Beitrag zur Entwicklungsmethodik für resiliente Systeme des Maschinenbaus

Fiona Schulte[1], Roland Engelhardt[2], Eckhard Kirchner[1], Hermann Kloberdanz[1]

[1] *Institute for Product Development and Machine Elements (pmd), Technische Universität Darmstadt, Germany*

[2] *Continental AG, Germany*

Abstract

Resilience in load-carrying systems enables to avoid catastrophes by avoiding a complete failure especially of highly safety-relevant systems. For its realisation a resilience design methodology is being developed. As part of the methodology a procedure for deducing resilient coping strategies from functional resilience characteristics and system requirements is shown. Furthermore the synthesis of suitable functional structures based on the coping strategy is introduced. The functional structure can be described via an extended representation form for functional structures that allows to depict the superior coping strategy as well as a system adaptivity which is required for resilient properties.

Keywords: resilience, design methodology, load-carrying systems, car break systems

1 Motivation

Resilienz ist ein bekanntes Konzept natürlicher Organismen ebenso wie sozioökonomischer Organisationen. Resiliente Organismen oder Organisationen

sind in der Lage, auch unvorhergesehene Krisen zu überstehen und sich schnell von einer möglichen Beeinträchtigung zu erholen oder sogar gestärkt aus der Krise hervorzugehen [1]. Das Erfolgskonzept der Resilienz beruht auf der Bewältigung extremer Einflüsse. Dabei treibt z. B. der Organismus unter normalen Bedingungen nur einen limitierten Aufwand, um möglichen Einflüssen zu widerstehen, während resilientes Verhalten im Krisenfall das Überleben sichert.

Seit Mitte der 80er Jahre existieren Bestrebungen, auch soziotechnische Organisationen [2] und später technische Systeme nach dem Resilienzkonzept zu entwickeln, wobei der Begriff Resilience Engineering geprägt worden ist [3]. Darauf folgend ist das Resilienzkonzept als Lösungsansatz in der Sicherheitsforschung diskutiert worden. Die Eigenschaft, auf äußere unvorhersehbare Einflüsse intelligent zu reagieren, gewinnt insbesondere für die Entwicklung von Systemen mit hoher Sicherheitsrelevanz, bei denen der Mensch nicht mehr flexibel eingreifen kann, um unerwarteten Störungen entgegenzuwirken, an Bedeutung. Beispiele hierfür sind by-wire Systeme oder autonome Systeme wie beim hochautomatisierten Fahren (HAF).

Im Rahmen der Forschung des *Sonderforschungsbereichs 805: Beherrschung von Unsicherheit in lasttragenden Systemen des Maschinenbaus (SFB 805)* wird angestrebt, lasttragende Systeme des Maschinenbaus nach dem Resilienzkonzept zu entwickeln, um Unsicherheit infolge Unwissens zu beherrschen. Unwissen (auch als „unknown unknowns" bezeichnet) umfasst nach Definition des SFB 805 die unbekannte Relevanz von Einflussgrößen bei der Modellbildung, die nicht bekannte Existenz bzw. Wirkung von Einflussgrößen, wodurch ihr Einfluss in der Modellbildung unberücksichtigt bleibt, unbekannte innere Systemzusammenhänge, die empirische anstelle von axiomatischen Modellen erfordern, und die fehlende Möglichkeit zur Modellbildung aufgrund der Systemkomplexität („globale Dimension") bzw. des zeitlichen Horizonts. Lasttragende Systeme mit Resilienzeigenschaften sind in der Lage, auch bei unvorhergesehenen oder aus wirtschaftlichkeitsgründen unberücksichtigten Betriebsbedingungen oder Systemzuständen katastrophale Folgen für Nachbarsysteme und Umwelt sowie Risiken für Menschen durch einen vollständigen Systemausfall zu vermeiden. Dazu ist vorgesehen, „immer" eine Mindestfunktionalität und eine nachfolgende schnelle Erholung zu garantieren. Unter lasttragenden Systemen des Maschinenbaus werden im SFB 805 passive Tragstrukturen (z. B. Fachwerke), semiaktive Systeme (z. B. Dämpfer), aktive und adaptive Systeme (z. B. aktive Fahrwerke) zusammengefasst. Ein System robust gegenüber unbekannten Einflüssen auszulegen, ist gemäß der Definition von Robust Design [4] nicht möglich, da lediglich die Aufrechterhaltung der vollständigen Systemfunktion in einem bekannten Toleranzbereich um den Auslegungspunkt sicher gewährleistet ist.

Die angestrebte Nutzung des Resilienzkonzepts zur Entwicklung lasttragender Systeme erweist sich als anspruchsvoll. Daher soll eine umfassende Methodik erarbeitet werden, die aufbauend auf der Modellierung von Resilienz, Analyse- und Synthesemethoden bereitstellt. Die hier präsentierten Ergebnisse sollen einen Beitrag zu einer entsprechenden Resilience-Design-Methodik für lasttragende Systeme leisten. Ziel der Methodik ist die gleichgestellte Behandlung der zweier Schwerpunkte. Zu einen das Sicherstellen der robusten Funktion im Auslegungspunkt und zum anderen die Realisierung resilienten Verhaltens im Fall unvorhergesehener Störungen oder Teilsystemausfälle, die beim Robust Design nicht berücksichtigt werden können.

2 Grundlagen, Forschungsfragen und Lösungsansatz

Als Grundlage ist im SFB 805 eine Arbeitsdefinition für resiliente lasttragende Systeme erarbeitet worden. Die Definition besagt, dass, „[…] resiliente lasttragende technische Systeme eine vorab festgelegte Mindestfunktionalität, auch im Fall von Störungen oder Versagen von Systemkomponenten, garantieren und die anschließende Möglichkeit der Erholung bis mindestens auf das Ausgangsniveau der Funktionalität bieten." [5] Ausgehend von der Definition ist zu erkennen, dass für die Charakterisierung und Beurteilung der Resilienzeigenschaften eines Systems die Abhängigkeit seiner funktionalen Performance von Veränderungen der Umgebungsbedingungen sowie der Zeit zu betrachten und ggf. veränderte Systemzustände zu berücksichtigen sind.

Das Resilienz-Einsatz-Modell (resilience application model) umfasst die statischen und dynamischen Resilienzeigenschaften eines Systems und der Einflussgrößen sowie damit korrelierende Signale [6]. Die Verwendung des Resilienz-Einsatz-Modells und die darauf aufbauende Definition von Bewältigungsstrategien werden im Folgenden anhand des Beispiels eines by-wire Kfz-Bremssystems erläutert. Eine stark vereinfachte Funktionsstruktur des by-wire Bremssystems im Fahrzeug ist in Abbildung 1, das Resilienz-Einsatz-Modell des Bremssystems in Abbildung 2 dargestellt.

Bei dem betrachteten System ist das Bremspedal im by-wire Betrieb durch Ventile hydraulisch von den Radbremsen entkoppelt und der Fahrer tritt in einen Simulator. Bei einem Bremsvorgang wird das Signal des Bremspedals über Sensoren erfasst und an die Steuer- und Regeleinheit weitergeleitet. Dort gehen auch weitere Signale über Fahrzeugzustand, Umgebung und Fahrsituation ein. Diese Einheit steuert einen elektrischen Aktor an, welcher die hydraulische Bremskraft an den Radbremsen erzeugt. Der Bremsdruck wird parallel durch zwei getrennte Bremsleitungskreise zu den Bremszylindern an den Radbremsen

geleitet. Hier wirken die Bremskräfte auf die Bremsscheiben und bewirken ein Bremsmoment, welches das Fahrzeug verzögert. [7]

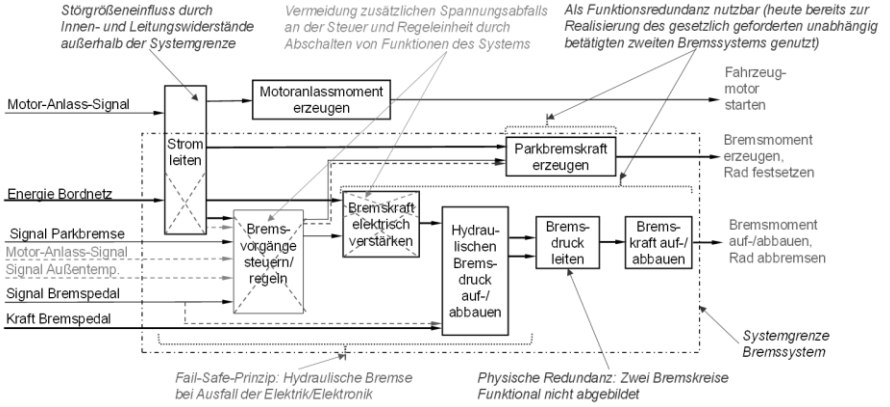

Abbildung 1: Vereinfachte Funktionsstruktur eine by-wire Bremssystem mit Erläuterungen zur Realisierung von Resilienzfunktionen [7]

Zur Betrachtung der Resilienzeigenschaften wird der Extremfall angenommen, dass bei niedriger Außentemperatur während des Anlassvorgangs eines (Verbrennungs-)Motors gleichzeitig eine Gefahrenbremsung eingeleitet wird. Während des Anlassvorgangs fließt ein hoher Strom aus der Starterbatterie zum Anlasser. Bedingt durch die Innen- und Leitungswiderstände der Batterie und des Bordnetzes kann es bei tiefen Außentemperaturen und geschwächtem Bordnetz zu einem Abfall der Versorgungsspannung des Bremssystems unter die Normalspannung kommen. Wird in dieser Situation eine Gefahrenbremsung durch ein elektrisches by-wire Bremssystem eingeleitet, fließt zusätzlich ein hoher Strom in den Aktuator der Bremskraftverstärkung. Bedingt durch die Widerstände kann die Versorgungsspannung im Bremssystem in den Unterspannungsbereich abfallen. Um das Bordnetz nicht weiter mit hohen Strömen zu belasten und einen vollständigen Bordnetzausfall zu vermeiden, werden Performance und Funktionen des Bremssystems, z. B. ABS, kurzzeitig reduziert. Dadurch kann das Bremssystem unmittelbar nach Bordnetzerholung die volle Funktionalität wiederherstellen und ein Neustart der Steuer- und Regelungseinheit ist nicht erforderlich.

Bei der Definition von Resilienzeigenschaften im Resilienz-Einsatz-Modell wird neben dem Auslegungspunkt die *funktionale Performance* des Bremssystems bei extremen Einflüssen definiert (Abbildung 2 a und b). Die robuste Auslegung toleriert Einflussgrößen bis hin zu einer kaum spürbaren Komfortein-

buße und irrelevanten Sicherheitsbeeinträchtigungen. Für Resilienzbetrachtungen über die robuste Auslegung hinaus ist jedoch eine erhebliche Komfort- und Funktionsreduktion bis zur Mindestfunktionalität gegeben.

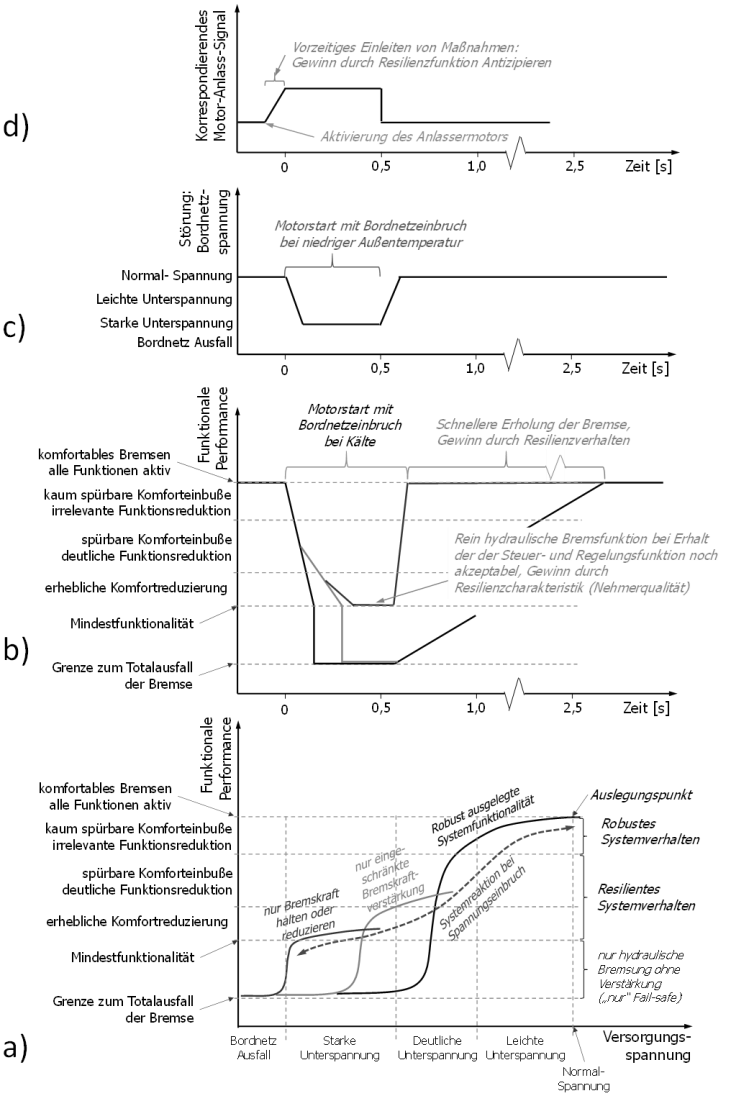

Abbildung 2: By-wire Bremssystem abgebildet im Resilienz-Einsatz-Modell

Für die Entwicklung resilienter lasttragender Systeme ist die Betrachtung des zeitlichen Verlaufs während und nach einer äußeren Störung oder einem Teilausfall einer Komponente oder eines Bauteils bedeutend. Der zeitliche Verlauf der funktionalen Performance repräsentiert das *dynamische Resilienz-Verhalten* (Abbildung 2 b) während der Systemreaktion und -erholung. Bei dem Beispiel des Motor-Startvorgangs ist erkennbar, dass insbesondere die Zeit bis zur Wiederherstellung der vollen Funktionalität nach einem Abfall auf die Mindestfunktionalität relevant ist. Die Steuer- und Regelungseinheit stellt das Subsystem mit der höchsten Vulnerabilität dar, dessen Ausfall unbedingt zu vermieden ist.

Parallel zum zeitlichen Verhalten wird die Abhängigkeit der funktionalen Performance von den Einflussgrößen berücksichtigt. Im Beispiel führt der Motor-Startvorgang zu einem erheblichen Abfall der Bordnetzspannung. Die Systembeeinflussung wird durch die Bordnetzspannung als *Einflussgröße* repräsentiert. Der kausale Zusammenhang zwischen funktionaler Performance und Einflussgrößen wird durch die *statische Resilienz-Charakteristik* (Abbildung 2 a) dargestellt. Im Beispiel bewirkt der Strombedarf des Bremssystems bei einem starken Bremsvorgang einen zusätzlichen Abfall seiner Versorgungsspannung. Bei üblicher Ausführung des Systems führt diese Einflussgröße bei einem völligen Bordnetzspannungseinbruch zum Abschalten der Steuer- und Regelungseinheit und damit zu einem Ausfall der by-wire Bremsunterstützung.

Die konkreten statischen und dynamischen Resilienzeigenschaften von Systemen können durch weitere, als *Resilienzmetriken* bezeichnete, Parameter beschrieben und quantifiziert werden [6]. Die grundlegenden Resilienzeigenschaften der Systeme werden durch funktionale Resilienzcharakteristiken, vereinfacht als „Resilienzfunktionen" bezeichnet, definiert. [8]

Für lasttragende Systeme haben sich die Resilienzfunktionen *Reagieren (responding)*, *Überwachen (monitoring)*, *Antizipieren (anticipating)* und *Lernen* (*learning*) als geeignet erwiesen [9]. Die Resilienzfunktion *Reagieren* beschreibt die Adaption des Systems an neue Umgebungsbedingungen bzw. innere Zustände abhängig von einer Einflussgröße. Oft werden hierzu bei Überlast oder Komponentenausfällen bereits vorgesehene alternative Lastpfade genutzt. Die Bedeutung für die Resilienzeigenschaften geht allerdings über die des Fail-safe Prinzips hinaus, da eine Systemanpassung nicht erst durch bzw. nach einem Komponentenausfall erfolgt und zusätzlich eine Erholung des Systems einbezogen wird. Die Resilienzfunktionen *Überwachen* und *Antizipieren* adressieren die Möglichkeit einer frühzeitigen bzw. vorsorglichen Reaktion mithilfe von Signalverarbeitung. Beim *Überwachen* werden i. d. R. der Verlauf und die Höhe der

Einflussgröße detektiert, wodurch eine zeitnahe Störung erkannt und eine adäquate Systemreaktion frühzeitig eingeleitet werden kann. Die Resilienzfunktion *Antizipieren* geht von der Verarbeitung eines (ggf. zusätzlichen) Signals aus, das mit der Einflussgröße korreliert. So kann sich das System vorzeitig an den Störungseintritt anpassen (*predictive adaption*) und eine höhere funktionale Performance bereitstellen.

Die Forschungsfragen im Zusammenhang mit der Entwicklung einer Resilience-Design-Methodik konzentrieren sich hauptsächlich auf die Problematik der begrenzten Flexibilität lasttragender Systeme und den oft wenig ausgeprägten Fähigkeiten der Signal- oder Informationsverarbeitung. In diesem Zusammenhang sind folgende Forschungsfragen relevant.

- Wie können basierend auf den Resilienzcharakteristiken *resiliente Bewältigungsstrategien* für extreme Störungen abgeleitet werden?

- Wie können die Bewältigungsstrategien in *resiliente funktionale Systemstrukturen* überführt werden?

Bei der Entwicklung resilienter lasttragender Systeme sind Systemreaktionen auf unbekannte oder nicht berücksichtigte äußere Einflüsse oder veränderte Systemzustände zu definieren und zu realisieren. Dafür wird ein methodischer Lösungsansatz angestrebt, mit dem zeitlich veränderliche Systemreaktionen über die „normalen" Systemfunktionen hinaus berücksichtigt werden können. Hauptsächlich sollen dazu situationsabhängige Systemanpassungen (System-Adaptivität) genutzt werden. Für die Synthese resilienter Systemstrukturen wird ein zweistufiges Vorgehen vorgeschlagen. Zunächst erfolgt die Planung von Bewältigungsstrategien mithilfe der Resilienzfunktionen, -charakteristiken und -metriken und des Resilienz-Einsatz-Modells [5, 6, 9]. Anschließend werden die adaptiven funktionalen Systemstrukturen, ggf. orientiert an systematischen Lösungsansätzen zur Adaptivität, modelliert [6, 9].

3 Definition resilienter Bewältigungsstrategien

Die Vermeidung eines Unterschreitens der Mindestfunktionalität z. B. durch Herunterfahren der Steuer- und Regelungseinheit des Bremssystems, wie im Beispiel beschrieben, ist Ziel des *Resilience-Designs.* Mit dem Resilienz-Einsatz-Modell können die Resilienzeigenschaften (Abbildung 2) dargestellt, analysiert und Maßnahmen zur Beherrschung der Extremsituation geplant werden, die als *Bewältigungsstrategien* (*coping-strategies*) bezeichnet werden. Die Bewältigungsstrategien werden anhand der Systemanforderungen basierend auf den

Resilienzfunktionen entwickelt und definiert. Wird die Resilienzfunktion *Reagieren* als alleinige Strategie angestrebt, werden nur passive Reaktionen eingeleitet. Im Beispiel des Bremssystems ist dies dadurch gewährleistet, dass nach dem Fail-safe Prinzip eine durch Muskelkraft betätigte hydraulische Bremsung ohne Bremskraftregelung und -verstärkung als Mindestfunktionalität möglich ist. Die Bewältigungsstrategie einer Systemreaktion ohne die Nutzung von Signalen kann durch die Verbesserung der Nehmerqualitäten [5] des Systems erreicht werden. Im Beispiel wäre das durch eine Elektronik, die bei niedrigeren Spannungen funktionsfähig bleibt, oder durch einen Energiespeicher, der die Funktionsfähigkeit des gesamten Systems für einen gewissen Zeitraum aufrechterhält, erreichbar. Beide Maßnahmen sind mit erheblichem Mehraufwand verbunden. Zusätzlich ist die Wirksamkeit von Puffern zeitlich begrenzt [6].

Mit einer Bewältigungsstrategie, welche die Resilienzfunktionen *überwachen* und *reagieren* nutzt, ist eine bessere Beherrschung der Einflüsse möglich [10]. Beim Beispiel des Bremssystems wird die by-wire Funktionalität so lange wie möglich aufrechterhalten, indem verschiedene Degradationsstrategien durchlaufen werden. In der ersten Phase reicht die Reduktion der Performance des Bremsaktors, um ein überlastetes Bordnetz nicht zusätzlich zu belasten. Sinkt die Spannung weiter ab, wird der Bremsdruck gehalten oder reduziert, jedoch nicht mehr aktiv aufgebaut. Sollte der Fahrer mehr Bremsdruck benötigen wird in die hydraulische Rückfallebene geschaltet und der Fahrer hat einen mechanisch-hydraulischen Durchgriff auf die Radbremsen. Bei weiterem Spannungsabfall, kann noch der Prozessor mit Strom aktiv gehalten werden. Dadurch wird eine schnelle Wiederherstellung der by-wire Funktionalität des Systems unmittelbar bei Ansteigen der Bordnetzspannung gewährleistet.

Eine Bewältigungsstrategie basierend auf der Kombination der Resilienzfunktionen *Überwachen*, *Antizipieren* und *Reagieren* geht von einer Systemreaktion abhängig von einem oder mehreren Signalen aus. Die Signale korrelieren mit den Einflussgrößen und ermöglichen, den zeitlichen Störungsverlauf vorherzusehen (Abbildung 2 d). Das setzt voraus, dass weitere Signale überwacht werden und auf den Eintritt eines Ereignisses geschlossen werden kann. Im Beispiel des Bremssystems wird zusätzlich zur Bordnetzspannung die Außentemperatur überwacht, die über den Innenwiderstand des Systems mit dem zu erwartenden Spannungsabfall korreliert. Außerdem könnte die Reaktion des Bremssystems abhängig von der Ursache des Spannungsabfalls eingeleitet werden, wenn das Anlassersignal überwacht wird. Die Verbesserung der Resillienzeigenschaften besteht in der frühzeitigeren, weniger umfangreichen und verkürzten Abschaltung bzw. in der gezielteren Begrenzung der Leistungsaufnahme der Verbraucher im Bremssystem.

4 Resiliente funktionale Systemstrukturen

Beim Robust Design lasttragender Systeme beginnt die Systemsynthese mit der Festlegung einer Funktionsstruktur. Die Teilfunktionen werden üblicherweise als Blackbox mit verbaler Beschreibung der Funktion bzw. Operation dargestellt [11]. Die Betrachtung beschränkt sich i. d. R. auf wenige Strukturvarianten, die als determiniert angenommen werden. Bei der Entwicklung resilienter lasttragender Systeme ist zusätzlich die zuvor festgelegte Bewältigungsstrategie (vgl. Kapitel 3) und die dafür erforderliche Adaptivität beim Modellieren der funktionalen Struktur zu berücksichtigen. Die Adaptivität wird durch die angestrebten Resilienz-Lösungsprinzipien und -lösungsansätze [6] oder die gewählten Resilienz-Konstruktionsprinzipien z. B. in Anlehnung an [12] bestimmt. Zur funktionalen Modellierung resilienter lasttragender Systeme werden zusätzliche Darstellungsformen als Erweiterung der Funktionsmodelle der konventionellen methodischen Produktentwicklung vorgeschlagen [12].

Zur Berücksichtigung veränderter Systemstrukturen z. B. beim Ausfall oder „Abschalten" eines Funktionsträgers (i. d. R. Bauteil oder Komponente) werden die entsprechenden Teilfunktionen teilweise oder vollständig mit gestrichelten Linien durchkreuzt. Im Beispiel des by-wire Bremssystems wird dies bei der Bewältigungsstrategie *Reagieren* anhand Durchkreuzens der Teilfunktionen „Bremsvorgänge steuern/regeln" und „Bremskraft verstärken" dargestellt (Abbildung 1). Die Systemanpassung zum Realisieren der Resilienzfunktion *Reagieren* besteht darin, dass bei einer Bremsung eine durch Muskelkraft betätigte hydraulische Bremsung ohne Kraftverstärkung als alternativer Lastpfad genutzt wird (Abbildung 1). In der Funktionsstruktur wird dies als zusätzliche, teilweise parallele gestrichelte Linie dargestellt. Hierdurch wird jedoch nicht die Mindestfunktionalität sichergestellt. Üblicherweise wird in Bremssystemen der Bremsdruck über zwei unabhängige Leitungskreise zu den Radbremszylindern geleitet. Diese Gestaltung ist im Sinne einer *physischen Redundanz*. Als Erweiterung der funktionalen Modellierung werden hier *physisch redundante Strukturen* innerhalb der Teilfunktion-Blackbox dargestellt.

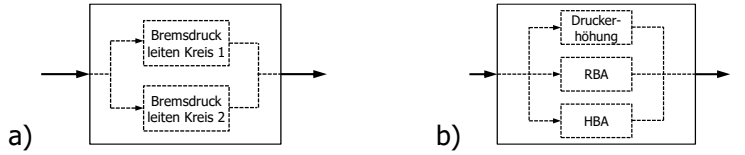

Abbildung 3: a) Zweikreisbremse; b) Bremsassistenzsysteme: Druckerhöhung bei Fading, Rain Break Assist für Nässe, Hydraulic Breaking Assist für eine Vollverzögerung in Notsituationen

Im Gegensatz zu physischen Redundanzen, bei denen Funktionsträger mehrfach vorgesehen bzw. vorgehalten werden, bieten *Funktionsredundanzen* eine wirtschaftlichere Möglichkeit zur Realisierung alternativer Signal- oder Lastpfade. Bei einer Funktionsredundanz wird eine Teilfunktion im Fall eines Komponentenausfalls oder einer -abschaltung durch einen nicht primär hierfür vorgesehenen Funktionsträger (ggf. nur partiell) realisiert [13]. Im Beispiel des by-wire-Bremssystems kann im Fall eines Ausfalls der by-wire Funktionalität die Bremskraftsteuer- und –regelungseinheit noch zusätzlich zur hydraulischen Bremse die elektrische Parkbremse ansteuern, die eine Fahrzeugverzögerung in reduziertem Maße ermöglicht. In der Funktionsstruktur wird diese Funktionsredundanz als gestrichelte Linie, ggf. parallel zur durchgezogenen Linie der Funktion im Auslegungspunkt dargestellt (Abbildung 1).

Im Rahmen der Entwicklung resilienter lasttragender Systeme kann eine deutlich veränderte Transformationscharakteristik einer Teilfunktion ebenfalls als *Funktionsredundanz* interpretiert werden. Die verschiedenen Abhängigkeiten zwischen den Eingangs- und Ausgangsgrößen der Funktion können durch Signale angesteuert werden. Dieser Fall tritt beispielsweise ein, wenn von der Resilienzfunktion *Überwachen* oder *Antizipieren* erkannt wird, dass eine kritische Situation in naher Zukunft eintreten kann. Diese Art der Funktionsredundanz kann in der Funktionsstruktur durch eine verbale oder symbolhafte Beschreibung der Funktionscharakteristik-Alternativen innerhalb der Teilfunktion-Blackbox dargestellt werden. Als Beispiel wird der Fall betrachtet, dass das Bremsmoment bei einer hohen thermischen Belastung der Bremsscheiben aufgrund eines verringerten Reibkoeffizienten deutlich absinkt. Wenn unter diesen Voraussetzungen eine Notbremsung eingeleitet wird, sinkt die Bremskraft weiter ab. Dies wird als Fading bezeichnet. Um darauf zu reagieren und gefährliche Situationen zu vermeiden, erfasst das by-wire-Bremssystem die Bremsscheibentemperatur und *antizipiert* damit ein mögliches Fading. *Prädiktiv* bereitet das System die mögliche Erhöhung des Bremsdrucks vor, um eine gewohnte Bremsperformance zu gewährleisten. Im Sinne des Resilience-Designs ist diese Erhöhung der Bremskraftverstärkung als *Funktionsredundanz* anzusehen und wird in der Funktionsstruktur innerhalb der Teilfunktion-Blackbox der Bremskraftverstärkung als alternative Transformation dargestellt.

In ähnlicher Weise wird die Bremsmomentreduktion infolge eines Wasserfilms auf der Bremsscheibe durch die Auswertung des Scheibenwischersignals *antizipiert*. Der Rain Break Assist (RBA) des Bremssystems leitet eine prädiktive Adaption ein, indem er wiederholt die Bremsbacken leicht anlegt und die Bremsscheiben trocken bremst, damit den Reibbeiwert auf einem hohen Niveau bleibt. Ebenso wird eine unmittelbar bevorstehende Notbremsung von dem

Hydraulic Breaking Assist (HBA) antizipiert, beispielsweise durch Umgebungssensoren oder die Fahrerreaktion eines schnellen Lupfens des Fahrpedals. Wird dies erkannt, legt das System die Bremsbeläge dicht an die Bremsscheibe an. Beide Funktionsvarianten sind ebenfalls mit gestrichelten Linien innerhalb der Teilfunktion-Blackbox der Bremskraftverstärkung in Abbildung 3 (b) als alternative Transformation dargestellt.

5 Ergebnisse und Diskussion

Das Resilienzkonzepts birgt für lasttragende Systeme des Maschinenbaus Potentiale insb. für Systeme hoher Sicherheitsrelevanz, wie das Beispiel der Fahrzeugbremse zeigt. In dem Konzept sind bereits Maßnahmen realisiert, die einem Unterschreiten der Mindestfunktionalität des Bremssystems entgegenwirken [7]. Erste Ansätze resilienter Eigenschaften und resilienten Verhaltens sind erkennbar, jedoch sind diese nicht methodisch entwickelt worden.

Die Umsetzung von Resilienz in lasttragenden Systemen erhöht die Komplexität des Entwicklungsprozesses signifikant und erfordert ein Umdenken hin zu neuen Strukturen und insb. die Berücksichtigung und Umsetzung der Systemadaptivität [5, 6, 9]. Im Rahmen des SFB 805 wird eine umfassende Methodik zur Unterstützung des Entwicklungsprozesses angestrebt. Dazu ist eine Möglichkeit zur Integration der resilienten Bewältigungsstrategie und der Systemadaptivität in die Funktionsstruktur durch eine Erweiterung der Darstellungsform entwickelt worden. Dadurch soll dem Entwickler ermöglicht werden, ein umfassendes Resilienzkonzept für das betrachtete System abzuleiten und zu realisieren.

Danksagung

Gefördert durch die Deutsche Forschungsgemeinschaft (DFG) – Projektnummer 57157498 – SFB 805.

Literatur

[1] Goethe J. (2013). Resilienz und Effizienz – Architektur für nachhaltigen Unternehmenserfolg. In: Landes M., Steiner E. (eds) Psychologie der Wirtschaft. Psychologie für die berufliche Praxis, Springer, Wiesbaden, S. 804

[2] Trist, E. L. (1981). The evolution of socio-technical systems: a conceptual framework and an action research program, Toronto, Ont.: Ontario Ministry of Government Services, S. 1-67

[3] Hollnagel, E. (2006). Epilogue: Resilience Engineering Precepts, in: Resilience Engineering: Concepts and Precepts, S. 347-358

[4] Freund, T. (2018). Konstruktionshinweise zur Beherrschung von Unsicherheit in technischen Systemen, Darmstadt, S. 43-44

[5] Altherr, L. C. et al. (2018). Resilience in Mechanical Engineering - A Concept for Controlling Uncertainty during Design, Production and Usage Phase of Load-Carrying Structures, in: Applied Mechanics and Materials, Vol. 885, S. 187-198.

[6] Schulte, F. et al. (2019). Analysis and Synthesis of Resilient Load-carrying Systems, International Conference on Engineering Design 2019, Delft

[7] Breuer, B. et al. (2017). Bremsenhandbuch – Grundlagen, Komponenten, Systeme, Fahrdynamik, Wiesbaden, Springer, S. 179

[8] Woods, D. D. (2010). Essential Characteristics of Resilience, in: Resilience Engineering – Concepts and Precepts, Ashgate, Farnham, S. 21-34.

[9] Schlemmer, P. D. et al. (2018). Adaptivity as a Property to Achieve Resilience of Load-Carrying Systems, in: Applied Mechanics and Materials, Vol. 885, S. 77-87.

[10] Hollnagel, E. (2014). Resilience engineering and the built environment, Building Research & Information 42 (2), S. 221-228

[11] Feldhusen, J., Grote, K.-H. (2013). Pahl/Beitz Konstruktionslehre – Methoden und Anwendung erfolgreicher Produktentwicklung. 8. vollständig überarbeitete Auflage, Berlin, Heidelberg, Springer Vieweg Verlag, S. 240-254

[12] Jackson, S. et al. (2012). Resilience principles for engineered systems, in: System Engineering, 16 (2):S. 152–164

[13] Sun, Z. et al. (2011). On the concept of the resilient machine, in: 6th IEEE Conference on Industrial Electronics and Applications, Beijing, S. 357-360