug übertragen wird. Am Lenkrad wird dem Fahrer eine Kraft zurückgemeldet, die Aufschluss über den aktuellen Lenkzustand liefert. Das Lenksystem muss auch nach dem Auftreten eines beliebigen Einzelfehlers die Lenkfähigkeit entsprechend der gesetzlichen Anforderungen gewährleisten. Die zuvor genannten Zusatzfunktionen, wie die variable Lenkübersetzung oder die automatische Spurführung, müssen in diesem Fall jedoch nicht zwangsläufig aufrecht erhalten werden. Für diese ist daher eine fail-safe Auslegung ausreichend.

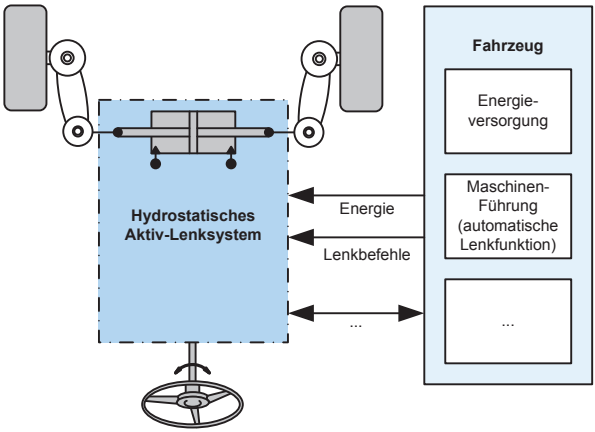


Abb. 3.3: Schematische Darstellung der Betrachtungseinheit und dessen Schnittstellen zum Fahrer, zum Fahrzeug und zur Umgebung

3.2.2 Gefahrenanalyse

Bei der Ableitung der Gefahren, die von dem oben beschriebenen Lenksystem ausgehen, ist es vorteilhaft, dessen Grundfunktionen zu betrachten. Da für die Bewertung der Gefahren keine Kenntnis über die genaue Ursache des Fehlers erforderlich ist, muss die interne Struktur des Aktiv-Lenksystems nicht näher spezifiziert werden. Im Folgenden werden die Fehlfunktionen beziehungsweise Gefahren aus den Top-Level-Funktionen an den jeweiligen Schnittstellen abgeleitet und bedarfsgerecht weiter herunter gebrochen. Sämtliche zur Produktsicherheit gehörenden Gefahren wie *»elektrischer Schlag«* oder *»heiße Bauteile«* werden an dieser Stelle nicht betrachtet. Zudem werden auch solche Gefahren nicht betrachtet, die von dem Traktor an sich ausgehen und nicht mit einer Fehlfunktion der Lenkung verknüpft sind, wie beispielsweise das Anfahren einer Person beim Wenden.

- Funktion 1: Räder entsprechend der Fahrervorgabe verstellen
  ⇒ Fehlfunktion 1: Räder verstellen sich nicht entsprechend der Fahrervorgabe
  ⇒ Gefahr 1.1: Die Räder verstellen sich selbstständig und folgen nicht mehr dem Fahrerwunsch. Dadurch verliert der Fahrer die Kontrolle über das Fahrzeug. Im Stand kann eine selbstständige Lenkbewegung der Räder die Personen, die sich im Umfeld der Räder aufhalten, verletzen oder einquetschen.
  ⇒ Gefahr 1.2: Die Räder können nicht mehr verstellt werden[3]. In diesem Gefahrenfall verliert der Fahrer ebenfalls die Kontrolle über das Fahrzeug.
- Funktion 2: Rückmeldung von Kraft am Lenkrad
  ⇒ Fehlfunktion 2: Falsche Kraft wird zurückgemeldet
  ⇒ Gefahr 2: Durch einen Fehler bei der Kraftrückmeldung verliert

[3] Verglichen mit anderen Anwendungen ist der Stillstand des Aktors während der Fahrt bei einem Lenksystem kein sicherer Zustand.

der Fahrer das Gefühl über den aktuellen Lenkzustand und damit schlimmstenfalls die Kontrolle über das Fahrzeug.

- Funktion 3: Informationsübertragung zwischen Lenksystem und Fahrzeug[4]
  ⇒ Fehlfunktion 3: Falsche Informationen werden ausgetauscht
  ⇒ Gefahr 3.1: Durch eine falsch übermittelte Fahrzeuggeschwindigkeit oder falsche Signale der korrigierenden Lenkfunktion wird ein falscher Sollwert für den Radlenkwinkel berechnet[5].
  ⇒ Gefahr 3.2: Durch einen falsch übermittelten Fehlerstatus wird fälschlicherweise eine Drosselung der Fahrgeschwindigkeit eingeleitet[6].

- Funktion 4: Eine automatische oder autonome Verstellung der Räder für die Feldbearbeitung ermöglichen
  ⇒ Missbräuchliche Fehlbedienung/Gefahr 4: Verwendung einer automatischen oder autonomen Lenkfunktion während der Straßenfahrt. Eine Verwendung während der Straßenfahrt ist nicht zugelassen, da der Fahrer nicht die Kontrolle über das Fahrzeug hat.

3.2.3 Risikobewertung

Im Folgenden werden die zuvor genannten Gefahren und Fehlfunktionen näher betrachtet, um eine Risikobewertung durchführen zu können. Die Bewertung erfolgt dabei qualitativ und ohne die Festlegung eines bestimmten

[4] Fehler bei der Energie- und Stoffübertragung führen zu Gefahren, die bereits in den Gefahren 1.1 und 1.2 enthalten sind.

[5] Diese Gefahr kann in einer selbstständigen Lenkbewegung resultieren, die bereits durch Gefahr 1.1 abgedeckt ist.

[6] Die Drosselung der Fahrgeschwindigkeit sollte langsam erfolgen, damit ein Auffahren von nachfolgenden Fahrzeugen ausgeschlossen werden kann. Dieser Fall stellt unter diesen Bedingungen keine Gefahr dar, da keine Verletzung von Personen zu erwarten ist. Die Drosselung ist notwendig, um das Fahrzeug in einen sicheren Zustand zu überführen.

»AgPL«, da dieser nur dann bestimmt werden kann, wenn das konkrete Fahrzeug und damit auch die vom System ausgehenden Gefahren bekannt sind. Wesentliche Einflussfaktoren sind dabei die Maximalgeschwindigkeit des Fahrzeugs, dessen Gierdynamik sowie die maximal erreichbare Geschwindigkeit des Lenkzylinders.

Zur Funktion 4 wurden keine technischen Fehlfunktionen aufgelistet, da der Fahrer stets die Verantwortung der Fahrzeugführung hat und im Falle eines Fehlers durch eine Lenkbewegung die automatische Spurführung deaktivieren kann. In der ISO-Norm 10975 [41] sind dafür einige Anforderungen aufgelistet, wann und wie der Fahrer die Kontrolle über das Fahrzeug zurückerlangen kann. Da dort ebenfalls festgelegt ist, dass im Handbuch darauf hingewiesen werden soll, dass automatische Lenkfunktionen nicht auf öffentlichen Straßen verwendet werden dürfen, wird die Gefahr 4 nicht weiter betrachtet.

Für die genaue Bewertung von Gefahr 2 sind detailliertere Kenntnisse über die Art und Weise der Kraftrückwirkung und der Fahrerreaktion erforderlich. Bei rein hydrostatischen Überlagerungslenkungen ist die vom Fahrer spürbare Kraft eine Reaktionskraft, die von dem Konstruktionsprinzip des hydrostatischen Lenkventils und der Unterstützungswirkung durch die Hydraulikpumpe abhängig ist. Sprünge in dieser Kraft treten beispielsweise dann auf, wenn die Hydraulikpumpe und damit die Servounterstützung wegfällt. In diesem Fall ist die notwendige Betätigungskraft um ein Vielfaches höher als im nominalen Betriebszustand. Bei allen am Markt befindlichen Lenksystemen wird dieses Ausfallverhalten toleriert, wenn die gesetzlich vorgeschriebenen Maximalkräfte nicht überschritten werden. Im Steer-by-Wire System wird das Lenkmoment von einem Handkraftaktor entsprechend der Vorgabe eines Steuergeräts generiert, der entweder aktiv, semiaktiv oder passiv sein kann. Passive und semiaktive Systeme setzen der Lenkbewegung des Fahrers beispielsweise über einen passiven Dämpfer oder eine aktive Lenkradbremse eine bestimmte Kraft entgegen. Eine selbstständige Drehung

des Lenkrads kann jedoch nicht erzeugt werden. Der komplette Wegfall oder die vollständige Aktivierung des Bremsmoments sind dabei die beiden schlimmsten Fehlerfälle. Aktive Systeme verwenden in der Regel einen elektrischen Motor, um ein Lenkmoment auch bei Stillstand des Lenkrads erzeugen zu können. Zusätzlich zu den bereits genannten Fehlerfällen ist daher auch ein Anlaufen des Lenkrads möglich, falls der Fahrer das Lenkrad nicht fest genug in der Hand hält.

Für ein hydrostatisches Aktiv-Lenksystem stellen die Gefahren 1.1 und 1.2 mit Abstand das höchste Gefahrenpotential dar. Dabei ist eine nicht kontrollierbare Lenkbewegung (Gefahr 1.1) kritischer als nicht mehr verstellbare Räder (Gefahr 1.2). In beiden Fällen sind bei der Feldbearbeitung, vor allem jedoch bei der Straßenfahrt, schlimmste Verletzungen zu erwarten, da das nicht mehr lenkbare Fahrzeug mit anderen Verkehrsteilnehmern kollidieren oder von der Straße abkommen kann (Kriterium *»Schwere der Verletzung«*). Je nach Einsatzbereich des Traktors (siehe Abbildung 3.2) befindet sich der Fahrer häufig in einer Situation, in der ein derartiger Fehler gefahrbringend sein kann (Kriterium *»Exposition in Situation«*). Befindet sich der Fahrer in einer solchen Situation und tritt die Gefahr tatsächlich ein, so bleiben dem Fahrer und anderen beteiligten Personen nur wenig Möglichkeiten zur Reaktion (Kriterium *»Kontrollierbarkeit der Situation«*). Der Fahrer des Traktors kann lediglich einen Bremsvorgang einleiten, andere beteiligte Verkehrsteilnehmer können zudem ausweichen. Um die Wirksamkeit eines Bremseingriffs in solchen Gefahrensituationen besser einschätzen zu können, wird im Folgenden das Simulationsmodell eines Traktors verwendet, das in [60] näher beschrieben ist und mit Hilfe von Messungen der Quer- und Längsdynamik validiert wurde. In diesem Modell ist die Kinematik und Dynamik der Traktorbewegung über ein Mehrkörpersimulationsmodell des Rumpfes und der Vorderachsfederung abgebildet. Der für ein Simulationsmodell wichtige Fahrzeug-Boden-Kontakt wird durch das *»Hohenheimer Reifenmodell«* abgebildet [25]. Die folgenden Ergebnisse dienen lediglich einer

ersten Einschätzung der Wirksamkeit eines Fahrereingriffs und können detailliertere Untersuchungen sowie experimentelle Probandenversuche nicht ersetzen, insbesondere, da die notwendigen Annahmen zur Reaktion des Fahrers am Bremspedal mit einer großen Unsicherheit behaftet sind.

Für die beiden Gefahren wurden die folgenden Annahmen und Randbedingungen für die Simulation getroffen:

- Fahrzeug: Das Fahrzeug hat ein Leergewicht von 6770 kg, eine Maximalgeschwindigkeit von 50 km/h und eine Motornennleistung von 145 kW (197 PS). Das Fahrzeug ist mit einem ABS ausgestattet[7].

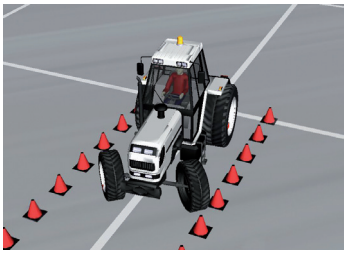
- Randbedingungen: Der Traktor fährt auf einer geraden Strecke beziehungsweise in eine Kurve mit einem Radius von 80 m ein. Die Simulation erfolgt bei unterschiedlichen Fahrzeuggeschwindigkeiten.

- Annahmen für Gefahr 1.1 (Ausschlag der Räder): Die Räder bewegen sich mit der maximalen Lenkgeschwindigkeit bis zum Anschlag. Es wird die Annahme getroffen, dass der Fahrer durch die von der plötzlichen Radbewegung ausgelösten Änderung des Fahrzustands nach einer Sekunde eine reflexartige Vollbremsung auslöst.

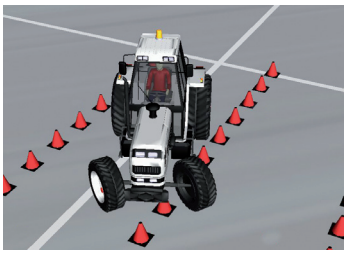
- Annahmen für Gefahr 1.2 (Blockieren der Lenkbewegung der Räder): Es wird davon ausgegangen, dass der Fahrer auch bei einer Geradeausfahrt von Zeit zu Zeit Lenkkorrekturen durchführt und ein Blockieren der Lenkbewegung der Räder innerhalb von 2,5 Sekunden erkennt und einen Bremsvorgang einleitet. Falls das Fahrzeug zuvor bereits eine Fahrbahnmarkierung überschritten hat, wird der Fahrer ebenfalls den Bremsvorgang einleiten. Für die Geradeausfahrt wird angenommen, dass sich das Fahrzeug vor Eintritt des Fehlers am rechten Rand des eigenen Fahrstreifens befindet und leicht nach links lenkt.

[7] Die Annahme des Vorhandenseins eines ABS stellt eine Abschätzung zur sicheren Seite dar, da in diesem Fall das Fahrzeug trotz starker Verzögerungen den fehlerhaft eingeprägten Lenkbewegungen folgen kann.

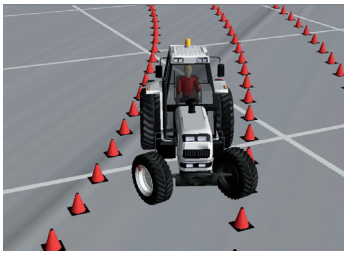
Abbildung 3.4 zeigt die Simulationsergebnisse für die Geradeaus- und Kurvenfahrt bei einer Fahrgeschwindigkeit von 5 beziehungsweise 10 km/h. In der jeweiligen Abbildung ist die Position dargestellt, in der der Traktor nach dem Bremsvorgang zum Stillstand kommt. Die Ergebnisse verdeutlichen, dass der Traktor bei ausschlagenden Rädern selbst bei niedrigen Geschwindigkeiten von 10 km/h teilweise in die Gegenfahrbahn eindringt. Bei höheren Geschwindigkeiten verlässt das Fahrzeug die gesamte Fahrbahn, ab einer Geschwindigkeit von 30 km/h hebt sogar das kurveninnere Hinterrad von der Fahrbahn ab und es besteht die Gefahr, dass der Traktor umkippt. Diese qualitativen Ergebnisse verdeutlichen, dass die von einem derartigen Fehlerfall ausgehende Gefahr durch einen Bremseingriff im üblichen Geschwindigkeitsbereich nicht nennenswert reduziert werden kann.



(a) Geradeausfahrt - 5 km/h



(b) Geradeausfahrt - 10 km/h

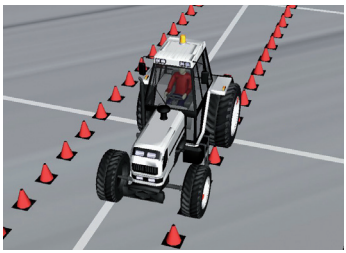


(c) Kurvenfahrt - 5 km/h

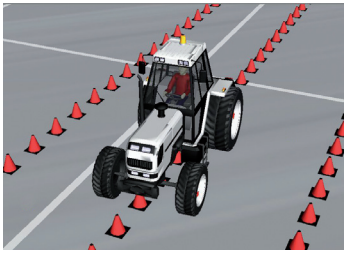
(d) Kurvenfahrt - 10 km/h

Abb. 3.4: Stillstandsposition des Traktors nach Einleitung der Gefahr 1.1 im Simulationsmodell für unterschiedliche Fahrzeuggeschwindigkeiten

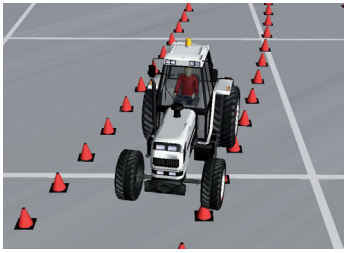
Die Simulationsergebnisse für den Fall der blockierten Lenkung sind in Abbildung 3.5 dargestellt. Die Ergebnisse bei einer Fahrzeuggeschwindigkeit von 30 km/h deuten darauf hin, dass für diesen Fall das Gefahrenpotential der blockierten Lenkung durch einen rechtzeitigen Bremseingriff wirkungsvoll reduziert werden kann, da das Fahrzeug bei dieser Geschwindigkeit auf dem eigenen Fahrstreifen zum Stillstand kommt. Bei höheren Geschwindigkeiten dringt das Fahrzeug in den Verkehrsraum der anderen Verkehrsteilnehmer ein, so dass diese dem Traktor ausweichen müssen, um einen Unfall zu verhindern oder abzumildern. Die Schwere der zu erwartenden Verletzungen kann daher bei diesen Geschwindigkeiten nur bedingt durch einen Bremseingriff reduziert werden.



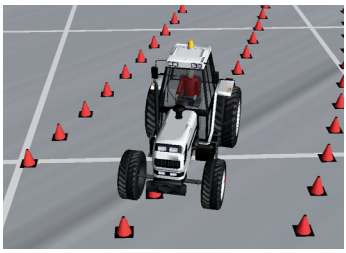
(a) Geradeausfahrt - 30 km/h



(b) Geradeausfahrt - 40 km/h



(c) Kurvenfahrt - 30 km/h



(d) Kurvenfahrt - 40 km/h

Abb. 3.5: Stillstandsposition des Traktors nach Einleitung der Gefahr 1.2 im Simulationsmodell für unterschiedliche Fahrzeuggeschwindigkeiten

Die dargestellten Ergebnisse decken sich bezüglich der Größenordnung mit den Forderungen der Lenkungsrichtlinie ECE-R 79 für Fremdkraftlenkanlagen [22]: Danach wird eine dauerhafte Weiterfahrt im Falle eines Einzelfehlers für Geschwindigkeiten unter 10 km/h nicht untersagt. Bei Weiterfahrt ist der Eintritt von Gefahr 1.1 möglich. Die Simulationsergebnisse deuten an, dass ein Fahrzeug bei einer derartigen Geschwindigkeit sicher zum Stillstand gebracht werden kann, ohne den Gegenverkehr oder andere Verkehrsteilnehmer zu gefährden. Die Lenkungsrichtlinie legt zudem fest, dass eine zweite Fremdkraftquelle nur für Fahrzeuge mit einer bauartbedingten Höchstgeschwindigkeit über 25 km/h notwendig ist. Bei Fahrzeugen mit nur einer Fremdkraftquelle ist bei einem Ausfall dieser die Lenkbarkeit nicht mehr möglich (Gefahr 1.2). Auch hier deuten die Simulationsergebnisse an, dass ein Ausfall der Lenkbarkeit bei dieser Geschwindigkeit durch ein vom Fahrer eingeleitetes Bremsmanöver kontrolliert werden kann. Für die Risikobewertung eines konkreten Fahrzeugs muss detaillierter geprüft werden, welche Geschwindigkeit im Falle welchen Fehlers als vom Fahrer kontrollierbar angesehen werden kann. Neben den hier dargestellten Manövern mit dauerhaften Fehlern wurden auch temporäre Fehler entsprechend der Gefahren 1.1 und 1.2 untersucht. Dabei wurde der Zeitraum bestimmt, innerhalb derer der Fehler erkannt, diagnostiziert und kompensiert sein muss, so dass der Fahrer anschließend das Fahrzeug wieder kontrolliert lenken kann. Für die Gefahr 1.1 liegt dieser Zeitraum bei einer pessimistischen Annahme zu der Kompensationsfähigkeit des Fahrers in der Größenordnung zwischen 10 und 100 ms, für die Gefahr 1.2 eine Größenordnung darüber (zwischen 100 und 1000 ms).

3.2.4 Sicherheitsziele und Zusammenfassung

Basierend auf den zuvor ermittelten Gefahren ergeben sich die folgenden Sicherheitsziele:

- Sicherheitsziel 1.1:
  Verhindern, dass die Räder maximal 10 - 100 ms unkontrolliert ausschlagen
- Sicherheitsziel 1.2:
  Verhindern, dass sich die Räder maximal 100 - 1000 ms nicht verstellen lassen
- Sicherheitsziel 2:
  Verhindern, dass sich die Lenkradposition oder -kraft plötzlich zu stark ändert[8]
- Sicherheitsziel 3:
  Verhindern, dass falsche Werte vom Fahrzeug zum Lenksystem übertragen werden beziehungsweise verhindern, dass durch falsche Werte das Sicherheitsziel 1.1 oder 1.2 verletzt wird

Die Ergebnisse der Gefahrenanalyse und Risikobewertung für die Hauptfunktion 1 sind zusammenfassend in Tabelle 3.1 dargestellt. Die Bewertung der einzelnen Szenarien ist dabei rein qualitativ und dient primär dem relativen Vergleich der verschiedenen Situationen. Die absolute Bewertung und die Zuordnung eines Performancelevels zu den Gefahren muss für das konkrete Fahrzeug erfolgen. Der Ausschlag der Räder während der Straßenfahrt stellt die größte Gefahr dar, da schwerste Verletzungen zu erwarten sind, der Fahrer sich je nach Einsatzbereich des Traktors häufig auf Transportfahrten befindet und die Möglichkeit der Kontrollierbarkeit der Situation quasi nicht gegeben ist. In Situationen außerhalb öffentlicher Straßen, wie beispielsweise bei der Feldbearbeitung, sind die Fahrgeschwindigkeiten in der Regel niedriger, so dass die Schwere der zu erwartenden Verletzungen ebenfalls niedriger ist. Darüber hinaus ist die Wahrscheinlichkeit geringer, dass sich der Traktor in direktem Umfeld zu anderen Personen oder Maschinen befindet.

[8] Dieses Sicherheitsziel muss für die jeweilige Anwendung konkretisiert und quantifiziert werden.

Nr.	Gefährdung	Risikoszenario / Fahrsituation	Mögliche Konsequenzen	Risikobewertung			Sicherheitsziel
				Schwere der Verletzung	Exposition in Szenario	Kontrollierbarkeit der Situation	
1	1.1 Ausschlag der Räder	On-road - Fehler in Hauptlenkanlage oder korrigierender Lenkfunktion	Fahrzeug kommt von Straße ab oder kommt in Gegenverkehr: Umkippen, Zusammenstoß mit Fahrzeugen oder Personen	✓✓✓	✓✓✓	✓✓✓	Verhindern, dass die Räder maximal 10 - 100 ms unkontrolliert lenken
2		Off-road - Fehler in Hauptlenkanlage oder korrigierender Lenkfunktion	Fahrzeug verlässt gewünschte Fahrspur: Umkippen (am Hang), Zusammenstoß mit anderen Maschinen oder Personen	✓✓	✓✓	✓✓✓	
3		Off-road - Fehler in automatischer Lenkfunktion	Fahrzeug verlässt Fahrspur: Umkippen (am Hang), Zusammenstoß mit anderen Maschinen oder Personen				
4		Person steht im Stand des Fahrzeugs in der Nähe der Räder - Fehler in Hauptlenkanlage oder korrigierender Lenkfunktion	Quetschen, Stoßen, Stolpern	✓	✓	✓	
5	1.2 Blockierung der Lenkbewegung	On-road mit sehr hoher Geschwindigkeit - Fehler in Hauptlenkanlage oder korrigierender Lenkfunktion	Fahrzeug kommt von Straße ab oder kommt in Gegenverkehr: Umkippen, Zusammenstoß mit Fahrzeugen oder Personen	✓✓✓	✓✓	✓✓✓	Verhindern, dass sich die Räder maximal 100 - 1000 ms nicht lenken lassen
6		On-road mit mittlerer oder niedriger Geschwindigkeit - Fehler in Hauptlenkanlage oder korrigierender Lenkfunktion		✓✓	✓✓✓	✓✓	
7		Off-road	Fahrzeug verlässt gewünschte Fahrspur: Umkippen (am Hang), Zusammenstoß mit anderen Maschinen oder Personen	✓✓	✓✓	✓	

✓ niedrig
✓✓ mittel
✓✓✓ hoch

✓ niedrig
✓✓ mittel
✓✓✓ hoch

✓ hoch
✓✓ mittel
✓✓✓ niedrig

Tab. 3.1: Gefahrenanalyse und Risikobewertung für die Hauptfunktion 1 des betrachteten Aktiv-Lenksystems

Liegt die Ursache des Lenkausschlags in der Hauptlenkanlage oder der korrigierenden Lenkfunktion, so ist die Situation für den Fahrer nicht kontrollierbar. Demgegenüber kann der Fahrer das Fahrzeug einfach unter Kontrolle bringen, wenn der Lenkausschlag durch einen Fehler in der automatischen Lenkung verursacht wurde, da in diesem Fall die Hauptlenkanlage weiterhin funktionsfähig ist. Verhältnismäßig ungefährlich ist ein unmotivierter Lenkausschlag, wenn sich das Fahrzeug im Stillstand befindet.

Für die Gefahr 1.2 wurde das Szenario Straßenfahrt in zwei Geschwindigkeitsbereiche aufgeteilt, um durch eine differenzierte Bewertung der Parameter zum Ausdruck zu bringen, dass diese Gefahr weniger kritisch ist als Gefahr 1.1. Eine derartige Aufteilung ist zulässig, wenn gewährleistet ist, dass dadurch keine unzulässige Erniedrigung der Risikoeinstufung resultiert [43][9]. Im vorliegenden Fall ist die Schwere der zu erwartenden Verletzungen bei hohen Geschwindigkeiten sehr hoch und die Möglichkeiten zur Vermeidung oder Abschwächung des Verletzungsrisikos sehr niedrig, der Anteil der Straßenfahrt mit sehr hohen Geschwindigkeiten an der Gesamtnutzungsdauer eines Traktors jedoch nicht so hoch wie der allgemeine Anteil der Straßenfahrt an der Gesamtnutzungsdauer[10]. Wesentlich häufiger ist der Traktor mit mittleren Geschwindigkeiten unterwegs, in welchem Fall die Schwere der zu erwartenden Verletzungen geringer und die Möglichkeiten zur Vermeidung einer Gefährdung wesentlich größer sind. In allen off-road Szenarien ist der Anteil der Situationen in denen eine blockierte Lenkung gefährlich sein kann moderat und die Möglichkeiten zur Reaktion für den Fahrer und andere beteiligte Personen vergleichsweise groß.

Beispiele für eine quantitative Risikobewertung der Lenksysteme von mobilen Arbeitsmaschinen liefern [14, 73, 79]. Demnach wird die Gefahr 1.1 für

[9] Dies wäre beispielsweise dann der Fall, wenn ein Szenario fein aufgeteilt wird, um den Parameter *»Exposition in Situation«* zu reduzieren, ohne dass die anderen beiden Parameter für die verschiedenen Subszenarien unterschiedlich bewertet werden.

[10] Der Anhaltspunkt für eine Herabstufung dieses Parameters ist laut ISO 25119 [42] ein Anteil von 10 % oder weniger an der Gesamtnutzungsdauer.

off-road Anwendungen mit dem *»AgPL d«* beziehungsweise dem quantitativ vergleichbaren *»SIL 2«* eingestuft [73, 79]. In Anwendungen, die für die Verwendung auf öffentlichen Straßen über 6 km/h vorgesehen sind, wird die Einstufung mit *»SIL 3«* (quantitativ vergleichbar mit *»AgPL e«*) als notwendig erachtet [14, 73].

3.3 Synthese von Systemarchitekturen

Die Generierung verschiedener Systemarchitekturen für hydrostatische Aktivlenksysteme erfolgt durch die systematische Betrachtung des kompletten Lösungsraums, um verschiedenartige Prinziplösungen systematisch zu erfassen. Anschließend erfolgt eine Auswahl einzelner vorteilhafter Lösungen für den Entwurf des Sicherheitskonzepts und die weitere Ausgestaltung der Architekturen. Bei der Ausgestaltung müssen die zuvor ermittelten Gefahren berücksichtigt werden.

3.3.1 Lösungsraum

Entsprechend der in Kapitel 2.1.2 erläuterten Klassifikation können hydrostatische Aktivlenksysteme in Überlagerungslenkungen und Steer-by-Wire Systeme untergliedert werden. Bei den Überlagerungslenkungen ist prinzipbedingt sowohl eine Überlagerung auf hydraulischer als auch auf mechanischer Seite möglich, siehe Abbildung 3.6. Bei den Steer-by-Wire Systemen lässt sich unterscheiden, ob die einzelnen Kanäle diversitär oder nicht diversitär realisiert sind. Sowohl bei den Überlagerungslenkungen als auch bei den Steer-by-Wire Systemen lässt sich unterscheiden, ob zur Erzeugung einer Lenkbewegung eine bereits vorhandene Energie einer Energiequelle verteilt (Drosselsteuerung) oder die notwendige Energie bedarfsgerecht gewandelt und direkt dem Verbraucher zugeführt wird (Verdrängersteuerung).

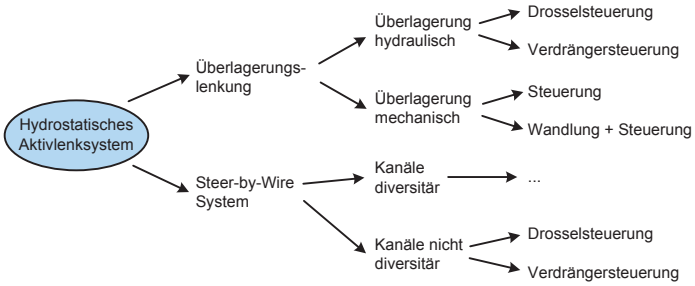


Abb. 3.6: Lösungsraum zur Generierung von hydrostatischen Aktivlenksystemen

Mögliche Lösungen zur Realisierung einer hydrostatischen Überlagerungslenkung sind schematisch in Abbildung 3.7 dargestellt. Überlagerungslenkungen haben definitionsgemäß einen Durchgriff zwischen dem Lenkrad und den gelenkten Rädern, der bei einem Ausfall der Energieversorgung die Lenkbarkeit gewährleistet. Basis für alle Lösungen bildet die hydrostatische Lenkeinheit, die eine Verbindung zwischen dem mechanischen Teilsystem *»Lenkrad«* und dem hydraulischen Lenkzylinder herstellt. Für die Verteilung bereits vorhandener Energie wird lediglich ein elektrisch ansteuerbares Ventil benötigt, das von einem Steuergerät aktuiert wird. Zur Energiewandlung in einer Verdrängersteuerung kann entweder eine mechanische oder eine elektrische Energiequelle verwendet werden. Derartige Lösungen sind zur Realisierung einer Überlagerungslenkung jedoch ungeeignet, weil eine Energiewandlung mit zusätzlichen Hydraulikpumpen durchgeführt wird, anstatt auf die bestehende Hydraulikversorgung zurückzugreifen. Bei der Wandlung der mechanischen Energie[11] ergibt sich zudem der Nachteil, dass die Antriebsdrehzahl der Verdrängereinheit nicht konstant ist und daher bei der Ansteuerung der elektrisch verstellbaren Verdrängereinheit berücksichtigt werden muss. Eine mechanische Überlagerungslenkung, bei der die Energie einer bestehenden Energiequelle verteilt wird, scheitert an der Realisierbarkeit, da in der Kabine keine mechanische Energiequelle vorhanden ist. Die beiden

[11] Als Energiequelle zum Antrieb der Hydraulikpumpe kann beispielsweise die kinetische Energie des Fahrzeugs genutzt werden.

dargestellten Prinziplösungen der Wandlung von elektrischer oder hydraulischer in mechanische Energie sind ungeeignet, da durch das mechanische Überlagerungsgetriebe und den Elektro- beziehungsweise Hydraulikmotor viel Platz in der Fahrerkabine benötigt wird und dadurch eine zusätzliche Geräuschquelle vorhanden ist. Im PKW und NFZ Bereich werden mechanische Überlagerungsgetriebe jedoch eingesetzt [104]. Bei allen Überlagerungslenkungen muss beachtet werden, dass durch die mechanische oder hydraulische Verbindung zwischen Lenkrad und Überlagerungseinheit Eingriffe der Überlagerungseinheit für den Fahrer haptisch spürbar sein können, vor allem wenn diese Eingriffe zeitverzögert, sprungförmig oder pulsierend sind. Dadurch kann das Fahrgefühl und der Fahrkomfort negativ beeinflusst werden.

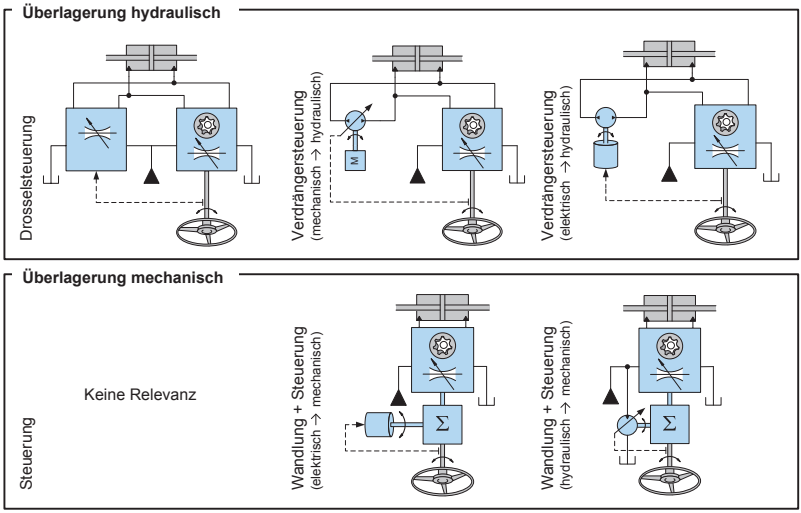


Abb. 3.7: Schematische Darstellung von Lösungen zur Realisierung einer hydrostatischen Überlagerungslenkung auf hydraulischer und mechanischer Ebene

Bei einem Steer-by-Wire System mit diversitär realisierten Kanälen ist die Wahrscheinlichkeit niedriger, dass beide Kanäle auf Grund einer gemeinsamen Ursache zeitgleich ausfallen. Gleichermaßen ist jedoch der Entwicklungsaufwand für solche Systeme höher. Die Tatsache, dass sichere Lenk-

systeme mit nicht-diversitären Kanälen zulassungsfähig sind [81] zeigt, dass dieser Zusatzaufwand für ein Traktor-Lenksystem nicht zwingend erforderlich ist. Für ein Steer-by-Wire System mit nicht diversitär realisierten Kanälen sind in Abbildung 3.8 zwei Prinziplösungen dargestellt. Bei der Energieverteilung mittels zweier Hydraulikventile ist eine zusätzliche Energiequelle nötig, da bei einem Ausfall der bereits vorhandenen Hydraulikversorgung die Lenkbarkeit durch eine weitere Hydraulikversorgung aufrecht erhalten werden muss. In der Praxis werden dazu elektrisch oder mechanisch durch die Bewegungsenergie angetriebene Notlenkpumpen eingesetzt [81, 103, 102], damit beide Hydraulikversorgungen entsprechend der Vorschriften der ECE-Richtlinie 79 [22] nicht direkt von derselben Energiequelle (Verbrennungsmotor) gespeist werden. Soll die Lenkbewegung mit einer Verdrängersteuerung realisiert werden, so kommt nur die Wandlung aus elektrischer Energie in Frage, da die Verwendung der mechanischen Energie des Verbrennungsmotors oder der Bewegungsenergie des Fahrzeugs zu aufwändig ist. Dies ist dadurch begründet, dass diese mechanischen Energiequellen die Energie bei einer nicht durch die Lenkung beeinflussbaren variablen Drehzahl zur Verfügung stellen und daher verstellbare hydrostatische Verdrängereinheiten notwendig wären, die die Komplexität der Architektur erhöhen.

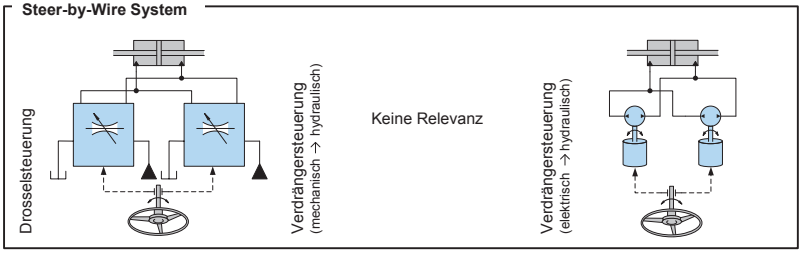


Abb. 3.8: Schematische Darstellung von Lösungen zur Realisierung eines hydrostatischen Steer-by-Wire Systems

Alle Lösungen mit Verdrängersteuerung haben jedoch den Nachteil, dass die bereits vorhandene Hydraulikversorgung nicht genutzt wird. Zudem wird

bei der dargestellten Lösung eine elektrische Energieversorgung benötigt, die nicht nur fehlertolerant ist, sondern auch noch im Fehlerfall die zum Lenken benötigte elektrische Leistung der Aktuatoren für eine ausreichend lange Zeitdauer zur Verfügung stellen kann. Im Vergleich dazu muss die Stromversorgung bei der Drosselsteuerung nur die Energie für den Betrieb der Sensorik, der Steuergeräte und der elektrischen Ansteuerung der Ventile bereitstellen. Wie in Kapitel 2.1.2 bereits dargestellt, gibt es Traktoren, für deren Betrieb auch bei Verwendung eines konventionellen Lenksystems eine Notlenkpumpe erforderlich ist, um die gesetzlichen Anforderungen an die maximale Betätigungskraft zu erfüllen. Aus diesem Grund sind Steer-by-Wire Systeme mit Drosselsteuerungen vorteilhafter als Verdrängersteuerungen, da diese eine gute Austauschbarkeit und Kompatibilität mit konventionellen Lenksystemen ermöglichen und einfach in das bestehende Hydrauliksystem integriert werden können.

3.3.2 System-Architekturen

Die Gesamtsystemarchitektur für die hydraulische Überlagerungslenkung und das Steer-by-Wire System sind schematisch in Abbildung 3.9 dargestellt. In der Überlagerungslenkung stellt die konventionelle Lenkeinheit die Rückfallebene im Fehlerfall dar und ermöglicht die Einhaltung des mit Gefahr 1.2 verknüpften Sicherheitsziels *»Gewährleistung einer Lenkbewegung«*. Zur Realisierung der geforderten Zusatzfunktionen muss der Radlenkwinkel oder die Position des Lenkzylinders sowie die Stellung der Eingabegeräte wie Lenkrad oder Joystick[12] erfasst werden. Auf Basis dieser Signale wird von einem Steuergerät das notwendige Ansteuersignal für das Überlagerungsventil berechnet und ausgegeben. Da die Höhe des Überlagerungsvolumenstroms in der Regel in der Größenordnung des maximalen Volumenstroms der Lenkeinheit liegt, kann im Falle eines Fehlers in der Überlagerungseinheit

[12] Der Joystick wird im Folgenden in prinzipieller Weise als alternatives Eingabegerät betrachtet, obwohl dieser bei der Gefahrenanalyse und Risikobewertung nicht betrachtet wurde.

nicht davon ausgegangen werden, dass der Fahrer diesen Volumenstrom übersteuern kann. Das Überlagerungsventil muss daher zur Vermeidung der Gefahr 1.1 so entwickelt werden, dass eine Fehlererkennung möglich ist und der Volumenstrom durch das Überlagerungsventil mit Hilfe eines zweiten Abschaltpfads sicher unterbrochen werden kann. Durch den zweiten Abschaltpfad im Überlagerungsventil ist das mit Gefahr 1.1 verknüpfte Sicherheitsziel *»Verhindern einer unkontrollierten Lenkbewegung«* zweikanalig sichergestellt. Diese Zweikanaligkeit ist erforderlich, da die Gefahr 1.1 in der Risikobewertung als sehr kritisch eingestuft wurde.

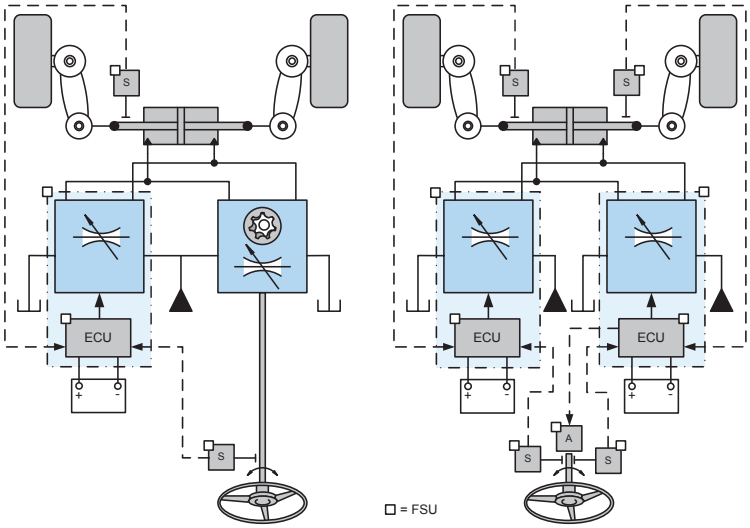


Abb. 3.9: Schematische Darstellung der Gesamtsystem-Architektur für eine hydrostatische Überlagerungslenkung (links) und ein Steer-by-Wire System (rechts)

Darüber hinaus muss sichergestellt werden, dass Fehler in elektrischen und elektronischen Komponenten nicht zu einer fehlerhaften Ansteuerung des Überlagerungsventils führen (Gefahr 1.1). Für diese Komponenten wird daher ein fail-silent Verhalten gefordert. Zudem müssen die Komponenten den durch die Risikobewertung zu ermittelnden Performancelevel für Gefahr 1.1

erfüllen. Bei Verwendung eines alternativen Eingabegeräts ist die Überlagerungslenkung nicht fehlertolerant, da bereits ein Einzelfehler zum Verlust der Lenkbarkeit an diesem Eingabegerät führen kann. In diesem Fall müsste der Fahrer auf das Lenkrad umgreifen, um das Fahrzeug wieder steuern zu können. Der sichere Zustand ist bei diesem Lenksystem dann erreicht, wenn das Überlagerungsventil sicher abgeschaltet ist und der Fahrer das Fahrzeug mit dem Lenkrad lenkt oder sich im Stillstand befindet. Eine Weiterfahrt ist in diesem Fall durch die fehlertolerante Lenkeinheit bei reduziertem Funktionsumfang aus sicherheitstechnischer Perspektive uneingeschränkt möglich, bis ein weiterer Fehler im Lenksystem auftritt.

Im Steer-by-Wire System entfällt die bewährte Rückfallebene und die Fehlertoleranz muss durch eine Redundanz im Lenkventil gewährleistet werden. Die Anforderung der Fehlertoleranz muss in gleichem Maße auch von der Sensorik, der Energieversorgung und der Steuergeräte-Architektur erfüllt werden. In der Forschung und im Stand der Technik von Steer-by-Wire Systemen für PKW und mobile Arbeitsmaschinen hat sich für die Realisierung eine zweikanalige Systemstruktur durchgesetzt, die jeweils aus Komponenten mit fail-silent Verhalten bestehen (fail-silent unit FSU) [19, 101, 81]. Jeweils zwei dieser FSUs werden logisch zu einer FTU (fault-tolerant unit) zusammengefasst und bieten den Vorteil, dass eine komplexe Fehlerbehandlungsstrategie auf Systemebene nicht erforderlich ist, da eine lokale Fehlererkennung und -kapselung auf Komponentenebene stattfindet. Dadurch wird auch das in der ISO 25119 [42] empfohlene Prinzip der Modularisierung erfüllt, mit dem systematische Fehler reduziert werden können. Nachteilig an dieser Architektur ist jedoch der höhere gerätetechnische Aufwand zur sicheren Erkennung von Fehlern in jedem Kanal und zur sicheren Abschaltung jedes Kanals. Durch die in Abbildung 3.9 dargestellte Systemstruktur können die Gefahren 1.1 und 1.2 verhindert werden. Die vom Fahrer am Lenkrad spürbare Betätigungskraft muss bei Steer-by-Wire Systemen durch einen Handkraftaktor nachgebildet werden. Durch die Möglichkeit der elektronischen Festlegung

der spürbaren Betätigungskraft kann gegenüber konventionellen, rein hydrostatischen Lenksystemen das Fahrgefühl verbessert werden [47]. Im Falle eines Fehlers, der zu einer Abschaltung eines Kanals führt, wird der Fahrer gewarnt und die Fahrgeschwindigkeit gedrosselt, da ein weiterer Fehler zum Ausfall des gesamten Lenksystems führen kann. Eine unbegrenzte Weiterfahrt mit Geschwindigkeiten über 10 km/h ist nicht zulässig [22]. Weitere Details zu dem in dieser Arbeit betrachteten System- und Sicherheitskonzept werden in Kapitel 4 erläutert.

Die Schnittstelle zum Informationsaustausch mit dem Fahrzeug (siehe Abbildung 3.3) muss für beide Architekturen ein fail-silent Verhalten aufweisen; Fehlertoleranz ist in der Regel nicht erforderlich. Durch Maßnahmen wie ein doppeltes Versenden von Nachrichten, die Einführung von Prüfsummen oder das Versenden von Bestätigungsnachrichten muss sichergestellt werden, dass Übertragungsfehler erkannt werden können. Fehler in anderen Systemen als der Übertragungseinheit können trotzdem zu einer Übermittlung von falschen Signalen führen. Für Schnittstellengrößen, wie der Fahrgeschwindigkeit, die für die Berechnung der variablen Lenkübersetzung verwendet wird, muss daher sichergestellt werden, dass ein plötzlicher Ausfall oder Sprung nicht zu einer plötzlichen Änderung des Lenkwinkels führt. Wird die Lenkcharakteristik derart durch die variable Lenkübersetzung beeinflusst, dass bei hohen Geschwindigkeiten die sichere Lenkbarkeit nur mit sicherer Kenntnis über die aktuelle Fahrgeschwindigkeit gewährleistet werden kann, so müssen weitere Maßnahmen zur Plausibilisierung der übermittelten Fahrgeschwindigkeit getroffen werden. Bei der automatischen Lenkfunktion ist es vorgeschrieben, dass diese nur bei Erfüllung gewisser Randbedingungen, wie beispielsweise der Anwesenheit des Fahrers, aktiviert werden darf [41]. Während der Aktivierung dieser Funktion hat der Fahrer weiterhin die übergeordnete Verantwortung über die Fahrzeugführung. Die automatische Lenkfunktion muss sich selbständig deaktivieren, wenn der Fahrer eine gefährliche Lenkbewegung des Fahrzeugs erkennt und am Lenkrad korrigierend eingreift. Anders

ist dies bei korrigierenden Lenkfunktionen, die beispielsweise für fahrstabilisierende Lenkeingriffe verwendet werden: Derartige Lenkbefehle werden dem Fahrerwunsch überlagert und können durch den Fahrer nicht deaktiviert, allenfalls übersteuert werden. Da fahrstabilisierende Lenkeingriffe in der Regel hochdynamisch und damit im Fehlerfall vom Fahrer nicht kompensierbar sind, muss die fail-silent Anforderung für diese Schnittstellengrößen nicht nur vom Übertragungskanal sondern auch von dem Steuergerät erfüllt werden, das diese Eingriffe berechnet und an das Lenksystem übermittelt. Idealerweise werden derartige Funktionen daher direkt im Steuergerät des Lenksystems berechnet.

3.4 Gegenüberstellung und Vergleich

Die Gegenüberstellung und der Vergleich der beiden betrachteten Architekturen erfolgt qualitativ anhand der Kriterien *»realisierbare Funktionen«*, *»Komponentenaufwand und Bauraum«* sowie *»Verhalten im Fehlerfall«*, siehe Tabelle 3.2. Ein quantitativer absoluter Vergleich ist dabei nicht möglich, da die Bewertung und Eignung beider Architekturen vom jeweiligen Anwendungsbereich und damit den benötigten Funktionalitäten abhängig ist: Steer-by-Wire Systeme haben den Vorteil, dass neben den Basisfunktionalitäten auch viele weitere Funktionen wie der Rückfahrbetrieb oder die variable Lenkübersetzung fehlertolerant realisiert werden können. Dies führt dazu, dass sich das Fahrverhalten im Fehlerfall nicht oder nur unwesentlich verändert. Da in der Regel jedoch ein weiterer Fehler zum Ausfall des Lenksystems führen kann, ist die unbegrenzte Weiterfahrt mit Geschwindigkeiten über 10 km/h nicht erlaubt. Demgegenüber geht die hydrostatische Überlagerungslenkung nach Detektion eines kritischen Fehlers in der Überlagerungseinheit in den sicheren Zustand über, in dem die Überlagerungseinheit deaktiviert ist[13]. Durch die Abschaltung ändert sich die aktuelle Lenkübersetzung (falls die

[13] Hydrostatische Überlagerungslenkungen mit fehlertoleranter Überlagerungseinheit werden nicht betrachtet, da der Komponentenaufwand und Bauraumbedarf zu hoch ist.

variable Lenkübersetzung aktiv war) und sämtliche elektronische Zusatzfunktionalitäten stehen nicht mehr zur Verfügung. Bei Verwendung eines alternativen elektrischen Eingabegeräts führt dies zur Gefahr 1.2 und damit zu der Notwendigkeit für den Fahrer, auf das Lenkrad umzugreifen. Aus diesem Grund können elektrische Eingabegeräte in dieser Architektur nur bei niedrigen Geschwindigkeiten verwendet werden. Bei einem Ausfall der Druckversorgung kommt es zu einem starken Anstieg der notwendigen Betätigungskraft, da der Fahrer die Lenkkraft in dieser Situation selbst aufbringen muss.

Realisierbare Funktionen	Überlagerungslenkung	Steer-by-Wire System
Adaptive Lenkübersetzung	realisierbar (FS)	realisierbar (FT)
Alternative elektrische Eingabegeräte (inkl. Rückfahrbetrieb)	realisierbar (nicht FS*)	realisierbar (FT)
Automatische und korrigierende Lenkfunktionen	realisierbar	realisierbar
Konfigurierbare Lenkrad-Rad-Rückstellung	-	realisierbar
Aktive haptische Fahrerwarnung	-	realisierbar

Verhalten im Fehlerfall	Überlagerungslenkung	Steer-by-Wire System
Druckversorgung	Anstieg Lenkkraft (Muskelkraftlenkung) Fahrerwarnung	Fahrerwarnung und Geschwindigkeitsdrosselung
Spannungsversorgung	Wegfall der Überlagerung Fahrerwarnung	Fahrerwarnung und Geschwindigkeitsdrosselung
Lenkventil	Wegfall der Überlagerung Fahrerwarnung	Fahrerwarnung und Geschwindigkeitsdrosselung

Komponentenaufwand	Überlagerungslenkung	Steer-by-Wire System
Hydraulik	Konventionelle Pumpe Hydrostatische Lenkeinheit Überlagerungsventil (FS)	Konventionelle Pumpe Notlenkpumpe Lenkventil (FT)
Elektrik	Konventionelles Bordnetz 1 Steuergerät (FS) Sensorik (FS)	Fehlertolerantes Bordnetz 2 Steuergeräte (jeweils FS) Sensorik (2xFS oder 1xFT)
Sonstiges	Lenkgestänge zur Lenkeinheit	Handkraftaktor

Bauraum / Gestaltung	Überlagerungslenkung	Steer-by-Wire System
Innerhalb Kabine	Flexibilität ungünstig (Hydrostatische Lenkeinheit, Lenkgestänge, Lenkrad)	Flexibilität günstig (Lenkrad mit Handkraftaktor) Keine Hydraulik in Kabine
Außerhalb Kabine	Flexibilität und Bauraum günstig	Flexibilität günstig / Bauraum weniger günstig

* = ein Einzelfehler kann zum Verlust der Lenkbarkeit führen

Tab. 3.2: Qualitativer Vergleich der beiden System-Architekturen aus Abbildung 3.9

In einem Steer-by-Wire System entfällt das gesamte Lenkgestänge zwischen dem Lenkrad und der hydrostatischen Lenkeinheit sowie die hydrostatische Lenkeinheit an sich und damit auch eine Geräusch- und Wärmequelle in der Kabine [72]. Stattdessen ist zwingend eine Notlenkpumpe und ein fehlertolerantes elektrohydraulisches Lenkventil nötig. Das für die Überlagerungslenkung notwendige Steuergerät muss in einem Steer-by-Wire System doppelt vorhanden sein, wobei die Sicherheitsanforderungen an jedes einzelne dieser Steuergeräte vergleichbar ist zu den Sicherheitsanforderungen an das Steuergerät der Überlagerungslenkung. Darüber hinaus muss auch die Stromversorgung und die Sensorik bei einem Steer-by-Wire System fehlertolerant ausgelegt sein. Als Eingabegerät dient ein Lenkrad mit fehlertoleranter Winkelsensorik und einem Handkraftaktor, das mit verhältnismäßig geringen Gestaltungsrestriktionen in der Kabine platziert und ergonomisch optimal angepasst werden kann[14]. Außerhalb der Fahrerkabine benötigen hydrostatische Überlagerungslenkungen im Vergleich zu konventionellen Lenksystemen lediglich Bauraum für das Überlagerungsventil, im Steer-by-Wire System wird Bauraum für das fehlertolerante Lenkventil, die Notlenkpumpe und das fehlertolerante Bordnetz benötigt.

Der qualitative Vergleich zeigt, dass mit hydraulischen Überlagerungslenkungen Zusatzfunktionalitäten wie eine automatische Spurführung oder eine variable Lenkübersetzung mit vergleichsweise moderatem Zusatzaufwand sicher realisiert werden können. Nichtsdestotrotz bieten Steer-by-Wire Systeme Vorteile bezüglich der Gestaltung, Modularität und Ergonomie in der mobilen Arbeitsmaschine sowie bei dem Verhalten des Lenksystems im Fehlerfall. Durch die Anpassung der vom Fahrer spürbaren Betätigungskräfte und der Lenkrad-/Rad-Rückstellung kann zudem das Fahrverhalten verbessert und die Fahrsicherheit situationsabhängig gesteigert werden. Eine Anpassung dieser Lenkcharakteristik ist ohne konstruktive Änderungen an der Lenkein-

[14] Demgegenüber muss das Lenkrad in hydrostatischen Überlagerungslenkungen einen gewissen Mindestdurchmesser haben, um die Anforderungen an die maximale Betätigungskraft im Fehlerfall gewährleisten zu können.

heit oder der Achsgeometrie möglich. Ein weiterer Vorteil von Steer-by-Wire Systemen ist die Tatsache, dass Zusatzfunktionen wie die variable Lenkübersetzung fehlertolerant realisiert werden können und dem Fahrer daher nicht die Verantwortung übertragen wird, diese Funktionen bei der Straßenfahrt zu deaktivieren. Der zusätzliche Komponentenaufwand zur Gewährleistung der Fehlertoleranz, der bei Steer-by-Wire Systemen erforderlich ist, hängt entscheidend davon ab, wie und mit welchen Komponenten das Steer-by-Wire System realisiert ist. Diese Konzeptionierung erfolgt im nächsten Kapitel.

4 Konzeptionierung eines Steer-by-Wire Systems

Das vorgestellte System- und Sicherheits-Konzept für ein Steer-by-Wire System wird im Folgenden konkretisiert und ausgestaltet (Schritt 3 und 4[1]). Der Fokus liegt dabei auf dem fehlertoleranten Lenkventil als wesentlicher Unterschied zum Stand der Technik und Forschung für PKW und mobile Arbeitsmaschinen. Im Anschluss an die Konzeptionierung erfolgt eine sicherheitstechnische Bewertung des Lenkventils auf Konzeptebene (Schritt 5).

4.1 Synthese

Die Synthese des fehlertoleranten Steer-by-Wire Systems erfolgt auf Basis einer konventionellen hydrostatischen Einkreis-Lenkung in einem Closed-Center Load-Sensing (LS) System (siehe Kapitel 4.1.2). Zudem werden Komponenten wie der Lenkzylinder, die Schläuche oder die Druckbegrenzungs- und Nachsaugventile als bewährte Komponenten übernommen und bei der Bewertung der Fehlertoleranz nicht näher betrachtet, da diese Komponenten unter identischen Bedingungen im Stand der Technik eingesetzt werden. Gleichermaßen werden auch die grundlegenden und bewährten Sicherheitsprinzipien [18, 44], die bei der Entwicklung in den Bereichen Mechanik, Hydraulik, Elektrik/Elektronik sowie bei der Softwareentwicklung beachtet werden müssen, im Rahmen der Konzeptionierung nicht näher thematisiert. Beispiele für solche Prinzipien sind die geeignete Dimensionierung, Materialauswahl und Herstellung, die Verlegung von Rohren, so dass diese nicht als Leiter oder Griff verwendet werden können, die geeignete Abschirmung von Kabeln oder die Vermeidung undefinierter Zustände in Elektronik und Software.

[1] Siehe vorgestellte Vorgehensweise in Kapitel 2.2.2.

4.1.1 Steer-by-Wire Lenkventil

Bevor ein fehlertolerantes Lenkventil konzipiert werden kann, muss bekannt sein, welche Fehler in Hydraulikventilen prinzipiell auftreten können und welche davon bei der Wahl der Ventilarchitektur zwingend berücksichtigt werden müssen, weil diese nicht durch geeignete Methoden und Verfahren verhindert werden können. Die in Tabelle 4.1 aufgelisteten Fehler und Fehlerausschlüsse für Wegeventile inklusive Magnetspule basieren auf den Informationen einschlägiger Normen [18] und Forschungsarbeiten [76, 51].

Nr.	Fehlerbeschreibung	Mögliche Ursachen (Beispiele)	Anforderungen für Ausschluss	Kommentar
1	Selbsttätige Veränderung der Ausgangsschaltstellung	- Schwingungsbeanspruchung - Trägheits- und Gewichtskräfte	Bei zwangsläufig mechanischer Betätigung mit ausreichend hoher Kraft oder bei Einsatz bewährter Federn und üblichen Einbau- und Betriebsbedingungen.	Fehler wird hier ausgeschlossen, da Verwendung bewährter Federn und üblichen Einbau- und Betriebsbedingungen
2	Bersten Gehäuse / Bruch bewegtes Bauteil / Bruch Befestigung	- mechanische Überbeanspruchung	Konstruktion, Dimensionierung und Einbau entsprechend Erfahrungswerten.	Fehler wird hier ausgeschlossen, da Einhaltung der Anforderungen
3	Veränderung der Schaltzeiten	- Temperatureinfluss - Alterung / Verschleiß (Erhöhte Reibung) - Verschmutzung - Windungsschluss in Magnetspule	Nur bei zwangsläufig mechanischer Betätigung mit ausreichend hoher Betätigungskraft.	Fehler kann hier nicht ausgeschlossen werden
4	Veränderung der Durchflusscharakteristik	- Temperatureinfluss - Alterung / Verschleiß - Windungsschluss in Magnetspule	Kein Ausschluss möglich.	
5	Nichtschalten oder nicht vollständiges Schalten / Hängenbleiben in Ausgangs-, Zwischen- oder Endstellung	- Partikel (z.B. Späne) - Verschmutzung - Kabelbruch in Magnetspule - Federbruch	Nur bei zwangsläufig mechanischer Betätigung mit ausreichend hoher Kraft.	Fehler kann hier nicht ausgeschlossen werden
6	Interne Leckage und Veränderung der Leckage	- Verschleiß - Partikel - Konstruktionsprinzip (z.B. Schieberventil)	Kein Ausschluss möglich.	

Tab. 4.1: Mögliche Fehler und Fehlerausschlüsse bei einem Wegeventil mit Magnetspule [18, 76, 51]

Für die Konzeptionierung des Steer-by-Wire Lenkventils kann Fehler 1 und 2 ausgeschlossen werden, da deren Auftreten bei einer geeigneten Ventilentwicklung quasi nicht möglich ist. Die Fehler 3, 4 und 6 sind in der Regel keine plötzlich eintretenden Fehler sondern beschreiben Abweichungen des Ventilverhaltens vom Nominalzustand, die stets vorhanden sind. Durch die Vielzahl der nicht zu vermeidenden Ursachen wie Verschleiß, Alterung und Temperatureinfluss lassen sich diese Fehler nicht ausschließen. Die Auswirkung sind jedoch typischerweise gering und werden in einem Lageregelkreis

kompensiert, müssen also nicht bei der Konzeptionierung berücksichtigt werden. Der relevante Fehler für die Konzeptionierung ist daher der Fehler 5.

Nach [86] ist die häufigste Ursache für Ventilausfälle die Verschmutzung der Hydraulikflüssigkeit. Durch Schmutz oder Partikel beziehungsweise Späne, die in den Dichtspalt eindringen (Silting), kann sich die Reibung des Ventilschiebers erhöhen. Im Extremfall tritt sogar ein vollständiges Blockieren ein. Die Ausfallrate von Hydraulikventilen lässt sich bezüglich dieser Ursache durch ein geeignetes Filtrationssystem nennenswert reduzieren [86]. In der Luftfahrt eingesetzte Ventile werden zum Teil darauf ausgelegt, dass in die Steuerkante eingedrungene Partikel abgeschert werden können, um ein Klemmen zu verhindern [51, 76]. Dazu sind sehr hohe Betätigungskräfte notwendig, die von konventionellen direktgesteuerten Proportionalventilen nicht erreicht werden können [76], so dass alternative Maßnahmen ergriffen werden müssen. In der Regel wird dazu in Anwendungen außerhalb der Luftfahrt die Ventilöffnung mit einem Positionssensor überwacht und nach Erkennung eines Fehlers der Volumenstrom über ein separates Abschaltventil unterbrochen. Dadurch wird eine ungewollte Zylinderbewegung verhindert und ein sicherer Stopp im stromlosen Zustand gewährleistet. Die zweithäufigste Ursache für Ventilausfälle ist das Versagen der Rückstellfedern [86]. Ausfälle auf Grund dieser Ursache lassen sich durch eine dauerfeste Auslegung der verwendeten Federn vergleichsweise einfach vermeiden.

In dieser Arbeit werden für Wegeventile die folgenden beiden Worst-Case Fehlerfälle bei der Wahl der Ventilarchitektur berücksichtigt[2]:

- **Fehlertyp A:**
  Das Ventil ist geschlossen und kann nicht mehr geöffnet werden
- **Fehlertyp B:**
  Das Ventil ist geöffnet und kann nicht mehr geschlossen werden

[2] Andere Fehler, wie beispielsweise Leckage, werden beim Nachweis berücksichtigt, haben aber keinen Einfluss auf die Wahl der Ventilarchitektur.

Eine nahe liegende Lösung ist die Verwendung von 4/3-Wegeventilen für die Realisierung eines Steer-by-Wire Ventils, wie sie auch bei hydrostatischen Überlagerungslenkungen zum Einsatz kommen. Zur Kompensierung von Fehlern des Typs B im Wegeventil müssen zusätzliche Absperrventile eingesetzt werden, die das Wegeventil im Fehlerfall deaktivieren. Da auch Fehler des Typs A im Wegeventil auftreten können, muss die gesamte Struktur doppelt vorhanden sein, siehe Abbildung 4.1. Ein ähnliches Ventilkonzept wird in [34] beschrieben. Um den Fehlertyp B und damit die Notwendigkeit für eine Abschaltung eines Kanals erkennen zu können, sind an beiden Wegeventilen Positionssensoren nötig. Je nach verwendetem Ventil werden diese Sensoren auch zur Regelung der Ventilschieberposition verwendet. Bei einem Verzicht auf diese Sensoren bestünde die Möglichkeit, im fehlerfreien Fall nur einen der beiden Kanäle zum Verstellen des Lenkzylinders zu verwenden. Im Fehlerfall B wäre dann jedoch eine äußerst schnelle Fehlererkennung auf Basis der Regelabweichung und ein anschließendes Ab- sowie Umschalten notwendig, damit die Lenkbarkeit erhalten bleibt [72]. Diese Bedingung ist dann erfüllt, wenn die Reaktionszeit des Systems geringer als die Fehlertoleranzzeit ist [42]. Dabei berechnet sich die Reaktionszeit aus der Zeitdifferenz zwischen dem Fehlereintritt und der Fehlererkennung anhand einer Abweichung der Lenkzylinderposition, der Abschaltung und dem Schließen des Absperrventils sowie der Aktivierung des Notlenkventils (*cold stand-by*). Die Fehlertoleranzzeit ist die Zeit zwischen dem Auftreten des Fehlers (unerwartete Auslenkung des Lenkzylinders) und dem Erreichen einer als gefährlich definierten Abweichung zwischen Soll- und Ist-Position[3]. Das bedeutet auch, dass sich ein Fehler in dieser Architektur ohne Sensorik am Ventil bereits auf die Lenkbewegung ausgewirkt haben muss, bevor dieser erkannt werden kann und die Fehlertoleranz gewährleistet ist. Ein weiterer Nachteil bei dieser Lösung ist die Notwendigkeit, dass jeder einzelne Kanal auf den maximal benötigten Volumenstrom ausgelegt sein muss, da

[3] In der Risikobewertung wurde ermittelt, dass die Fehlertoleranzzeit für die mit Fehlertyp B verknüpfte Gefahr 1.1 in einem Bereich zwischen 10 und 100 ms liegt.

der fehlerhafte Kanal nur dann ermittelt werden kann, wenn nur einer der beiden Kanäle gleichzeitig aktiv ist. Dies führt dazu, dass beide Wegeventile in Summe überdimensioniert sind. Die Funktionsfähigkeit des Absperrventils kann in dem in Abbildung 4.1 dargestellten Konzept durch einen einfachen Selbsttest während des Starts der Maschine auch ohne Positionssensor am Absperrventil überprüft werden.

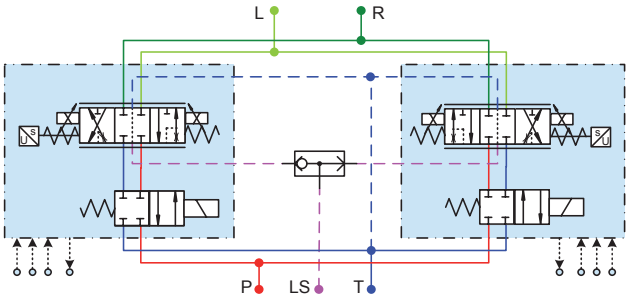


Abb. 4.1: Schaltplan eines hydrostatischen Steer-by-Wire Ventils mit 4/3-Wegeventilen

In [83] wird ein Lenkventil beschrieben, das 4/2-Wegeventile zur Realisierung der Fehlertoleranz einsetzt, siehe Abbildung 4.2. Innerhalb jedes Kanals wird eines der beiden proportionalen Wegeventile für Lenkbewegungen nach links ① und das jeweils andere für Lenkbewegungen nach rechts ② verwendet. Ein drittes Schaltventil ③ wird als Absperrventil eingesetzt. Der Abgriff des LS-Signals erfolgt auf der jeweiligen Zulaufseite der Rückschlagventile durch Wechselventile. Auch in diesem Konzept müssen Fehler des Typs B durch Positionssensoren an den jeweiligen Wegeventilen schnell erkannt werden, um den dazugehörigen Kanal zu deaktivieren und die Lenkfähigkeit zu gewährleisten.

Die beiden vorgestellten Konzepte entsprechen der in Abbildung 3.9 dargestellten Struktur aus zwei unabhängigen FSUs. Fehlertolerante Systeme allgemeiner Art mit zwei FSUs weisen häufig jeweils eine interne Redundanz

auf, so dass insgesamt eine Vierfach-Redundanz vorliegt[4]. Fehlertolerante Systeme lassen sich jedoch bereits mit einer Dreifach-Redundanz darstellen, wenn keine zweikanalige fail-silent Struktur benötigt wird [19].

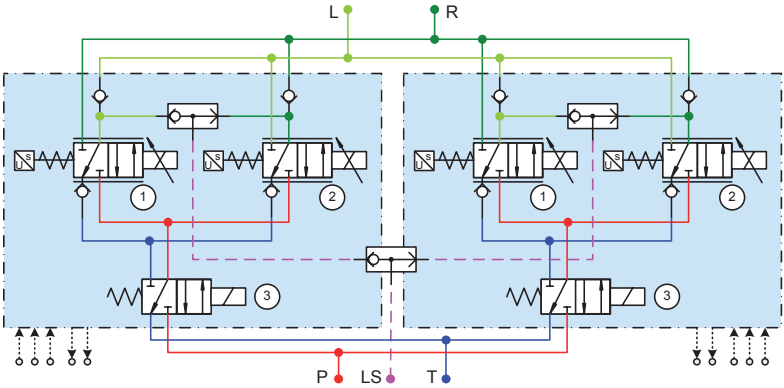


Abb. 4.2: Schaltplan eines hydrostatischen Steer-by-Wire Ventils mit 4/2-Wegeventilen nach [83]

Zur weiteren Reduktion der Komplexität und des Komponentenaufwands kann auch das Lenkventil als FTU konzipiert werden, die nicht in zwei unabhängige FSUs unterteilt werden kann (siehe Abbildung 4.3). Dies kann dadurch realisiert werden, dass das Lenksystem nicht als aktiv fehlertolerantes System mit Rekonfiguration sondern als passiv fehlertolerantes System ausgelegt wird. Im optimalen Fall kann dann auf Positionssensoren zur Fehlererkennung und Absperrventile zur Rekonfiguration verzichtet werden, da das System Ventilfehler inhärent kompensieren und die Lenkbarkeit gewährleisten kann. Bei Verzicht auf Positionssensoren muss gewährleistet sein, dass Ventilfehler rechtzeitig vor dem Eintritt eines Zweitfehlers auf andere Weise erkannt werden können[5]. Dabei ist es umso leichter, ein System passiv

[4] In den dargestellten Ventil-Konzepten gibt es durch die Wegeventile und die beiden Absperrventile vier separate Abschaltpfade. Des Weiteren gibt es Positionssensoren an den Wegeventilen, die funktional nicht zwingend notwendig sind.

[5] Nähere Informationen zur notwendigen Häufigkeit der Fehlererkennung werden in Kapitel 4.2.3 vorgestellt.

fehlertolerant auszulegen, je geringer die Auswirkungen eines Einzelfehlers auf das Gesamtsystem sind. In den beiden zuvor genannten Konzepten ist die Auswirkung eines Einzelfehlers bei Verzicht auf die Abschaltventile sehr groß, da beispielsweise im Falle eines Fehlers des Typs B im stromlosen Zustand eine ungewollte und gefahrbringende Lenkzylinderbewegung auftritt und kein sicherer Stopp gewährleistet werden kann.

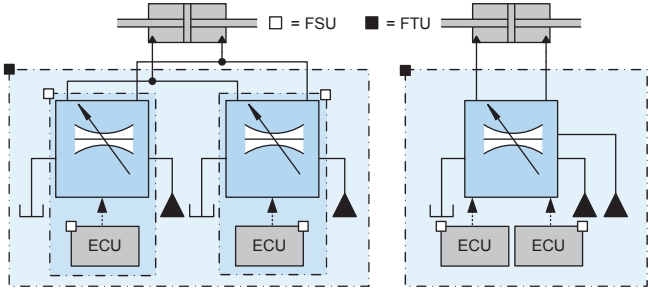


Abb. 4.3: Konzeptionierung eines fehlertoleranten Steer-by-Wire Ventils aus zwei FSUs oder einer FTU

Ein Ventilkonzept mit unabhängigen Steuerkanten, bei dem ein sicherer Stopp im stromlosen Zustand prinzipiell auch ohne Absperrventil gewährleistet werden kann, ist in Abbildung 4.4 dargestellt. In diesem Konzept werden jeweils zwei identische Ventile pro Steuerkante verwendet, um die notwendige Redundanz und damit die notwendige Toleranz gegenüber Fehlern des Typs A darstellen zu können. Bei der Ansteuerung der Ventile ist es notwendig, die jeweils zueinander redundanten Ventile gleichzeitig zu betreiben, da im Fehlerfall keine Umschaltung stattfindet. Durch die hohe Anzahl der Freiheitsgrade wird der Entwurf eines passiv fehlertoleranten Reglers, der die Fehlertoleranz gegenüber Fehlern des Typs B während der Fahrt auch ohne Rekonfiguration gewährleistet, stark vereinfacht. Im Vergleich zu den zuvor dargestellten Ventilkonzepten kann daher im Konzept mit unabhängigen Steuerkanten die Gefahr 1.1 *»unmotivierte Lenkbewegung«* durch einen hydraulischen Einzelfehler nicht eintreten. Selbst bei Blockade eines Zulauf-

ventils durch einen Fremdkörper, wie einen Metallspan, kann durch Schließen des Ablaufventils eine Zylinderbewegung unterbrochen werden[6].

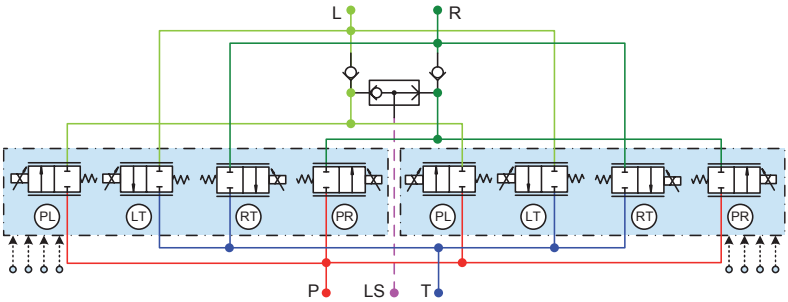


Abb. 4.4: Schaltplan eines hydrostatischen Steer-by-Wire Ventils mit 2/2-Wegeventilen nach [65]

Ventilkonzepte mit unabhängigen Steuerkanten werden bisher überwiegend dann eingesetzt, wenn die Energieeffizienz und das Rekuperationspotential eines hydraulischen Systems erhöht oder durch den Einsatz der Mehrgrößenregelung zusätzliche Funktionen, wie die Regelung das Ablaufdrucks, realisiert werden sollen, siehe unter anderem [59, 23]. Untersuchungen zur Fehlertoleranz solcher Architekturen erfolgen im Wesentlichen für digital-hydraulische Anwendungen mit einer deutlich höheren Anzahl an Ventilen [87]. In [95] wird ein Konzept mit unabhängigen Steuerkanten zur Realisierung einer fail-silent *»Kopilot-Lenkanlage«* (semi-aktives Lenksystem) für PKW vorgestellt. Dieses System besteht jedoch auf Grund der geringeren Sicherheitsanforderungen (fail-silent Verhalten) aus nur vier 2/2-Wegeventilen (Schaltventile) sowie einem Absperrventil, das parallel zum konventionellen mechanischen Lenkgestänge angeordnet ist. Ein Lenksystem mit unabhängigen Steuerkanten bestehend aus vier piezo-gesteuerten Schaltventilen für

[6]Bei einem Fehler des Typs B in einem Ablaufventil können externe Lasten zu einer Zylinderbewegung führen, da hydrostatische Lenksysteme mit Rückschlagventilen ausgestattet sind, die ein Nachsaugen von Fluid aus dem Reservoir in den Lenkzylinder ermöglichen, siehe Abbildung 2.4. Sowohl während der Fahrt als auch im Stand des Fahrzeugs wirken im stromlosen Zustand jedoch nur rückstellende Kräfte, die zu einer automatischen Selbstzentrierung der Lenkung führen würden.

Flurförderfahrzeuge wird zudem in [3] mit sieben anderen Konzepten in einem Prinzipvergleich gegenübergestellt. Der Aspekt der Fehlertoleranz wird dabei jedoch nicht betrachtet.

Die Realisierung des vorgestellten Ventilkonzepts mit unabhängigen Steuerkanten erfolgt mit robusten 2/2-Wegeventilen geringer Komplexität. Diese können als konventionelle stromgeregelte Proportionalventile oder als Schaltventile in Sitz-Bauweise ausgeführt sein, die durch eine pulsweitenmodulierte Ansteuerungsmethode quasi-proportional betrieben werden [80, 84]. Für das vorgeschlagene Ventilkonzept werden zwei wichtige Annahmen aufgestellt, die die Grundlage für die Realisierbarkeit des Konzepts mit unabhängigen Steuerkanten bilden und in dieser Arbeit in den folgenden Kapiteln detailliert untersucht werden:

- **Annahme 1 (Fehlertoleranz):**
  Eine Auslegung des Lenksystems als passiv fehlertolerantes System ist möglich. Durch den fehlertoleranten Regler ist es im relevanten Lastbereich in den zulassungsrelevanten Fahrmanövern möglich, Einzelfehler des Typs A und B an Ein- und Auslassventilen inhärent zu kompensieren, ohne dass eine Fehlererkennung und Rekonfiguration notwendig ist.

- **Annahme 2 (Fehlererkennung):**
  Durch einen Selbsttest oder durch eine modellbasierte Fehlererkennungsmethode ist es auch ohne Positionssensoren an den einzelnen Ventilen möglich, Ventilfehler des Typs A und B rechtzeitig zu erkennen, bevor das Risiko eines Zweitfehlers zu groß wird[7].

Der Vergleich der betrachteten Ventilarchitekturen in Tabelle 4.2 stellt die Unterschiede hinsichtlich des Komponentenaufwands, der Fehlertoleranzstrategie sowie der Struktur gegenüber. Es ist ersichtlich, dass sowohl die

[7] In [35] wird beschrieben, dass eine Testrate als ausreichend angesehen werden kann, wenn diese mindestens um den Faktor 100 höher ist als die Ausfallrate der jeweiligen Komponenten, siehe auch Kapitel 4.2.3.

Komponentenkomplexität der Einzelventile als auch die Komplexität der Fehlertoleranzstrategie durch das Ventilkonzept mit unabhängigen Steuerkanten reduziert werden kann. In den ersten beiden Konzepten ist eine schnelle, robuste und zuverlässige Fehlererkennung zur Gewährleistung der Fehlertoleranz notwendig, da die Fehlertoleranzzeit sehr gering ist, siehe Kapitel 3.2.3. Im Konzept mit unabhängigen Steuerkanten wird das grundlegende Sicherheitsprinzip der *Funktionstrennung* angewendet und die Gewährleistung der Fehlertoleranz durch einen passiv fehlertoleranten Regler von der Gewährleistung der Fehlererkennung komplett getrennt[8].

		4/3-Wegeventile	4/2-Wegeventile	2/2-Wegeventile
Komponentenaufwand	Wegeventile	2x 4/3-Wegeventile* 2x 4/2-Wegeventile	4x 4/2-Wegeventile 2x 4/2-Wegeventile	8x 2/2-Wegeventile
	Steuerkanten	16*	18	8
	Magnetspulen	6	6	8
	Sensoren	2	4	-
	Steckverbinder	8	10	8
	Sonstiges	1x LS-Wechselventil	3x LS-Wechselventil 8x Rückschlagventil (im Leistungsfluss)	1x LS-Wechselventil 2x Rückschlagventil (im Leistungsfluss)
Fehlertoleranz-strategie		Aktive Fehlertoleranz (Fehlererkennung, Fehlerdiagnose, Rekonfiguration)		Passive Fehlertoleranz (inhärente Fehlerkompensation)
Struktur		2x FSU		1x FTU

* 4/3-Wegeventile mit zusätzlichen Steuerkanten zum LS-Abgriff

Tab. 4.2: Qualitativer Vergleich der betrachteten Ventilkonzepte

Im Gegensatz zu den anderen Ventilkonzepten führt im Konzept mit unabhängigen Steuerkanten ohne Fehlererkennung kein hydraulischer Einzelfehler zur der worst-case Gefahr 1.1 *»unmotivierte Lenkbewegung«* und damit zu einer Unwirksamkeit der vorhandenen Redundanz. Die Fehlertoleranzzeit ist

[8] Die Gewährleistung der Lenkbarkeit hängt hier nicht von einer schnellen Fehlererkennung ab. Fehler müssen trotzdem erkannt werden, damit der Fahrer gewarnt und verhindert werden kann, dass das Fahrzeug dauerhaft mit einer Geschwindigkeiten über 10 km/h gefahren wird.

für dieses Ventilkonzept daher die mittlere Zeit bis zu einem gefahrbringenden Zweitfehler und damit vergleichsweise groß.

4.1.2 Hydraulische Energieversorgung

Das Konzept für eine fehlertolerante Druckversorgung hängt entscheidend davon ab, welche Art von Hydrauliksystem im jeweiligen Traktor bereits vorhanden ist. Kleinsttraktoren mit einer Leistung unter 50 kW sind häufig aus Kostengründen mit einem Open-Center System ausgestattet [37]. Die Realisierung einer fehlertoleranten LS-Druckversorgung für das Closed-Center Lenkventil wäre daher mit einem vergleichsweise hohen Aufwand verbunden, was die Sinnhaftigkeit der Integration eines Steer-by-Wire Systems in Traktoren dieser Leistungsklasse weiter reduziert. Durch die Entwicklung und Einführung von kompakten und kostengünstigen Closed-Center LS-Aggregaten [34] werden derartige Systeme jedoch zunehmend auch in Traktoren mit Leistungen um die 70 kW eingesetzt, um Energieverluste zu minimieren und die Anforderungen an die neuen Abgasrichtlinien einzuhalten. In Traktoren der höheren Leistungsklassen werden fast ausschließlich Closed-Center LS Systeme eingesetzt, bei denen über ein Prioritätsventil gewährleistet wird, dass die hydrostatische Lenkeinheit gegenüber der Arbeitshydraulik priorisiert mit Öl versorgt wird. Da die konventionelle hydrostatische Lenkeinheit sehr empfindlich auf Änderungen des Versorgungsdrucks und des Volumenstroms reagiert, wird in manchen Traktoren eine separate Lenkpumpe (häufig eine Konstantstrompumpe) eingesetzt, die nur die Open-Center Lenkeinheit versorgt [37]. In großen Traktoren, bei denen die Grenzwerte für die Betätigungskräfte bei einem Ausfall der zentralen Druckversorgung nicht eingehalten werden, muss eine zusätzliche Not-Lenkpumpe vorhanden sein, siehe beispielsweise [49]. Derartige Systeme werden dann nicht mehr als Muskelkraftlenkanlage, sondern wie Steer-by-Wire Systeme als Fremdkraftlenkanlage eingestuft [96]. Fehlertolerante Druckversorgungen sind daher schon bereits heute in Serie verfügbar.

Zur Realisierung einer fehlertoleranten Druckversorgung kann in Übereinstimmung mit den geltenden Richtlinien auch eine erschöpfliche Energiequelle, wie ein Hydraulikspeicher, eingesetzt werden [12]. Nachteilig an einer derartigen Lösung ist jedoch der hohe Bauraumbedarf, da das Fahrzeug im Fehlerfall noch eine festgelegte Mindeststrecke zurücklegen können muss[9]. Ein zusätzlicher Aufwand ergibt sich außerdem aus der Integration des Speichers in die Druckversorgung mit variablem Druckniveau und die Abstimmung des Speichervorspanndrucks auf den zum Lenken benötigten Druck und Volumenstrom.

Da in einigen Traktoren neben der Pumpe für die Arbeitshydraulik bereits eine weitere (Not-)Lenkpumpe integriert ist, ist die Realisierung einer fehlertoleranten Druckversorgung auf Basis dieser beiden Pumpen am zweckmäßigsten. Dabei ist zu beachten, dass die Not-Lenkpumpe und die Pumpe der Arbeitshydraulik nicht von der gleichen Energiequelle versorgt werden. In der Praxis wird die Not-Lenkpumpe beispielsweise über den Getriebeausgang (Bewegungsenergie) oder bedarfsgerecht über einen Elektromotor angetrieben [96, 49]. Gegenüber konventionellen hydrostatischen Lenkeinheiten sind Steer-by-Wire Ventile durch den geschlossenen elektronischen Regelkreis und das Fehlen einer hydraulischen Kopplung zwischen dem Lenkrad und den gelenkten Rädern deutlich weniger empfindlich gegenüber Schwankungen des Drucks und des Volumenstroms der Arbeitshydraulik. Daher führt eine Kombination von Arbeits- und Lenkhydraulik über ein Prioritätsventil nicht zu einem Nachteil für das Lenkgefühl. Wird die Not-Lenkpumpe nur im Bedarfsfall bei Ausfall der primären Pumpe aktiviert (cold stand-by), so muss beachtet werden, dass die Not-Lenkpumpe innerhalb der durch die Risikobewertung ermittelten Fehlertoleranzzeit (siehe Kapitel 3.2.4) die Versorgung übernehmen kann.

[9] Es wird gefordert, dass das Fahrzeug mindestens 25 *Achten* mit einem Bahndurchmesser von 40 *m* fahren können muss.

4.1.3 Elektrische Energieversorgung

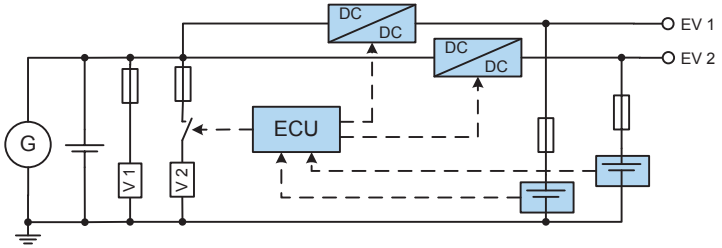
Für die Realisierung einer fehlertoleranten elektrischen Energieversorgung kann auf vielfältige Lösungen aus dem Stand der Technik zurückgegriffen werden, siehe Abbildung 4.5. Für ein Brake-by-Wire System wird in [33] ein Bordnetz beschrieben, das galvanisch vom Basisbordnetz getrennt ist und für jeden Bremskanal eine Zusatzbatterie beinhaltet. Lastspitzen, die während des schnellen Schließens einer elektromechanischen Bremse entstehen, werden von diesen Batterien abgedeckt, so dass das Basisbordnetz nur den mittleren Leistungsbedarf der Bremse abdecken muss. Innerhalb des Bordnetzes wird der Zustand sämtlicher Komponenten überwacht. Im Fehlerfall können Hochlastverbraucher durch ein Bordnetzmanagement deaktiviert werden, damit die Bremskreise bevorzugt mit Energie versorgt werden. Die Architektur bietet den Vorteil, dass die Struktur des konventionellen Bordnetzes beibehalten werden kann und eine klare Trennung zwischen dem konventionellen Bordnetz und dem sicherheitsrelevanten sowie fehlertoleranten Inselbordnetz besteht [33].

In einem X-by-Wire[10] Projekt wird eine Bordnetzarchitektur vorgeschlagen, die insgesamt aus einem Generator und zwei Batterien besteht [101]. Damit ist dieses Konzept mit dem generellen Trend der Fahrzeugindustrie vereinbar, zwei Batterien in einem Fahrzeug zu installieren, um die immer größer werdende Zahl der elektrischen Verbraucher zuverlässig zu versorgen [101]. Unklar ist jedoch, auf welchem Spannungsniveau die zweite Batterie in zukünftigen Bordnetzen arbeiten wird [11]. Die beiden Schalter im Bordnetz dieses Konzepts sind *normally-closed* und werden von einer Fehlerüberwachungseinheit bedarfsgerecht angesteuert.

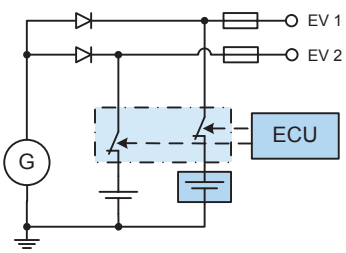
Eine andere Struktur wird für ein Steer-by-Wire System in Traktoren vorgeschlagen. Dieses System besteht aus einem *»Power Supply Module«*, das

[10] X-by-Wire ist der Oberbegriff für Systeme mit rein elektrischer Signalübertragung wie Steer-by-Wire, Brake-by-Wire oder Throttle-by-Wire.

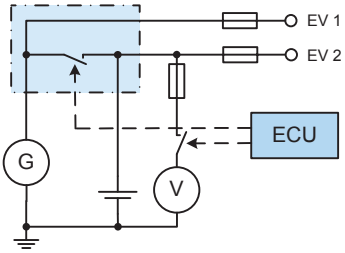
mit dem Generator und der Batterie sowie mit den beiden Kanälen des Lenksystems verbunden ist [82]. Das Modul sorgt dafür, dass im Falle eines Fehlers in der Batterie der erste Kanal weiterhin über den Generator und im Falle eines Fehlers im Generator der zweite Kanal weiterhin über die Batterie versorgt wird [81]. Gleichzeitig ermöglicht das Modul, dass die Fahrzeugbatterie im fehlerfreien Fall über den Generator geladen werden kann. Der Test der Batterie kann dadurch erfolgen, dass ein Verbraucher wie eine Notlenkpumpe zugeschaltet wird, während die Verbindung zum Generator unterbrochen ist [82].



(a) Brake-by-Wire Bordnetz für PKW nach [33, 1]



(b) X-by-Wire Bordnetz für PKW nach [101]



(c) Steer-by-Wire Bordnetz für Traktoren nach [82]

Abb. 4.5: Schematische Darstellung bekannter Konzepte für eine fehlertolerante Bordnetzarchitektur

Alle hier vorgestellten Konzepte erfüllen die qualitative Anforderung an die Fehlertoleranz (Einfehlersicherheit) und sorgen dafür, dass die Strom-

versorgung auf mindestens einem Kanal auch im Fehlerfall gewährleistet ist. Die quantitative Ausfallrate der unterschiedlichen Konzepte ist jedoch verschieden und muss mit den aus der Risikobewertung ermittelten quantitativen Anforderungen für die jeweilige Anwendung verglichen werden. Diese quantitative Bewertung muss im Einzelfall mit Hilfe geeigneter Methoden erfolgen [1]. Im Folgenden wird die elektrische Energieversorgung als fehlertolerant und ausreichend ausfallsicher angenommen und nicht näher betrachtet.

4.1.4 Sensorik

Die Auswahl und Festlegung einer geeigneten Sensorik hängt sehr stark von dem verwendeten Messprinzip, der Messstelle und der Schnittstelle zum Steuergerät ab, so dass eine allgemeingültige Festlegung nicht sinnvoll ist [101]. Zur Realisierung einer FSU besteht jedoch sowohl die Möglichkeit, einen einzigen Sensor zu verwenden, der die fail-silent Eigenschaft intern gewährleistet[11], als auch zwei einzelne Sensoren, die jeweils einkanalig aufgebaut sind und keine Fehlerbehandlung vornehmen. In diesem Fall findet die Plausibilisierung im zentralen Steuergerät statt.

Für die Verbindung der Sensoren mit den beiden Steuergeräten bestehen zwei verschiedene Möglichkeiten: Entweder wird jeder einzelne Sensor nur mit einem Steuergerät oder die jeweils redundanten Sensoren werden mit beiden Steuergeräten verbunden. Bei letztgenannter Variante besteht sowohl das Potential, Sensoren einzusparen, als auch die Gefahr, dass durch die Querkopplung der beiden Kanäle zusätzliche Ausfälle auftreten können, die die Zuverlässigkeit des Gesamtsystems reduzieren. In einem Steer-by-Wire System ist es sinnvoll, dass zwischen beiden Kanälen ein Austausch der Sensorinformation des Lenkwinkels oder der Position des Lenkzylinders

[11] Die Messaufnehmer derartiger Sensoren sind häufig intern redundant aufgebaut.

stattfindet. Andernfalls würden die Regler der beiden Steuergeräte bei kleinen Abweichungen der Ist-Werte gegeneinander arbeiten.

Zur Reduktion der Komplexität der Sensorik kann zudem von der strukturellen auf die analytische Redundanz übergegangen werden. Die Grundidee der analytischen Redundanz ist es, dass statt der direkten Messungen einer Systemgröße auch eine Berechnung dieser Systemgröße aus einer anderen Messgröße in Verbindung mit einem Systemmodell möglich ist. Dadurch kann auf einzelne Sensoren oder deren interne Redundanz verzichtet und die Komplexität der Hardwarekomponenten reduziert werden. Auf der anderen Seite erhöht sich jedoch der Entwicklungsaufwand und die Komplexität der Software und damit auch die potentielle Fehleranfälligkeit. In [28] wird nachgewiesen, dass durch Nutzung der analytischen Redundanz in einem Kraftfahrzeug die Sensoren für die Erfassung des querdynamischen Verhaltens bezüglich Sensorfehlern wie Offsetfehler oder Signaldrift überwacht werden können. Im betrachteten Steer-by-Wire System kann dieses Verfahren dazu genutzt werden, um die beiden Lenkwinkelsensoren mit failsilent Verhalten durch zwei weniger komplexe Lenkwinkelsensoren ohne failsilent Verhalten und je einen einkanaligen Gierratensensor im Steuergerät zu substituieren. Mit Hilfe der Gierratensensoren und der Information über die Fahrzeuggeschwindigkeit, die vom Fahrzeug an das Lenksystem übermittelt wird, können die beiden einkanaligen Lenkwinkelsensoren gegeneinander plausibilisiert werden, so dass auch ohne Drei- oder Vierfachredundanz stets der korrekte Lenkwinkel bekannt ist. Basis dafür ist der Zusammenhang zwischen dem Radlenkwinkel δ, der Gierrate $\dot{\varphi}$, der Fahrzeuggeschwindigkeit v und dem Radstand l für das ideale Einspurmodell und kleine Lenkwinkel [28]:

$$\dot{\varphi} = \frac{v}{l} \cdot \delta \tag{4.1}$$

Ein weiterer Vorteil ergibt sich aus der Tatsache, dass im fehlerfreien Fall (bei Gleichheit der beiden Signale der Lenkwinkel- und Gierratensensoren) ebenfalls die vom Fahrzeug übermittelte Fahrgeschwindigkeit plausibilisiert

werden kann. Damit ist gewährleistet, dass zur optimalen Berechnung der variablen Lenkübersetzung stets ein korrekter Wert der Geschwindigkeit verfügbar ist.

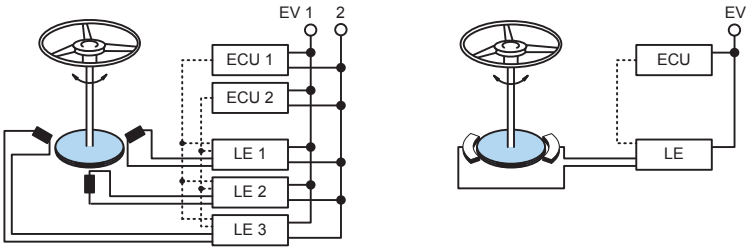
4.1.5 Handkraftaktor

Die allgemeine Festlegung der notwendigen Fehlertoleranz und Redundanz des Handkraftaktors ist nicht möglich, da der Handkraftaktor die zentrale Schnittstelle zwischen dem Lenksystem und dem Fahrer ist und die Fahrerreaktion bei Ausfall der Kraftrückmeldung stark vom jeweiligen Fahrzustand und der Art des Handkraftaktors (passiv, semi-aktiv, aktiv) abhängt. Es besteht beispielsweise bei einem plötzlichen Wegfall des Betätigungsmoments die Gefahr, dass der Fahrer das Lenkrad verreißt und von der Spur abkommt. Zudem hängt die Kritikalität eines Fehlers im Handkraftaktor auch von der Art ab, wie der Fahrer das Lenkrad festhält [64]. Insgesamt ist die Definition von zulässigen Obergrenzen für den Betätigungsmomentenfehler schwierig und eine Bestimmung von Grenzen für die zulässige Gierratenänderung im Fehlerfall scheint sinnvoller [64]. Dies würde zudem berücksichtigen, dass Betätigungsmomentenfehler bei unterschiedlichen Geschwindigkeiten unterschiedlich kritisch eingestuft werden. Die wichtigste Voraussetzung ist in jedem Fall die Anforderung, dass ein mechanisches Blockieren des Lenkrads konstruktiv ausgeschlossen sein muss und auch im Fehlerfall die gesetzlichen Grenzwerte für die Betätigungskraft nicht überschritten werden.

Neben den Sicherheitsanforderungen sind auch die funktionellen Anforderungen stark von der jeweiligen Anwendung abhängig und gehen weit über die reine Kraftrückmeldung hinaus. Ist die Simulation eines physikalischen Endanschlags der Lenkung gewünscht, so muss der Handkraftaktor einen großen Momentenbereich abdecken und es muss sichergestellt werden, dass während der Fahrt im Fehlerfall derart hohe Momente nicht auftreten können. Soll das Lenkrad eine variable Lenkradrückstellung bieten, so sind akti-

ve Handkraftaktoren notwendig, bei denen das Lenkradmoment über einen Elektromotor eingeprägt wird. Bei derartigen Systemen besteht im Fehlerfall die Gefahr, dass sich das Lenkrad unkontrolliert dreht, wenn der Fahrer das Lenkrad nicht fest genug hält. Mit Hilfe des Handkraftaktors kann zudem eine haptische Fahrerwarnung realisiert werden, entweder indirekt durch einen Anstieg des Betätigungsmoments wie bei konventionellen Lenksystemen oder direkt durch Aufprägen einer Vibration beziehungsweise einer dezenten Rüttelbewegung [55]. Darüber hinaus kann mit einem Handkraftaktor auch detektiert werden, ob der Fahrer noch aufmerksam ist und die Hände am Lenkrad hat [47].

Zur Realisierung eines Handkraftaktors sind passive Systeme in der Regel nicht ausreichend, da der Fahrer keine Rückmeldung des Lenksystems über den aktuellen Fahrzustand erhält [71]. Dabei muss jedoch beachtet werden, dass die Fahrgeschwindigkeit und der vom Fahrer gewohnte Grad an Rückmeldung bei Traktoren deutlich niedriger ist als bei PKW. In [54] wird ein aktiver Handkraftaktor für PKW konzipiert, der die Redundanz der drei Wicklungsstränge einer permanenterregten Synchronmaschine nutzt, um ein fail-operational Verhalten zu gewährleisten, siehe Abbildung 4.6.



(a) Fehlertoleranter aktiver Handkraftaktor für PKW nach [54]

(b) Semi-aktiver Handkraftaktor für Traktoren nach [81]

Abb. 4.6: Schematische Darstellung bekannter Konzepte für einen Handkraftaktor

Auf Grund der redundanten Spannungsversorgung und der beiden Steuergeräte sowie der dreifach vorhandenen Leistungselektronik kann auch im Fehlerfall das Betätigungsmoment aufrecht erhalten werden. In einem Steer-by-Wire System für Traktoren, das in [81] beschrieben ist, wird ein semi-aktiver Handkraftaktor eingesetzt, der im wesentlichen aus einer elektrisch ansteuerbaren Lenkradbremse beziehungsweise einem Dämpfer besteht. Die Bremse wird von nur einem Steuergerät angesteuert, da dessen Ausfall im Fehlerfall toleriert wird. In [99] werden weitere Beispiele für Eingabegeräte und Handkraftaktoren für Steer-by-Wire Fahrzeuge aufgeführt.

In Anlehnung an [70, 68] wird im Folgenden ein semi-aktiver Handkraftaktor mit einer passiven Rückfallebene als Kompromiss zwischen den beiden zuvor genannten Lösungen betrachtet:

- Elektrische Bremse oder Dämpfer: Ein Aktor dient der Modulierung des Betätigungsmoments in Abhängigkeit der jeweiligen Fahrsituation. Eine konstruktiv realisierte Grund-Dämpfung sorgt auch bei Stromausfall dafür, dass sich das Lenkrad nicht widerstandslos drehen lässt [38].
- Sicherer Strom-Abschaltpfad: Ein redundanter Abschaltpfad vermeidet die dauerhafte Aktuierung von Bremse oder Dämpfer im Fehlerfall.
- Federzentrierung: Eine Federzentrierung bietet eine Tendenz zur Selbstzentrierung der Räder ohne die Gefahr einer ungewollten Lenkradbewegung, die im Fehlerfall bei aktiven Handkraftaktoren auftreten kann, wenn der Fahrer die Hände nicht fest genug am Lenkrad hält.

4.1.6 Steuergeräte-Architektur

Bei der Steuergeräte-Architektur stellt die Verwendung einer einzigen FTU in einem Gehäuse den geringsten Komponentenaufwand dar. Die Entwicklung und Realisierung eines fehlertoleranten Steuergeräts ist jedoch eine

Herausforderung, da sich Fehler gemeinsamer Ursache wie Ausfälle in Folge von Wärmeentwicklung, Feuchtigkeitseintritt oder Überspannung kaum vermeiden und absichern lassen. Auf der anderen Seite entsteht durch die Realisierung einer FTU mit drei separaten Steuergeräten ein sehr großer Komponenten- und Bauraumbedarf sowie Verkabelungsaufwand, der ebenfalls schwer beherrschbar ist. Darüber hinaus ist die gewählte Architektur der restlichen Systemkomponenten nicht zum Betrieb mit drei Steuergeräten geeignet. Für das Gesamtsystem ist daher eine Steuergeräte-Architektur bestehend aus zwei FSUs zielführend, wie sie in Abbildung 4.3 dargestellt ist. Zur Reduktion von Fehlern gemeinsamer Ursache sollten die Steuergeräte an unterschiedlichen Montagestellen angeordnet und verkabelt sein. Falls neben der Lenkfunktion auch andere Maschinenfunktionen von den Steuergeräten übernommen werden müssen, so ist dabei besonders auf Querkopplungen zu achten, die die Ausfallrate des Lenksystems negativ beeinflussen.

4.1.7 Gesamtsystem

Der schematische Aufbau des konzipierten Steer-by-Wire Systems für Traktoren ist in Abbildung 4.7 und 4.8 dargestellt. Die Position des Lenkzylinders wird von zwei einkanaligen Sensoren erfasst und an die beiden Steuergeräte übermittelt. Als Absicherung gegen zu hohe und zu niedrige Drücke ist an jeder Zylinderkammer ein Druckbegrenzungs- und ein Nachsaugventil angeordnet. Der hydraulische Abgriff des Drucks für die Ansteuerung der Load-Sensing Verstellpumpe erfolgt im Zulauf zum Lenkzylinder mit Hilfe eines Wechselventils. Jeweils vier der acht 2/2-Wegeventile sind logisch zu einer Ventilgruppe zusammengefasst und werden von jeweils einem Steuergerät angesteuert. Die beiden hydraulischen Druckversorgungen sind über Rückschlagventile mit der gemeinsamen Zulaufleitung des Lenkventils verbunden. Die Hauptpumpe ist eine LS-Regelpumpe, die eine Lastmeldung durch ein Wechselventil sowohl von weiteren Verbrauchern als auch vom Lenksystem erhalten kann. Ein Prioritätsventil wird dazu verwendet, die

Lenkung gegenüber den weiteren Verbrauchern bevorzugt zu beliefern und dient der Abdrosselung des Pumpendrucks auf den notwendigen Zulaufdruck für die Lenkung, falls durch einen Nebenverbraucher ein höherer Druck angefordert wird. Dadurch wird der Druckabfall über den Zulaufventilen auf einen konstanten Wert eingeregelt. Die Notlenkpumpe ist eine Konstantstrompumpe, die beispielsweise über die Bewegungsenergie des Traktors angetrieben wird[12]. Eine Druckwaage an der Notlenkpumpe, die nur auf den Lastdruck der Lenkung reagiert, sorgt für die Bereitstellung des notwendigen Drucks. Durch eine geeignete Abstimmung von Prioritätsventil und Druckwaage kann die Notlenkpumpe zur Versorgung während der Fahrt und die Hauptpumpe zum Lenken im Stand eingesetzt werden. Durch einkanalige Drucksensoren an den beiden Zulaufleitungen, die mit beiden Steuergeräten verbunden sind, kann während der Fahrt eine Fehlererkennung in der Druckversorgung durchgeführt werden, um auf Pumpen- sowie Drucksensorfehler zu schließen. Durch eine geeignete Anordnung beziehungsweise Gestaltung des Öl-Reservoirs muss gewährleistet werden, dass das Lenksystem bei Undichtigkeiten in einem Nebenverbraucher auf Dauer funktionfähig bleibt, so lange das Fahrzeug in Bewegung ist.

Der semi-aktive Handkraftaktor besteht, wie in Kapitel 4.1.5 vorgestellt, aus einer elektrisch ansteuerbaren Bremse (siehe Abbildung 4.8). Die Ansteuerung erfolgt nur von einem Kanal, da ein Ausfall des Bremsmoments toleriert wird. Zusätzlich weist der Handkraftaktor eine Grunddämpfung und eine Federzentrierung auf, die verhindert, dass das Lenkrad kraftfrei drehbar ist und die ermöglicht, dass sich das Lenkrad selbstständig zentriert. Der Lenkradwinkel wird über zwei Winkelsensoren mit fail-silent Verhalten erfasst und an die beiden fail-silent Steuergeräte übermittelt. Auf Basis dieses Fahrerwunschs wird das Lenkventil angesteuert.

[12] Auf die Gleichrichtung der Bewegungsenergie bei der Vorwärts- und Rückwärtsfahrt wird an dieser Stelle nicht näher eingegangen. Die Wahl einer durch die Bewegungsenergie angetriebenen Notlenkpumpe zeigt nur ein mögliches Ausführungsbeispiel für eine fehlertolerante Druckversorgung.

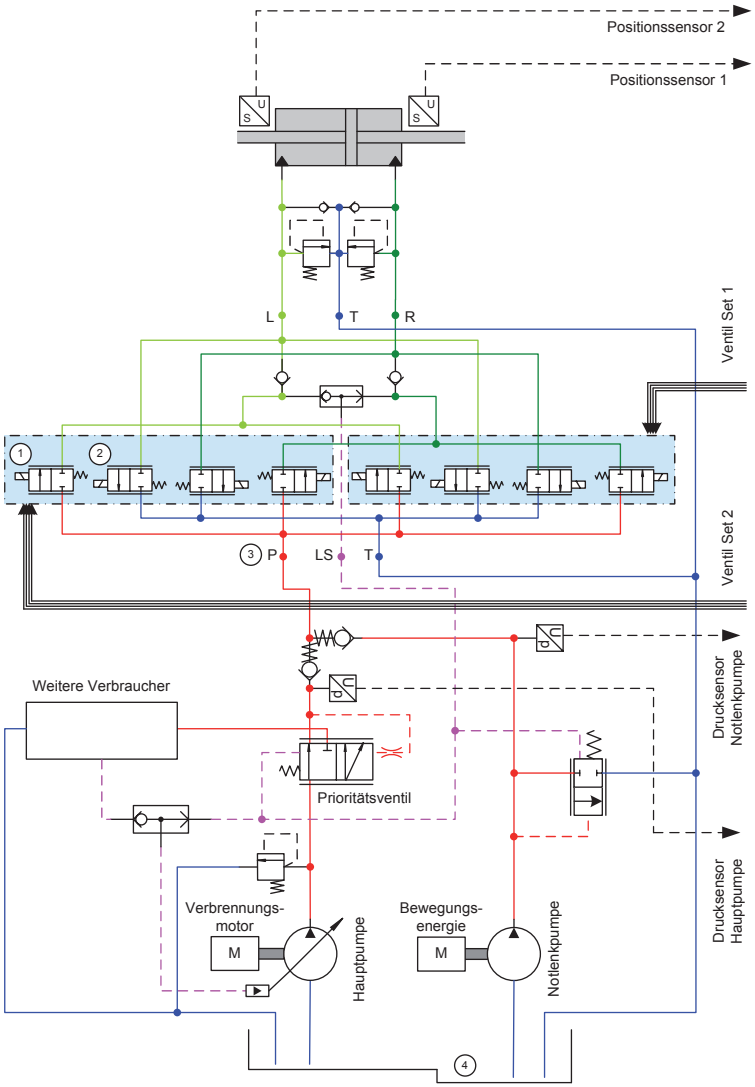


Abb. 4.7: Schematische Darstellung des entworfenen Steer-by-Wire Systems (1. Teil)

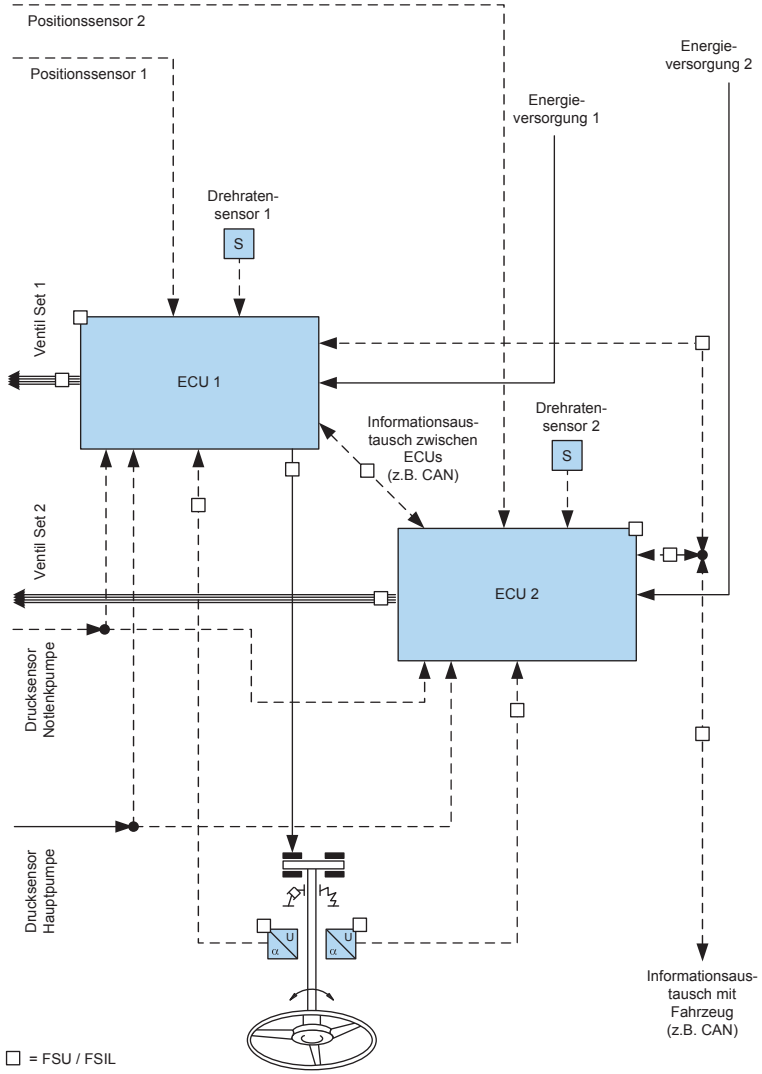


Abb. 4.8: Schematische Darstellung des entworfenen Steer-by-Wire Systems (2. Teil)

Über eine geeignete Schnittstelle mit fail-silent Verhalten können beide Steuergeräte Informationen austauschen. Jedes Steuergerät ist mit einem Gierratensensor ausgestattet, um die vom Fahrzeug übermittelte Fahrgeschwindigkeit mit dem aktuellen Lenkwinkel und der Gierrate zu plausibilisieren. Die Realisierung der fehlertoleranten Energieversorgung ist in Abbildung 4.8 nicht dargestellt.

4.2 Analyse

Im Anschluss an die Konzipierung des Steer-by-Wire Systems erfolgt eine sicherheitstechnische Analyse auf qualitativer und quantitativer Ebene. Dadurch soll die Entscheidung getroffen werden, ob die gewählte Architektur zur Realisierung einer fehlertoleranten Lenkung für Traktoren geeignet ist. Die qualitative Analyse dient dabei der Überprüfung der Fehlertoleranz (Einfehlersicherheit) und deckt unter anderem mögliche Probleme und Schwachstellen auf, die sich durch Querkopplungen innerhalb der Zweikanaligkeit oder durch Ausfälle in Folge gemeinsamer Ursachen ergeben könnten. In der quantitativen Analyse wird die Ausfallrate des Systems unter Berücksichtigung von Mehrfachfehlern betrachtet. Dies ist notwendig, um zu überprüfen, ob das konzipierte System die für die jeweilige Sicherheitseinstufung zulässige maximale Ausfallrate einhalten kann.

Die Beschreibung der Betrachtungseinheit für die folgende Analyse erfolgte bereits umfassend in Kapitel 4.1.7. Die Gefahrenanalyse und Risikobewertung sowie die Ableitung der Sicherheitsziele ist deckungsgleich mit der aus Kapitel 3.2, da das betrachtete Steer-by-Wire System auf Maschinenebene keine Gefahrenpotentiale bietet, die nicht schon bei der Betrachtung eines allgemeinen hydrostatischen Aktiv-Lenksystems analysiert wurden. Mit Kenntnis der genauen Systemstruktur ist es nun jedoch möglich, die zu berücksichtigenden Ursachen und konkrete Gegenmaßnahmen für die zuvor

ermittelten Gefahren zu bestimmen. Dies erfolgt im Rahmen der qualitativen Sicherheitsanalyse.

4.2.1 Sicherheitskonzept

Das Sicherheitskonzept des konzipierten Steer-by-Wire Systems wird im Folgenden für die Teilbereiche *»Fehlertoleranz und Fehlererkennung«* sowie *»Fahrerwarnung und Degradation«* zusammengefasst.

Fehlertoleranz und Fehlererkennung
Während des Starts des Fahrzeugs wird ein Selbsttest durchgeführt, bei dem die Funktionsfähigkeit aller Komponenten überprüft wird. In dem Selbsttest werden die 2/2-Wegeventile überprüft, indem diese in geeigneter Weise bestromt werden und aus der Systemreaktion auf Fehlerfreiheit geschlossen wird[13]. Während der Fahrt werden alle elektrischen und elektronischen Komponenten sowie die hydraulische Druckversorgung mit Hilfe der redundanten Sensorik oder durch analytische Redundanz überprüft. Die Überwachung des Lenkventils während der Fahrt auf hydraulische Fehler, die einen nennenswerten Einfluss auf das dynamische Verhalten der Lenkwinkelregelung haben, wird mit Hilfe einer modellbasierten Fehlererkennung realisiert, bei der verschiedene Mess- und Systemgrößen ausgewertet werden.

Die Fehlertoleranz im Lenkventil ist inhärent durch die gewählte Ventilarchitektur in Kombination mit dem passiv fehlertoleranten Regler gewährleistet. Die Ventilarchitektur und der Regler sind dabei so aufeinander abgestimmt, dass Einzelfehler des Typs A und B ohne Rekonfiguration bei nur geringem Einfluss auf die Regelgüte toleriert werden können. Der notwendige Volumenstrom wird im fehlerfreien Fall von beiden Ventilen gleichermaßen erzeugt. Die Fehlertoleranz in der Energieversorgung, der Sensorik und der

[13] Die Methoden zur Fehlererkennung für das fehlertolerante Lenkventil werden in Kapitel 5 hergeleitet und umfangreich beschrieben.

Steuergerätearchitektur ist durch die zuvor beschriebene Systemstruktur mit struktureller beziehungsweise analytischer Redundanz gewährleistet.

Fahrerwarnung und Degradation

Während des Selbsttests leuchten die Warnlampen des Lenksystems, bis dieser erfolgreich abgeschlossen ist. Anschließend ist das Fahrzeug lenkbereit. Nach Detektion eines Fehlers, der das Lenksystem in einen Zustand überführt, in dem ein weiterer Fehler zu einem Ausfall des Lenksystems führen könnte, wird der Fahrer optisch, akustisch oder haptisch gewarnt. Gleichzeitig wird in einer angemessenen Weise eine kontrollierte Drosselung der Geschwindigkeit eingeleitet und damit das Fahrzeug in einen sicheren Zustand überführt. Nach Eintritt eines Erstfehlers bleibt das Fahrzeug sicher lenkbar, ohne dass über das normale Maß hinausgehende kompensatorische Eingriffe oder höhere Betätigungskräfte oder -wege durch den Fahrer notwendig sind. Dies ist auch dann der Fall, wenn Ventilfehler des Typs B aufgetreten sind.

4.2.2 Qualitative Sicherheitsanalyse

Die qualitative Sicherheitsanalyse des konzipierten Steer-by-Wire Systems erfolgt in zwei Schritten I und II. In Schritt I werden alle Komponentenarten betrachtet, die im System eingesetzt werden[14]. Für diese Komponentenarten werden alle tatsächlich zu erwartenden Fehlerarten aufgelistet und darauf aufbauend Fehlerausschlüsse begründet. In Schritt II erfolgt die individuelle Betrachtung jedes einzelnen Bauteils des in Abbildung 4.7 und 4.8 dargestellten Lenksystems. Dabei werden alle nicht auszuschließenden Fehler der Komponentenarten aus Schritt I detaillierter analysiert, um zu ermitteln, welche Auswirkungen diese Fehler auf das Lenksystem haben und welche Maßnahmen zur Erkennung und Kompensierung nötig beziehungsweise

[14] Mechanische Bauteile, Lenkzylinder, Rohrleitungen aus Metall, Schlauchleitungen, Rückschlagventile, Wechselventile, Druckbegrenzungsventile, Wegeventile, Ölreservoir, Hydraulikpumpen, Sensoren, Kabel, Steuergeräte, Stromversorgung, Lenkradbremse

möglich sind. Durch die qualitative Sicherheitsanalyse werden damit Anforderungen an die spätere Funktionsentwicklung abgeleitet. Der Schritt II wird mit einer modifizierten und erweiterten Variante der bewährten Methode der *Fehlermöglichkeits- und Einflussanalyse (FMEA)* in Anlehnung an [1] durchgeführt. Die Bewertung der Fehlerfolgen erfolgt dabei differenziert entsprechend der Auswirkungen auf die Komponenten selbst, den einzelnen Kanal und das gesamte System. Statt der Bewertung der *»Bedeutung für den Kunden (B)«*, der *»Auftretenswahrscheinlichkeit (A)«* und der *»Entdeckungswahrscheinlichkeit (E)«* erfolgt in dieser modifizierten Variante ein Verweis zu den in der Gefahrenanalyse und Risikobewertung ermittelten Gefahren. Durch diese Analyse kann nachgewiesen werden, dass alle relevanten Fehler erkannt und kompensiert werden können und kein Einzelfehler zu einem gefährlichen Ausfall des Systems führt (*Single Point of Failure*). Zudem ist es auf Basis dieser Analyse möglich, Folgefehler und Fehler gemeinsamer Ursache im betrachteten System zu identifizieren und deren Relevanz einzuschätzen.

Entsprechend der in Tabelle 4.1 dargestellten Liste wurden die Fehlerarten und Fehlerausschlüsse für die zuvor genannten Komponentenarten in Schritt I bestimmt. Auf eine Darstellung der anderen Komponentenarten wird an dieser Stelle verzichtet. Tabelle 4.3 zeigt einen Ausschnitt der Fehlerliste von Schritt II für diejenigen Komponenten, die erst im Zusammenspiel mit anderen Teilsystemen die Fehlertoleranz gewährleisten und daher kein fail-silent Verhalten auf Komponentenebene aufweisen. Für die nicht aufgeführten Komponenten (FSUs) ist eine Komponentenentwicklung und Validierung ohne Betrachtung der Systemebene möglich. Aus der dargestellten Tabelle lassen sich die wesentlichen Anforderungen an den Regler und die Fehlererkennung ableiten, die in den folgenden Kapiteln nachgewiesen werden. Die Zeilen der Fehler, die im Rahmen des Nachweises weiter betrachtet werden, sind farblich markiert.

Funktion	Fehler	Ursachen (Beispiele)	Auswirkungen bzw. Folgen auf...		Fehler- bzw. Folgenvermeidung	Fehlererkennung
			... Komponente	... System		
Komponente ① : Einlassventil						
	Veränderung der Schaltzeiten	- Temperatureinfluss - Alterung / Verschleiß (Erhöhte Reibung) - Verschmutzung - Windungsschluss in Magnetspule	Weniger dynamische/genaue Dosierung des Volumenstroms	Reduktion der Regelgüte	Kompensierung durch robusten Regler	Modellbasierte Erkennung (sobald Regelgüte zu schlecht wird bzw. sobald Verhalten zu stark von nominalem Verhalten abweicht)
	Veränderung der Durchflusscharakteristik	- Temperatureinfluss - Alterung / Verschleiß - Windungsschluss in Magnetspule	Weniger genaue Dosierung des Volumenstroms	Reduktion der Regelgüte	Kompensierung durch robusten Regler	Modellbasierte Erkennung (sobald Regelgüte zu schlecht wird bzw. sobald Verhalten zu stark von nominalem Verhalten abweicht)
Ölzufluss in die Zylinderkammern dosieren	Nichtschalten oder nicht vollständiges Schalten / Hängenbleiben in Ausgangs-, Zwischen- oder Endstellung	- Partikel (Späne) - Verschmutzung - Kabelbruch in Magnetspule - Federbruch	Dosierung eines fehlerhaften Volumenstroms, ggf. auch wenn Volumenstrom nicht gewünscht ist	Reduktion der Regelgüte und ggf. erhöhte Systemdrücke	Kompensierung durch robusten Regler	Erkennung während Selbsttest und modellbasierte Erkennung (sobald Regelgüte zu schlecht wird bzw. sobald Verhalten zu stark von nominalem Verhalten abweicht)
	Interne Leckage und Veränderung der Leckage	- Verschleiß - Partikel - Konstruktionsprinzip (z.B. Schieberventil)	Dosierung eines fehlerhaften Volumenstroms, ggf. auch wenn Volumenstrom nicht gewünscht ist	Reduktion der Regelgüte und erhöhte Systemdrücke	Kompensierung durch robusten Regler	Erkennung während Selbsttest und modellbasierte Erkennung (sobald Regelgüte zu schlecht wird bzw. sobald Verhalten zu stark von nominalem Verhalten abweicht)
Komponente ② : Auslassventil						
	Veränderung der Schaltzeiten	- Temperatureinfluss - Alterung / Verschleiß (Erhöhte Reibung) - Verschmutzung - Windungsschluss in Magnetspule	Weniger dynamische/genaue Dosierung des Volumenstroms	Erhöhte oder erniedrigte Systemdrücke, ggf. Reduktion der Regelgüte	Kompensierung durch Druck-Regler in Prioritätsventil und Umlaufdruckwaage	Modellbasierte Erkennung (sobald Regelgüte zu schlecht wird bzw. sobald Verhalten zu stark von nominalem Verhalten abweicht)
	Veränderung der Durchflusscharakteristik	- Temperatureinfluss - Alterung / Verschleiß - Windungsschluss in Magnetspule	Weniger genaue Dosierung des Volumenstroms	Erhöhte oder erniedrigte Systemdrücke, ggf. Reduktion der Regelgüte	Kompensierung durch Druck-Regler in Prioritätsventil und Umlaufdruckwaage	Modellbasierte Erkennung (sobald Regelgüte zu schlecht wird bzw. sobald Verhalten zu stark von nominalem Verhalten abweicht)
Ölabfluss aus den Zylinderkammern ermöglichen	Nichtschalten oder nicht vollständiges Schalten / Hängenbleiben in Ausgangs-, Zwischen- oder Endstellung	- Partikel (Späne) - Verschmutzung - Kabelbruch in Magnetspule - Federbruch	Dosierung eines fehlerhaften Volumenstroms, ggf. auch wenn Volumenstrom nicht gewünscht ist	Reduktion der Regelgüte und erhöhte Systemdrücke	Kompensierung durch robusten Regler	Erkennung während Selbsttest und modellbasierte Erkennung (sobald Regelgüte zu schlecht wird bzw. sobald Verhalten zu stark von nominalem Verhalten abweicht)
	Interne Leckage und Veränderung der Leckage	- Verschleiß - Partikel - Konstruktionsprinzip (z.B. Schieberventil)	Dosierung eines fehlerhaften Volumenstroms, ggf. auch wenn Volumenstrom nicht gewünscht ist	Reduktion der Regelgüte und erhöhte Systemdrücke	Kompensierung durch robusten Regler	Erkennung während Selbsttest und modellbasierte Erkennung (sobald Regelgüte zu schlecht wird bzw. sobald Verhalten zu stark von nominalem Verhalten abweicht)
Komponente ③ : Redundante Druckversorgung (virtuelle Komponente)						
Öl auf dem notwendigen Druckniveau zum Lenken zur Verfügung stellen	Druckaufbau zu langsam	- Schwergängiges LS-Wechselventil	Druck kurzzeitig zu niedrig oder zu hoch (in beiden Pumpen)	Volumenstrom durch Einlassventile kurzzeitig zu hoch oder zu niedrig	Kompensierung durch robusten Regler	Modellbasierte Erkennung (sobald Regelgüte zu schlecht wird bzw. sobald Verhalten zu stark von nominalem Verhalten abweicht)
	Druck zu niedrig	- Interne Leckage in LS-Wechselventil - Externe Leckage in LS-Leitung	Druck dauerhaft leicht zu niedrig (in beiden Pumpen)	Volumenstrom durch Einlassventile dauerhaft leicht zu niedrig	Kompensierung durch robusten Regler	Erkennung während Selbsttest und modellbasierte Erkennung (sobald Regelgüte zu schlecht wird bzw. sobald Verhalten zu stark von nominalem Verhalten abweicht)
	Druck zu hoch	- Hängenbleiben von Umlaufdruckwaage oder Prioritätsventil in Endstellung	Druck dauerhaft zu hoch (Maximaldruck durch Druckbegrenzungsventil limitiert)	Volumenstrom durch Einlassventile dauerhaft zu hoch	Kompensierung durch robusten Regler	Signalbasierte Erkennung durch Vergleich der Sensorsignale beider Drucksensoren
Komponente ④ : Ölwanne						
u.a. Ölvorrat für die Pumpen zur Verfügung stellen	Externe Leckage in einer beliebigen Komponente	- mechanische Belastung - Korrosion - Verschleiß/Alterung von Dichtungen	Ölverlust in die Umgebung	Ölverlust in die Umgebung Bei zu niedrigem Ölstand Verlust der Lenkfähigkeit	Durch konstruktive Tank-Gestaltung Notölpumpe priorisiert mit Öl versorgen	Durch konstruktive Tank-Gestaltung Erkennung durch Ausfall der Hauptpumpe und/oder durch Füllstandsüberwachung in Tank

Tab. 4.3: Fehlerliste (modifizierte FMEA Vorlage) aus Schritt II für einzelne Bauteile des in Abbildung 4.7 und 4.8 dargestellten Steer-by-Wire Systems

Aus der qualitativen Sicherheitsanalyse lassen sich auch Beispiele für Folgefehler ableiten, die in Sicherheitsbetrachtungen als Einzelfehler und nicht als Mehrfachfehler zählen. Ein Folgefehler ergibt sich beispielsweise dann, wenn auf Grund einer externen Leckage in einer Komponente der Arbeitshydraulik das Ölreservoir leer läuft und infolge dessen die Hauptpumpe ausfällt. Dies muss durch eine entsprechende Auslegung des Systems verhindert werden. Von entscheidender Bedeutung sind auch solche Fehler, die auf einer gemeinsamen Ursache (*Common-Cause*) beruhen. Einige dieser Fehler und mögliche Abhilfemaßnahmen sind in der folgenden Liste aufgeführt:

- Durch eine mechanische oder thermische Belastung werden mehrere an der gleichen Stelle verlegte Kabel oder Bauteile zerstört. Durch eine einzelne Ursache könnten auf diese Weise beide Kanäle gleichzeitig ausfallen. Die Kabel der einzelnen Kanäle sollten daher an unterschiedlichen Stellen verlegt werden, falls diese außergewöhnlich hohen mechanischen oder thermischen Belastungen ausgesetzt sind.

- Eine Verschmutzung im Hydrauliksystem führt zu einer Schwergängigkeit oder Leckage in mehreren Ventilen zur gleichen Zeit. Dies muss durch den passiv fehlertoleranten Regler kompensierbar sein. Zur Vermeidung muss ein geeignetes Filtrationssystem vorgesehen werden.

- Durch einen elektrischen Fehler in einem Kommunikations-Bus fallen alle mit diesem Bus verbundenen Teilnehmer aus. Durch eine geeignete elektrische Trennung muss gewährleistet sein, dass durch den Bus-Ausfall lediglich die Kommunikation der Bus-Teilnehmer, nicht jedoch die eigentliche Funktionalität der Teilnehmer ausfällt. Dadurch ist gewährleistet, dass die anderen Komponenten durch redundante Signale einen Notbetrieb aufrecht erhalten können.

- Durch einen Programmierfehler fallen zwei redundante Module zur gleichen Zeit aus. Dadurch kann die Fehlertoleranz gefährdet werden. Die Komplexität der Software sollte so gering wie möglich gehalten

werden. In besonderen Fällen kann eine unabhängige und diversitäre Softwareentwicklung notwendig sein.

Die Überprüfung des Systems auf Common-Cause-Fehler (CCF) entsprechend der Vorgaben der ISO-Norm 25119 erfolgt durch die Bewertung von verschiedenen unterschiedlich stark gewichteten Kriterien, siehe Tabelle 4.4. In Summe müssen mindestens 65 Punkte erreicht werden, um einen angemessenen Schutz gegenüber Fehlern gemeinsamer Ursache zu gewährleisten. Anhand der Liste ist erkennbar, dass auch nicht-diversitär realisierte redundante Systeme, wie das vorgeschlagene Steer-by-Wire Konzept, bei Erfüllung der anderen Kriterien einen angemessenen Schutz gegenüber CCF bieten können.

Trennung	
Physikalische Trennung zwischen Signal- und Leistungspfaden?	ja = 15 Punkte
Diversität	
Verwendung unterschiedlicher Prinzipien, Konstruktionen oder Technologien für redundante Pfade?	ja = 20 Punkte
Konstruktion	
Absicherung gegenüber Überspannung und -strom sowie nicht elektrische Überbeanspruchung?	ja = 15 Punkte
Existieren langjährige Erfahrungen mit den ausgewählten Komponenten in der jeweiligen Belastungssituation?	ja = 5 Punkte
Analyse	
Berücksichtigung der Ergebnisse der FMEA bezüglich CCF?	ja = 5 Punkte
Qualifikation	
Ausreichende Schulung der Entwickler bezüglich CCF?	ja = 5 Punkte
Umgebungsbedingungen	
Überprüfung bezüglich elektromagnetischer Verträglichkeit?	ja = 25 Punkte
Überprüfung bezüglich Verträglichkeit gegenüber Bedingungen wie Temperatur, Vibration, Feuchtigkeit, …?	ja = 10 Punkte

Tab. 4.4: Bewertungskriterien zur Verhinderung von Fehlern gemeinsamer Ursache nach [42]

Die in Kapitel 4.1.1 formulierten Annahmen zur Fehlertoleranz und Fehlererkennung können auf Grundlage der qualitativen Bewertung um weitere

relevante Fehlerfälle ergänzt werden. Aufgelistet werden lediglich die Fehlerfälle, die im Rahmen der Arbeit betrachtet werden:

- Offene oder geschlossene Ein- oder Auslassventile (entspricht Fehlertyp A und B)
- Leckage an mehreren Wege-Ventilen
- Ausfall der Druckversorgung (Versorgungsdruck maximal)

4.2.3 Quantitative Sicherheitsanalyse

Für die Quantifizierung der Zuverlässigkeitseigenschaften eines sicherheitsrelevanten Systems gibt es verschiedene Methoden, die für unterschiedliche Systeme und Fragestellungen geeignet sind. Laut [1] bieten Markov-Modelle vielfältige Vorteile und Freiheiten für die Modellierung komplexer sicherheitsrelevanter Systeme. Bei Wahl dieser Methode lassen sich insbesondere Effekte wie die Unterscheidung von entdeckten und unentdeckten Fehlern bei der Fehlererkennung sowie eine am System durchgeführte Reparatur oder Wartung sehr einfach abbilden. In [4] wird demgegenüber die Ausfallrate eines stationären hydraulischen Systems mit unabhängigen Steuerkanten mit Hilfe eines Sicherheitsblockdiagramms für die Sicherheitsfunktion *»Sicherer Stopp«* berechnet. Für ein fehlertolerantes Steer-by-Wire System mit vielfältigen Kombinationsmöglichkeiten für gefahrbringende Ventil-Ausfälle (Fehlertyp A und B) und bei dem der Stopp des Aktuators kein sicherer Zustand ist, liefert dieser Ansatz jedoch eine zu pessimistische Abschätzung, mit der das notwendige Sicherheitslevel quantitativ nicht nachgewiesen werden kann.

Markov-Modelle sind diskrete Zustandsmodelle, bei denen für jeden möglichen Zustand die Wahrscheinlichkeit festgelegt ist, mit der ein Wechsel

in einen der anderen System-Zustände erfolgt. Bei homogenen Markov-Prozessen ist die Aufenthaltswahrscheinlichkeit in den Zuständen exponentialverteilt, da von einer zeitlich konstanten Übergangsrate ausgegangen wird [1]. Für den kontinuierlichen Fall hat das Markov-Modell die Struktur eines Differentialgleichungssystems erster Ordnung:

$$\frac{d\mathbf{P}(t)}{dt} = \mathbf{Q} \cdot \mathbf{P}(t) \tag{4.2}$$

In dieser Gleichung bezeichnet der Vektor

$$\mathbf{P}(t) = \begin{pmatrix} P_1(t) \\ P_2(t) \\ \dots \\ P_n(t) \end{pmatrix} \tag{4.3}$$

die zeitabhängige Aufenthaltswahrscheinlichkeit für jeden der modellierten Zustände 1 bis n. Die Generatormatrix

$$\mathbf{Q} = \begin{bmatrix} -\sum_{k=2}^{n} \lambda_{1k} & \lambda_{21} & \dots & \lambda_{n1} \\ \lambda_{12} & -\sum_{\substack{k=1 \\ k\neq 2}}^{n} \lambda_{2k} & \dots & \lambda_{n2} \\ \dots & \dots & \dots & \dots \\ \lambda_{1n} & \lambda_{2n} & \dots & -\sum_{k=1}^{n-1} \lambda_{nk} \end{bmatrix} \tag{4.4}$$

enthält die Übergangsraten λ_{ij}, die beschreiben, wie wahrscheinlich der Übergang vom Zustand i in den Zustand j ist[15].

Im vorliegenden Steer-by-Wire System erfolgt die Berechnung der Ausfallrate für das Aktor-Teilsystem *»fehlertolerantes Lenkventil«*, da dieses den Kern der Arbeit und den Unterschied zum Stand der Technik darstellt. Die

[15] Auf der Hauptdiagonale ist die negative Gesamtrate für einen Wechsel in einen anderen Zustand angeordnet.

Berechnung der Ausfallraten der anderen Teilsysteme (Sensorik, Steuergeräte, Energieversorgung) muss erfolgen, sobald eine konkrete Anwendung und die Art der Realisierung dieser Komponenten festgelegt wurde. Da die durchschnittliche Ausfallrate eines sicherheitsbezogenen Systems in der Regel zu 50 Prozent von der Aktorik bestimmt wird [26], ergibt sich durch deren Berechnung ein guter Anhaltspunkt für die zu erwartende Ausfallrate des Gesamtsystems. Für die Erstellung des in Abbildung 4.9 dargestellten Markov-Modells wurden verschiedene Annahmen getroffen und Abschätzungen zur sicheren Seite vorgenommen, um die Modellkomplexität ausreichend gering zu halten:

- Das Lenkventil ist einfehlersicher, da Einzelfehler in einem beliebigen Wegeventil toleriert werden können (Annahme 1 *»Fehlertoleranz«*). Der Zustand, in dem ein Einzelfehler im Lenkventil vorliegt, ist sicher (Zustand 2). Für die Modellierung wird jeder Zweitfehler (Zustand 3) als gefahrbringend angesehen, auch wenn viele Zweitfehler nicht zu einem Ausfall des Lenksystems führen[16]. Für die mittlere Zeit bis zum gefahrbringenden Ausfall eines einzelnen Ventils (Übergang von Zustand 1 in Zustand 2) kann ein Wert von 150 Jahren[17] angenommen werden wenn gewährleistet ist, dass bei der Ventilentwicklung grundlegende und bewährte Sicherheitsprinzipien angewendet werden und das Ventil innerhalb der Spezifikationen des Herstellers betrieben wird [18]. Daraus ergibt sich unter Annahme einer exponentialverteilten Überlebenswahrscheinlichkeit eine Ausfallrate von $\lambda_V = \frac{1}{MTTF_d} = 7,7 \cdot 10^{-7}$ 1/h. Durch die Annahme einer über die Lebensdauer konstanten Ausfallrate können Alterungs- und Verschleißeffekte nicht abgebildet werden. Befindet sich das Lenkventil im fehlerfreien Zustand 1, so ist die Ausfallrate um den Faktor 8 größer, da alle acht Ventile ausfallen

[16] Dies ist beispielsweise dann der Fall, wenn zwei Fehler des Typs A auf unterschiedlichen Seiten des Lenkzylinders auftreten.

[17] Ein $MTTF_d$-Wert von 150 Jahren bedeutet bei einer exponentialverteilten Überlebenswahrscheinlichkeit, dass nach 150 Jahren 63 Prozent der Ventile gefahrbringend ausgefallen sind.

können. Sobald ein Ventil ausgefallen ist (Zustand 2 und 5), können anschließend nur noch sieben Ventile ausfallen.

- Wenn das System gefahrbringend ausgefallen ist, wird es nicht mehr repariert. Dies führt dazu, dass gefahrbringende Zustände (Zustand 3) absorbierend sind und nicht mehr verlassen werden können [1].

- Die mittlere Zeit bis zum Selbsttest ($MTTT$) wird mit 24 Betriebsstunden angenommen. Daraus ergibt sich eine Testrate von $\lambda_T = 4,2 \cdot 10^{-2}$ 1/h. Es wird davon ausgegangen, dass durch den Selbsttest alle Ventilfehler des Typs A und B sicher erkannt werden können und daher der höchstmögliche Diagnosedeckungsgrad (DC) von 0,99 für die Berechnung verwendet wird (Zustand 4). Das bedeutet, dass in jedem hundertsten Test ein Fehler nicht erkannt wird (Zustand 5). Obwohl zu einem späteren Zeitpunkt unter anderen Randbedingungen die Möglichkeit besteht, dass der Fehler dennoch erkannt wird, wird die pessimistische Annahme getroffen, dass eine Wiederholung des Tests zum gleichen Ergebnis führt (kein Übergang von Zustand 5 in Zustand 2 möglich). Die modellbasierte Fehlererkennung einzelner Ventilfehler wird für die quantitative Berechnung vernachlässigt.

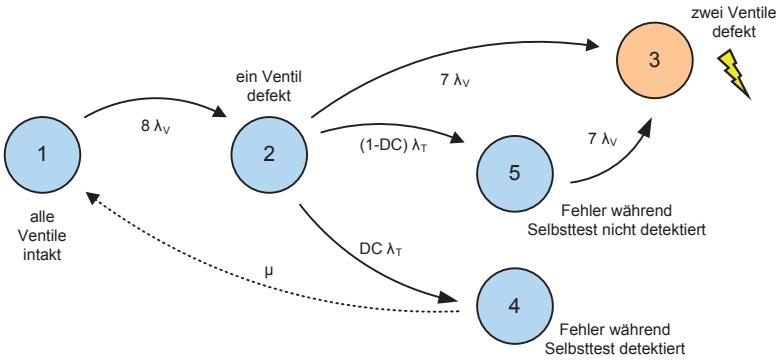


Abb. 4.9: Grafische Darstellung des vereinfachten Markov-Modells für das Steer-by-Wire Ventil mit unabhängigen Steuerkanten

- Nach der Fehlererkennung durch den Selbsttest im Stand bleibt das Fahrzeug bis zur Reparatur im sicheren Zustand (Fahrgeschwindigkeit gedrosselt). Es wird die Annahme getroffen, dass das Fahrzeug nach einer mittleren Betriebsdauer von 24 Betriebsstunden durch Reparatur in den fehlerfreien Ausgangszustand versetzt wird ($MTTR$). Daraus ergibt sich eine Reparaturrate von $\mu = 4,2 \cdot 10^{-2}$ 1/h (Übergang von Zustand 4 in Zustand 1).
- Die maximale Betriebsdauer des Lenksystems t_{max} beträgt 10.000 Stunden. Zur quantitativen Beschreibung des Lenkventils wird statt der durch die einschlägigen Normen vorgeschlagenen durchschnittlichen Ausfallrate die maximale Ausfallrate entsprechend der in [1] vorgestellten Fehlersequenzrate verwendet (siehe Gleichung 4.5).

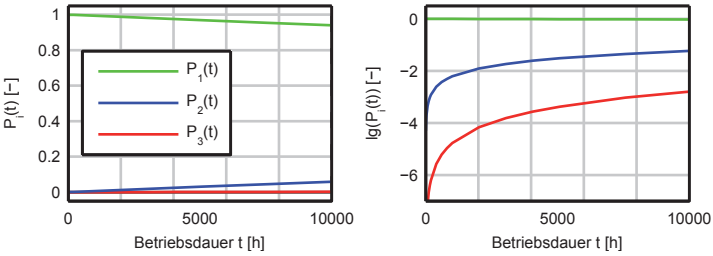
$$FSR_3(t) = \lambda_{13}(t) = \frac{\frac{dP_3(t)}{dt}}{P_1(t)} \tag{4.5}$$

Für das fehlertolerante Lenkventil ergibt sich unter Berücksichtigung der zuvor genannten Annahmen die folgende Generatormatrix:

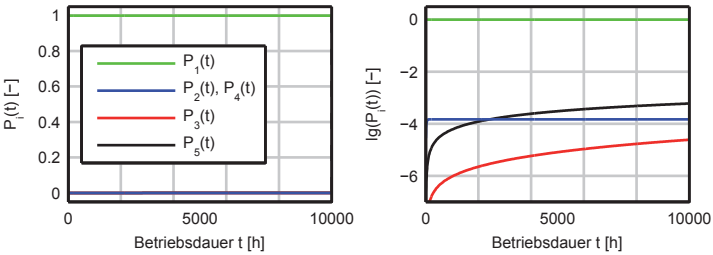
$$\mathbf{Q} = \begin{bmatrix} -8 \cdot \lambda_V & 0 & 0 & \mu & 0 \\ 8 \cdot \lambda_V & -7 \cdot \lambda_V - \lambda_T & 0 & 0 & 0 \\ 0 & 7 \cdot \lambda_V & 0 & 0 & 7 \cdot \lambda_V \\ 0 & DC \cdot \lambda_T & 0 & -\mu & 0 \\ 0 & (1-DC) \cdot \lambda_T & 0 & 0 & -7 \cdot \lambda_V \end{bmatrix} \tag{4.6}$$

Die dritte Spalte enthält keine Einträge, da der dritte Zustand ein absorbierender Zustand ist, der beschreibt, dass zwei Ventile defekt und damit das Lenkventil definitionsgemäß gefahrbringend ausgefallen ist, auch wenn es in der Realität Zweitfehler gibt, die nicht zu einem Verlust der Lenkfähigkeit führen. Unter der Annahme, dass sich das System zum Zeitpunkt $t = 0$ h mit einer Wahrscheinlichkeit von 100 Prozent im Zustand 1 befindet, ergeben

sich nach numerischer Lösung von Gleichung 4.2 die in Abbildung 4.10 dargestellten Aufenthaltswahrscheinlichkeiten für die verschiedenen Zustände sowie die resultierende Fehlersequenzrate.



(a) Ohne Selbsttest und Reparatur ($FSR_3(t_{max}) = 2,9 \cdot 10^{-7}$ 1/h)



(b) Mit Selbsttest und Reparatur ($FSR_3(t_{max}) = 4,0 \cdot 10^{-9}$ 1/h)

Abb. 4.10: Numerische Lösung der Zustandswahrscheinlichkeiten für das vereinfachte Markov-Modell in zwei verschiedenen Konfigurationen

Als Referenz wurde das System ohne Selbsttest und Reparatur modelliert (Zustand 4 und 5 existieren nicht). Es ist erkennbar, dass die Wahrscheinlichkeit von Zustand 1 im Laufe der Betriebsdauer abfällt, während die Wahrscheinlichkeit von Zustand 2 und 3 ansteigt. Auf Grund der im Vergleich zur maximalen Betriebsdauer niedrigen Ausfallraten wird ein stationärer Zustand während der Betriebsdauer nicht erreicht. Dieser ist dadurch gekennzeichnet, dass sich alle Lenkventile im ausgefallenen Zustand 3 befinden ($P_3(t) = 1$). Das bedeutet, dass die Wahrscheinlichkeit für den Übergangszustand 2 zu

einem bestimmten Zeitpunkt ein Maximum hat und anschließend auf den Wert Null abfällt. Für die Fehlersequenzrate ergibt sich ein Wert, der dem Performancelevel d[18] zugeordnet werden kann, siehe Abbildung 4.11. Für ein fehlertolerantes Lenkventil für Traktoren ist dieses Sicherheitslevel nicht ausreichend. Am Ende der Betriebsdauer haben 5,8 Prozent aller Lenkventile einer großen Grundgesamtheit ein defektes Ventil, während 0,16 Prozent aller Lenkventile ausgefallen sind (2 defekte Ventile).

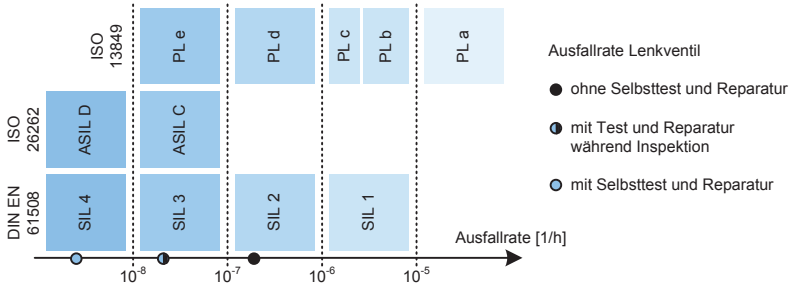


Abb. 4.11: Ausfallrate der zuvor untersuchten Varianten im Vergleich zu den qualitativen Anforderungen der einschlägigen Sicherheitsnormen bezüglich zufälliger Hardwarefehler [18, 16, 43]

Bei Berücksichtigung des Selbsttests und der Reparatur ergeben sich Wahrscheinlichkeiten, die etwa um zwei Größenordnungen besser sind als ohne Selbsttest und Reparatur. Die Fehlersequenzrate entspricht mit $FSR_3(t_{max}) = 4,0 \cdot 10^{-9}$ 1/h einem Wert, der quantitativ im Bereich des Levels *SIL 4* oberhalb des Performancelevels *e* liegt. Am Ende der Betriebsdauer ergibt sich für den Zustand 3 eine Wahrscheinlichkeit von unter 0,003 Prozent. Die Zustände 2, 4 und 5 haben ebenfalls eine sehr niedrige Wahrscheinlichkeit, da verglichen mit der geringen Ausfallrate eines Ventils der Selbsttest häufig und die Reparatur schnell durchgeführt wird und sich das Lenkventil daher fast

[18] In der ISO-Norm 25119 [42] sind keine quantitativen Anforderungen an die zulässige Ausfallrate angegeben, so dass die entsprechende Einstufung der ISO-Norm 13849 [18] verwendet wurde. Zudem ist die ISO-Norm 25119 nur für elektrische und elektronische Systeme anwendbar.

ausschließlich im Zustand 1 befindet. Auch in dieser Modellierungsvariante wird der stationäre Zustand nicht erreicht. Das Markov-Modell bietet die Möglichkeit, mit geringem Aufwand die Abhängigkeit der Ausfallrate des Lenkventils von der mittleren Testrate zu ermitteln. Eine Reduktion dieser auf Werte unter 24 Betriebsstunden bringt dabei nur einen marginalen Vorteil für die Ausfallrate. Demgegenüber würde ein lediglich während der regulären Inspektion (alle 1.000 Betriebsstunden) durchgeführter Selbsttest des Lenkventils zu einer um den Faktor 10 höheren Ausfallrate von $3,6 \cdot 10^{-8}$ 1/h führen. Es kann daher die Aussage getroffen werden, dass eine Durchführung des Selbsttests alle 24 Betriebsstunden ausreichend ist. Der Faktor zwischen der Testrate und der Rate für den Eintritt eines Zweitfehlers ist ungefähr 7.500 und liegt damit weit über dem vorgeschlagenen Wert von 100 [35]. Zur Gewährleistung einer niedrigen Ausfallrate ist es in der Praxis daher ausreichend, den Selbsttest nicht häufiger als bei jedem Start der Maschine durchzuführen.

Die quantitative Bewertung zeigt, dass selbst mit dem Pauschalwert für den $MTTF_d$-Wert von Hydraulikventilen von 150 Jahren eine niedrige Gesamt-Ausfallrate für das fehlertolerante Lenkventil mit unabhängigen Steuerkanten und damit auch für das Gesamtsystem erreicht werden kann. Trotz dieses Ergebnisses ist es erforderlich, dass die 2/2-Wegeventile eine möglichst geringe Komplexität und damit hohe Zuverlässigkeit aufweisen, da auch nichtgefahrbringende Ausfälle des Lenksystems einen finanziellen und zeitlichen Aufwand (Reparatur) für den Endanwender bedeuten.

5 Funktionsentwurf für ein fehlertolerantes Lenkventil

Ziel dieses Kapitels ist die Darstellung des Entwurfs des passiv fehlertoleranten Reglers und der Fehlererkennungsmethoden, die für die Realisierung des zuvor beschriebenen Steer-by-Wire Ventils notwendig sind. Die Validierung dieser Methoden erfolgt in Kapitel 6. Um geeignete Methoden auswählen zu können, erfolgt vor dem Entwurf eine umfassende Analyse des Systemverhaltens im Falle des Vorliegens von Fehlern des Typs A und B.

5.1 Systemverhalten

Für die Analyse des Systemverhaltens des Lenkventils wird die Systemstruktur, wie in Abbildung 5.1 dargestellt, vereinfacht. Ohne Beschränkung der Allgemeinheit der folgenden Aussagen für das Lenkventil wird dabei auf die Betrachtung der Redundanz in der Energieversorgung, der Sensorik und bei den Steuergeräten verzichtet. Das Lenkventil wird mit dem Pumpendruck p_P versorgt, der von der variablen Druckversorgung so eingeregelt wird, dass dieser um eine definierte Druckdifferenz Δp über dem Lastdruck p_{LS} liegt. Der Lastdruck ergibt sich wiederum durch den Abgriff am Lenkzylinder mittels eines Wechselventils aus dem höheren der beiden Drücke p_L und p_R im Zulauf zum Lenkzylinder. Die einzelnen Wegeventile werden als ideale Blende mit variablem Querschnitt und turbulenter Strömung betrachtet, dessen Durchströmung durch Gleichung 5.1 beschrieben wird [66].

$$Q = \alpha_D \cdot A(u) \cdot \sqrt{2\Delta p/\rho} \tag{5.1}$$

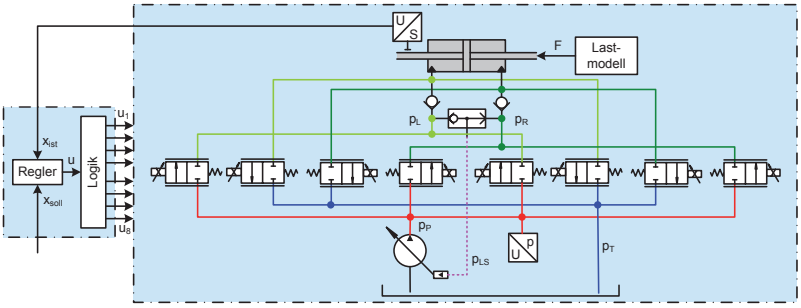


Abb. 5.1: Vereinfachte Darstellung der Systemstruktur für die Analyse des Verhaltens des fehlertoleranten Lenkventils

Da durch die LS-Regelung der Druckabfall über den Einlassventilen auf einen konstanten Wert eingeregelt wird, kann durch die Öffnungsfläche der Einlassventile der Volumenstrom proportional verstellt werden. Das Prioritätsventil (siehe Abbildung 4.7) sorgt dafür, dass diese Druckdifferenz auch dann anliegt, wenn ein an die gleiche Pumpe angeschlossener Nebenverbraucher einen höheren Druck anfordert. Der Volumenstrom Q ist, bei Modellierung des Ventils als Blende mit turbulenter Strömung, keine Funktion der Viskosität[1] und damit unabhängig von der Temperatur des Fluids [27]. Aus Gleichung 5.1 ergibt sich damit der in Gleichung 5.2 dargestellte proportionale Zusammenhang zwischen der Stellgröße u und dem Volumenstrom Q.

$$Q \sim A(u) \cdot \sqrt{\Delta p} = A_V \cdot u \cdot \sqrt{\Delta p} \tag{5.2}$$

Im Lenkzylinder baut sich durch den zufließenden Volumenstrom ein Druck auf, der eine Bewegung entgegen der Lastkraft F ermöglicht. Das Modell der Lastkraft wurde aus Fahrzeugmessungen abgeleitet und parametriert,

[1] Durch weitere hydraulische Widerstände im realen Ventil und innerhalb des Ventilblocks wird sich eine Viskositäts- und damit Temperaturabhängigkeit für den Volumenstrom ergeben, der bei der Auslegung des Ventils auf den maximal benötigten Volumenstrom berücksichtigt werden muss. Unter der Annahme, dass die Temperatur innerhalb des Ventilblocks identisch ist, hat diese Abhängigkeit jedoch keinen Einfluss auf die Bilanzgleichung 5.3 und damit auf die in diesem Kapitel gemachten Aussagen zur Fehlertoleranz.

siehe Anhang A.2.1. Da die Höhe der Rückstellkräfte und der Anteil des visko-elastischen Verhaltens stark variieren, wurden für unterschiedliche Fahrzeuggeschwindigkeiten Parametersätze bestimmt. Dabei sind die auftretenden Lenkkräfte im Stand am höchsten und fallen bereits bei sehr niedrigen Geschwindigkeiten stark ab. Die Ist-Position x_{ist} des Lenkzylinders wird durch den Regler erfasst und mit dem Soll-Signal x_{soll} verglichen, das vom Fahrer oder einem überlagerten Spurführungsregler vorgegeben wird. Aus der Regeldifferenz berechnet der Regler die Stellgröße u, die in einem separaten Logik-Modul auf die einzelnen Ventile aufgeteilt wird ($u_{1..8}$). Da bei einem Sprung der Stellgröße u die Lenkzylinderposition x kontinuierlich ansteigt, weist die Regelstrecke ein integrales Verhalten auf.

Im Fehlerfall ändert sich das dynamische Verhalten des Systems. Bei Fehlertyp A an einem Auslassventil ist in eine Lenkrichtung der Ablaufquerschnitt reduziert, was zu einem höheren Druckabfall am intakten Auslassventil führt. Dieser erhöhte Druckabfall führt zu höheren Kammerdrücken und damit auch zu einem erhöhten Versorgungsdruck. Durch den konstanten Druckabfall an den Einlassventilen hat dieser Fehler jedoch keine Auswirkungen auf den fließenden Volumenstrom und damit das Lenkverhalten, solange der maximale Zulaufdruck der Pumpe nicht erreicht ist. Fehlertyp A an Einlassventilen führt dazu, dass der Volumenstrom in eine Lenkrichtung nur noch von einem Ventil erzeugt wird. Dies entspricht einer Reduktion der Systemverstärkung um 50 Prozent. Um die gewünschte Lenkgeschwindigkeit zu erreichen, muss das intakte Ventil stärker angesteuert werden. Dies ist bis zur halben Maximalgeschwindigkeit des Lenkzylinders möglich. Durch die geringen Auswirkungen von Fehlertyp A müssen Fehler dieser Art im Reglerentwurf nicht gesondert berücksichtigt werden.

Wesentlich gravierendere Auswirkungen haben im Vergleich dazu Fehler des Typs B. In Abbildung 5.2 sind alle Kombinationen aus Fehler- und Lastfällen für eine Lenkrichtung dargestellt, die auftreten können. Besonders kritisch

sind dabei die Fälle, in denen die vom Fahrer gewünschte Lenkzylindergeschwindigkeit nicht mehr erreicht werden kann.

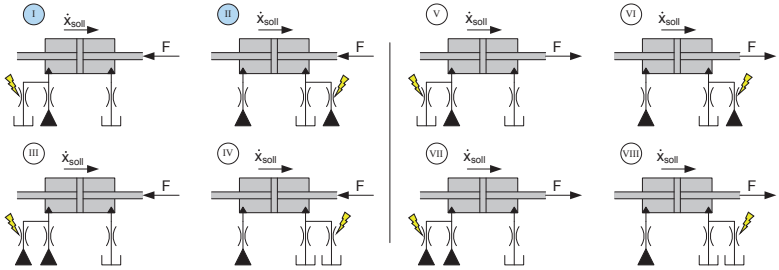


Abb. 5.2: Mögliche Fehler- und Lastfälle für Fehlertyp B

- Fall I: Ein offenes Auslassventil auf der Zulaufseite sorgt dafür, dass nur ein Teil der zufließenden Ölmenge zu einer Bewegung des Lenkzylinders führt. Externe Lastkräfte, die entgegen der Bewegungsrichtung wirken, erhöhen den Kammerdruck p_L und führen zu einem höheren Volumenstrom durch das fehlerhafte Ventil. Sobald die Lastkräfte einen kritischen Wert erreichen, fließt der gesamte zufließende Volumenstrom zum Tank ab und der Lenkzylinder kann nicht mehr verstellt werden.

- Fall II: Ein offenes Einlassventil auf der Ablaufseite erhöht den Kammerdruck p_R, da der fehlerhaft zufließende Volumenstrom über das Ablaufventil abgeführt werden muss. Solange die Pumpe nicht in der Sättigung ist, kann über die intakten Zulaufventile der zum Lenken benötigte Volumenstrom zugeführt werden. Sind die externen Lastkräfte jedoch so hoch, dass der Maximaldruck oder die maximale Fördermenge der Pumpe erreicht ist, dann reduziert sich die verfügbare Lenkgeschwindigkeit.

- Fall III: In diesem Fall besteht durch das offene Einlassventil die Gefahr, dass sich der Lenkzylinder schneller als gewünscht bewegt.

In diesem Fall kann der Volumenstrom jedoch über das Ablaufventil gedrosselt werden.

- Fall IV: Dieser Fall hat vernachlässigbar geringe Auswirkungen auf die gewünschte Lenkzylinderbewegung, da die Lenkgeschwindigkeit weiterhin über den Zulaufquerschnitt bestimmt werden kann.
- Fall V: Wirkt die externe Lastkraft in Richtung der gewünschten Bewegungsrichtung, so reduziert sich der Kammerdruck p_L und damit der über das offene Auslassventil fließende Volumenstrom. Die Fehlerauswirkungen sind daher geringer als in Fall I.
- Fall VI: Durch externe Lastkräfte, die in Richtung der gewünschten Bewegungsrichtung wirken, erhöht sich der Kammerdruck p_R. Dadurch ist der Druckabfall über dem fehlerhaft geöffneten Ventil und damit dessen Volumenstrom geringer. Die Auswirkungen sind daher weniger kritisch als in Fall II.
- Fall VII: Die externen Lastkräfte erhöhen die Gefahr, dass sich der Lenkzylinder zu schnell bewegt. Dies führt zu einer Umkehr der Regelabweichung und damit zu einer Richtungsumkehr von $\dot{x}_{soll}$. Damit liegt Fall II vor.
- Fall VIII: Dieser Fall kann mit der zuvor genannten Argumentation auf Fall I zurückgeführt werden.

Aus der Analyse der möglichen Fehler- und Lastfälle geht hervor, dass die Fälle I und II die stärksten Auswirkungen auf das Systemverhalten und die verfügbare Lenkgeschwindigkeit haben. Im Folgenden soll die prinzipbedingte Grenze der Fehlertoleranz eines Lenkventils mit unabhängigen Steuerkanten ohne Absperrventil für externe Lasten bestimmt werden, die auch von einem idealen Regler nicht überschritten werden kann. Dazu wird die Abhängigkeit der in Abbildung 5.3 dargestellten Drücke und Volumenströme von der wirkenden Lastkraft F analytisch hergeleitet. Die Berechnung

erfolgt für den statischen Fall unter der Annahme, dass alle für die jeweilige Lenkrichtung relevanten Ventile komplett geöffnet sind, während ein Ventil fehlerhaft in komplett geöffneter Stellung klemmt. Zusätzlich zu dieser statischen open-loop Betrachtung wird in Kapitel 6.1 das closed-loop Verhalten des Lenkventils im Zusammenspiel mit dem Lenkwinkelregler analysiert.

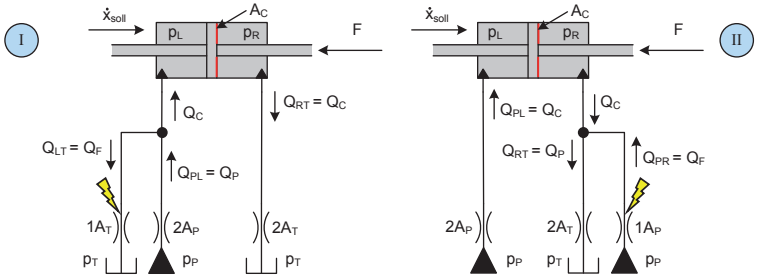


Abb. 5.3: Relevante Fehler- und Lastfälle für Fehlertyp B

Für Einlassventile wird eine Öffnungsfläche von A_P und für Auslassventile eine Öffnungsfläche von A_T angenommen. Die Systemgrößen ergeben sich für den Fall I als Lösung des folgenden nichtlinearen Gleichungssystems[2]:

$$\left\| \begin{array}{c} p_L = p_R + F/A_C \\ p_P = p_L + \Delta p \\ (Q_C =) Q_{RT} = Q_{PL} - Q_{LT} \end{array} \right\| \tag{5.3}$$

$$\left\| \begin{array}{c} p_L = p_R + F/A_C \\ p_P = p_L + \Delta p \\ 2 \cdot A_T \cdot \sqrt{p_R - p_T} = 2 \cdot A_P \cdot \sqrt{p_P - p_L} - A_T \cdot \sqrt{p_L - p_T} \end{array} \right\| \tag{5.4}$$

Die Lösung des Gleichungssystems liefert die Erkenntnis, dass der wichtigste Einflussfaktor für die Fehlertoleranz das Verhältnis der Öffnungsflächen der Ein- und Auslassventile A_P/A_T ist. In Abbildung 5.4 ist der zum Lenken

[2]Das Gleichungssystem für Fall II ist in Anhang A.2.2 dargestellt.

verfügbare Volumenstrom Q_C für unterschiedliche Flächenverhältnisse im Vergleich zum maximalen Volumenstrom $Q_{C,max}$ dargestellt. Der schraffierte Bereich repräsentiert den Bereich der Volumenströme, der zur Erfüllung der gesetzlichen Anforderungen für die Einfahrt in die Kreisfahrt nicht mehr ausreichend ist, siehe Kapitel 3.1. Bei einem Flächenverhältnis von 1 ist erkennbar, dass Fall I deutlich kritischer ist als Fall II. Dies ist dadurch begründbar, dass bei Fall I nur ein Teil des zufließenden Volumenstroms in den Lenkzylinder gelangt und im Vergleich dazu bei Fall II die gesamte Menge zur Verfügung steht, bis die Pumpe die Druck- oder Volumenstromsättigung erreicht.

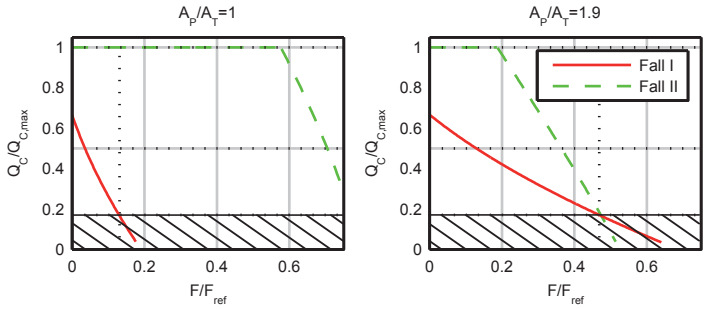


Abb. 5.4: Vergleich der Toleranz gegenüber Fehlertyp B im statischen Fall für unterschiedliche Flächenverhältnisse der Ein- und Auslassventile

Durch Erhöhung des Flächenverhältnisses ist es möglich, den Druckabfall an den vollständig geöffneten Auslassventilen zu erhöhen und damit Fall I zu verbessern, aber gleichzeitig Fall II zu verschlechtern. Dadurch kann der benötigte Volumenstrom auch noch bei höheren Lastkräften zur Verfügung gestellt werden[3]. Die zusätzliche Drosselung des abfließenden Volumenstroms kann im fehlerfreien Betrieb durch eine stärkere Ansteuerung der Ablaufventile kompensiert werden, so dass im Kleinsignalbereich keine höheren Energieverluste auftreten. In der Praxis kann statt der Verwendung

[3] Die Bewertung der verfügbaren Lenkkraft im Fehlerfall ($F/F_{ref} \approx 0,45$) erfolgt am Ende von Kapitel 5.1.

von Ventilen mit unterschiedlichen maximalen Öffnungsflächen auch eine Androsselung durch eine zusätzliche Düse mit konstantem Strömungsquerschnitt in der Rücklaufleitung zum Tank erfolgen.

In Abbildung 5.5 sind die wesentlichen Systemgrößen dargestellt, die sich bei einem Flächenverhältnis von $A_P/A_T = 1,9$ ergeben[4]. In Fall I wird der Druckabfall über den vollständig geöffneten Einlassventilen von der Pumpe konstant gehalten, so dass auch der von der Pumpe geförderte Volumenstrom Q_P konstant ist. Da mit steigender Lastkraft F auch der Kammerdruck p_L steigt, verschlechtert sich das Verhältnis, mit dem sich der Volumenstrom Q_P in Q_C und Q_F aufteilt. Da der Volumenstrom Q_C mit steigender Lastkraft F geringer wird, reduziert sich auch der Druckabfall über dem Auslassventil und damit der Kammerdruck p_R. In Fall II kann der Druckabfall über dem Einlassventil nur solange konstant gehalten werden, bis die Lastkraft F so hoch ist, dass die Pumpe die Drucksättigung erreicht. Bis zu diesem Punkt kann der Lenkzylinder weiterhin mit maximaler Geschwindigkeit verfahren werden, da der zusätzlich fließende Volumenstrom Q_F lediglich zu einer Erhöhung der Fördermenge der Pumpe Q_P und zu einer Erhöhung der Druckdifferenz über dem Auslassventil und damit zu einer Erhöhung aller Systemdrücke führt[5]. Ab der Lastkraft F, bei der die Pumpe an der Druckbegrenzung arbeitet, reduziert sich die Druckdifferenz an den Einlassventilen und damit der zum Lenken verfügbare Volumenstrom Q_C. Durch die Reduktion dieses Volumenstroms reduziert sich auch die über das Auslassventil fließende Menge und damit auch die an den Auslassventilen anliegende Druckdifferenz und der Kammerdruck p_R. Es ist erkennbar, dass das Auslassventil in Fall II sehr hohen Druckdifferenzen ausgesetzt ist, die sich aus der Verbindung der rechten Zylinderkammer mit der Pumpe ergeben.

[4] Die Ergebnisse für ein Flächenverhältnis von $1,0$ sind in Anhang A.2.3 dargestellt.

[5] Da die Pumpe auch die Arbeitshydraulik versorgt, wird angenommen, dass diese Pumpe die Volumenstromsättigung nicht erreicht, da sie auf ein Vielfaches des Volumenstroms $Q_{C,max}$ ausgelegt ist.

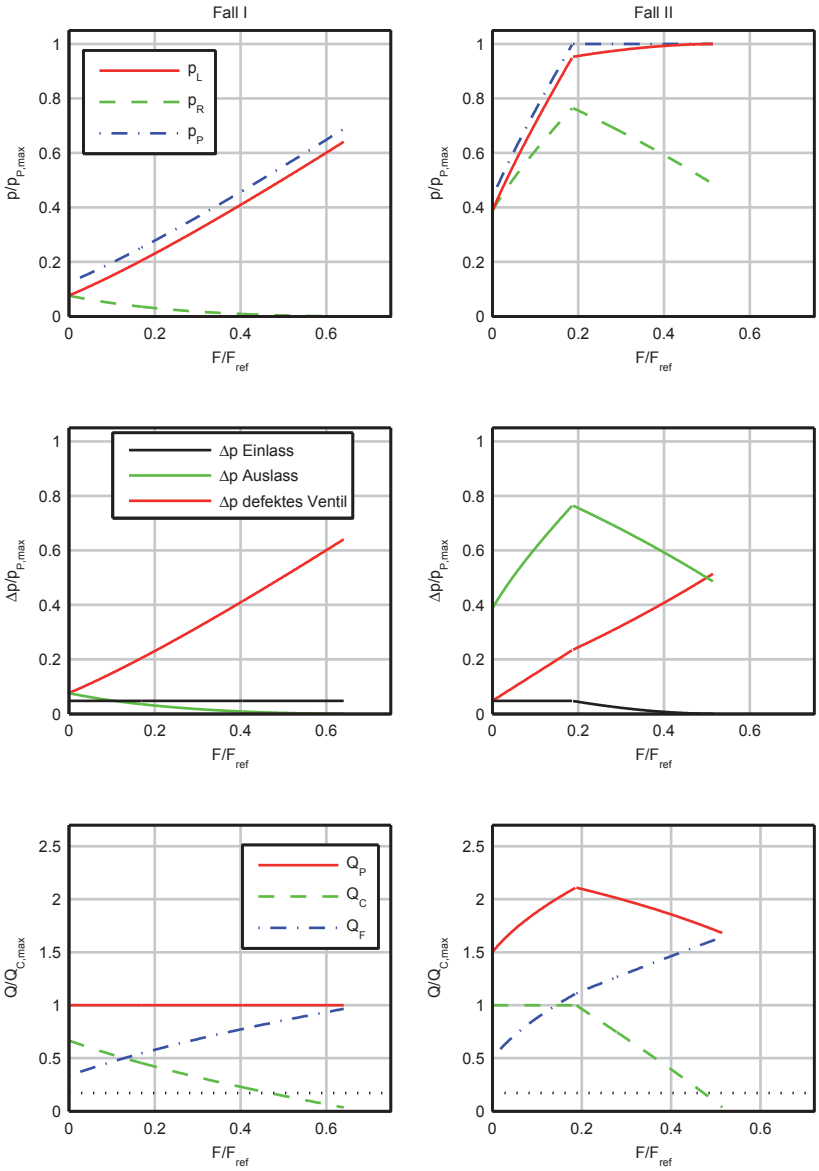


Abb. 5.5: Systemgrößen bei Fehlertyp B im statischen Fall für $A_P/A_T = 1{,}9$

Die verwendeten Ventile müssen konstruktiv darauf ausgelegt sein, auch bei solchen Druckdifferenzen zu öffnen und in geöffneter Stellung zu bleiben, da andernfalls die über das fehlerhaft geöffnete Einlassventil fließende Menge nicht in ausreichendem Maße abgeführt werden kann. Dies würde dazu führen, dass sich der Volumenstrom Q_C bereits bei niedrigeren Lastkräften F reduziert.

Um die Toleranz von Lenksystemfehlern unter dem Einfluss von Lastkräften einschätzen zu können, wird das in Abbildung 5.4 dargestellte Ergebnis mit einem Flächenverhältnis von $A_P/A_T = 1,9$ mit einer konventionellen hydrostatischen Lenkeinheit verglichen. Bei dieser hängt der maximal erreichbare Lenkdruck im Notlenkbetrieb ohne Servounterstützung von dem Verdrängungsvolumen der Gerotorpumpe, dem Durchmesser des Lenkrads und der zulässigen Betätigungskraft am Lenkrad ab. Für einen Lenkraddurchmesser von 40 cm und eine Betätigungskraft von 600 N (entspricht einem Drehmoment von 120 Nm) ergibt sich nach [37] der in Abbildung 5.6 dargestellte erreichbare Lenkdruck[6].

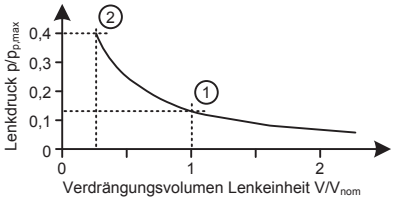


Abb. 5.6: Maximaler Lenkdruck im Notlenkbetrieb bei Ausfall der Hydraulikpumpe für eine rein hydrostatische Lenkeinheit in Anlehnung an [37]

Aus dem Diagramm ist erkennbar, dass der erreichbare Druck hyperbolisch mit dem Verdrängungsvolumen abfällt. Zur Gewährleistung einer komfortablen Lenkübersetzung im Normalbetrieb und einem ausreichenden Notlenkbetrieb bei Ausfall der Hydraulikpumpe, gibt es auf dem Markt Lenkeinheiten

[6] Die Annahme bezüglich der erreichbaren Betätigungskraft entspricht der gesetzlichen Vorgabe der maximalen Betätigungskraft im Fehlerfall.

mit mehreren Gerotorpumpen oder Gerotorpumpen mit abschaltbaren Kammern [96]. Bei diesen Lenkeinheiten reduziert sich bei einem Ausfall der Druckversorgung automatisch das Fördervolumen der Pumpe, so dass höhere Lenkkräfte erreichbar sind (zum Beispiel von Punkt ① auf Punkt ②). Für den betrachteten Beispieltraktor aus Kapitel 3.2.3 ergibt sich bei Berücksichtigung von Abbildung 5.6 im Notlenkbetrieb bei reduziertem Fördervolumen (Punkt ②) eine maximale Lenkkraft von $F/F_{ref} \approx 0,4$. Dieser Wert liegt niedriger als der von dem betrachteten Steer-by-Wire Lenkventil erreichbare Wert von $F/F_{ref} \approx 0,45$. Dabei muss berücksichtigt werden, dass der Fahrer mit einem konventionellen Lenksystem bei einer Betätigungskraft von 600 N zwar den zuvor bestimmen Lenkdruck erreichen kann, aber nicht bekannt ist, mit welcher Geschwindigkeit der Fahrer das Lenkrad während des Aufprägens dieser hohen Kraft drehen kann, um einen Volumenstrom für eine Lenkbewegung zu erzeugen. Der Fahrer des Traktors mit einem Steer-by-Wire System kann eine Lenkbewegung im Fehlerfall ohne nennenswerten Kraftaufwand erzeugen, da sich durch die rein elektronische Übertragung des Fahrerwunschs die geänderten Druckverhältnisse im Lenkzylinder nicht auf die benötigte Betätigungskraft auswirken. Im Vergleich dazu traten bei Messungen mit dem Versuchstraktor bei einer Fahrgeschwindigkeit von 2 km/h auf Asphalt Lenkkräfte im Bereich von lediglich $F/F_{ref} \approx 0,2$ auf.

Aus der Analyse wird deutlich, dass bei statischer Betrachtung von einer ausreichenden Fehlertoleranz ausgegangen werden kann. Vorteilhaft ist zudem, dass in Situationen mit großem Gefahrenpotential (hohe Fahrgeschwindigkeit) die Lenkkräfte geringer sind und die Fehlertoleranz damit besser ist als bei niedrigen Geschwindigkeiten. Die in Annahme 1 postulierte passive Fehlertoleranz des Lenksystems wird daher zum größten Teil durch die gewählte Ventilarchitektur mit aufgelösten Steuerkanten gewährleistet statt durch einen Lenkwinkelregler mit einer speziellen Struktur oder besonderen Reglerauslegung.

5.2 Lenkwinkelregelung

Entsprechend der in Kapitel 3.1 dargestellten Anforderungen muss das Lenksystem das einfache und sichere Lenken des Fahrzeugs ermöglichen. Der Fahrer nimmt im Prozess der Fahrzeugquerführung eine entscheidende Rolle ein, so dass diese Anforderungen nicht in eindeutiger Weise auf quantitative Anforderungen für die Lenkwinkelregelung übertragen werden können. Dies erschwert einen objektiven Reglerentwurf. Wie in Abbildung 5.7 schematisch dargestellt, bildet der Fahrer einen überlagerten Regelkreis zum Lenkwinkelregler. Auf Basis vielfältiger Umgebungsbedingungen wie Straßenverlauf, Straßenbreite oder vorhandenen Hindernissen generiert der Fahrer die gewünschte Soll-Trajektorie für das Fahrzeug. Andere Informationen wie Position, Geschwindigkeit oder Beschleunigung nimmt der Fahrer auf, um ein Gefühl für die Ist-Trajektorie zu erhalten. Die Informationen können dabei durch unterschiedliche Sinneskanäle aufgenommen werden. Die eigentliche Stellgröße zur Trajektorienregelung ist letztlich der gewünschte Lenkwinkel oder die gewünschte Lenkzylinderposition x_{soll}, die der Fahrer über das Eingabegerät (Lenkrad) vorgibt und aus der Abweichung zwischen Soll- und Ist-Trajektorie ermittelt.

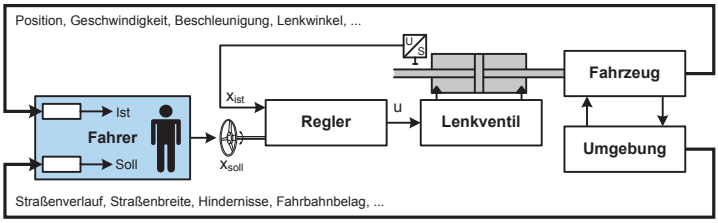


Abb. 5.7: Einbindung des Fahrers in den Prozess der Fahrzeugquerführung in Anlehnung an [71]

Der Fahrer ist daran gewohnt, Abweichungen zwischen x_{soll} und x_{ist} auszuregeln, insbesondere da bei konventionellen hydrostatischen Lenksystemen kein fester Zusammenhang zwischen dem Lenkrad- und dem Radlenkwinkel

besteht. Dies ist dadurch begründet, dass externe Kräfte durch die stets vorhandene Leckage in den verschiedenen Komponenten eine Lenkzylinderbewegung erzeugen können, ohne dass sich dabei das Lenkrad bewegt. Ein kontinuierliches und feinfühliges Übertragungsverhalten ohne Überschwinger ist für einen Lenkwinkelregler daher wichtiger als beispielsweise eine möglichst geringe stationäre Regelabweichung. Subjektive Aspekte wie die Erreichung eines angenehmen Lenkgefühls können bei einer Konzeptentwicklung ohne Probandenversuche nicht berücksichtigt werden.

Bei einer konventionellen hydrostatischen Lenkeinheit gibt der Fahrer über die Lenkraddrehzahl einen Volumenstrom vor, der in einer Lenkzylinderbewegung resultiert. Dies entspricht einer open-loop Steuerung oder einer closed-loop Geschwindigkeitsregelung bei einem Steer-by-Wire System, bei dem ebenfalls kein fester Zusammenhang zwischen Lenkradwinkel und Radlenkwinkel besteht. Vorteilhafter ist die direkte Regelung des Radlenkwinkels auf den Lenkradwinkel, um dem Fahrer ein Übertragungsverhalten wie bei einem PKW zu bieten und Störungen inhärent im Lenkwinkelregelkreis zu kompensieren. Dabei muss beachtet werden, dass bei der Positionsregelung im Vergleich zur Geschwindigkeitsregelung Regler-Effekte wie beispielsweise Überschwinger deutlich direkter vom Fahrer wahrgenommen werden können. Im Gegensatz zu einer PKW-Lenkung mit direktem mechanischen Durchgriff muss zudem berücksichtigt werden, dass der Fahrer das elektrische Lenkrad möglicherweise schneller drehen kann, als sich die Räder durch die Volumenstrombegrenzung der verwendeten Ventile bewegen können. In diesem Fall kommt es zu einem unerwünschten Nachlauf der Räder, wenn der Fahrer die Lenkbewegung abrupt stoppt. Dieses Problem kann dadurch gelöst werden, dass durch eine Erhöhung der vom Fahrer spürbaren Handkraft ein zu schnelles Drehen verhindert wird oder dass zu schnelle Lenkradbewegungen durch eine im Steuergerät hinterlegte Anstiegsratenbegrenzung abgefangen werden[7].

[7] Bei der Begrenzung der Anstiegsrate muss ein anschließender Nachlauf der Räder unterbunden werden. Dies führt nach der Lenkbewegung zu einem Offset zwischen der Position

Durch die Wahl eines Closed-Center Systems mit Load-Sensing müssen die unbekannten Lenkkräfte nicht im Reglerentwurf berücksichtigt werden, da diese von der Verstellpumpe und der Druckwaage kompensiert werden. Gleiches gilt auch für Fehler des Typs A an Auslassventilen. Demgegenüber führen Fehler dieser Art an Einlassventilen zu einer Reduktion der Systemverstärkung um 50 Prozent und liegen damit über den Schwankungen, die durch Umgebungsparameter wie der Temperatur oder durch Leckage einzelner Ventile beziehungsweise einer Veränderung des Durchflussverhaltens durch Verschleiß hervorgerufen werden. Fehler des Typs B an Auslassventilen äußern sich ebenfalls in einer Reduktion der Systemverstärkung, da nur ein Teil des von den Einlassventilen dosierten Volumenstroms tatsächlich in den Lenkzylinder fließt. Zusätzlich dazu führt dieser Fehler zu einer richtungsabhängigen Totzone: Um den Lenkzylinder zu bewegen, müssen die Einlassventile bei einem offen klemmenden Auslassventil soweit geöffnet werden, bis der fehlerhaft abfließende Volumenstrom so stark angedrosselt ist, dass die Lenkkräfte überwunden werden können. Durch den Einsatz eines Reglers mit integralem Verhalten könnte die Regelabweichung im Fehlerfall reduziert werden. Der integrale Anteil führt jedoch auch zu einem Überschwingen bei sprungförmigen Soll-Signalen, so dass ein Regler mit DT_1-Anteil für den experimentellen Nachweis verwendet wird, der die Stellgröße erhöht, wenn sich die Regelabweichung zu stark ändert. In der zuvor dargestellten analytischen Betrachtung wurde gezeigt, dass bei einem Fehler des Typs B an Einlassventilen bei niedrigen Lenkkräften nur ein geringer Fehlereinfluss auftritt. Bei höheren Lenkkräften tritt jedoch auch hier eine richtungsabhängige Verringerung der Streckenverstärkung und Vergrößerung des Totbereichs ein. Einen wesentlichen Einfluss auf den Reglerentwurf hat auch der in Tabelle 4.3 beschriebene Fehlerfall in der Druckversorgung, bei dem der Versorgungsdruck auf den Maximaldruck ansteigt. Dieser Fehlerfall führt zu einer höheren Streckenverstärkung, da der Zulaufdruck in diesem Fall

des Lenkrads und der Räder. Dieser Offset kann im Laufe der nächsten Lenkvorgänge stetig reduziert werden.

maximal und der Druckabfall über den Ein- und Auslassventilen hoch ist. Bei der Bewertung des Reglers muss dieser Fehlerfall berücksichtigt werden, da eine erhöhte Streckenverstärkung bei einem aggressiv ausgelegten Regler zu Instabilität führen kann. Fahrzeuge für off-road Anwendung benötigen sehr robuste Regler, da im Vergleich zu on-road Anwendungen höhere Variationen bei den Anwendungs- und Umgebungsbedingungen auftreten [105].

Die Annahme 1 zur Fehlertoleranz des Lenkventils mit unabhängigen Steuerkanten aus Kapitel 4.1.1 soll mit Hilfe der in Abbildung 5.8 dargestellten Reglerstruktur unter dynamischen Bedingungen nachgewiesen werden. Diese besteht aus einem DT_1-Anteil, einem P-Anteil und einer nichtlinearen invertierten Ventilkennlinie. Die invertierte Kennlinie wird zur Kompensation der realen Ventilkennlinie verwendet, die den Zusammenhang zwischen dem Ansteuersignal des Ventils und dessen Volumenstroms beschreibt. Eine derartige Kompensation von Nichtlinearitäten ist möglich, wenn die Regelstrecke in guter Näherung einem Hammerstein-Modell[8] entspricht. Durch die Kombination aus einem P-Anteil im Regler mit dem integralen Verhalten der Regelstrecke wird bei Vernachlässigung von Störungen, die auf den Streckenausgang wirken, ein statisch genaues Regelverhalten erreicht [56]. Da in Kapitel 5.1 mit Hilfe einer statischen Betrachtung bereits nachgewiesen wurde, dass sich die Fehlertoleranz nicht durch die Regelung sondern durch die gewählte Ventilarchitektur ergibt, wird an dieser Stelle auf einen formalen Reglerentwurf inklusive Stabilitätsnachweis verzichtet.

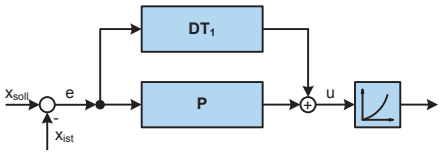


Abb. 5.8: PDT_1-Lenkwinkelregler mit einer nichtlinearen invertierten Ventilkennlinie

[8] Ein Hammerstein-Modell besteht aus der Reihenschaltung einer statischen Nichtlinearität und einem dynamischen Übertragungsglied [85].

5.3 Fehlererkennung

Die Fehlererkennung ist bei dem Ventilkonzept mit unabhängigen Steuerkanten durch den passiv fehlertoleranten Regler nicht zur Gewährleistung der Fehlertoleranz, sondern lediglich zur rechtzeitigen Fahrerwarnung und Überführung in den sicheren Zustand notwendig. Folglich muss keine Lokalisierung der Fehlerquelle (Fehlerdiagnose) durchgeführt werden und die Fehlererkennung ist nicht zeitkritisch[9]. An die Methoden zur Fehlererkennung wird die Anforderung gestellt, dass keine zusätzlichen Sensoren benötigt werden, insbesondere keine Positionssensoren an allen acht Wegeventilen. Fehlerursachen im elektrischen Teilsystem, wie Kurzschluss oder Kabelbruch, werden im Folgenden nicht weiter berücksichtigt, da diese sehr einfach über eine Auswertung von Ansteuerstrom und -spannung erkannt werden können.

Entsprechend der Definition aus dem Bereich der funktionalen Sicherheit gelten alle vier der für das Lenkventil zu betrachtenden Fehler (Fehlertyp A und B an Ein- und Auslassventilen) als gefahrbringende Ausfälle[10], auch wenn keiner dieser Fehler zu einem Verlust der Lenkbarkeit führt und die gesetzlichen Anforderungen an das Lenksystem weiterhin erfüllt werden. Alle vier gefahrbringenden Fehler sollen durch einen off-duty Selbsttest bei Systemstart erkannt werden, siehe Tabelle 5.1.

Zusätzlich dazu sollen während der Fahrt auch solche Fehler erkannt werden, die einen nennenswerten Einfluss auf die Lenkperformance haben. Dadurch soll verhindert werden, dass ein schlafender Fehler in einer Gefahrensituation dazu führt, dass der Fahrer das Fahrzeug nicht in ausreichendem Maße lenken kann. Entsprechend der in Kapitel 5.1 ausgeführten Beschreibung der Fehler-

[9] In Kapitel 4.2.3 wurde ermittelt, dass eine Erkennung alle 24 Betriebsstunden ausreichend ist.

[10] Ein gefahrbringender Ausfall ist ein Ausfall der das Potential hat, den sicherheitsbezogenen Teil einer Steuerung in einen gefährlichen Zustand zu bringen. In einem fehlertoleranten System mit Redundanz führt ein gefahrbringender Hardwareausfall weniger wahrscheinlich zu einem gefährlichen Ausfall des Gesamtsystems [18].

auswirkung sind dies vor allem die Fehler des Typs B. Zusätzlich dazu führt auch ein Fehler des Typs A an Einlassventilen zu einer richtungsabhängig halbierten maximalen Lenkgeschwindigkeit. Für die Fehlererkennung sind die Messgrößen Radlenkwinkel, Lenkradwinkel, Zulaufdruck, Gierrate und Fahrzeuggeschwindigkeit sowie interne Systemgrößen wie die Regelabweichung oder die Stellgröße verfügbar.

Fehler	Einfluss auf Lenkperformance	Maßnahme
Typ A an Auslassventil	Nicht vorhanden	Selbsttest bei Systemstart
Typ A an Einlassventil	Vorhanden	Selbsttest bei Systemstart + modellbasierte Fehlererkennung
Typ B an Auslassventil	Hoch (je nach Lenkkraft)	
Typ B an Einlassventil	Hoch (je nach Lenkkraft)	

Tab. 5.1: Liste der Fehler und der dazugehörigen Erkennungsmaßnahmen

5.3.1 Off-duty Selbsttest

Um die Funktionsfähigkeit der Wegeventile zu überprüfen, ist deren Aktivierung erforderlich. Trotzdem darf in einer sicherheitskritischen Anwendung durch den Selbsttest während dessen Durchführung keine Gefahr entstehen. Dies wäre der Fall, wenn sich der Lenkzylinder unkontrolliert bewegt. In [88] wird ein aktiver Selbsttest zur Fehlererkennung und -diagnose für Ventilkonzepte mit unabhängigen Steuerkanten vorgeschlagen, bei dem zusätzlich zum Versorgungsdruck auch die beiden Kammerdrücke überwacht werden, um aus deren Druckniveau und der Bewegungstendenz des Zylinders auf Ventilfehler schließen zu können. Durch eine Druckversorgung mit variabel einstellbarem Druck und durch die Drucksensoren an den Zylinderkammern ist es möglich, die genaue Fehlerquelle und bei dem Fehler *»Leckage«* auch die Fehlerschwere zu bestimmen. Da eine Fehlerdiagnose für das betrachtete Steer-by-Wire Ventilkonzept nicht notwendig ist, kann der Selbsttest für

die betrachtete Anwendung mit weniger Sensorik und auf einfachere Weise erfolgen, siehe Abbildung 5.9.

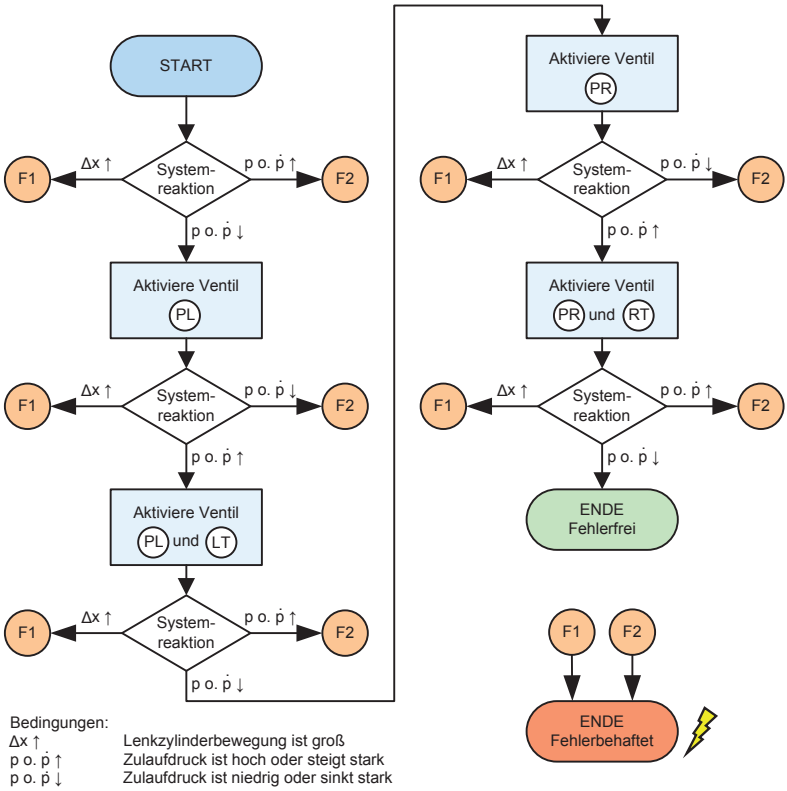


Abb. 5.9: Ablaufdiagramm eines aktiven Selbsttests für einen Kanal eines Steer-by-Wire Ventils mit unabhängigen Steuerkanten nach [84]

Die Ein- und Auslassventile werden bei diesem Selbsttest sequentiell bestromt, so dass aus dem Verlauf des Zulaufdrucks auf die Fehlerfreiheit geschlossen werden kann [84]. Durch die unabhängigen Steuerkanten und die Möglichkeit der Aktivierung von Ein- und Auslassventilen einer Zylinderkammerseite kann eine Bewegung des Lenkzylinders ausgeschlossen werden. Im fehlerfreien Fall ergibt sich lediglich auf Grund der Ölkompressibilität

eine minimale Auslenkung des Lenkzylinders, die ungefährlich ist. Im Falle eines Fehlers des Typs B an einem Auslassventil ist eine Bewegung des Lenkzylinders prinzipiell möglich. Die Bewegungstendenz kann durch den Positionssensor am Lenkzylinder erkannt und durch Deaktivierung aller Ventile unterbunden werden, bevor eine potentiell gefahrbringende Auslenkung der Räder erreicht ist. Durch eine geeignete Applikation der Erkennungsschwellen für einen Druckanstieg beziehungsweise -abfall ist es in diesem Selbsttest auch möglich, Leckage in einem oder mehreren Ventilen zu erkennen, da Leckage an einem Einlassventil zu einem ungewollten Druckanstieg und Leckage an einem Auslassventil zu einer Bewegungstendenz führt. Fehler in der Druckversorgung, die zu einem hohen Versorgungsdruck führen, können vor Beginn des Selbsttests signalbasiert erkannt werden. Die Applikation der Aktivierungslevel der Ein- und Auslassventile sowie der zuvor genannten Erkennungsschwellen erlauben eine Festlegung des Druckgradienten und des Druckniveaus während des Selbsttests und damit eine Auslegung bezüglich der Kriterien *»Robustheit«* und *»Zeitbedarf«*.

5.3.2 On-duty Fehlererkennung

Mit Hilfe der on-duty Fehlererkennung sollen Ventilfehler während der Fahrt erkannt werden, die einen nennenswerten Einfluss auf die Lenkperformance haben können. Für das betrachtete Steer-by-Wire Ventil sind dies Fehler des Typs B an Ein- und Auslassventilen sowie Fehler des Typs A an Einlassventilen, siehe Tabelle 5.1. Dabei besteht die Schwierigkeit, dass der Regler versucht, Lenkwinkelfehler möglichst gut zu kompensieren. Mitunter führt dies dazu, dass Fehler anhand der Regelabweichung oder der Regelgröße nicht erkannt oder nicht von in der Praxis auftretenden Abweichungen durch Störungen oder Parameterschwankungen unterschieden werden können [45]. Fehler können daher bei Auswertung einzelner Mess- und Systemgrößen erst dann erkannt werden, wenn die Fehlerauswirkung bereits so groß ist, dass beispielsweise die Regelabweichung deutlich höher als im nominalen Fall

ist. Diesen Nachteil haben modellbasierte Methoden nicht zwangsläufig, da bei diesen aus der Abweichung des Eingangs-/Ausgangsverhaltens zwischen dem nominalen und dem aktuellen Zustand eines Teilsystems auf Fehler geschlossen werden kann, die nicht direkt mit einer einzelnen Messgröße erfassbar sind [45]. Weiterhin muss beachtet werden, dass bestimmte Ventilfehler nur bei Lenkbewegungen in eine der beiden Lenkrichtungen erkannt werden können, weil nur in dieser Richtung das entsprechende Ventil vom Steuergerät aktiviert wird.

Für die Überwachung von Magnetventilen ohne Positionssensoren existieren im Stand der Technik verschiedene Konzepte, die kurz vorgestellt, aber im Folgenden nicht näher betrachtet werden. In [24] ist ein Verfahren beschrieben, bei dem die Schaltstellung eines Ventils mit Hilfe eines an dem Ventilblock angebrachten Schallsensors erfasst werden kann. Durch die Auswertung des Sensorsignals kann erfasst werden, ob und wann das Ventil die offene oder geschlossene Stellung erreicht hat. Vorteilhaft an dieser Lösung ist, dass mit Hilfe eines Schallsensors alle Ventile innerhalb eines Ventilblocks überwacht werden können und die Integration eines derartigen Sensors einfacher ist als die Integration eines Positionssensors[11]. Eine andere Möglichkeit zur Überwachung mittels Strom- und Spannungsmessung wird unter anderem in [98] beschrieben. Darin wird vorgeschlagen, aus dem Verlauf des Spulenstroms auf die differentielle Induktivität der Spule und damit auf die Position des Ankers zu schließen. Für die Anwendung dieser Methode ist es notwendig, dass eine eindeutige Abhängigkeit zwischen der Ankerposition und der differentiellen Induktivität besteht und dass der Magnetkreis nicht in der Sättigung betrieben wird. Eine weitere Möglichkeit zur Fehlererkennung besteht, wenn ein Drucksignal ausgewertet und mit dem Ansteuersignal eines Ventils verglichen wird [57]. Diese Methode nutzt die Kompressibilität eines Fluids, die dazu führt, dass der Versorgungsdruck bei einer sprungförmigen Aktivierung eines Magnetventils kurzzeitig einbricht.

[11] Bei der Integration eines Positionssensors muss auf die Abdichtung zur Umgebung und die Druckfestigkeit des Sensorelements geachtet werden.

Wie in Kapitel 5.1 ausgeführt, ändert sich bei einem Fehler des Typs A an einem Auslassventil lediglich das Druckniveau, da der Fehler durch den Druckregler der Regelpumpe kompensiert wird. Eine signal- oder modellbasierte Erkennung wird dadurch erschwert, da das Druckniveau ebenfalls von den am Lenkzylinder wirkenden Lenkkräften abhängig ist, die je nach Fahrgeschwindigkeit und Untergrund unbekannt und stark schwankend sind. Bei dem Entwurf einer Fehlererkennungsmethode ist es jedoch möglich, das Druckniveau in Abhängigkeit der jeweiligen Bewegungsrichtung auszuwerten. Dabei muss jedoch beachtet werden, dass Hindernisse wie Bordsteine oder Furchen auf dem Acker ebenfalls zu richtungsabhängig unterschiedlichen Druckniveaus führen können. Da Fehler dieser Art auf die Lenkperformance nahezu keinen Einfluss haben, wird keine über den Selbsttest hinausgehende Fehlererkennung für diesen Fehler entworfen. Die drei restlichen Ventilfehler haben die Gemeinsamkeit, dass sich die Systemverstärkung der Regelstrecke situationsabhängig reduziert. In Lenkmanövern mit geringer Dynamik bei geringen Volumenströmen wird diese Reduktion nahezu ideal von dem Regler kompensiert, so dass sich der Verlauf der Regelgröße und der Regelabweichung kaum vom nominalen Verlauf unterscheidet. Eine signalbasierte Überwachung der Regelabweichung ist daher nur für die Fehlererkennung während schneller Lenkbewegungen oder hoher Lenkkräfte wirkungsvoll, da der Fehler sich in diesen Fällen stärker auf die Regelgüte auswirkt.

Um Fehler frühzeitig zu erkennen wird eine modellbasierte Fehlererkennung mit einer Paritätsgleichung entworfen, dessen Struktur schematisch in Abbildung 5.10 dargestellt ist. Die Stellgröße des Reglers u, die durch die invertierte Ventilkennlinie in ein Ansteuersignal umgerechnet und auf die acht Ventile verteilt wird, dient parallel dazu auch als Eingangsgröße für ein Modell der Regelstrecke. Aufgrund der Druckkompensation der Pumpe bei Änderungen der Lenkkraft besteht unter Vernachlässigung von Störungen und Ungenauigkeiten der invertierten Ventilkennlinie ein bekannter Zusammenhang zwischen der Lenkzylindergeschwindigkeit v_{ist} und der Stellgröße u.

Dieser Zusammenhang wird für den fehlerfreien Fall über das Strecken-Modell abgebildet. Durch den Vergleich von v_{ist} und v_{modell} kann auf Fehler geschlossen werden. Da sich die Geschwindigkeit des Lenkzylinders v_{ist} nicht unmittelbar nach Änderung von u verändert, sondern mit einer unbekannten und variablen Totzeit sowie Verzögerung reagiert, ist es sinnvoll, dies beim Vergleich beider Geschwindigkeitssignale zu berücksichtigen. Das ist beispielsweise dadurch möglich, dass die aktuelle Geschwindigkeit $v_{ist}(t)$ mit der Modell-Geschwindigkeit innerhalb des Zeitintervalls $[t - t_1 \ldots t]$ verglichen wird und die Werte mit dem geringsten Abstand ausgewählt werden. Damit durch kurze Abweichungen in den Geschwindigkeitssignalen keine Fehlalarme ausgelöst werden, ist es zudem zweckmäßig, die Abweichung der Geschwindigkeitssignale über ein Zeitintervall Δt_2 zu mitteln und zu normieren und damit die Fehlererkennung robuster zu machen. Bei der Festlegung der Erkennungsschwelle für das Residuum r sind Modellunsicherheiten bei der invertierten Ventilkennlinie sowie Störungen und Schwankungen von Umgebungsbedingungen zu beachten.

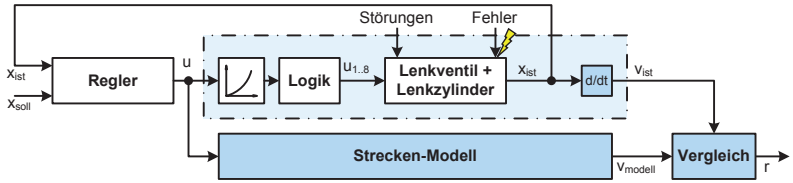


Abb. 5.10: Schematische Darstellung der Struktur der modellbasierten Fehlererkennung mittels einer Paritätsgleichung

Im Folgenden wird die Funktionsweise der modellbasierten Fehlererkennung am Beispiel eines Fehlers des Typs A an einem Einlassventil beschrieben. Im fehlerfreien Fall entspricht das Strecken-Modell der realen Strecke, so dass sich die beiden Geschwindigkeitswerte kaum unterscheiden und das Residuum r einen niedrigen Wert annimmt. Nach dem Ausfall eines Einlassventils in die stille Richtung muss die einseitig um 50 Prozent reduzierte Streckenverstärkung durch das Aufprägen von höheren Stellgrößen u

durch den Regler kompensiert werden. Bei einer niedrigen Lenkgeschwindigkeitsvorgabe v_{soll} erfolgt dies nahezu ohne Abweichung zur resultierenden Lenkgeschwindigkeit v_{ist}. Die erhöhte Stellgröße u führt jedoch zu einer erhöhten Geschwindigkeit des Streckenmodells v_{modell} und damit zu einem Anschlagen des Residuums r.

Fehler des Typs B an Einlassventilen können darüber hinaus auch signalbasiert mit Hilfe des Versorgungsdrucks erkannt werden, da bei offen klemmenden Einlassventilen der Versorgungsdruck bei einem Stillstand der Lenkung bis zur Druckbegrenzung ansteigt. Um Fehlalarme zu vermeiden ist es jedoch notwendig, den Fehlerfall von fehlerfreien Situationen, in denen der Druck ebenfalls ansteigt, sicher zu unterscheiden. Dies tritt beispielsweise dann auf, wenn die Räder gegen ein starres Hindernis ausgelenkt werden.

6 Nachweis und Bewertung der Ergebnisse

Der Nachweis und die Bewertung des entworfenen Konzepts erfolgt in zwei Stufen auf unterschiedlichen Abstraktionsebenen. In Kapitel 6.1 werden die in Kapitel 5 entworfenen Methoden zur Regelung des Lenkzylinders und zur Erkennung von Ventilfehlern experimentell an einem Prüfstand überprüft. Mit den Ergebnissen wird die Annahme 1 *»Fehlertoleranz«* und Annahme 2 *»Fehlererkennung«* auf der Ebene der Lenkzylinderregelung nachgewiesen. Anschließend erfolgt in Kapitel 6.2 die Abschätzung des Einflusses der Lenkwinkelregelung auf das Fahrverhalten des Traktors mit Hilfe des in Kapitel 3.2.3 vorgestellten Simulationsmodells. Dadurch soll die Aussage generiert werden, ob die fehlertolerante Lenkwinkelregelung auch eine einfache und sichere Lenkbarkeit des Traktors gewährleistet. Kapitel 6.2 bewertet damit die Annahme 1 *»Fehlertoleranz«* auf Fahrzeugebene. Auf Basis der erzielten Erkenntnisse wird in Kapitel 6.3 der in Kapitel 3 durchgeführte Vergleich verschiedener Aktiv-Lenksysteme aufgegriffen und mit den neu gewonnen Ergebnissen konkretisiert.

Nach [30] können während der Entwicklung von komplexen mechatronischen Systemen, die die Fahrdynamik eines Fahrzeugs beeinflussen, die Entwicklungswerkzeuge *»Fahrversuch«*, *»Fahrsimulator«* und *»Rechnersimulation«* eingesetzt werden. Fahrversuche mit Probanden sind sehr gut dazu geeignet, den Einfluss von Systemfehlern auf das Fahrverhalten zu untersuchen und können dazu genutzt werden, einen finalen Nachweis für die Sicherheit eines mechatronischen Systems zu generieren. Nachteilig ist jedoch der hohe Zeit- und Kostenaufwand zur Generierung von statistisch abgesicherten Aussagen. Bei Versuchen mit Probanden hängt das Ergebnis zudem davon ab, ob diese vorbereitet sind und sich schon ein Gewöhnungseffekt eingestellt hat [63]. Bei dem Einsatz von Fahrsimulatoren hängt es von der Realitätstreue der Abbildung der Schnittstelle zwischen Fahrer und

Fahrzeug ab, ob lediglich relative oder auch absolute Ergebnisse aus den Versuchen gezogen werden können [30]. Gegenüber Probandenversuchen im realen Fahrzeug bieten Fahrsimulatoren den Vorteil, dass diese etwas weniger zeit- und kostenintensiv sind und dass Fehler, Szenarien und Parametervariationen überprüft werden können, die in der Realität nicht oder nur schwer durchführbar sind. Demgegenüber können Rechnersimulationen mit noch geringerem Aufwand zur Untersuchung von Fehlern und deren Auswirkungen eingesetzt werden. Da sich jedoch in Simulationsmodellen die Reaktion des Fahrers bei auftretenden Störungen oder Fehlern nur schwer abbilden lässt, eignen sich Rechnersimulationen nur für die open-loop Untersuchung der Fahrzeugreaktion infolge von Systemstörungen, bei denen Einfluss des Fahrers vernachlässigt wird [30].

Bei Überlagerungslenkungen mit fail-safe Verhalten führt ein Verlust der Überlagerungsfunktion im Fehlerfall zu einer Veränderung der Lenkübersetzung und zu additiven Lenkwinkelfehlern, deren Sicherheitsrelevanz im Regelkreis mit dem Fahrer untersucht werden muss [63]. Im entwickelten fehlertoleranten Steer-by-Wire System werden Systemfehler automatisch kompensiert, so dass der Fahrereinfluss je nach Regelgüte im Fehlerfall weniger relevant ist. Zur Bewertung des Systemverhaltens auf Fahrzeugebene werden daher die Messergebnisse des fehlerbehafteten Lenkwinkelregelkreises open-loop in eine Rechnersimulation eingeprägt und die resultierende Trajektorie untersucht. Dadurch soll nachgewiesen werden, dass dem Fahrer in derartigen Manövern keine über das normale Maß hinausgehende Kompensationsaufgabe übertragen wird. In Anlehnung an die Richtlinie für die Prüfung der Lenkanlage von Kraftfahrzeugen [12] und der ISO-Norm 7401 mit Testverfahren für das querdynamische Übertragungsverhalten [15] werden die folgenden open-loop Fahrmanöver zur Bewertung herangezogen:

- **Manöver 1: Einfahrt in die stationäre Kreisfahrt**
  Die Einfahrt in eine stationäre Kreisfahrt mit einem Wenderadius von 12 m muss bei Fremdkraftlenkanlagen bei Schrittgeschwindigkeit

(hier: 2 km/h) innerhalb von 3 s möglich sein [12]. In den Messungen werden Soll-Werte vorgegeben, mit denen der stationäre Endwert innerhalb von 1 s erreicht wird.

- **Manöver 2: Dauersinuseingabe (*Slalom*)**
  Die sinusförmige Lenkwinkeleingabe führt dazu, dass sich das Fahrzeug slalomförmig bewegt. Bei einer Fahrgeschwindigkeit von 25 km/h und einer Frequenz von 0,33 Hz wird die Amplitude der sinusförmigen Lenkwinkeleingabe so gewählt, dass sich eine maximale Querbeschleunigung a_y von ungefähr 3 m/s^2 einstellt.

- **Manöver 3: Lenkwinkelsprung (*Anreißen*)**
  Bei dem Lenkwinkelsprung wird das Lenkrad während der Geradeausfahrt bei 40 km/h so schnell wie möglich bis zu einem zuvor definierten Winkel eingeschlagen. Der notwendige Winkel wird in der stationären Kreisfahrt ermittelt, so dass sich aus der Kombination von Fahrgeschwindigkeit und Lenkradeinschlag eine konstante Querbeschleunigung a_y von ungefähr 4 m/s^2 einstellt.

6.1 Experimenteller Nachweis am Prüfstand

Im Folgenden wird der für den experimentellen Nachweis verwendete Prüfstandsaufbau beschrieben und exemplarische Messergebnisse der Lenkwinkelregelung und Fehlererkennung präsentiert, die dem Nachweis von Annahme 1 *»Fehlertoleranz«* und Annahme 2 *»Fehlererkennung«* dienen.

6.1.1 Prüfstandsaufbau

Für den experimentellen Nachweis des fehlertoleranten Lenkventils wird ein *Hardware in the Loop* Prüfstand verwendet, da bei diesem zwingend nur der eigentliche Prüfling als reale Komponente vorhanden sein muss,

während die weiteren Komponenten oder die in der Realität vorliegenden Belastungen modelliert und als Druck beziehungsweise Volumenstrom an einer Schnittstelle eingeprägt werden können. Für die Wahl der Schnittstelle zwischen dem realen und dem simulierten Teilsystem existieren verschiedene Möglichkeiten [92]. Für die experimentelle Untersuchung eines Lenksystems ist die in Abbildung 6.1 dargestellte Schnittstelle zweckmäßig: Das Steer-by-Wire Ventil ist mit dem realen Lenkzylinder und der Druckversorgung verbunden und regelt dessen Position, während mit Hilfe eines weiteren Hydraulikzylinders die zum Verstellen des Lenkzylinders benötige Radkraft nachgebildet wird.

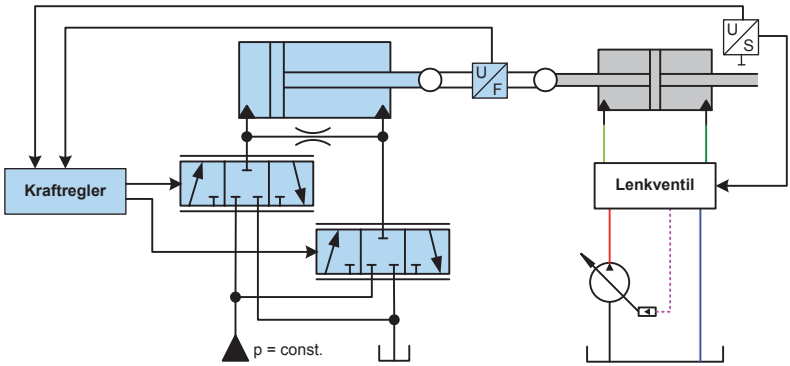


Abb. 6.1: Schematische Darstellung der Lenkkraftregelung am Prüfstandsaufbau

In dem verwendeten System wird die Koppelkraft beider Zylinder über eine Kraftmessdose erfasst und dem Kraftregler zugeführt. Dieser vergleicht den Ist-Wert mit dem aus einem Last-Modell gewonnenen Soll-Wert und berechnet die notwendigen Ansteuersignale für die hydraulisch vorgesteuerten Servoventile. Mit Hilfe dieser 3/3-Wegeventile können die Kammerdrücke variiert und damit die gewünschte Kraft eingeregelt werden. Zwischen beiden Zylinderkammern ist eine Bypassdrossel angeordnet, die die Systemdämpfung vergrößert und die Regelgüte verbessert [62]. Die Geschwindigkeit des Lenkzylinders wirkt als Störgröße für den Lastregelkreis, da sich

durch die Bewegung des Lenkzylinders das Kammervolumen im Lastzylinder und damit auch der Kammerdruck ändert. Dieser Effekt wird durch eine Störgrößenaufschaltung reduziert. Für die Versorgung der Servoventile wird ein separates Konstantdrucksystem verwendet, das unabhängig von der Druckversorgung des Lenksystems ist. Für die Versorgung des Steer-by-Wire Systems wird eine einzelne verstellbare Axialkolbenpumpe eingesetzt, da die Fehlertoleranz der Druckversorgung nicht Untersuchungsgegenstand dieser Arbeit ist und der in Kapitel 4.2.2 aufgelistete Fehlerfall der Druckversorgung (Versorgungsdruck ist maximal) auch mit einer Pumpe erzeugt werden kann.

Als 2/2-Wegeventile im Lenkventil werden robuste Ventile in Sitzbauweise ausgewählt, da den Ventilen in dieser Architektur neben der eigentlichen Regelfunktion auch eine Absperrfunktion im stromlosen Zustand zukommt, um gefahrbringende Bewegungen bei einem Fehler des Typs B zu verhindern. Um den Einfluss verschiedener Ventileigenschaften zu untersuchen, werden zur Realisierung sowohl direktgesteuerte Schalt- als auch Proportionalventile eingesetzt. Damit auch bei Einsatz eines Schaltventils der Volumenstrom quasi-kontinuierlich verändert werden kann, wird das Schaltventil mit einem geeigneten pulsweitenmodulierten Ansteuersignal (PWM-Signal) betrieben, so dass bei jeder steigenden Flanke der Ventilkörper kurz vom Sitz abhebt (*ballistischer Betrieb*) und einen definierten Ölfluss ermöglicht [84, 80]. Dazu muss die PWM-Frequenz f entsprechend hoch und der Tastgrad g entsprechend niedrig gewählt werden, so dass sich eine Pulsbreite $t = g/f$ ergibt, die niedriger als die Schaltzeit des Ventils ist. Exemplarisch ergibt sich dabei die in Abbildung 6.2 dargestellte Ventilkennlinie. Prinzipbedingt ist die Ventilkennlinie im Bereich II, der für die Regelung verwendet wird, absolut hysteresefrei mit einer vergleichsweise guten Reproduzierbarkeit und Robustheit gegenüber Schwankungen von Umgebungsbedingungen. Das verwendete Schaltventil bleibt in geöffneter Stellung (Bereich III), sobald der Tastgrad einen Wert erreicht, bei dem der Ventilkörper den oberen Anschlag

des Ventils berührt. Ventilfehler des Typs B werden am Prüfstand bei den Schaltventilen durch eine dauerhafte Bestromung der Magnetspulen eingeleitet.

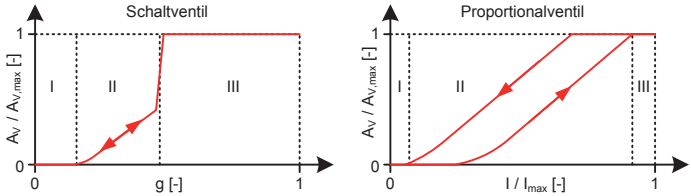


Abb. 6.2: Schematische Darstellung der statischen Ventilkennlinien für das verwendete Schaltventil bei pulsweitenmodulierter und das Proportionalventil bei stromgeregelter Ansteuerung

Als Proportionalventil wurde ein direktgesteuertes stromgeregeltes Sitzventil ausgewählt, das eine ausgeprägte Hysterese im regelungstechnisch relevanten Bereich II hat, siehe Abbildung 6.2. Der Beginn und Verlauf der dargestellten Kennlinie weist zudem eine starke Abhängigkeit von der Dynamik der Stromänderung und der Höhe der anliegenden Systemdrücke auf. Vor allem im Feinsteuerbereich führt diese ungenau bekannte und hysteresebehaftete Kennlinie zu einem großen Kompensationsaufwand für den Lenkwinkelregler. Aus diesem Grund wird der in Abbildung 5.8 dargestellte Block der nichtlinearen invertierten Ventilkennlinie um ein phänomenologisches Modell der Hysterese im nominalen Fall derart erweitert, dass der von diesem Block berechnete Stromwert auch von der Änderungsrichtung des gewünschten Volumenstroms abhängig ist. Bei dem verwendeten Ventil ist aufgrund der Tatsache, dass es sich um ein nicht-druckkompensiertes Ventil handelt, die Betätigungskraft der Magnetspule bei hohen am Ventil anliegenden Druckdifferenzen nicht groß genug, um das Ventil in die vollständig geöffnete Stellung zu bringen und zu halten. Aus diesem Grund werden Ventilfehler des Typs B bei großen Druckdifferenzen durch eine mechanische Blockierung des Ventilkörpers in der geöffneten Stellung realisiert.

6.1.2 Lenkwinkelregelung

Der Nachweis der Annahme 1 *»Fehlertoleranz«* erfolgt im Folgenden mit Hilfe der Proportionalventile und der zuvor festgelegten Manöver. Einzelne Validierungsmessungen bei Verwendung der Schaltventile sind in [84] beziehungsweise in Anhang A.3 zu finden.

Abbildung 6.3 stellt die Messergebnisse der Lenkwinkel- und Lastregelung für Manöver 2 in unterschiedlichen Lastsituationen im fehlerfreien Fall dar. Die Bewegung des Lenkzylinders wirkt als Störgröße für den Lastregelkreis, so dass F_{ist} der Soll-Lenkkraft F_{soll} nur prinzipiell folgen kann.

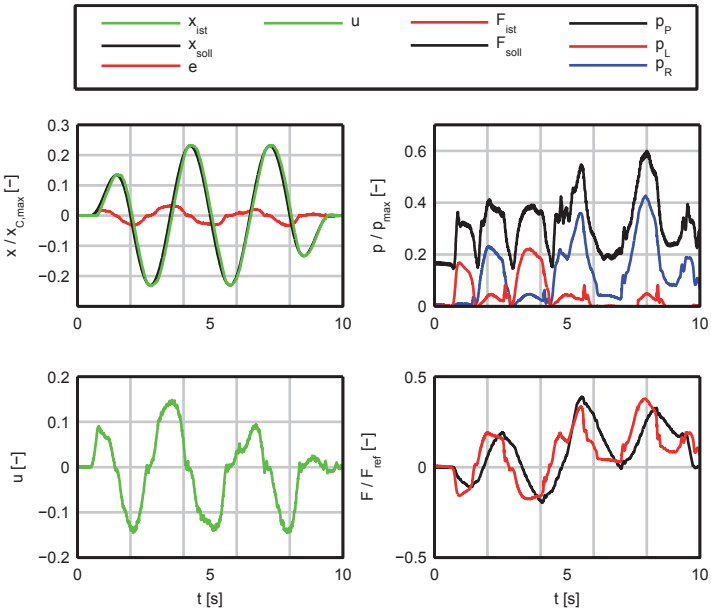


Abb. 6.3: Messergebnisse für Manöver 2 mit Proportionalventilen bei unterschiedlichen Lastsituationen im fehlerfreien Fall

Da die Höhe der eingeprägten Kräfte mit ausreichender Genauigkeit dem maximalen Soll-Wert entsprechen, ist der Lastregler für den notwendigen Nachweis der Lenkwinkelregelung unter Last geeignet. In Abbildung 6.3 wird zum Zeitpunkt $t = 5$ s ein rampenförmiger Lastsprung eingeleitet, der so hoch ist, dass die Lenkkräfte nur noch in eine Richtung wirken. Es ist erkennbar, dass bei Lastschwankungen eine automatische Anpassung des Versorgungsdrucks durch die Regelpumpe und das Prioritätsventil erfolgt, so dass in Betrag und Richtung schwankende Lasten keinen nennenswerten Einfluss auf die Positionsregelung haben.

Bei der Untersuchung der Fehlertoleranz des betrachteten Lenkventils muss zwischen temporären und dauerhaften Fehlern sowie zwischen dem Verhalten des Lenksystems zum Zeitpunkt der Fehlereinleitung und nach der Fehlereinleitung unterschieden werden. Temporäre Fehler treten beispielsweise dann auf, wenn ein oder mehrere Ventile durch ein Fehler im Steuergerät falsch angesteuert werden. Dieser Fehler muss innerhalb der Fehlertoleranzzeit für Gefahr 1.1 durch das Steuergerät selbst erkannt und durch Abschaltung der Endstufen der Ventile behoben werden. Da die für diesen Anwendungsbereich eingesetzten Hydraulikventile verglichen mit der internen Fehlererkennung eines Steuergeräts träge sind, haben temporäre Fehler eine geringe Auswirkung auf die Lenkwinkelregelung und werden nicht betrachtet.

Das unterschiedliche Verhalten der Lenkwinkelregelung zum Zeitpunkt der Fehlereinleitung und nach dem Fehlereintritt ist für Manöver 1 und Fehler des Typs A und B in Abbildung 6.4 gegenübergestellt. In allen dargestellten Fällen wurden Ventilfehler eingeleitet, die die Lenkbewegung verlangsamen. Für Ventilfehler des Typs A entspricht dies beispielsweise einer Unterbrechung in einer der Magnetspulen. Plötzlich eintretende Ventilfehler des Typs B, die die Lenkzylinderbewegung verlangsamen, sind nur bei einem Doppelfehler möglich, der vernachlässigt werden kann[1].

[1] Dieser Fall tritt zum Beispiel bei einer fehlerhaften Ansteuerung eines eigentlich nicht betätigten Ventils und Verklemmen des Ventils in der geöffneten Stellung auf.

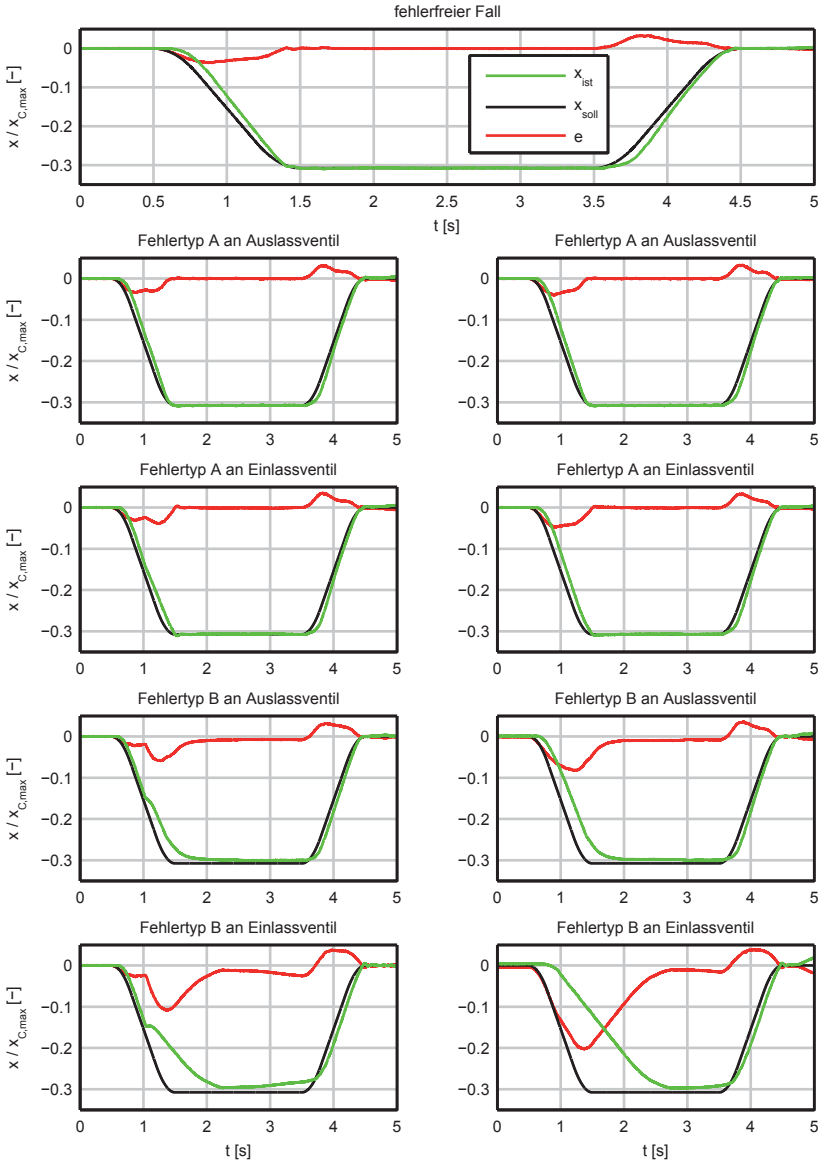


Abb. 6.4: Messergebnisse für Manöver 1 mit Proportionalventilen für zum Zeitpunkt $t = 1\ s$ plötzlich eintretende (links) und bereits zuvor vorliegende Fehler (rechts)

Die Fehler des Typs B wurden bei allen Messungen durch Bestromung der Magnetspulen mit dem maximal zulässigen Strom eingeleitet, um den Zeitpunkt der Fehlereinleitung elektronisch vorgeben zu können. Die Ergebnisse machen deutlich, dass plötzliche eintretende Fehler jeglicher Art von der Lenkwinkelregelung sehr gut kompensiert werden können und zu keinen kritischen oder unkontrollierten Bewegungen des Lenkzylinders führen. Im folgenden Nachweis werden daher plötzlich eintretende Fehler nicht näher betrachtet. Es werden lediglich die Regelgüte und Lenksystemperformance nach Eintritt des Fehlers bewertet, die in Abbildung 6.4 in der rechten Spalte dargestellt sind. Darin zeigt sich, dass die gesetzliche Vorgabe, die das Erreichen der stationären Kreisfahrt innerhalb von drei Sekunden fordert, auch im Fehlerfall eingehalten wird. Für den Fehlertyp B an einem Einlassventil ist die Lenkzylindergeschwindigkeit durch die niedrige Fahrgeschwindigkeit (2 km/h) und die damit verbundenen hohen Lenkkräfte deutlich niedriger als die Fahrervorgabe. Durch die geringe Fahrgeschwindigkeit ergibt sich daraus jedoch kein Gefahrenpotential.

Obwohl die analytische Betrachtung der Fehlertoleranz im statischen Fall das Ergebnis geliefert hat, dass die Fehlertoleranz bei einem offenen Auslassventil schlechter ist als bei einem offenen Einlassventil, ist für die betrachteten Proportionalventile das Gegenteil der Fall. Bedingt durch die hohe an den Auslassventilen anliegende Druckdifferenz (siehe Abbildung 5.5) und die Ventilkonstruktion (nicht-druckkompensiertes Ventil) können die Auslassventile durch die zur Verfügung stehende Magnetkraft nicht weit genug geöffnet werden. Dadurch kann der notwendige Volumenstrom und damit die notwendige Lenkgeschwindigkeit nicht erreicht werden. Trotzdem lassen sich auch in diesem Fehlerfall bei Verwendung dieser Ventile die Räder in beide Richtungen ausreichend schnell verstellen. Da dieser Fehlerfall signalbasiert mit geringem Aufwand innerhalb kurzer Zeit erkannt werden kann, wird der Fahrer gewarnt und die Fahrgeschwindigkeit gedrosselt, bevor der Fahrer in eine Situation kommt, in der die reduzierte Lenkgeschwindigkeit

sicherheitskritische Auswirkungen haben kann. Die ausgewählten Schaltventile sind druckkompensiert und weisen diesen Effekt deutlich weniger stark auf, so dass bei diesen der Soll-Verlauf vergleichsweise gut erreicht werden kann (siehe Abbildung A.5).

Für Manöver 2 ist das Verhalten der Lenkwinkelregelung im Fehlerfall in Abbildung 6.5 und 6.6 dargestellt. Neben der Soll- und Ist-Position sowie der Regelabweichung ist auch die Stellgröße u (Ausgangsgröße des Reglers) dargestellt. Bei den Messergebnissen mit aufgeschaltetem Fehler ist der Verlauf der Stellgröße im fehlerfreien Fall als Referenz in schwarz dargestellt. Für den Fehlertyp A an einem Auslassventil ergibt sich kein nennenswerter Unterschied, da Druckschwankungen in den Zylinderkammern durch das Prioritätsventil und die Regelpumpe und nicht durch den Lenkwinkelregler kompensiert werden. Im Falle dieses Fehlers an einem Einlassventil muss der Regler die richtungsabhängig unterschiedliche Systemverstärkung durch eine größere Stellgröße kompensieren. Die Regelabweichung erhöht sich durch die geänderte Streckenverstärkung nur leicht. Im Falle eines Fehlers des Typs B am Auslassventil muss der Regler richtungsabhängig stark kompensatorisch eingreifen, um den direkt zum Tank abfließenden Volumenstrom zu kompensieren. Das notwendige Maß der Erhöhung hängt von den anliegenden Radkräften ab, da durch diese die Höhe des abfließenden Ölstroms bestimmt wird. Für Ventilfehler des Typs B an Einlassventilen sowie im Fehlerfall *»maximaler Pumpendruck«* ist die Regelgüte durch den zuvor beschriebenen Effekt der hohen Druckdifferenzen und der nicht-druckkompensierten Ventile deutlich reduziert. Der Vergleich mit den Messergebnissen bei Verwendung der Schaltventile in Abbildung A.5 macht deutlich, dass Fehler dieser Art in einer Ventilarchitektur mit unabhängigen Steuerkanten bei Verwendung druckausgeglichener Ventile nicht kritischer sind als Fehler des Typs B an Auslassventilen (siehe Abbildung 6.5). In Abbildung 6.6 ist ebenfalls das Messergebnis für einen Fehlerfall mit Leckage an mehreren Ventilen dargestellt.

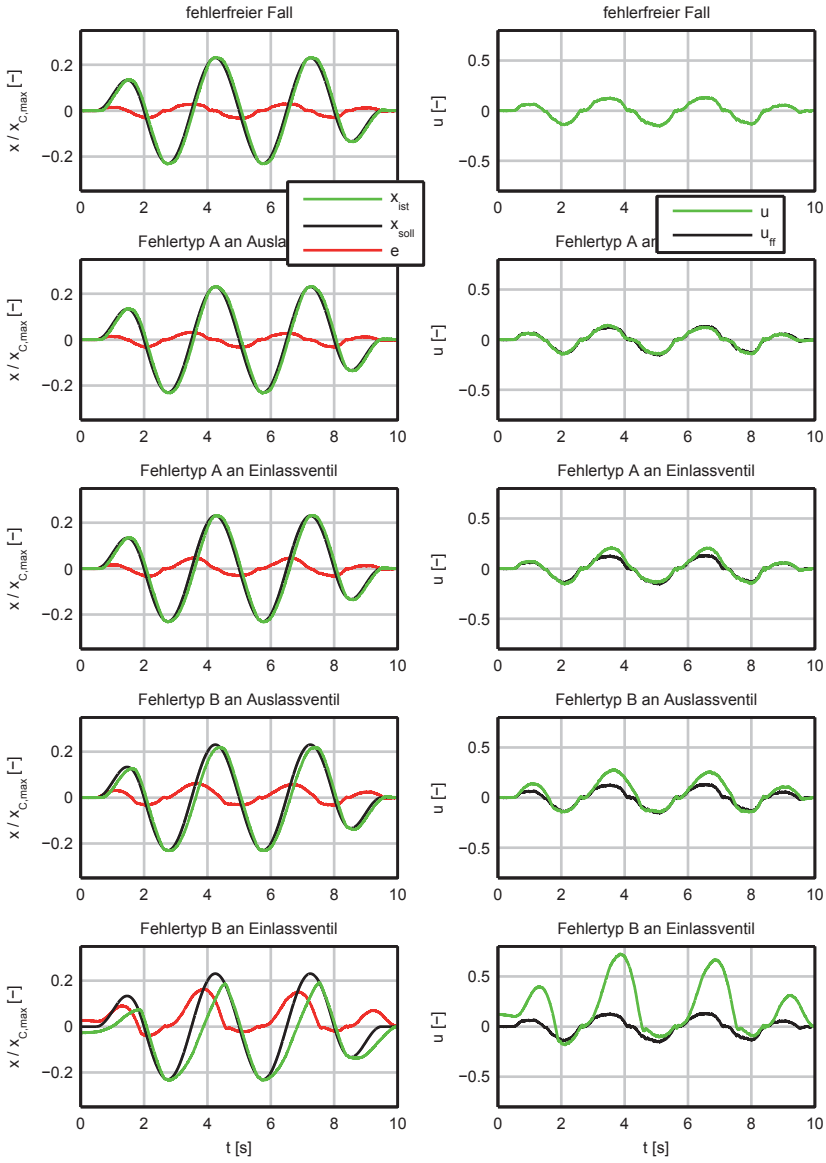


Abb. 6.5: Messergebnisse für Manöver 2 mit Proportionalventilen für Fehler des Typs A und B

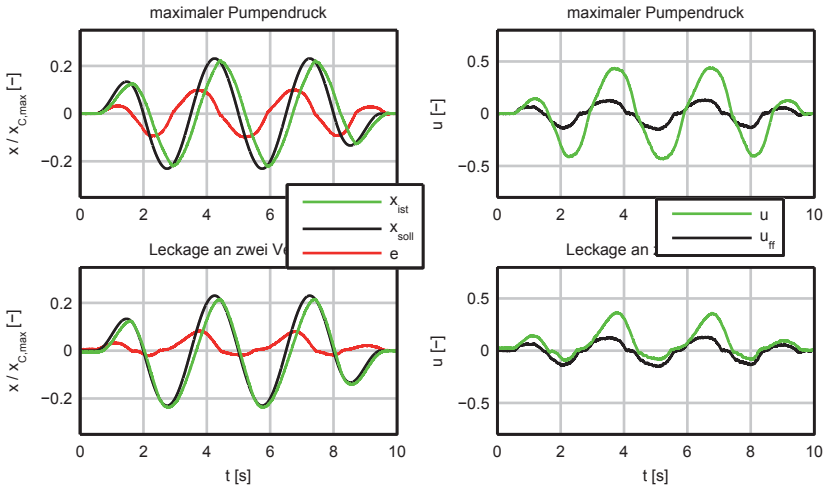


Abb. 6.6: Messergebnisse für Manöver 2 mit Proportionalventilen in weiteren Fehlerfällen

Die Leckage wurde dabei an einem Ein- und Auslassventil auf unterschiedlichen Seiten eingeprägt und erzeugt bei dem nominalen Druckabfall über dem Einlassventil einen fehlerhaften Volumenstrom von ungefähr 25 Prozent des maximalen Volumenstroms. Selbst bei einer derart hohen Leckage in zwei Ventilen ist die Lenkbarkeit gewährleistet.

Die gezeigten Messergebnisse verdeutlichen, dass die Lenkbarkeit der Räder in beide Richtungen bei der gewählten passiv fehlertoleranten Ventilarchitektur auch im Fehlerfall unter Last ohne Rekonfiguration möglich ist. Die Auswirkungen der Ventilfehler werden vom Lenksystem inhärent kompensiert, so dass die vom Fahrer gewünschte Lenkbewegung auch im Fehlerfall ausgeführt wird. In Kapitel 6.2 wird simulativ abgeschätzt, ob sich im Fehlerfall für den Fahrer über das normale Maß hinaus der Bedarf ergibt, kompensatorisch einzugreifen, um die im Vergleich zum fehlerfreien Fall schlechtere Regelgüte auszugleichen.

6.1.3 Fehlererkennung

Während der Durchführung des Selbsttests hängt die Geschwindigkeit des Druckauf- und -abbaus von der Ansteuerung der einzelnen Ventile in den verschiedenen Phasen des Selbsttests ab. Da in den jeweiligen Druckaufbauphasen nur ein Einlassventil aber kein Auslassventil geöffnet ist, muss der Ölstrom sehr feinfühlig dosiert werden, um einen zu starken Druckanstieg in der im Schlauch eingeschlossenen Ölsäule zu vermeiden. In Abbildung 6.7 sind für den fehlerfreien Fall und für verschiedene Fehlerfälle die Messergebnisse des Selbsttests bei Verwendung der Proportionalventile dargestellt. In der Darstellung für den fehlerfreien Fall sind die vier Druckauf- und abbauphasen erkennbar, in denen jeweils eines der vier Ein- und Auslassventile getestet wird. Bedingt durch den Druckanstieg und die Kompressibilität des Öls und der Hydraulikschläuche kommt es zu einer geringen Lenkzylinderbewegung von unter einem Prozent, von der keine Gefahr ausgeht. Verglichen mit dem Ergebnis der Schaltventile in Abbildung A.6 ist erkennbar, dass bei den verwendeten Proportionalventilen, bedingt durch das ungenaue Ventilverhalten, der Druckauf- und -abbau an den verschiedenen Ventilen unterschiedlich ausgeprägt ist, während der Volumenstrom mit den Schaltventilen wesentlich reproduzierbarer eingestellt werden kann.

Bei einem Ventilfehler des Typs A an einem Auslassventil kann der Druck im jeweiligen Testzyklus nicht mehr abgebaut werden. Infolge des Druckanstiegs kommt es zu einer Lenkzylinderbewegung. Der Test wird anschließend durch Deaktivierung aller Ventile abgebrochen, bevor eine gefahrbringende Lenkzylinderauslenkung oder ein zu hoher Systemdruck erreicht ist. Liegt ein Fehler des Typs A an einem Einlassventil vor, so bleibt der jeweilige Druckanstieg aus und der Test ist unmittelbar beendet. Klemmt ein Auslassventil in geöffneter Stellung (Fehlertyp B), so hängt die Systemreaktion davon ab, auf welcher Zylinderkammerseite der Fehler vorliegt. Ist der Fehler auf der Seite, dessen Einlassventil zuerst getestet wird (linke Kammer), dann bricht der Test ab, weil kein Druckaufbau stattfindet.

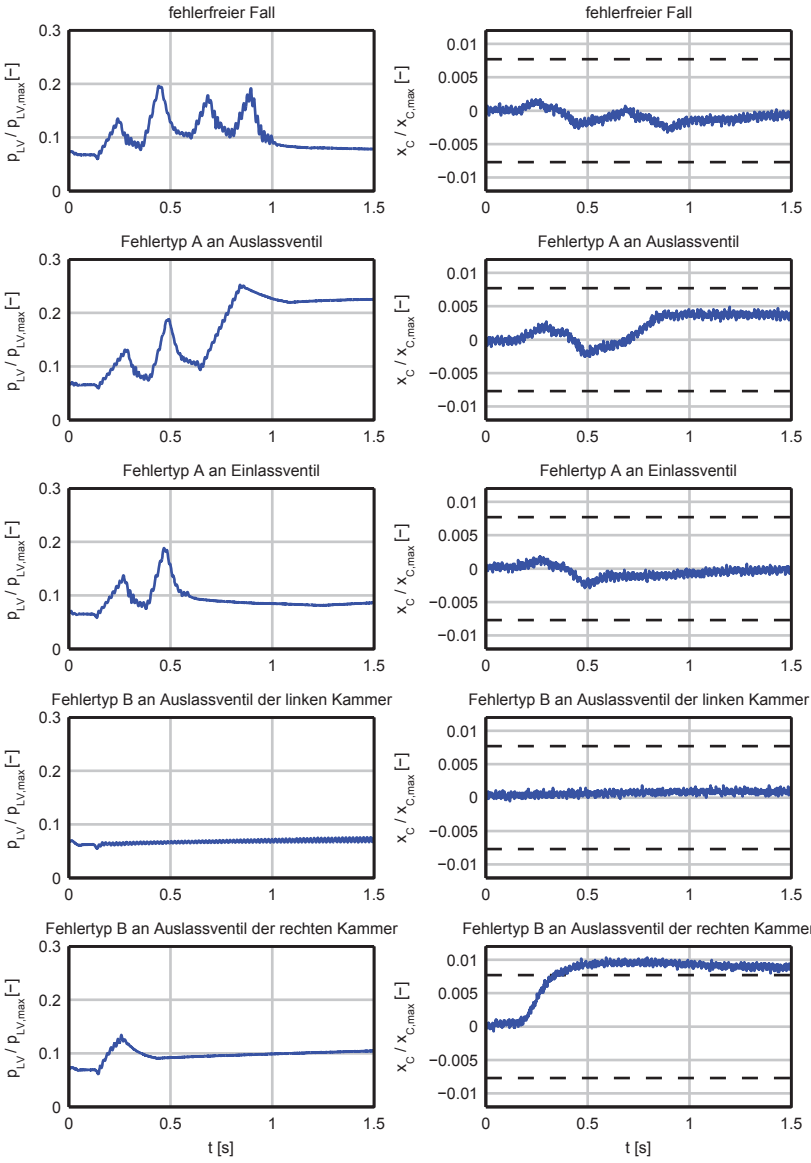


Abb. 6.7: Messergebnisse des Selbsttests mit Proportionalventilen für Fehler des Typs A und B

Im anderen Fall bricht der Test ab, weil eine Lenkzylinderbewegung durch den geöffneten Ein- und Auslass auftritt. Ein Fehler des Typs B an Einlassventilen führt auch ohne Ventilansteuerung zu einem hohen Systemdruck. In einer derartigen Situation wird der Test nicht gestartet. Daher ist zu diesem Fehler keine Messung dargestellt.

Durch die Messungen wird deutlich, dass die unterschiedlichen Fehler im vorgeschlagenen Selbsttest zu eindeutig erkennbaren Systemreaktionen führen. Auf Grund dieser Systemreaktionen ist es möglich, alle Fehler sicher in einer angemessenen Zeit zu erkennen, ohne dass eine gefahrbringende Radbewegung am Fahrzeug während des Selbsttests auftritt. Eine Fehlerdiagnose zur Bestimmung der genauen Art und des genauen Orts des Fehlers ist zur Erfüllung des Sicherheitskonzepts nicht erforderlich und würde zu einem komplexeren und damit auch zeitintensiveren Selbsttest führen.

Für das in Abbildung 5.10 dargestellte Verfahren zur modellbasierten Fehlererkennung ist es notwendig, dass das Eingangs-/Ausgangsverhalten zwischen der Stellgröße u und der Geschwindigkeit v_{ist} ausreichend genau bekannt und konstant ist. Andernfalls führen Schwankungen von Strecken- oder Umgebungsparametern sowie Exemplarstreuungen ebenfalls zu einem Ausschlag des Residuums r, so dass diese nicht von Ventilfehlern unterschieden werden können. Dies ist bei den ausgewählten Proportionalventilen der Fall, da die Ventilkennlinie eine starke Hysterese und Abhängigkeiten von anderen Systemparametern aufweist. Daher erfolgt der Nachweis der modellbasierten Fehlererkennung mit Hilfe der ausgewählten Schaltventile, die durch die gewählte Ansteuerungsstrategie keine Hysterese und eine sehr reproduzierbare Kennlinie aufweisen, siehe Abbildung 6.2. Innerhalb des Bereichs II lässt sich der Volumenstrom durch die gewählte Ansteuerungsstrategie proportional verstellen und sehr fein dosieren. Die experimentellen Ergebnisse sind in Abbildung 6.8 für den fehlerfreien Fall und Fehler des Typs B dargestellt. Im Anhang in Abbildung A.7 sind die Fehler des Typs A dargestellt, die nur einen geringen oder keinen Einfluss auf die Lenkperformance haben.

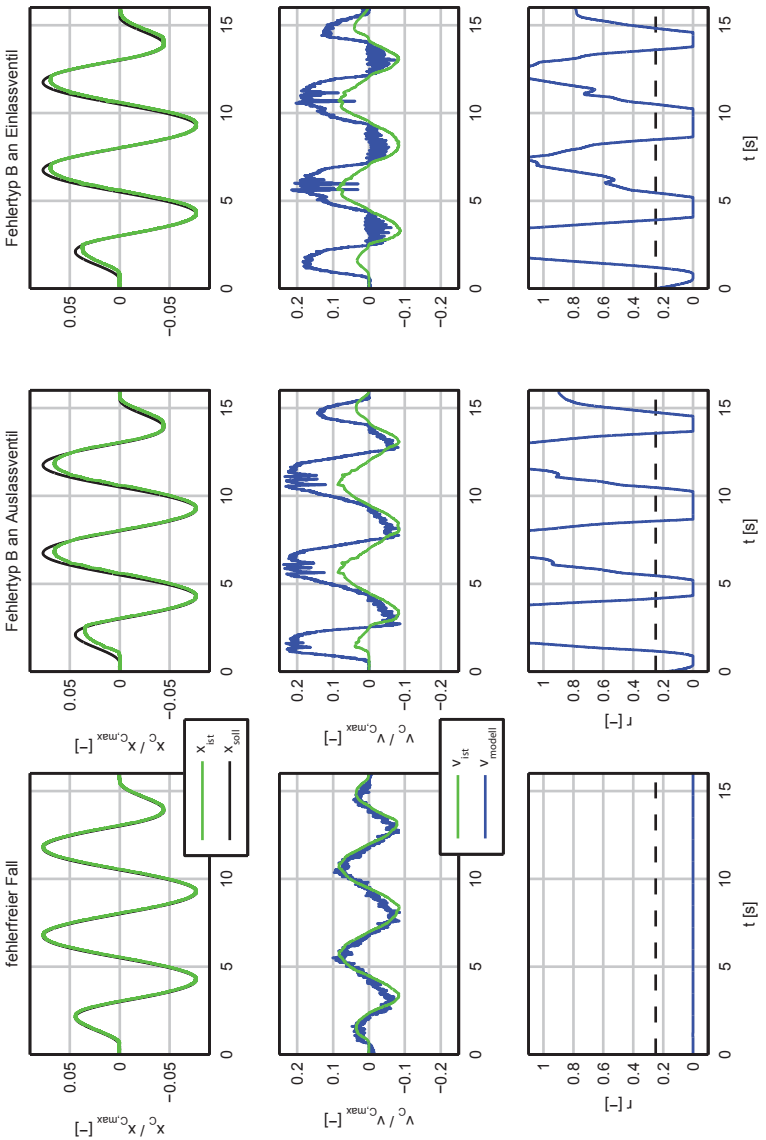


Abb. 6.8: Messergebnisse der modellbasierten Fehlererkennung mit Schaltventilen für Fehler des Typs B

Der fehlerfreie Fall ist dadurch gekennzeichnet, dass die reale und vorhergesagte Zylindergeschwindigkeit übereinstimmen und das Residuum r nahezu Null ist. Bei Fehlertyp A an einem Einlassventil (siehe Abbildung A.7) ist die Systemverstärkung richtungsabhängig halbiert. Der Regler kann dies durch Vergrößerung der Stellgröße bei geringer Verschlechterung der Regelgüte kompensieren. Durch die erhöhte Stellgröße erhöht sich ebenfalls die vorhergesagte Geschwindigkeit v_{modell}, was zu einem Ausschlag des Residuums führt. Verglichen mit dem fehlerfreien Fall kann eine Erkennungsschwelle festgelegt werden, mit der fehlerfreie und fehlerbehaftete Fälle eindeutig voneinander unterschieden werden können. Im Falle eines Fehlers des Typs B (siehe Abbildung 6.8) sind die Auswirkungen auf das Residuum noch größer, da die Stellgröße zur Kompensierung des fälschlicherweise fließenden Volumenstroms sehr stark vergrößert werden muss.

Durch die dargestellten Ergebnisse des Selbsttests und der modellbasierten Fehlererkennung wird klar, dass zur sicheren Fehlererkennung in einem Lenkventil mit unabhängigen Steuerkanten Positionssensoren an jedem einzelnen Ventil nicht benötigt werden und Annahme 2 *»Fehlererkennung«* damit gültig ist. Durch den entworfenen Selbsttest können sämtliche Ventilfehler bei Systemstart zuverlässig erkannt werden. Die modellbasierte Fehlererkennung eignet sich zur Erkennung von kritischen Fehlern, die in dynamischen Fahrsituationen einen nennenswerten Einfluss auf die Systemperformance haben können. Die Tatsache, dass Fehler durch die modellbasierte Fehlererkennung nicht unmittelbar, sondern mit einer Zeitverzögerung und nur während einer Lenkbewegung erkannt werden können, ist akzeptabel, da das System auch ohne Fehlererkennung fehlertolerant ist und diese Information nicht zur Rekonfiguration benötigt wird.

6.2 Simulative Bewertung auf Fahrzeugebene

Für die simulative Bewertung der zuvor dargestellten Ergebnisse auf Fahrzeugebene wird die am Prüfstand ermittelte Lenkzylinderposition open-loop in das in Kapitel 3.2.3 vorgestellte und in [60] validierte Fahrdynamikmodell eines Traktors eingespeist. Durch die geringe Fahrgeschwindigkeit und die gute Regelgüte in Manöver 1 wird auf eine Fahrdynamiksimulation dieser Messungen verzichtet. Für Manöver 2 (Dauersinus) ist in Abbildung 6.9 die Trajektorie der Fahrzeugbewegung für ein ideales Lenksystem[2] mit der des fehlerfreien und fehlerbehafteten Steer-by-Wire Systems mit unabhängigen Steuerkanten gegenübergestellt. Abbildung 6.10 zeigt eine räumliche Visualisierung der Simulationsergebnisse für Manöver 2. Für die Simulation wurde der Fehlerfall *»Leckage an zwei Ventilen«* ausgewählt, da dieser die kritischsten Auswirkungen hat. Die Regelabweichung ist bei einem Fehler des Typs B an Einlassventilen sowie bei einem Fehler in der Druckversorgung zwar größer, dies kann jedoch auf das Verhalten der nicht-druckkompensierten Proportionalventile bei hohen Druckdifferenzen zurückgeführt werden und ist nicht charakteristisch für das entwickelte Steer-by-Wire Lenkventil (siehe Abbildung 6.5 und 6.6).

Bedingt durch die Tatsache, dass der Lenkwinkelregelkreis der Fahrervorgabe am Lenkrad nur mit einer endlichen Genauigkeit folgen kann, entsteht auch für das fehlerfreie Lenksystem bei open-loop Einspeisung der Messergebnisse in das Fahrzeugmodell eine Abweichung und Drift bezüglich der Trajektorie der Referenzkurve des idealen Lenksystems[3]. Eine Drift tritt durch Effekte wie Seitenwind, Fahrbahnunebenheiten, Schlupf oder interne hydraulische Leckage auch bei konventionellen Lenksystemen auf und wird durch den Fahrer intuitiv kompensiert.

[2] Bei einem idealen Lenksystem folgt die Lenkzylinderposition in direkter Weise der Fahrervorgabe am Lenkrad.

[3] Es ist zu beachten, dass die dargestellte Abbildung eine unterschiedliche Skalierung für die x- und y-Achse aufweist.

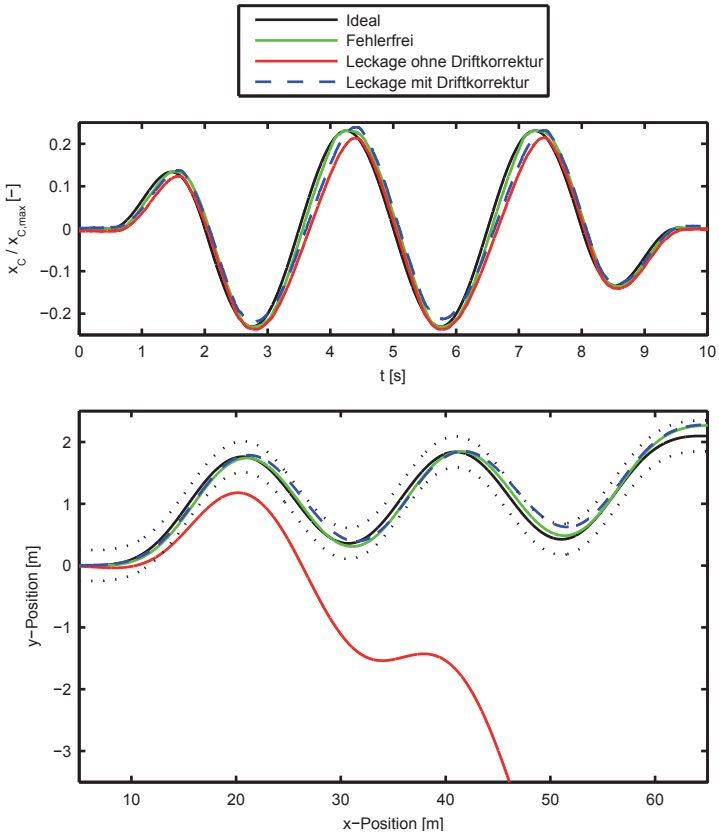


Abb. 6.9: Fahrzeugtrajektorie für Manöver 2 mit Darstellung eines Toleranzbands (+/- 0,25 *m*) sowie Darstellung der dazugehörigen Verläufe der Lenkzylinderposition

Im dargestellten Fehlerfall ergibt sich vor allem durch die bereits bei Beginn der Messung vorhandene Regelabweichung und die einseitige Fehlerauswirkung eine deutlich größere Drift nach rechts als im fehlerfreien Fall. Um das notwendige Ausmaß der Kompensation durch den Fahrer für den dargestellten Fehlerfall abzuschätzen, wird das Messergebnis der Lenkzylinderposition

additiv und open-loop mit einem Korrektursignal überlagert, so dass die Drift kompensiert und das Fahrzeug möglichst gut der Referenztrajektorie folgt. Das dargestellte Ergebnis mit Driftkorrektur ergibt sich bei additiver Überlagerung eines linear ansteigenden und wieder abfallenden und offsetbehafteten Signals mit einem Maximalwert von lediglich $1,3°$ Lenkwinkel am Rad. Ein derartiger Kompensationsaufwand ist sicherheitstechnisch unbedenklich, auch wenn dieser für den Fahrer möglicherweise wahrnehmbar sein sollte.

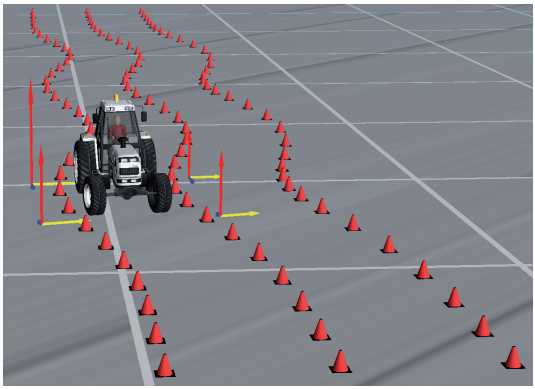


Abb. 6.10: Visualisierung der Trajektorie von Manöver 2 mit Hilfe des Simulationsmodells

In Abbildung 6.11 sind die Simulationsergebnisse der für die Querdynamik relevanten Systemgrößen *Lenkwinkel* δ, *Querbeschleunigung* a_y und *Gierrate* $\dot{\varphi}$ für Manöver 3 (Lenkwinkelsprung) im idealen, fehlerfreien und fehlerbehafteten Fall (Fehlertyp B an einem Auslassventil[4]) dargestellt. Zur Bewertung kann aus diesem Fahrmanöver die Ansprechzeit des Fahrzeugs als Bewertungsmaßstab für das querdynamische Verhalten ermittelt werden. Nach [15] ergibt sich diese als Differenz zwischen dem Zeitpunkt des Erreichens des halben stationären Endwerts des Lenkradwinkels und dem Errei-

[4]Zum Ausgleich der stationären Regelabweichung im Fehlerfall wurde die Sprunghöhe des Soll-Signals soweit angepasst, dass sich der gleiche stationäre Endwert ergibt wie im fehlerfreien Fall. Der angegebene Fehlerfall wurde ausgewählt, da dieser in Manöver 3 die schlechteste Dynamik aufweist.

chen von 90 Prozent des stationären Endwerts der jeweiligen Systemgröße. Die Ansprechzeit verdeutlicht, wie agil das Fahrzeug auf Lenkvorgaben des Fahrers reagiert. Aus den Simulationen wurden für den Versuchstraktor die folgenden Werte ermittelt:

- **Ansprechzeit Querbeschleunigung:**

Ideal:	0,50 s
Fehlerfrei:	0,59 s
Fehlertyp B an Auslassventil:	0,72 s

- **Ansprechzeit Gierrate:**

Ideal:	0,30 s
Fehlerfrei:	0,38 s
Fehlertyp B an Auslassventil:	0,51 s

Die Ergebnisse machen deutlich, dass die Ansprechzeiten und damit die Fahrdynamik des betrachteten Fahrzeugs auch bei einem idealen Lenksystem durch die Massenträgheit und die vergleichsweise geringe Reifensteifigkeit limitiert sind und dass das simulierte Manöver im Grenzbereich der Fahrphysik des betrachteten Traktors liegt. Dies ist daran erkennbar, dass der Aufbau der Querbeschleunigung und der Gierrate deutlich gegenüber der Lenkradbewegung verzögert ist. Der Unterschied zwischen dem Aufbau der Querbeschleunigung und der Gierrate des realen fehlerfreien Lenksystems verglichen mit dem idealen Fall ist gering, obwohl der Lenkwinkel vergleichsweise langsam dem Soll-Verlauf (idealer Fall) folgt. Im Fehlerfall sind Einbußen im Ansprechverhalten vor allem bei der Gierrate erkennbar.

Die simulative Bewertung untermauert die Annahme, dass das Fahrzeug auch im Fehlerfall sicher gelenkt werden kann, ohne dass über das normale Maß hinausgehende kompensatorische Eingriffe des Fahrers notwendig sind (Annahme 1 *»Fehlertoleranz«*). Der Fahrer kann daher auch im Fehlerfall das

Fahrzeug in den relevanten Manövern mit unverändertem Kraft- und Lenkwinkelaufwand bei nur geringen Einbußen bezüglich der Lenkperformance führen. Eine ausreichende Sicherheit ist daher bei Eintritt eines Einzelfehlers gewährleistet. Die zusätzlich zum vorgestellten Selbsttest implementierte modellbasierte Fehlererkennung kann dazu genutzt werden, das Restrisiko für das Auftreten eines gefahrbringenden Zweitfehlers, der die Lenkbarkeit potentiell gefährdet, weiter zu reduzieren. Aus den experimentellen und simulativen Ergebnissen wird zudem deutlich, dass eine Rekonfiguration nach erfolgreicher Fehlererkennung für das betrachtete Ventilkonzept sicherheitstechnisch nicht sinnvoll ist, da dadurch die Systemkomplexität und damit auch die Fehleranfälligkeit erhöht wird, aber nur eine marginale Verbesserung des Fahrverhaltens zu erwarten ist.

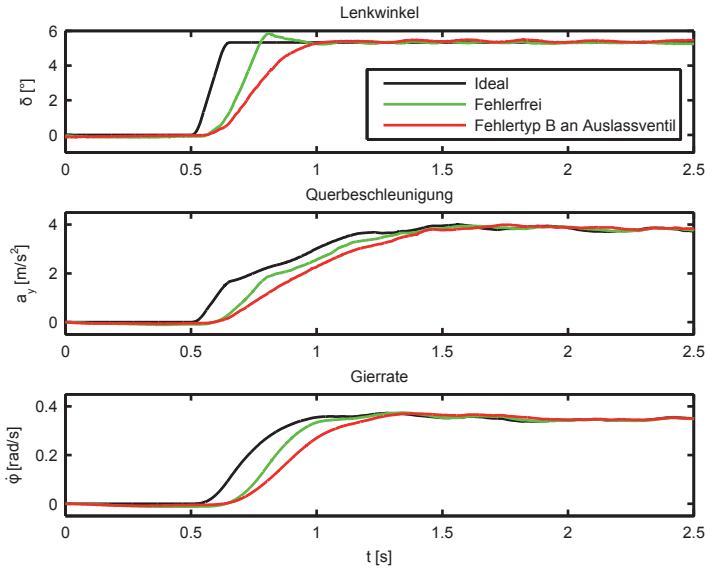


Abb. 6.11: Simulationsergebnis der für die Querdynamik relevanten Systemgrößen für Manöver 3

Durch die Messergebnisse der vorangegangenen Abschnitte wurde zudem verdeutlicht, dass bei der Auswahl der 2/2-Wegeventile neben der Erreichbarkeit einer akzeptablen Regelgüte und Feinsteuerbarkeit auch auf Aspekte bezüglich der Fehlertoleranz und Fehlererkennung geachtet werden muss. Für die Überprüfung der Eignung der Ventile ist im Wesentlichen der Fehlertyp B an einem Einlassventil relevant, der das Druckniveau im System erhöht und zu einem hohen Druckabfall über den intakten Auslassventilen führt. Im relevanten Lastbereich muss gewährleistet sein, dass über diese bei vollständiger Bestromung eine ausreichende Ölmenge zur Kompensierung des Fehlers fließen kann. Dazu sollten die verwendeten Ventile druckkompensiert sein. Für die Implementierung einer modellbasierten Fehlererkennung in der vorgestellten Art sind Ventile nötig, deren Durchflussverhalten bei konstantem Druckabfall ausreichend genau modellbasiert beschrieben werden können. Dazu ist beispielsweise eine möglichst geringe Hysterese erforderlich. Bei dem aktiven Selbsttest wird durch den Vergleich der Messergebnisse der ausgewählten Proportional- und Schaltventile deutlich, dass bei Ventilen mit einer reproduzierbaren und im Feinsteuerbereich gut aufgelösten Kennlinie (in diesem Fall: Schaltventile) bei gleicher Robustheit der Fehlererkennung ein niedrigeres Druckniveau für den Selbsttest ausreichend ist, siehe Abbildung 6.7 und A.6.

6.3 Abschlussvergleich

Nach der Konzeptionierung eines Steer-by-Wire Systems und dem Entwurf und Nachweis eines fehlertoleranten Lenkventils liegt nun eine detailliertere Grundlage für den in Kapitel 3.4 dargestellten Vergleich zwischen einer elektrohydraulischen Überlagerungslenkung und einem fehlertoleranten Steer-by-Wire System vor. Damit kann die naheliegende Einschätzung, dass der zusätzliche Aufwand zur Realisierung eines fehlertoleranten Steer-by-Wire Systems durch den doppelten Komponentenbedarf sehr hoch ist, differenzier-

ter bewertet werden. Für die hydraulische Energieversorgung wurde dargelegt, dass fehlertolerante Systeme in sehr großen Traktoren bereits Stand der Technik sind. In Traktoren, die mit einer separaten Lenkpumpe ausgestattet sind, kann diese mit der Pumpe für die Arbeitshydraulik kombiniert werden, um eine Fehlertoleranz zu gewährleisten. Dabei muss jedoch sicher gestellt sein, dass beide Pumpen nicht von der gleichen Energiequelle versorgt werden. Ebenfalls für die Realisierung einer fehlertoleranten elektrischen Energieversorgung wurden in Kapitel 4 einige Beispiele genannt, die zum Teil keine weitere Batterie und keinen weiteren Generator benötigen. Die zuverlässige Versorgung von elektrischen Komponenten mit Energie wird zukünftig immer relevanter, so dass auf langfristige Sicht fehlertolerante Bordnetze auch in Traktoren ohne Steer-by-Wire mehr und mehr Einsatz finden werden. Im Bereich der Sensorik wurde auf das Konzept der analytischen Redundanz verwiesen, bei dem mit Hilfe physikalischer Zusammenhänge unterschiedliche Messgrößen miteinander plausibilisiert werden können und damit Sensorik eingespart beziehungsweise auf interne Redundanz verzichtet werden kann. Für das elektronische Steuergerät werden wegen der Modularität und der Absicherung gegenüber Fehlern gemeinsamer Ursache zwei einzelne Steuergeräte mit fail-silent Verhalten bevorzugt, so dass hierbei der Hardware-Aufwand gegenüber fehlertoleranten Überlagerungslenkungen doppelt so hoch ist. Für die zentrale Komponente eines hydrostatischen Steer-by-Wire Systems, dem fehlertoleranten Lenkventil, wurde in den vorangegangenen Kapiteln ein Konzept mit unabhängigen Steuerkanten vorgestellt und bewertet, das gegenüber einer hydrostatischen Lenkeinheit und einem hydrostatischen Überlagerungsventil mit Sensorik und Abschaltventil eine vergleichsweise geringe Komplexität trotz Erfüllung aller Sicherheitsanforderungen aufweist. In dem vorgeschlagenen Konzept wird die Lenkeinheit, die zwangsweise in oder an der Kabine des Fahrzeugs montiert werden muss und mit einem mechanischen Lenkgestänge mit dem Lenkrad verbunden ist, durch ein elektronisches Lenkrad mit Handkraftaktor ersetzt.

In dem Vergleich der verschiedenen Ventilarchitekturen zur Realisierung eines fehlertoleranten Steer-by-Wire Systems aus Abbildung 4.2 wurde dargestellt, dass die Komplexität und die Anzahl der notwendigen Komponenten bei der Realisierung eines Lenkventils mit unabhängigen Steuerkanten gegenüber Zweikanalarchitekturen mit fail-silent Verhalten reduziert werden können. Die Funktionsfähigkeit und Sicherheit dieses Ansatzes wurde in diesem Kapitel nachgewiesen. Vorteilhaft ist dabei insbesondere die Tatsache, dass bei Realisierung eines passiv fehlertoleranten Reglers durch die inhärente Fehlerkompensation keine zeitkritische Fehlererkennung und Rekonfiguration notwendig ist. Durch die Bestätigung der beiden Annahmen zur Fehlertoleranz und Fehlererkennung aus Kapitel 4.1.1 in Kapitel 5 und 6 konnte nachgewiesen werden, dass Absperrventile und Positionssensoren an den Wegeventilen zur Gewährleistung der Sicherheitsanforderungen in dieser Architektur nicht erforderlich sind. Durch die Untersuchung wurde auch der Einfluss von Fehlern auf die zur Verfügung stehende Lenkgeschwindigkeit und damit auf die resultierende Regelgüte quantifiziert. Vor allem Ventilfehler des Typs B an Auslassventilen reduzieren, mit steigender am Lenkzylinder anliegender Kraft, die maximale Lenkzylindergeschwindigkeit. Durch zusätzliche Maßnahmen, wie beispielsweise eine geeignete Anpassung des Ablaufquerschnitts im Lenkventil, kann die Fehlerauswirkung auf ein akzeptables Maß reduziert werden. Diese Notwendigkeit besteht bei zweikanaligen Architekturen mit Absperrventilen nicht, da bei diesen durch Abschaltung eines Kanals die Beeinflussung des Systemverhaltens des intakten Kanals durch ein offen klemmendes Ventil im deaktivierten Kanal ausgeschlossen ist.

Aus dem detaillierteren Vergleich zwischen Überlagerungslenkungen und Steer-by-Wire Systemen wird deutlich, dass der Zusatzaufwand für ein fehlertolerantes Steer-by-Wire System primär im Bereich der Elektrik und Elektronik liegt, während für die mechanischen und hydraulischen Komponenten die Vor- und Nachteile beider System-Architekturen vergleichsweise ausge-

glichen sind. Der Zusatzaufwand eines Steer-by-Wire Systems gegenüber fehlertoleranten Überlagerungslenkungen kann daher bei einem geeigneten Systemdesign reduziert, jedoch nie vollständig eliminiert werden. Daher wird es zukünftig stets Anwendungsbereiche und Einsatzgebiete für beide Systemarchitekturen geben.

7 Zusammenfassung und Ausblick

Das Ziel dieser Arbeit ist der Entwurf eines fehlertoleranten Lenkventils für Steer-by-Wire Anwendungen bei Traktoren. Dabei besteht die Herausforderung darin, einen Kompromiss zwischen der Systemkomplexität und damit auch der Fehleranfälligkeit, sowie der notwendigen Redundanz zu finden, um eine ausreichende Sicherheit darstellen zu können. Die Lösung dieses Kompromisses stellt ein Lenksystem dar, das trotz Erfüllung aller Sicherheitsanforderungen eine möglichst geringe Komplexität aufweist.

In einem ersten Schritt werden bestehende Lösungen aus dem Stand der Technik klassifiziert und beschrieben sowie die Anforderungen ermittelt, die an Lenksysteme im Allgemeinen und Steer-by-Wire Systeme im Speziellen gestellt werden. Im nächsten Schritt wird ein Konzept für ein fehlertolerantes Steer-by-Wire System vorgeschlagen, das aus einem Lenkventil mit unabhängigen Steuerkanten besteht. Der wesentliche Unterschied gegenüber dem Stand der Technik besteht darin, dass in diesem Konzept Ventilfehler durch die gewählte Ventilarchitektur inhärent kompensiert werden können (passive Fehlertoleranz) und damit eine zeitkritische Rekonfiguration im Fehlerfall nicht notwendig ist. Dieses Lenkventil wird auf Konzeptebene sicherheitstechnisch bewertet und experimentell untersucht.

Aus den experimentellen und simulativen Untersuchungen ergibt sich, dass durch das Ventilkonzept mit unabhängigen Steuerkanten auch bei vollständiger Öffnung eines beliebigen Ventils im Fehlerfall die Lenkbarkeit des Fahrzeugs durch einen passiv fehlertoleranten Regler ohne Rekonfiguration gewährleistet ist. Durch eine analytische Betrachtung wird ermittelt, dass mit steigender, am Lenkzylinder wirkender Lenkkraft die Schwere der Fehlerauswirkung ansteigt, so dass die Lenkkraft bei der fehlertoleranten Auslegung des Lenkventils berücksichtigt werden muss. Sicherheitstechnisch vorteilhaft ist dabei jedoch die Tatsache, dass die Lenkkräfte dann am höchsten

sind, wenn das Gefahrenpotential des Fahrzeugs am niedrigsten ist, wie beispielsweise im Stillstand der Maschine. Abhängig von der Art des Fehlers und der Höhe der Lenkkräfte verschlechtert sich die Regelgüte der Lenkwinkelregelung gegenüber dem fehlerfreien nominalen Zustand. Mit Hilfe eines validierten Modells der Fahrdynamik des betrachteten Versuchstraktors wird der Einfluss der reduzierten Regelgüte auf das Fahrverhalten und die Fahrtrajektorie abgeschätzt. Hierbei zeigt sich, dass dieser Einfluss in den relevanten Fahrmanövern gering ist und nur zu wenig Kompensationsaufwand für den Fahrer führt, dessen Ausmaß sicherheitstechnisch unbedenklich ist. Zur Fehlererkennung und anschließenden Fahrerwarnung wird ein aktiver Selbsttest und eine modellbasierte Fehlererkennungsmethode mittels einer Paritätsgleichung entworfen. Beide Methoden verwenden zur Fehlererkennung ausschließlich Sensorsignale, wie die Lenkzylinderposition oder den Versorgungsdruck, die bereits von anderen Teilsystemen des Lenksystems zur Regelung der Lenkzylinderposition oder zur Überwachung der Druckversorgung benötigt werden.

Da Ventilfehler inhärent ohne Rekonfiguration kompensiert werden können, sind bei dem vorgeschlagenen Ventilkonzept Absperrventile, die bei anderen Steer-by-Wire Konzepten zur Abschaltung eines als defekt identifizierten Teilsystems verwendet werden, nicht erforderlich. Für die Gewährleistung der Fehlertoleranz ist daher auch keine direkte und zeitkritische Fehlererkennung nötig, so dass die oben genannten Methoden zur Fehlererkennung zum Einsatz kommen können und Positionssensoren an jedem einzelnen Ventil überflüssig sind. Durch beide Maßnahmen wird sowohl der gerätetechnische Aufwand als auch die Komplexität der sicherheitskritischen und rechenzeitkritischen Teile der Steuergeräte-Software reduziert. Im Gegensatz zu zweikanaligen Lenkventilen mit Abschaltventilen und aktiver Fehlertoleranz muss jedoch in Kauf genommen werden, dass bei einem fehlerhaft geöffneten Ventil die Lenkperformance abhängig von den am Lenkzylinder anliegenden Kräften beeinträchtigt ist. Bei der Auswahl der 2/2-Wegeventile

muss neben der Erreichbarkeit der erforderlichen Regelgüte vor allem auf das Ventilverhalten bei hohen Druckdifferenzen geachtet werden, da dieses die Fehlertoleranz entscheidend beeinflusst. Für eine robuste und zuverlässige Fehlererkennung werden zudem Anforderungen an die Öffnungskennlinie des Ventils gestellt.

In einem nächsten Schritt muss das entworfene System in ein Versuchsfahrzeug integriert und in einer Probandenstudie untersucht werden. Dabei muss neben dem finalen Nachweis der Fehlertoleranz auch eine Bewertung des Lenkgefühls in Zusammenspiel mit einem Handkraftaktor erfolgen, da dieser Aspekt für die Kundenakzeptanz essentiell ist. Nach der Auswahl beziehungsweise Entwicklung der notwendigen Hardware muss eine qualitative und quantitative Sicherheitsbetrachtung für das Gesamtsystem durchgeführt und dokumentiert werden, um den Anforderungen bezüglich der funktionalen Sicherheit gerecht zu werden.

Die vorliegende Arbeit zeigt, dass der Zusatzaufwand, der mit der Realisierung von Steer-by-Wire Systemen verbunden ist, vor allem im Bereich der Hydraulik gegenüber dem Stand der Technik reduziert werden kann. Marktfähige fehlertolerante Steer-by-Wire Systeme, die durch den Verzicht auf eine hydrostatische Lenkeinheit in der Kabine ein Maximum an Flexibilität für die modulare und ergonomische Maschinen- sowie Kabinengestaltung bieten und die Realisierung umfangreicher Lenk-, Komfort- und auch Sicherheitsfunktionen ermöglichen, rücken damit in greifbare Nähe.

A Anhang

A.1 Risikograph der ISO Norm 25119

Das Vorgehen zur Risikobewertung für die analysierten Gefahren entsprechend der ISO-Norm 25119 [42] ist grafisch in Abbildung A.1 dargestellt. Der beschriebene Ablauf muss für jede Kombination aus *»Gefahr«* und *»Szenario«* wiederholt werden. Im ersten Schritt werden die drei Kriterien *»Schwere der Verletzung«*, *»Exposition in Szenario«* und *»Kontrollierbarkeit der Situation«* entsprechend der Tabelle A.1 bewertet. Die einzelnen Bewertungsstufen unterscheiden sich jeweils um etwa eine Größenordnung. Sind für den betrachteten Fall keine signifikanten Verletzungen zu erwarten oder ist die Situation einfach kontrollierbar, so erfolgt keine AgPL-Einstufung. In diesem Fall sind übliche qualitätssichernde Maßnahmen (QM) zur Risikoreduktion ausreichend. In allen anderen Fällen erfolgt eine AgPL-Einstufung in die Stufen *»e«* bis *»a«* anhand der Summe der Einzelbewertungen. Dabei ist AgPL *»e«* die sicherheitskritischste Einstufung. Zwischen den unterschiedlichen Einstufungen liegt ebenfalls eine Größenordnung.

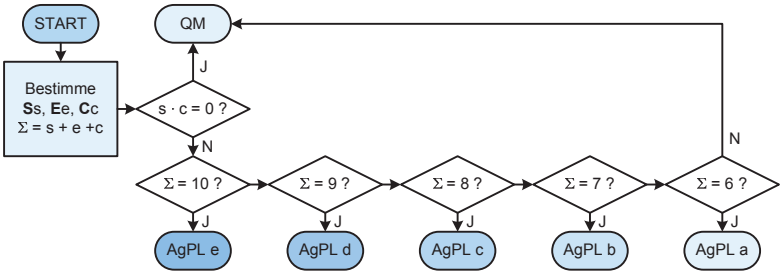


Abb. A.1: Vorgehen zur Bestimmung des notwendigen AgPL [42]

S: Severity of harm
S0: No significant injuries, requires only first aid
S1: Light and moderate injuries, requires medical attention, total recovery
S2: Severe and life-threatening injuries (survival probable), permanent partial loss in work capacity
S3: Life-threatening injuries (survival uncertain), severe disability

E: Exposure in the situation observed	$\frac{\text{exposure time}}{\text{average operating time}}$
E0: Improbable (theoretically possible; once during lifetime)	< 0,01 %
E1: Rare events (less than once per year)	0,01 % - 0,1 %
E2: Sometimes (more than once per year)	0,1 % - 1 %
E3: Often (more than once per month)	1 % - 10 %
E4: Frequently (almost every operation)	> 10 %

C: Controllability / Avoidance of harm
C0: Easily controllable: The operator or bystander controls the situation and the harm is avoided
C1: Simply controllable: More than 99% of people control the situation. In more than 99% of the occurrences the situation does not result in harm
C2: Mostly controllable: More than 90% of people control the situation. In more than 90% of the occurrences the situation does not result in harm
C3: None: The average operator or bystander cannot generally avoid the harm

Tab. A.1: Kriterien zur Risikobewertung [42]

A.2 Weiterführende Informationen zu Kapitel 5

A.2.1 Beschreibung des Lastmodells

Zur Generierung der Soll-Werte für den Lastregler am *Hardware in the Loop* Prüfstand ist ein Modell notwendig, das die am realen Fahrzeug auftretenden Lastkräfte am Lenkzylinder ausreichend genau abbildet. Die am Lenkzylinder wirkenden Kräfte resultieren aus den Kräften zwischen Reifen und Fahrbahn und bestehen daher im wesentlichen aus Reibungs- und Dämpfungsanteilen sowie Anteilen, die eine Rückstellung der Räder bewirken. Damit sind die Kräfte abhängig von der Achs- beziehungsweise Lenkgeometrie, dem Reibungskoeffizienten zwischen Reifen und Fahrbahn μ, der Vorderachslast (Normalkraft) sowie der Position beziehungsweise Geschwindigkeit des Lenkzylinders x beziehungsweise $\dot{x}$. Ein weiterer wesentlicher Einflussfaktor ist die Geschwindigkeit des Fahrzeugs v. Im Stand treten die höchsten Lenkkräfte auf, weil der Reifen nicht über die Fahrbahn abrollen kann, sondern darauf gleitet.

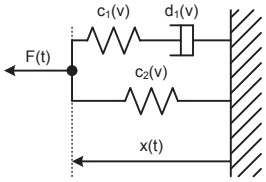


Abb. A.2: Phänomenologisches Biot-Modell mit fahrgeschwindigkeitsabhängigen Koeffizienten zur Beschreibung der Lastkräfte am Lenkzylinder

Messungen an einem Versuchsfahrzeug haben gezeigt, dass bei einem wiederkehrenden Lenken von Anschlag zu Anschlag eine mechanische Hysterese auftritt. Zu deren Beschreibung kann ein phänomenologisches Biot-Modell verwendet werden [67], das aus einer Parallelschaltung eines oder mehrerer Maxwell-Modelle und einer Feder besteht und ein visko-elastisches Verhalten

abbildet, siehe Abbildung A.2. Dabei wird durch die Feder das Rückstellverhalten der Lenkung abgebildet, während durch das Maxwell-Modell, das aus der Reihenschaltung einer Feder und eines Dämpfers besteht, sämtliche Reibungs- und Dämpfungsanteile mit einem zeitabhängigen Verhalten approximiert werden. Die in der Abbildung dargestellten Modellparameter wurden für verschiedene Fahrzeuggeschwindigkeiten v bestimmt, um eine gute Übereinstimmung zwischen dem Verhalten des Modells und der Messungen zu erhalten, siehe Abbildung A.3. Für die betrachtete Anwendung des Lastmodells ist die Modellgüte ausreichend. Der aus den Messungen ersichtliche starke Druckanstieg bei kleinen und großen Lenkzylinderpositionen resultiert aus dem mechanischen Anschlag des Lenksystems im realen Traktor, da bei Erreichen des Anschlags kein Volumenstrom mehr fließt und daher der Kammer- und Pumpendruck stark ansteigt. Dieser Druckanstieg muss von dem Lastmodell nicht abgebildet werden, da im Prüfstand ein realer Lenkzylinder mit Endanschlägen verwendet wird.

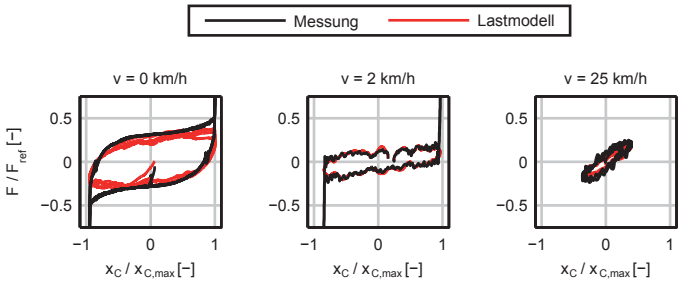


Abb. A.3: Vergleich zwischen dem entwickelten Lastmodell und Fahrzeugmessungen für unterschiedliche Fahrzeuggeschwindigkeiten v

A.2.2 Formeln zur Berechnung der Fehlertoleranz im statischen Fall II

Die Systemgrößen ergeben sich für den Fall II aus folgendem Gleichungssystem:

$$\left\| \begin{array}{c} p_L = p_R + F/A_C \\ p_P = p_L + \Delta p \\ (Q_C =) Q_{PL} = Q_{RT} - Q_{PR} \end{array} \right\| \tag{A.1}$$

$$\left\| \begin{array}{c} p_L = p_R + F/A_C \\ p_P = p_L + \Delta p \\ 2 \cdot A_P \cdot \sqrt{p_P - p_L} = 2 \cdot A_T \cdot \sqrt{p_R - p_T} - A_P \cdot \sqrt{p_P - p_R} \end{array} \right\| \tag{A.2}$$

Die Lösung dieses Gleichungssystems ist gültig, bis die Druckbegrenzung in der Pumpe p_{max} erreicht ist. Bei höheren Lenkkräften ist das folgende Gleichungssystem anzuwenden:

$$\left\| \begin{array}{c} p_L = p_R + F/A_C \\ p_P = p_{max} \\ (Q_C =) Q_{PL} = Q_{RT} - Q_{PR} \end{array} \right\| \tag{A.3}$$

A.2.3 Fehlertoleranz im statischen Fall

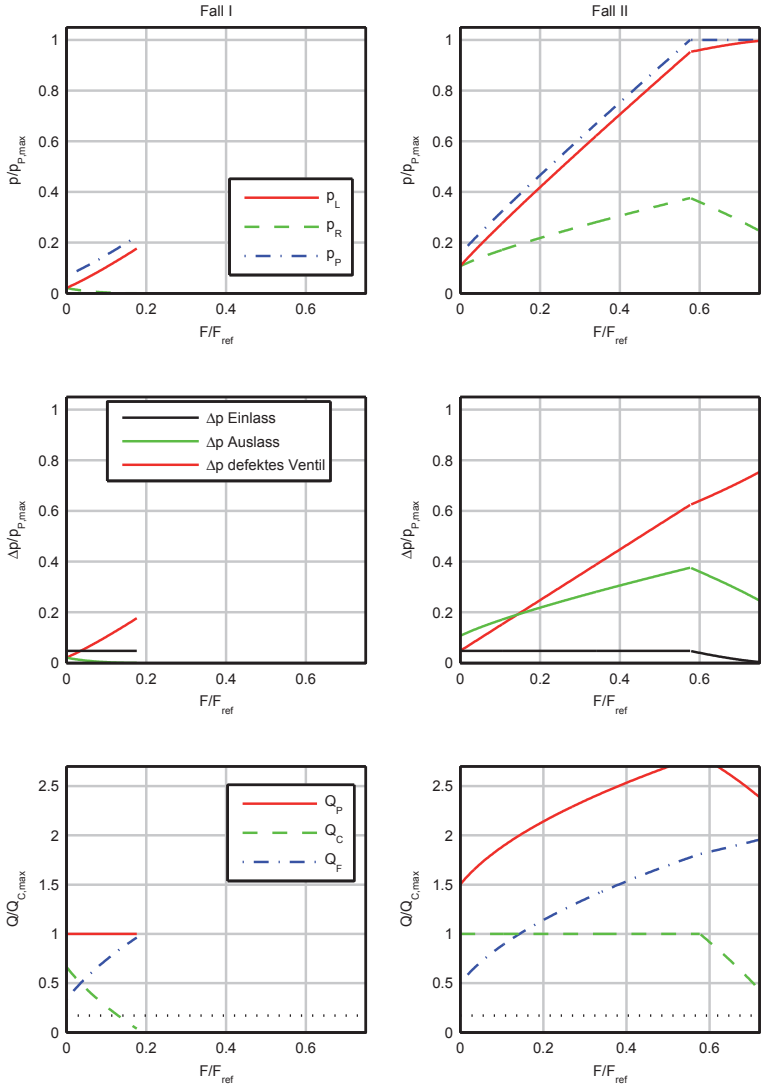


Abb. A.4: Systemgrößen bei Fehlertyp B im statischen Fall für $A_P/A_T = 1{,}0$

A.3 Weiterführende Informationen zu Kapitel 6

A.3.1 Lenkwinkelregelung

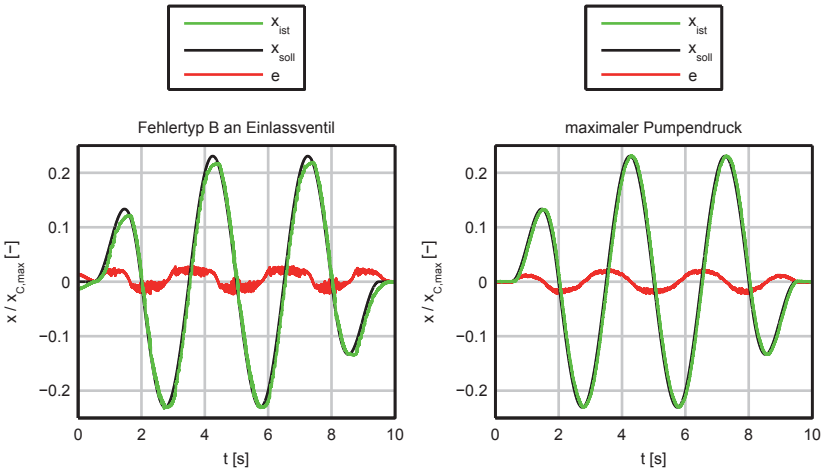


Abb. A.5: Messergebnisse für Manöver 2 mit Schaltventilen in verschiedenen Fehlerfällen

A.3.2 Fehlererkennung

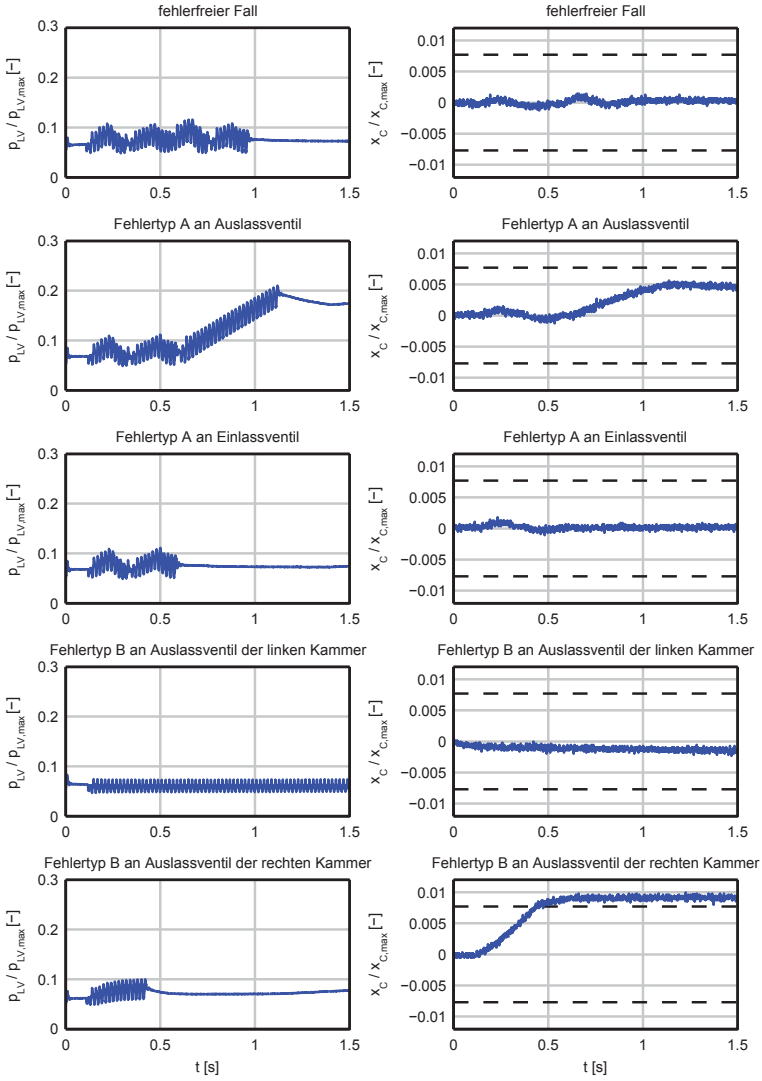


Abb. A.6: Messergebnisse des Selbsttests mit Schaltventilen (Fehlertyp A und B)

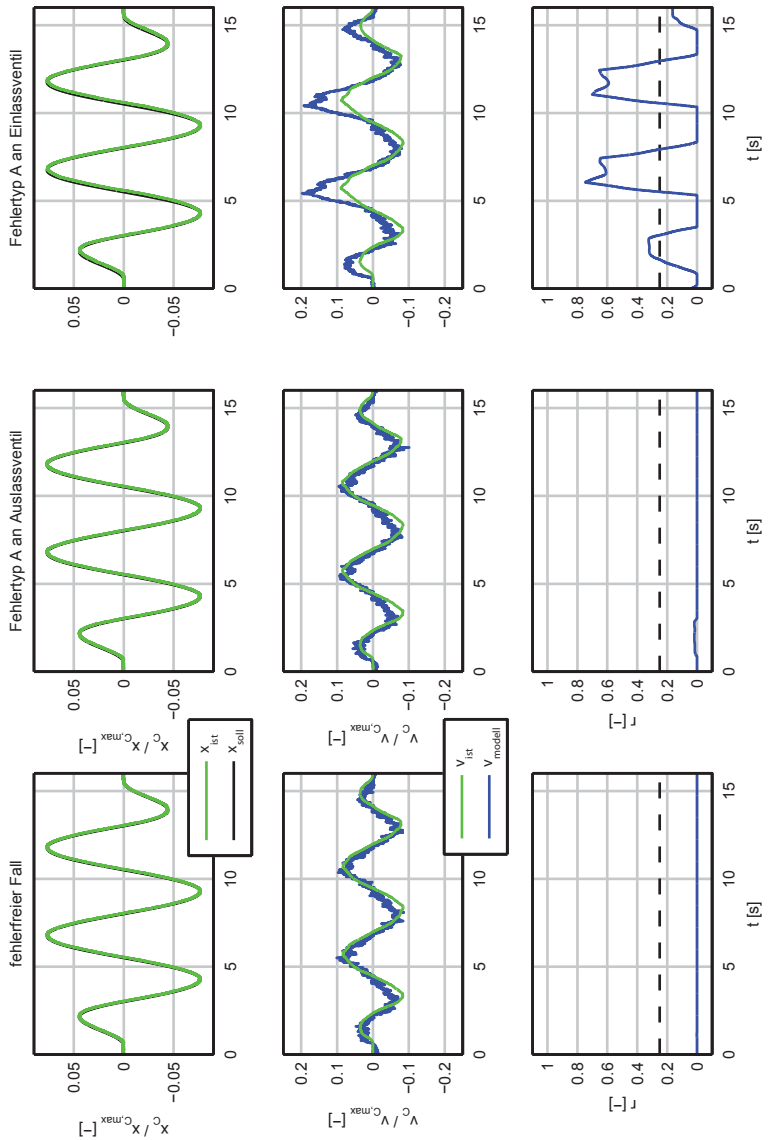


Abb. A.7: Messergebnisse der modellbasierten Fehlererkennung mit Schaltventilen für Fehler des Typs A

Literaturverzeichnis

[1] ABELE, M.: *Modellierung und Bewertung hochzuverlässiger Energiebordnetz-Architekturen für sicherheitsrelevante Verbraucher in Kraftfahrzeugen*. Dissertation, Universität Kassel, 2008.

[2] ALANEN, J.; HAATAJA, K.; LAURILA O.; PELTOLA J. UND AHO I.: *Diagnostics of mobile work machines*. VTT Research Notes 2343, VTT Technical Research Centre of Finland, 2006.

[3] AUGSBURG, K. UND SCHADY, H.: *Alternative Lenksysteme*. Interne Studie, Technische Universität Dresden, 1997.

[4] BARG, J.: *Safety in Digital-Hydraulics (EN ISO 13849)*. In: *The Fourth Workshop on Digital Fluid Power*, Linz, 2011.

[5] BARTHENHEIER, T.: *Potenzial einer fahrertyp- und fahrsituationsabhängigen Lenkradmomentgestaltung*. Dissertation, Technische Universität Darmstadt, 2004.

[6] BECK, M. UND ISERMANN, R.: *Fehlertolerante Systeme - Prinzipien und Ausführungsbeispiele*. Abschlussbericht, DFAM (Deutsche Forschungsgesellschaft für Automatisierung und Mikroelektronik), 2007.

[7] BLANKE, M.: *Diagnosis and fault-tolerant control*. Springer, Berlin, 2006.

[8] BOOG, M.: *Steigerung der Verfügbarkeit mobiler Arbeitsmaschinen durch Betriebslasterfassung und Fehleridentifikation an hydrostatischen Verdrängereinheiten*. Dissertation, Karlsruher Institut für Technologie, 2011.

[9] BOSCH REXROTH AG: *LAGC - Load-Sensing-Lenkaggregat*. http://www.boschrexroth.com/modules/BRMV2PDFDownload.dll?db=brmv2&lvid=1163115&mvid=6803&clid=1&sid=241F9DFDD0292BF9F0A961620C6D2D7B&sch=M. Poster, Stand: 01.04.2012.

[10] BOSCH REXROTH AG: *10 Schritte zum Performance Level: Handbuch zur Umsetzung der funktionalen Sicherheit nach ISO 13849*. Bosch Rexroth AG, Würzburg, 2011.

[11] BRAESS, H.-H. UND SEIFFERT, U.: *Handbuch Kraftfahrzeugtechnik*. Vieweg, Wiesbaden, 2007.

[12] BURGMANN, M.: *Nr. 260: Richtlinie für die Prüfung von Lenkanlagen von Kraftfahrzeugen und ihren Anhängern*, 01. Dezember 2003. Bundesministerium für Verkehr, Bau- und Wohnungswesen.

[13] CLAUSEN, M.: *Fault-Tolerant Electro Hydraulic Steering of Off-Highway Machines*. Dissertation, Aalborg University, 2006.

[14] CROW, S.: *Steer-by-Wire: A technology for tomorrow, or today?* . In: *51st National Conference on Fluid Power*, Milwaukee, 2008.

[15] DEUTSCHES INSTITUT FÜR NORMUNG: *DIN ISO 7401: Testverfahren für Querdynamisches Übertragungsverhalten*, 1989.

[16] DEUTSCHES INSTITUT FÜR NORMUNG: *DIN EN 61508: Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme*, 2002.

[17] DEUTSCHES INSTITUT FÜR NORMUNG: *DIN ISO 1219-1: Fluidtechnik - Graphische Symbole und Schaltpläne - Teil 1: Graphische Symbole für konventionelle und datentechnische Anwendungen*, 2007.

[18] DEUTSCHES INSTITUT FÜR NORMUNG: *DIN EN ISO 13849 - Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen*, 2008.

[19] DILGER, E.; FÜHRER, T.; MÜLLER B.; POLEDNA S. UND THURNER T.: *X-By-Wire - Design of Distributed Fault Tolerent and Safety Critical Applications in Modern Vehicles*. Technischer Bericht, 1997.

[20] DREESEN, M.: *Zulassungsvorschriften für Lenkanlagen mit elektronischen Übertragungseinrichtungen*. In: *MobilTron: Elektronisch-hydraulische Lenksysteme für mobile Arbeitsmaschinen*, Mannheim, 2005.

[21] DUDZINSKI, P.: *Lenksysteme für Nutzfahrzeuge*. Springer, Berlin, 2005.

[22] ECONOMIC COMMISSION FOR EUROPE: *ECE R-79 Rev. 2: Uniform Provisions concerning the Approval of Vehicles with regard to Steering Equipment*, 2005.

[23] ERIKSSON, B.: *Control Strategy for Energy Efficient Fluid Power Actuators - Utilizing Individual Metering*. Dissertation, Linköping University, 2007.

[24] FACK, C. UND SCHEMPP, R.: *Ventilanordnung mit Ventil und einem Sensor*, 2010. Offenlegungsschrift der Patentanmeldung DE 102008059712 A1.

[25] FERHADBEGOVIC, B.: *Entwicklung und Applikation eines instationären Reifenmodells zur Fahrdynamiksimulation von Ackerschleppern*. Dissertation, Universität Stuttgart, 2008.

[26] FEUCHT, P.: *SIL Approved Sensors for Mobile Machines and Innovative Technology*. In: *7th International Fluid Power Conference*, Aachen, 2010.

[27] FINDEISEN, D.: *Ölhydraulik*. Springer, Berlin, 2006.

[28] FISCHER, D.; BÖRNER, M.; SCHMITT J. UND ISERMANN R.: *Fault detection for lateral and vertical vehicle dynamics*. In: *Control Engineering Practice 15*, 2007.

[29] FREITAG, R.; MOSER, M.; HARTL M.; KOEPERNIK J. UND ECKSTEIN L.: *Anforderungen an das Sicherheitskonzept von Lenksystemen mit Steer-by-Wire Funktionalität*. In: *VDI Berichte Nr. 1646*, 2001.

[30] FUHR, F.; SCHÜLLKAMP, TH.; NEUKUM A. UND SCHUMACHER M.: *Integration von Fahrsimulatoren in den Entwicklungsprozess von aktiven Fahrwerkssystemen*. 2003.

[31] GERTLER, J: *Fault detection and diagnosis in engineering systems*. Dekker, New York, 1998.

[32] GORGS, K.-J.; GRIGULEWITSCH, W. UND KLEINBREUER W.: *Elektrohydraulische Stetig-Wegeventile mit Sicherheitsverantwortung*. O+P, 45(11-12):S. 745 ff., 2001.

[33] HAAS, W.: *Vorrichtung zur Spannungsversorgung für sicherheitsrelevante Verbraucher*, 2006. Offenlegungsschrift der Patentanmeldung WO 2006/082124 A1.

[34] HARTMANN, K.; JÜNEMANN, D.; KEMPER S.; ROBERT M.; ROOS L.; SCHATTENBERG J. UND UNTCH J.: *Trends bei Landmaschinen und Traktoren - Beobachtungen anlässlich der Agritechnica 2011*. O+P, 1-2:S. 33 ff., 2012.

[35] HAUKE, M.; SCHAEFER, M. UND APFELT R.: *Funktionale Sicherheit von Maschinensteuerungen: Anwendung der DIN EN ISO 13849*. Deutsche Gesetzliche Unfallversicherung, Sankt Augustin, 2008. BGIA-Report.

[36] HEISSING, B. UND ERSOY, M.: *Fahrwerkhandbuch - Grundlagen, Fahrdynamik, Komponenten, Systeme, Mechatronik, Perspektiven*. Vieweg + Teubner, Wiesbaden, 2008.

[37] HESSE, H.: *Traktorhydraulik: Komponenten und Systeme von landwirtschaftlichen Traktoren*. expert-Verlag, Renningen, 2004.

[38] HUANG, B.: *Regelkonzepte zur Fahrzeugführung unter Einbeziehung der Bedienelementeigenschaften*. Dissertation, Technische Universität München, 2004.

[39] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION: *ISO/TR 14121-2: Safety of machinery - Risk assessment*, 2007.

[40] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION: *ISO 10998: Agricultural tractors - Requirements for steering - Second Edition 2008-06-01*, 2008.

[41] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION: *ISO 10975: Tractors and machinery for agriculture - Auto-guidance systems for operator-controlled tractors and self-propelled machines - Safety requirements*, 2009.

[42] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION: *ISO 25119: Tractors and machinery for agriculture and forestry - Safety-related parts of control systems*, 2010.

[43] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION: *ISO 26262: Road vehicles - Functional Safety*, 2011.

[44] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION: *ISO 4413: Fluidtechnik - Allgemeine Regeln und sicherheitstechnische Anforderungen an Hydraulikanlagen und deren Bauteile*, 2011.

[45] ISERMANN, R.: *Fault diagnosis systems - An introduction from fault detection to fault tolerance*. Springer, Berlin, 2006.

[46] JCB: *8000 Series Fastrac*. http://www.fastrac8000.com/lib/downloads/UK-8000-Product-Brochure.pdf. Produktbroschüre, Stand: Juni 2011.

[47] JÁNOSI, L. UND KIS, J.: *Steer-by-Wire technology - Steering wheel as a new, intelligent Human Machine Interface*. In: *VDI Berichte Nr. 2111: Land Technik Tagung*, 2010.

[48] JOHANNSEN, G.: *Mensch-Maschine-Systeme*. Springer, Berlin, 1993.

[49] JOHN DEERE: *Serie 7R - Traktoren mit 230 bis 310 PS (97/68 EC) mit Intelligentem Power Management*. http://www.deere.de/de_DE/docs/product/equipment/tractors/7r_series/brochure/7r_series.html. Produktbroschüre, Stand: Mai 2011.

[50] JUNGHEINRICH: *EFG D30: Four wheel electric forklift with rotating cab (3000 kg)*. http://www.jungheinrich.gr/fileadmin/public/gr/files/EFG_D30_GRnew.pdf. Produktbroschüre, Stand: Mai 2007.

[51] KAZEMI-MOGHADDAM, A.: *Fehlerfrühidentifikation und -diagnose eines elektrohydraulischen Linearantriebssystems*. Dissertation, Technische Universtität Darmstadt, 1999.

[52] KNECHTGES, H.: *Entwicklungstendenzen bei Traktoren und Transportfahrzeugen*. Pressemitteilungen der DLG anlässlich der AGRITECHNICA 2009, Deutsche Landwirtschafts-Gesellschaft, 16.09.2009.

[53] KNECHTGES, H. UND RENIUS, K.: *Traktoren 2010/2011*. ATZoffhighway, November 2011.

[54] KRAUTSTRUNK, A.: *Fehlertolerantes Aktorkonzept für sicherheitsrelevante Anwendungen*. Dissertation, Technische Universität Darmstadt, 2005.

[55] LeRoy, D.F.: *Steer-by-Wire challenges hydraulics - Advanced tactile-feedback devices give electric drives the control and feel of hydraulic steering*. Machine Design, 78(15):S. 52–55, 2006.

[56] Lunze, J.: *Regelungstechnik 1 - Systemtheoretische Grundlagen, Analyse und Entwurf einschleifiger Regelungen*. Springer, Berlin, 2007.

[57] Maddock, J. B.: *Cylinder fault detection using rail pressure signal*, 1996. Patent US 005492099 A.

[58] Martinus, M.: *Funktionale Sicherheit von mechatronischen Systemen bei mobilen Arbeitsmaschinen*. Dissertation, Technische Universität München, 2004.

[59] Meyer, C.; Bosse, T.; Weiler D. und Murrenhoff H.: *Multi-variable Control Concepts for a differential cylinder with an independent metering valve configuration*. In: *8th International Fluid Power Conference*, Dresden, 2012.

[60] Müller, B.: *Analyse und Konzeption eines Antiblockiersystems für Traktoren*. Dissertation, Technische Universität Braunschweig, 2013.

[61] Münchhof, M.: *Model-based fault detection for a hydraulic servo axis*. Dissertation, Technische Universität Darmstadt, 2006.

[62] Murrenhoff, H. und Sgro, S.: *Servohydraulik - geregelte hydraulische Antriebe: Umdruck zur Vorlesung*. Inst. für Fluidtechnische Antriebe und Steuerungen, Aachen, 2012.

[63] Neukum, A. und Krüger, H.-P.: *Fahrerreaktion bei Lenksystemstörungen - Untersuchungsmethodik und Bewertungskriterien* . In: *VDI Berichte Nr. 1791*, Seiten S. 297–318, 2003.

[64] Neukum, A.; Paulig, J.; Frömmig-L. und Henze R.: *Untersuchung zur Wahrnehmung von Lenkmomenten bei Pkw*.

Studie der Forschungsvereinigung Automobiltechnik e.V. (FAT), Interdisziplinäres Zentrum für Verkehrswissenschaften (IZVW), 2009.

[65] NEUMANN, U.; BRUMMUND, S. UND SCHMITZ D.: *Elektrohydraulische Lenkung*, 2011. Offenlegungsschrift zu Patentanmeldung DE 102010020722 A1.

[66] NOACK, S.: *Hydraulik in mobilen Arbeitsmaschinen*. OMEGON Fachliteratur, Ditzingen, 2001.

[67] OTTL, D.: *Modellierung der mechanischen Hysteresis*. Naturwissenschaften, 80(9):S. 391–396, 1993.

[68] PARK, Y. UND JUNG, I.: *Semi-Active Steering Wheel for Steer-by-Wire System*. In: *Automotive and Transportation Technology Congress and Exposition*, Barcelona, 2001.

[69] PARK, S.; HWANG, S.; OH Y. UND LEE U.: *Development of the independent-type steer by wire system*. In: *Steering & Suspension Technology Symposium*, Detroit, 2007.

[70] PARK, Y. und I. JUNG: *Steer-by-Wire System using semi-active Actuator*, 2003. Patent US 6612392 B2.

[71] PFEFFER, P. UND HARRER, M.: *Lenkungshandbuch: Lenksysteme, Lenkgefühl, Fahrdynamik von Kraftfahrzeugen*. Vieweg + Teubner, Wiesbaden, 2011.

[72] PROFI: *Steer-by-Wire: Lenken mit mehr Freiheit und Komfort*. profi, 3:S. 92–93, 2008.

[73] PUDSZUHN, R.: *Elektrohydraulische Lenksysteme*. In: *Elektronisch-hydraulische Systeme*, Seiten S. 159–180, Renningen, 2008. expert Verlag.

[74] RENIUS, K. UND KNECHTGES, H.: *Traktoren 2007 bis 2009 - Trend und neue Entwicklungen*. ATZoffhighway, Seiten S. 6–19, 2009.

[75] RENIUS, K.: *Trends in Tractor Design with Particular Reference to Europe*. Journal of Agricultural Engineering Research, 57(1):S. 3–22, 1994.

[76] RICHTER, S.: *Sicherheit geregelter Antriebe der Fluidtechnik - Weiterentwicklung von Sicherheitskonzepten*. Abschlussbericht des VDMA Forschungsfonds Fluidtechnik Projekts, Technische Universität Dresden, 2011.

[77] RICHTER, S. UND HELDUSER, S.: *Integrated Safety in Closed-Loop Controlled Electro-Hydraulic Drives*. In: *7th International Fluid Power Conference*, Aachen, 2010.

[78] RICHTER, S.; HELDUSER, S. UND LOHMAIER O.: *EN ISO 13849 - Neue Möglichkeiten für sichere fluidtechnische Antriebe - Erläuterungen zum Gestaltungsprozess von Sicherheitsfunktionen an einem Beispiel*. O+P Konstruktionsjahrbuch, Seite S. 52 ff., 2009/2010.

[79] SAUER DANFOSS: *OSPE Electrohydraulic Steering Units - Rapid Response - Complete Control*. http://www.sauer-danfoss.com/stellent/groups/publications/documents/product_literature/11034787.pdf#page=1. Produktbroschüre, Stand: Oktober 2009.

[80] SCHEPERS, I.; SCHMITZ, D.; WEILER D.; COCHOY C. UND NEUMANN U.: *A novel model for optimized development and application of switching valves in closed loop control*. International Journal of Fluid Power, 12(3), 2011.

[81] SCHICK, T. UND KEARNEY, J.: *Steer-by-Wire for Large Row Crop Tractors - John Deere 8R Series Tractors*. In: *68. Internationale Tagung LAND.TECHNIK*, 2010.

[82] SCHICK, T.; KEARNEY, J.; WILLET D.; SOLDWISCH J. UND BLOOMQUIST D.: *Power Supply for by-wire System*, 2010. Offenlegungsschrift zu Patentanmeldung US 2010021191 A1.

[83] SCHICK, T.; WALLESTAD, S.; HERBST B.; BECKER M. UND MÜLLER B.: *Hydraulic Circuit for a Steer-by-Wire Steering System*, 2008. Offenlegungsschrift zu Patentanmeldung US 2008/0087014 A1.

[84] SCHMITZ, D. UND GEIMER, M.: *Fault-tolerant steer-by-wire valve for agricultural tractors based on independent metering with on/off valves*. In: *Bath/ASME Symposium on Fluid Power & Motion Control*, Bath, 2012.

[85] SCHRÖDER, D.: *Intelligente Verfahren: Identifikation und Regelung nichtlinearer Systeme*. Springer, Berlin, 2010.

[86] SCHUSTER, U.: *Untersuchung des Alterungsprozesses von hydraulischen Ventilen*. BIA-Report 6/2004, August 2004.

[87] SIIVONEN, L.; LINJAMA, M.; HUOVA M. UND VILENIUS M.: *Fault Detection and Diagnosis of Digital Hydraulic Valve System*. In: *The Tenth Scandinavian International Conference on Fluid Power SICFP*, Tampere, 2007.

[88] SIIVONEN, L.; LINJAMA, M.; HUOVA M. UND VILENIUS M.: *Pressure Based Fault Detection and Diagnosis of a Digital Valve System*. In: *Power Transmission and Motion Control*, Bath, 2007.

[89] SIIVONEN, L.; LINJAMA, M.; HUOVA M. UND VILENIUS M.: *Jammed on/off Valve Fault Compensation with distributed Digital Valve System*. International Journal of Fluid Power, 10(2), 2009.

[90] STOLL, H. UND REIMPELL, J.: *Fahrwerktechnik: Lenkanlagen und Hilfskraftlenkungen*. Vogel, Würzburg, 1992.

[91] THEIS, I.: *Das Steer-by-wire-System im Kraftfahrzeug: Analyse der menschlichen Zuverlässigkeit*. Dissertation, Technische Universität München, 2002.

[92] TRACHTE, A.; ALBRECHT, A.; KEUPER G. UND STACHNIK P.: *Mobile hydraulic valves in the HIL-simulation at negative pressure*. In: *The Twelth Scandinavian International Conference on Fluid Power*, Tampere, 2011.

[93] VDI/VDE: *VDI/VDE 3542: Sicherheitstechnische Begriffe für Automatisierungssysteme*, 2000.

[94] WECKER, T. UND GNAHM, K.: *Elektronisch-hydraulische Lenksysteme*. O+P, 41(4), 1997.

[95] WENNMACHER, G.: *Untersuchung und Anwendung schnellschaltender elektrohydraulischer Ventile für den Einsatz in Kraftfahrzeugen*. Dissertation, Rheinisch-Westfaelische Technische Hochschule Aachen, 1996.

[96] WIEDERMANN, A.: *Auslegung von Lenksystemen in modernen Traktoren*. In: *70. Internationale Tagung LAND.TECHNIK*, 2012.

[97] WIESEL, U.: *Hybrides Lenksystem zur Kraftstoffeinsparung im schweren Nutzfahrzeug : technische und methodische Ansätze*. Dissertation, Karlsruher Institut für Technologie, 2010.

[98] WINKES, G. UND LUEUES, H.: *Lagemessung eines in einer Magnetspule betätigten Magnetankers*, 2000. Offenlegungsschrift zu Patentanmeldung DE 19910497 A1.

[99] WINNER, H. UND HEUSS, O.: *X-by-Wire Betätigungselemente - Überblick und Ausblick*. In: *Darmstädter Kolloquium Mensch & Fahrzeug*, Darmstadt, 2005.

[100] WROBLEWSKI, D.: *Konzept einer fehlertoleranten, elektrohydraulischen steer-by-wire Lenkung für langsam fahrende Fahrzeuge*. Dissertation, Universität Rostock, 2011.

[101] X-BY-WIRE TEAM: *X-By-Wire - Safety Related Fault Tolerant Systems in Vehicles*. Abschlussbericht von Brite-EuRAM III-Projekt *Safety Related Fault Tolerant Systems in Vehicles (X-By-Wire)*, 1998.

[102] ZAREMBSKI, S.: *Top gear*. IVT International Off-Highway, 2012.

[103] ZF: *Eccom 5.0: Neues stufenloses Getriebe*. Presseinformation, Stand: 09.10.2008.

[104] ZF LENKSYSTEME: *Überlagerungslenkungen für Nutzfahrzeuge - Drehmoment- und Drehwinkelüberlagerung*. Automotive, (11):S. 81–82, 11 2006 2006.

[105] ZHANG, Q.; WU, D.; REID J.F. UND BENSON E.R.: *Model recognition and validation for an off-road vehicle electrohydraulic steering controller*. In: *Mechatronics 12*, Seiten S. 845–858, 2002.

[106] ZHANG, X.; GEIMER, M.; NOACK P.O. UND EHRL M.: *Elektronische Deichsel für landwirtschaftliche Arbeitsmaschinen*. In: *VDI Berichte Nr. 2111: Land Technik Tagung*, 2010.

Karlsruher Schriftenreihe Fahrzeugsystemtechnik (ISSN 1869-6058)

Herausgeber: FAST Institut für Fahrzeugsystemtechnik

Die Bände sind unter www.ksp.kit.edu als PDF frei verfügbar oder als Druckausgabe bestellbar.

Band 1 Urs Wiesel
Hybrides Lenksystem zur Kraftstoffeinsparung im schweren Nutzfahrzeug. 2010
ISBN 978-3-86644-456-0

Band 2 Andreas Huber
Ermittlung von prozessabhängigen Lastkollektiven eines hydrostatischen Fahrantriebsstrangs am Beispiel eines Teleskopladers. 2010
ISBN 978-3-86644-564-2

Band 3 Maurice Bliesener
Optimierung der Betriebsführung mobiler Arbeitsmaschinen. Ansatz für ein Gesamtmaschinenmanagement. 2010
ISBN 978-3-86644-536-9

Band 4 Manuel Boog
Steigerung der Verfügbarkeit mobiler Arbeitsmaschinen durch Betriebslasterfassung und Fehleridentifikation an hydrostatischen Verdrängereinheiten. 2011
ISBN 978-3-86644-600-7

Band 5 Christian Kraft
Gezielte Variation und Analyse des Fahrverhaltens von Kraftfahrzeugen mittels elektrischer Linearaktuatoren im Fahrwerksbereich. 2011
ISBN 978-3-86644-607-6

Band 6 Lars Völker
Untersuchung des Kommunikationsintervalls bei der gekoppelten Simulation. 2011
ISBN 978-3-86644-611-3

Band 7 3. Fachtagung
Hybridantriebe für mobile Arbeitsmaschinen. 17. Februar 2011, Karlsruhe. 2011
ISBN 978-3-86644-599-4

Karlsruher Schriftenreihe Fahrzeugsystemtechnik (ISSN 1869-6058)

Herausgeber: FAST Institut für Fahrzeugsystemtechnik

Band 8 Vladimir Iliev
Systemansatz zur anregungsunabhängigen Charakterisierung des Schwingungskomforts eines Fahrzeugs. 2011
ISBN 978-3-86644-681-6

Band 9 Lars Lewandowitz
Markenspezifische Auswahl, Parametrierung und Gestaltung der Produktgruppe Fahrerassistenzsysteme. Ein methodisches Rahmenwerk. 2011
ISBN 978-3-86644-701-1

Band 10 Phillip Thiebes
Hybridantriebe für mobile Arbeitsmaschinen. Grundlegende Erkenntnisse und Zusammenhänge, Vorstellung einer Methodik zur Unterstützung des Entwicklungsprozesses und deren Validierung am Beispiel einer Forstmaschine. 2012
ISBN 978-3-86644-808-7

Band 11 Martin Gießler
Mechanismen der Kraftübertragung des Reifens auf Schnee und Eis. 2012
ISBN 978-3-86644-806-3

Band 12 Daniel Pies
Reifenungleichförmigkeitserregter Schwingungskomfort – Quantifizierung und Bewertung komfortrelevanter Fahrzeugschwingungen. 2012
ISBN 978-3-86644-825-4

Band 13 Daniel Weber
Untersuchung des Potenzials einer Brems-Ausweich-Assistenz. 2012
ISBN 978-3-86644-864-3

Band 14 **7. Kolloquium Mobilhydraulik. 27./28. September 2012 in Karlsruhe.** 2012
ISBN 978-3-86644-881-0

Band 15 4. Fachtagung
Hybridantriebe für mobile Arbeitsmaschinen 20. Februar 2013, Karlsruhe. 2013
ISBN 978-3-86644-970-1

Karlsruher Schriftenreihe Fahrzeugsystemtechnik (ISSN 1869-6058)

Herausgeber: FAST Institut für Fahrzeugsystemtechnik

Band 16 Hans-Joachim Unrau
Der Einfluss der Fahrbahnoberflächenkrümmung auf den Rollwiderstand, die Cornering Stiffness und die Aligning Stiffness von Pkw-Reifen. 2013
ISBN 978-3-86644-983-1

Band 17 Xi Zhang
Untersuchung und Entwicklung verschiedener Spurführungsansätze für Offroad-Fahrzeuge mit Deichselverbindung. 2013
ISBN 978-3-7315-0005-6

Band 18 Stefanie Grollius
Analyse des gekoppelten Systems Reifen-Hohlraum-Rad-Radführung im Rollzustand und Entwicklung eines Rollgeräuschmodells. 2013
ISBN 978-3-7315-0029-2

Band 19 Tobias Radke
Energieoptimale Längsführung von Kraftfahrzeugen durch Einsatz vorausschauender Fahrstrategien. 2013
ISBN 978-3-7315-0069-8

Band 20 David Gutjahr
Objektive Bewertung querdynamischer Reifeneigenschaften im Gesamtfahrzeugversuch. 2014
ISBN 978-3-7315-0153-4

Band 21 Neli Ovcharova
Methodik zur Nutzenanalyse und Optimierung sicherheitsrelevanter Fahrerassistenzsysteme. 2014
ISBN 978-3-7315-0176-3

Band 22 Marcus Geimer, Christian Pohlandt
Grundlagen mobiler Arbeitsmaschinen. 2014
ISBN 978-3-7315-0188-6

Band 23 Timo Kautzmann
Die mobile Arbeitsmaschine als komplexes System. 2014
ISBN 978-3-7315-0187-9

Karlsruher Schriftenreihe Fahrzeugsystemtechnik (ISSN 1869-6058)

Herausgeber: FAST Institut für Fahrzeugsystemtechnik

Band 24 Roman Weidemann
Analyse der mechanischen Randbedingungen zur Adaption der oszillierenden Hinterschneidtechnik an einen Mobilbagger. 2014
ISBN 978-3-7315-0193-0

Band 25 Yunfan Wei
Spurführungsregelung eines aktiv gelenkten Radpaars für Straßenbahnen. 2014
ISBN 978-3-7315-0232-6

Band 26 David Schmitz
Entwurf eines fehlertoleranten Lenkventils für Steer-by-Wire Anwendungen bei Traktoren. 2014
ISBN 978-3-7315-0264-7

Karlsruher Schriftenreihe
Fahrzeugsystemtechnik

FAST
Institut für Fahrzeugsystemtechnik

An das Lenksystem eines Traktors werden immer höhere Anforderungen gestellt, um produktivitätssteigernde Funktionen realisieren zu können.Darüber hinaus gewinnen Aspekte wie die Ergonomie oder die Fahrsicherheit eines schweren Gespanns ebenfalls an Bedeutung. Steer-by-Wire Systeme ohne mechanischen oder hydraulischen Durchgriff zwischen Lenkrad und gelenkten Rädern bieten sehr große Freiheiten für die Umsetzung dieser Anforderungen.
In der vorliegenden Arbeit wird ein hydrostatisches Steer-by-Wire Ventil mit unabhängigen Steuerkanten untersucht und bezüglich der Eignung für die Nutzung in sicherheitskritischen Anwendungen bewertet. Durch experimentelle Untersuchungen wird nachgewiesen, dass Ventilfehler inhärent kompensiert werden können und die Lenkbarkeit auch im Fehlerfall gewährleistet ist. Der Verzicht auf eine strikt zweikanalige Struktur mit unabhängigen Abschaltpfaden und eine sensorische Positionsüberwachung aller Ventile sorgt dabei für eine niedrige Systemkomplexität.

ISSN 1869-6058
ISBN 978-3-7315-0264-7

ISBN 978-3-7315-0264-7