

Wann kommt By-Wire auch für Bremse und Lenkung?

When does By-Wire arrive brakes and steering?

H. Winner, R. Isermann, H. Hanselka, A. Schürr, Darmstadt

Kurzfassung

Die Entwicklung von Brems- und Lenksystemen mit X-by-Wire-Architektur ist zurzeit ausgesetzt. Die Gründe für diese Pause werden diskutiert. Aus einigen der Gründe lassen sich Forschungsaktivitäten ableiten, die bei Wiederaufnahme der X-by-Wire-Entwicklung die Entwicklungshürden absenken können. An der Technischen Universität Darmstadt werden entsprechende Aktivitäten fortgesetzt bzw. z.T. auch neu aufgesetzt. Dazu zählen Untersuchungen zur Fehlertoleranztechnik einschließlich der dynamischen Rekonfiguration, Konzepte für Aktoren und Sensoren mit Integrierter Redundanz, Entwicklung geeigneter und kompatibler Betätigungseinheiten, Methoden zur Zuverlässigkeitsvorhersage und die Weiterentwicklung von Software-Modellierungs-Methoden sowie Testmethoden. Neben diesen Forschungsansätzen führt auch die Weiterentwicklung mechatronischer Brems- und Lenkanlagen zu einer besseren Ausgangsposition für einen späteren Neustart der X-by-Wire-Entwicklung.

Abstract

At present the development of brake and steering systems with X-by-Wire architecture are suspended. Reasons for this interruption are discussed. From some of these reasons research activities can be derived in order to decrease the development hurdles at later resume of the X-by-Wire development. At the Darmstadt University of Technology researchers continue with or start such investigations. In the focus are investigations of fault tolerant systems using reconfiguration techniques, concepts for integrated redundancy for actuators and sensors, the development of driver operation elements which enhance the handling, but preserve the compatibility to conventional elements. The methodological focus lies on methods for prediction of system reliability as well as on the software development using suitable modelling tools and testing procedures. Beyond the research activities the continuous development of the mechatronic brake and steering systems will lead to a better position for the expected restart of the X-by-Wire development.

1. Einleitung

Bei X-by-Wire-Systemen ist die Betätigung durch den Fahrer und die tatsächliche Verstellung, z.B. am Rad, energetisch entkoppelt. Als Fly-by-Wire findet man diese Architektur seit 1978 in der Luftfahrt. Auch als Throttle-by-Wire (E-Gas, Elektronische Dieselregelung) und Shift-by-Wire konnte dieses Prinzip im Kraftfahrzeug Einzug halten. Ebenso wird dieses Prinzip seit langem für die Funktionen Bremse und Lenkung diskutiert. Seit etwa einem Jahrzehnt wird an der elektromechanischen Bremse (EMB) und fast so lange an Steer-by-Wire (SbW) mit beträchtlicher Entwicklungskapazität gearbeitet. Doch statt der für die Mitte der aktuellen Dekade geplanten Einführung im Markt werden die Entwicklungsaktivitäten zurzeit nahezu vollständig heruntergefahren. Oft heißt es, dass die Einführung nur um fünf Jahre verschoben wird. Von anderer Seite gibt es Stimmen, die davon ausgehen, dass X-by-Wire bei Lenkung oder Bremse nie zum Einsatz kommen wird. Gefördert wird diese negative Grundstimmung auch durch die Abkehr von der elektrohydraulischen Bremse (EHB), die aktuell in einigen Mercedes-Modellen unter dem Namen SBC eingesetzt wird. Denn die EHB wurde bisher als Zwischen- und Übergangsstufe zu einem vollständigen Brake-by-Wire in Art der EMB angesehen.

2. Definition X-by-Wire

Als X-by-Wire-System wird hier im Weiteren ein System bezeichnet, das zwei energetisch entkoppelte Regelkreise besitzt:

- Einen Regelkreis zur Erzeugung der fahrdynamischen Wirkung. Diese ist bei der Lenkung die Radverstellung und bei der Bremse die Erzeugung der Bremsmomente.
- Einen Regelkreis zur Erzeugung einer geeigneten Rückmeldung, die dem Fahrer eine gefühlvolle Betätigung der Brems- bzw. Lenkfunktion ermöglicht.

Für beide Regelkreise werden, wie für digitalelektronische Regelkreise üblich, Sensoren, Aktoren und Reglerrechner benötigt. Die Sensoren und Aktoren sind mit den auch zum X-by-

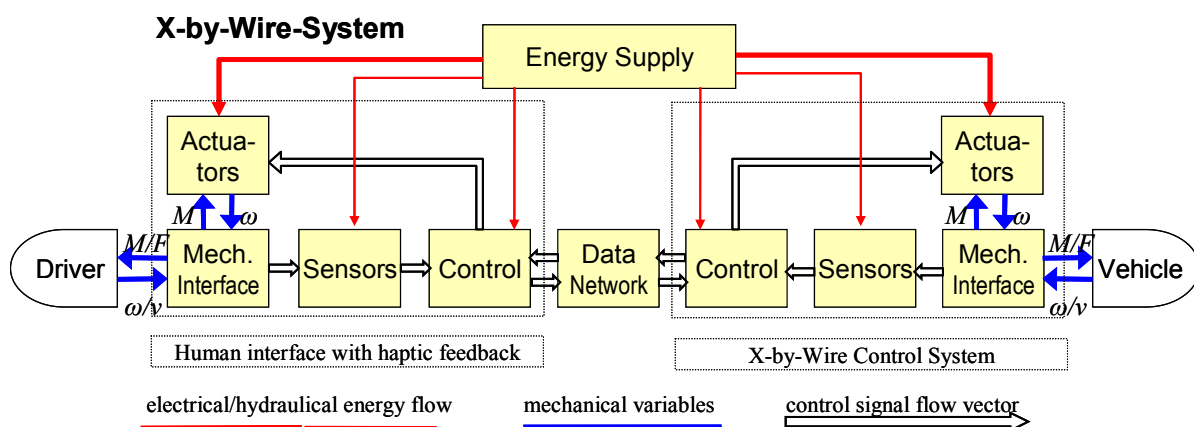


Bild 1: Blockschaltbild des X-by-Wire-Systems

Wire-System zählenden mechanischen Schnittstellen an Fahrzeug bzw. Fahrer angebunden. Die Kopplung zwischen den Regelkreisen erfolgt zwar nur über Informationsaustausch, der allerdings zu einer sehr engen funktionalen Kopplung der Regelkreise untereinander führt. Wie in Bild 1 eingezeichnet, ergeben sich vielfältige Energie- und Informationsflüsse, ohne die eine Systemfunktion nicht denkbar ist. Daher gehört zum System X-by-Wire auch das Daten- und Energienetzwerk.

3. Hindernisse für X-by-Wire bei Bremse und Lenkung

Für die Einstellung der Entwicklungsaktivitäten werden mehrere Faktoren genannt. Sie lassen sich in zwei Gruppen zusammenfassen:

- **Fehlende Marktfähigkeit**

Die vorgesehenen Technikkonzepte sind erheblich teurer als heutige Brems- oder Lenkanlagen. Die Mehraufwendungen lohnen aber erst, wenn die erweiterten Funktionsmöglichkeiten durch eine größere Zahl von Fahrerassistenzsystemen (FAS) genutzt wird. Die sind aber zum einen noch gar nicht marktreif (z.B. ACC mit Stop&Go oder Lane Keeping Support) und zum anderen nur als Sonderausstattung in einem Bruchteil der Fahrzeuge einer Modellreihe eingebaut. Dadurch ist der Fahrzeughersteller bei einem Einsatz von Brake- oder Steer-by-Wire gezwungen, entweder die Modelle ohne ausreichende Zahl von Fahrerassistenzsystemen mit dem Zusatzaufwand von X-by-Wire zu verteuern, oder nur die Modelle mit hoher FAS-Ausrüstung mit X-by-Wire auszurüsten, was wiederum den Aufwand deutlich erhöht und die Mehrkosten für diesen Weg (parallele Entwicklung, Variantenvielfalt, kleine Gesamtstückzahl) so erhöht, dass dann auch mit vielen FAS ausgerüstete Fahrzeuge mit X-by-Wire teurer kommen als mit herkömmlicher Technik, die durch Zusatzmodule (z.B. Active Booster oder Überlagerungslenkung) erweitert wird.

- **Zu hoher Initialaufwand**

Hier sind vor allem zwei Aspekte zu betrachten: das 42 V Bordnetz und die Entwicklungskosten für die Pilotentwicklung. Erst mit einer höheren Bordnetzspannung als das heutige 14 V Bordnetz hergibt, kann eine hinreichend dynamische Vorderradbremse oder eine Lenkung für ein 2 t Fahrzeug dargestellt werden. Die Einrichtung einer zweiten Spannungsversorgung oder die generelle Umstellung auf eine neue Bordnetzspannung ist mit erheblichen Zusatzkosten in der Ausrüstung (zusätzliche Batterie und Spannungswandler) und in der Entwicklung (z.B. Umstellung vieler Steuergeräte) verbunden. Daher spricht auch sehr viel dafür, dass die Einführung von Brake-by-Wire und von Steer-by-Wire gekoppelt erfolgt, damit dieser Zusatzaufwand geteilt werden kann.

Bei der Einführung von Brake- oder Steer-by-Wire kann in nur wenigen Fällen auf eine langjährige Erfahrung mit den Systemkomponenten zurückgeblickt werden. Parametrische Schätzungen durch Vergleich mit bekannten Pilotentwicklungen ähnlichen Neuigkeitsgrades

lassen neunstellige (>100 Mio. €) Entwicklungskosten erwarten. Eine Umlage auf kleinere Stückzahlen bei einem vorsichtigen Beginn ist wirtschaftlich nicht möglich. Ein Beginn mit der Ausrüstung von Großserien senkt natürlich diesen Anteil, hebt aber das Risiko, z.B. von Rückrufaktionen, erheblich.

4. Bedingungen für eine erfolgreiche X-by-Wire-Einführung bei Bremse und Lenkung

Aus den oben genannten Hindernissen und der Betrachtung des Standes der Technik lassen sich folgende notwendige Bedingungen für eine erfolgreiche Markteinführung ableiten:

- Hinreichende Nachfrage nach Fahrerassistenzsystemen, die von der X-by-Wire-Technik profitieren.
- Die Mensch-Maschine-Schnittstelle darf zumindest keine Nachteile bzgl. Bedienbarkeit und Bediengefühl haben und kompatibel zur bisher bekannten Bedientechnik sein. Verbesserte Handlungseigenschaften zur sicheren und komfortableren Führung des Fahrzeugs erhöhen den Wert von X-by-Wire.
- Bordnetztechnik mit hinreichender Zuverlässigkeit und Verfügbarkeit, um Lenk- und Bremsfunktion vom Bordnetz abhängig werden zu lassen. Dies gilt auch für die EMV.
- Komponenten (insbes. Aktoren u. Sensoren) mit nachgewiesenen guten Zuverlässigkeiten.

5. Forschungsansätze für die Zukunft

Einige der obigen Bedingungen lassen sich kaum beeinflussen. Dies gilt insbesondere für die Endkunden-Nachfrage nach Fahrerassistenzsystemen. Aber für andere Bedingungen lässt sich direkt Forschungs- und Entwicklungsbedarf ableiten.

Methoden der Ausfallsicherheit

Um die Sicherheitsanforderungen zu erfüllen, wurden spezielle Vorgehensweisen in verschiedenen technischen Disziplinen entwickelt, wie z.B. dem Eisenbahnwesen, der Luftfahrt, der Raumfahrt im Bereich des Militärs und der Kernkraftwerke. Diese Vorgehensweisen werden durch den Begriff Systemintegrität (System Integrity, System Dependability) beschrieben [1]. Einen Überblick über dort eingesetzte Methoden sowie deren Kombination sind in [2] beschrieben. Dass dieses Instrumentarium auch für die Luftfahrtindustrie noch nicht ausreicht, wird deutlich an dem EU-Forschungsprojekt ESACS (Enhanced Safety Assessment for Complex Systems) [3], das die Weiterentwicklung der Analysemethoden zum Ziel hat.

Entwurf fehlertoleranter Systeme

Systeme mit hoher Integrität (Ausfallsicherheit) müssen so viel Fehlertoleranz wie nötig besitzen. Dies bedeutet, dass Fehler automatisch so kompensiert werden, dass sie nicht zu einem Ausfall des Systems führen. Eine Möglichkeit, um dieses Ziel zu erreichen, ist die Re-

dundanz von Komponenten, Einheiten oder Untersystemen. Das heißt, dass das betrachtete Modul durch eine oder mehrere Module ergänzt wird, gewöhnlich in paralleler Anordnung. Diese redundanten Module können entweder identisch oder divers (verschieden) sein.

Es existieren hauptsächlich zwei verschiedene Anordnungen für fehlertolerante Systeme, die

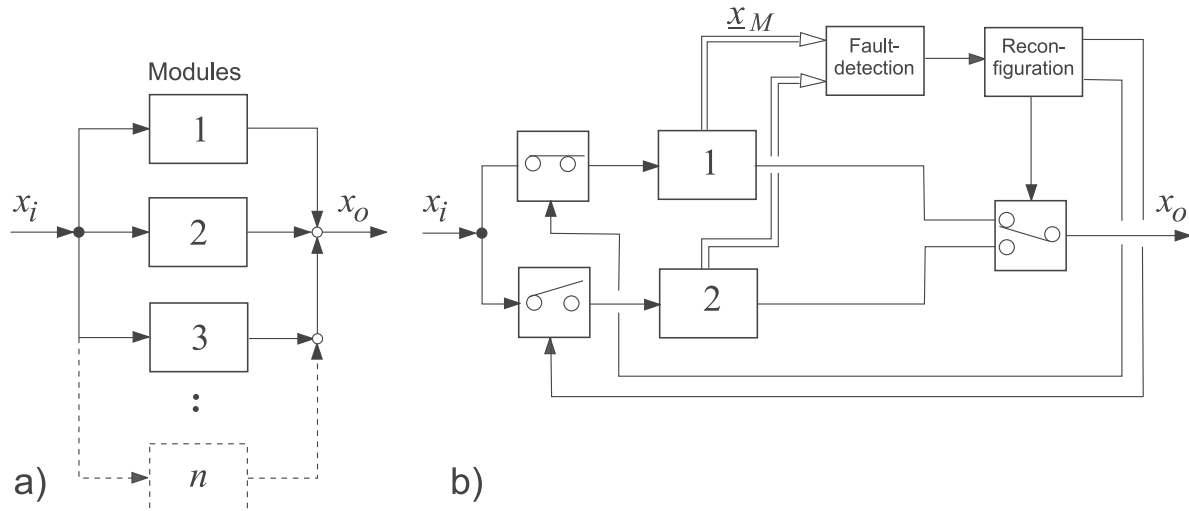


Bild. 2: Fehlertolerante Schemata für elektromechanische und mechatronische Systeme

- a) Statische Redundanz für mechanische und elektrische Komponenten: mehrfach redundante Elemente
- b) Dynamische Redundanz für elektromechanische und mechatronische Systeme: standby Modul, welches inaktiv ist, „cold-standby“.

\underline{x}_M : gemessener Eingang, Ausgang und dazwischen liegende Signale

statische Redundanz und die dynamische Redundanz. Bild 2a zeigt ein Schema für statische Redundanz. Es nutzt drei oder mehrere parallele Module, die dasselbe Eingangssignal haben und alle aktiv sind. Die dynamische Redundanz benötigt weniger Module auf Kosten von mehr Informationsverarbeitung. Eine minimale Konfiguration besteht aus zwei Modulen. Diese können beide permanent aktiv sein als (hot standby) oder wie in Bild 2b gezeigt, mit nur jeweils einem aktiven Modul ausgeführt sein (cold standby).

Die Fehlertoleranz mit dynamischer Redundanz und cold standby ist normalerweise für mechatronische Systeme geeignet, bei denen mehr gemessene Signale existieren, eingebettete Rechner bereits vorhanden sind, und deshalb eine Fehlererkennung wesentlich durch die Anwendung von prozessmodellbasierten Methoden verbessert werden kann, siehe [4].

Redundante Strukturen für Drive-by-Wire Komponenten

Hauptsächlich wegen der entstehenden Kosten, des Raumbedarfs und des Gewichtes muss für X-by-Wire Systeme in Kraftfahrzeugen ein geeigneter Kompromiss zwischen dem Grad der Fehlertoleranz und der Zahl der redundanten Komponenten gefunden werden. Im Ge-

gensatz zu Fly-by-Wire Systemen muss (bisher) nur ein einziger Fehler für gefährliche Zustände toleriert werden [5]. Das wird dadurch begründet, dass ein sicherer Zustand im Vergleich zu Flugsystemen leichter und viel schneller erreicht werden kann. Dies bedeutet aber nicht, dass an alle Komponenten von Drive-by-Wire Systemen sehr scharfe Anforderungen an die Fehlertoleranz gestellt werden.

Es können folgende Stufen einer Degradation (Reduzierung des Aufgabenumfangs) unterschieden werden:

Fail-operational (Fehleroperativ) (FO): Ein Fehler wird toleriert, d. h. die Komponente bleibt betriebsfähig nach einem Fehler. Dies ist erforderlich, wenn kein sicherer Zustand unmittelbar nach dem Ausfall einer Komponente existiert.

Fail-safe (Fehlersicher) (FS): Nach einem (oder mehreren) Fehler(n) besitzt die Komponente direkt einen sicheren Zustand (passives fail-safe, ohne externe Energie) oder wird in einen sicheren Zustand gebracht durch eine besondere Aktion (aktives fail-safe, mit externer Energie).

Fail-silent (Fehlerpassiv) (FSIL): nach einem (oder mehreren) Fehler(n) verhält sich die Komponente nach außen hin ruhig, d. h. sie bleibt passiv durch Ausschalten und beeinflusst deshalb nicht die anderen Komponenten in einer möglicherweise falschen Art.

Für Fahrzeuge wird vorgeschlagen, FO in "Langzeit" und "Kurzzeit" zu unterscheiden, [6].

Beispiele für Fehlertolerante Sensoren und Aktoren sind in [7] angegeben.

Integrierte Redundanz

Ein schon heute in der Automobilindustrie verwendeter Ansatz, kostengünstige eigensichere Komponenten zu ermöglichen, besteht darin, nur die ausfallkritischen Strukturen redundant auszuführen, d.h. nur die Teile, die ausfallgefährdet sind und bei Ausfall zu kritischen Auswirkungen führen können. Als Beispiele können Sensoren [8] für das Fahrpedal, die Drosselklappe und das Lenkradmoment einer elektromechanischen Servolenkung genannt werden. Neben der Redundanz eines zweiten Signalaufnehmers wird oft eine Ausführung gewählt, die über Eigendiagnoselogik auch Common Mode Failures erkennen lassen, z.B. durch gegenläufige Signale und Definition von zulässigen Wertebereichen. Diese bewährten Ansätze sind auf X-by-Wire-Systeme zu übertragen, um Ausfallsicherheit wirtschaftlich vertretbar zu erreichen.

Systemzuverlässigkeitsvorhersage

Spätestens bei der Zulassungsbeantragung und der Freigabe von X-by-Wire-Systemen, aber auch vorher schon im Entwicklungsprozess, ist eine vertrauenswürdige Systemzuverlässigkeitsvorhersage vonnöten. Das heute eingesetzte Instrumentarium deckt die bei X-by-Wire eingesetzten gemischten Mechatroniksysteme nur unzureichend ab. So wird das Lastkollek-

tiv mechanischer Komponenten im mechatronischen System stark von der Reglerauslegung beeinflusst. Wenn dann noch dynamische Rekonfigurationsmechanismen eingesetzt werden, wird die Vorhersage nochmals erschwert. Ein für ein redundantes System besonders wichtiger Punkt ist die Vermeidung von Common-Mode und Common-Cause-Failures, da mit diesen die beabsichtigte Aufgabenübernahme durch redundante Komponenten gefährdet ist. Die Besonderheit bei mechatronischen Systemen liegt also in der Multifunktionalität der Komponenten und der damit einhergehenden Wechselwirkungen zwischen den mechanischen, elektrischen, elektronischen und Softwarekomponenten. Bekannte Lastkollektive, die von der Aktion aus Straße und Fahrzeug auf die Reaktion des Subsystems Achse/Fahrwerk schließen lassen, verlieren ihre Bedeutung, da erstmals das Subsystem eine eigene Aktion ausführen kann. Entsprechend gewinnt die Frage nach der Bewertung einer technischen, integrierten Systemzuverlässigkeit an Bedeutung. Dabei geht es um die methodische Beschreibung des Verhaltens der Komponenten im einzelnen sowie insbesondere um die Beschreibung des Einflusses der Komponenten untereinander. Die wesentlichen Fragen sind hier, wie ein Aktor mit reduziertem Leistungsvermögen auf ein Gesamtsystem wirkt, und welche Komponenten dadurch veränderte Lasten ertragen müssen.

Klassische Methoden wie die FMEA, die Fehlerbaum-Analyse, die Markhoff-Theorie u.a. liefern hierzu nur qualitative Aussagen. In Verbindung mit der Last- Beanspruchungsanalyse, den Ausfalldaten einzelner Komponenten und vor allem der physikalischen Interaktion zwischen den Komponenten geht es zukünftig um die integrierte Beschreibung des Systemverhaltens und daraus abgeleitet der Bewertung der Systemzuverlässigkeit.

Funktionsverfügbarkeit von X-by-Wire-Systemen

X-by-Wire-Systeme haben nur dann eine Marktchance, wenn sie eine umfassende Funktionalität mit einer sehr hohen Verfügbarkeit verbinden. Allerdings wird aber auch überzogen, wenn für alle Funktionalitäten des X-by-Wire-Systems die gleichen Verfügbarkeitsanforderungen gestellt werden. Das nachfolgende Stufenkonzept ermöglicht eine differenzierte Betrachtung zur Verfügbarkeit des Systems am Beispiel von Steer-by-Wire (Bild 3). Für die oberste Funktionalitätsstufe gelten Verfügbarkeitsanforderungen von

Erweiterte Funktion Steer-by-Wire		
Agilitäts- verbesserung	Stabilitäts- verbesserung	Automatisierte Querführung
Grundfunktion Lenken		
geringer manueller Betätigungsenergiebedarf	keine Beeinträchtigung der Führungsfähigkeit im Normalfahrbereich	
Limp home		
Lenken unter Erschwernis		
Totalausfall		
kein Seitenkraft- aufbau möglich	unkontrollierter Seitenkraftaufbau	

Bild 3: Stufen der Funktionalität eines Steer-by-Wire-Systems von Vollfunktion bis Ausfall

heutigen ABS-Systemen oder der Überlagerungslenkung. Der Ausfall einer Funktion dieser Ebene reduziert zwar den Wert des Fahrzeugs, behindert aber nicht die Verfügbarkeit des Fahrzeugs als Ganzes. Die Grundfunktion ist möglichst lange aufrecht zu erhalten. Als Maßstab für die Verfügbarkeit dienen die Vergleichswerte einer konventionellen Servolenkung. Als Kriterium zur Beurteilung wird die Ausfallwahrscheinlichkeit $F'_{bf}(t_{op})^1$ bei spezifizierter Betriebsdauer t_{op} unter spezifizierter Belastung vorgeschlagen.

Wenn die Grundfunktion nicht mehr für eine hinreichend lange Zeit sicher betrieben werden kann, weil mit einem einzelnen, nicht auszuschließenden Fehler es zum Totalausfall kommen kann, ist eine Einschränkung der Nutzung z.B. durch eine Geschwindigkeitsbeschränkung vorzusehen.

Die stark reduzierte Limp home Funktionalität muss mit einer Verfügbarkeit A_{LH_SB} bereit stehen. Eine niedrigere Zuverlässigkeit kann durch Ausfallerkennung und kurze Instandsetzungszeit ausgeglichen werden. Bei Ausfall der Limp home capability, d.h. bei Ausfall der Fähigkeit, bei einem Fehler in den Notlauf-Betrieb zu wechseln, ist ebenfalls eine Nutzungseinschränkung zu definieren (z.B. niedrige Geschwindigkeiten).

Bei Eintritt des Limp-Home-Falls ist die zugehörige Restfunktionalität für die Restfahrstrecke x_r bzw. Restbetriebsdauer t_r mit einer Ausfallwahrscheinlichkeit von F'_{LH} zu gewährleisten.

Ist die Fahrzeugverfügbarkeit grundsätzlich gefährdet (z.B. Ausfall Bordnetz), so muss aus jedem Funktionszustand ein Shutdown-Prozess möglich sein, d.h. eine Restfunktion für kurze Dauer und ggf. mit aktiv eingeleiteter Abbremsung in den Stillstand.

Für alle Übergänge gilt es, ein Übergangsverhalten zu definieren, das gefährliche Fahrzeugreaktionen möglichst ausschließt. Mit dem beschriebenen Stufenkonzept kann die Architektur des X-by-Wire-Systems angepasst werden, so dass z.B. eine Komponente, die eine Funktion der obersten Ebene ausführt und in dieser Funktion nicht durch Redundanz unterstützt wird, als cold- oder hot standby für eine Basisfunktion dienen.

Softwareentwicklung

Die Erstellung qualitativ hochwertiger und insbesondere "sicherer" Software spielt bei der Entwicklung von X-by-Wire-Funktionen eine weitere Schlüsselrolle. Die traditionell eingesetzten lastenheft- und codezentrierten Softwareentwicklungsverfahren sind oft unpräzise und unvollständig. Darüber hinaus stehen sie erst spät für Tests zur Verfügung. Die Probleme drücken sich auch in dem hohen Anteil von Spezifikationslücken heutiger Entwicklungen aus, die, wie in [9] berichtet wird, Ursache für etwa 40% der Software-Fehler sein sollen. Diese

¹ Die Werte für diese und folgende Größen sind dabei ebenfalls noch mittels Vergleich mit dem Stand der Technik zu ermitteln.

Defizite führen neben anderen Gründen zur Hinwendung zu neuen modellbasierten Verfahren.

Mit Hilfe eines CASE-Tools (CASE = Computer Aided Software/System Engineering) wird die mit der Software darzustellende Funktion abstrakt und grafisch beschrieben, in dem eine geeignete Struktur und das gewünschte Verhalten modelliert wird. Das ausführbare Modell dient als Prototyp und wird als Vorlage für die Implementierung herangezogen, die u.U. auch automatisiert per Code-Generierung direkt aus dem Modell erfolgen kann. Damit ersetzt oder ergänzt das Modell das traditionelle statische Lastenheft. Die mit Hilfe des Modells bereits in frühen Entwicklungsphasen möglichen Funktionstests (Rapid Prototyping) erlauben eine frühzeitige Absicherung des angewendeten Konzeptes. Man spricht in diesem Zusammenhang von einem ausführbaren Lastenheft. Darüber hinaus erlaubt die modellbasierte Softwareentwicklung u.a. die

- systematische Bestimmung von Testfällen für die spätere Implementierung
- die formale Verifikation bestimmter Softwareeigenschaften und die
- systematischere Ableitung von "On-Board"-Diagnosefunktionen

Eine zweite wichtige Voraussetzung für die effiziente Entwicklung eines komplexen Softwaresystems ist seine Zerlegung in (relativ) einfache Bausteine. Diese Komponenten lassen sich unabhängig voneinander testen und können bei der Entwicklung anderer Systeme einer Produktfamilie wieder verwendet werden, so dass sowohl die Entwicklung des aktuellen Systems als auch die zukünftiger Varianten vereinfacht wird. Zudem können solche Systeme durch den Austausch einzelner Komponenten leichter gewartet und durch Hinzufügen neuer Komponenten ggf. sogar zur Laufzeit erweitert werden. Die komponentenorientierte Modellierung wird zwar heute schon in der Automobilindustrie eingesetzt, z.B. mit Hilfe der proprietären CASE-Tools wie z.B. ASCET-SD [10] oder Matlab [11]. Alternative Entwicklungsrichtungen setzen auf UML (Unified Modeling Language), aber erst in der für 2004 angekündigten Version 2.0 wird die Modellierung mit logischen Komponenten auch in Standard-UML möglich. Allerdings zeigen die bisherigen Erfahrungen mit dem Einsatz von UML1.5-Erweiterungen (z.B. UML/RT [12]) und den oben genannten proprietären Modellierungsansätzen, dass für die Modellierung und Realisierung ausfallsicherer "X-by-Wire"-Software folgende Probleme bislang nicht gelöst sind:

- Statechart-Modelle realer Softwaresteuerungen sind meist außerordentlich umfangreich und vermischen die Realisierung von Normalverhalten, Konsistenzprüfungen (für integrierte Redundanz) und Reaktionen auf Fehlverhalten: solche Modelle sind schwer verständlich, kaum wartbar und bilden keine geeignete Basis für die Erstellung vertrauenswürdiger, oft hochkomplexer Software für fehlertolerante X-by-Wire-Systeme. Die getrennte Betrachtung verschiedener Aspekte einer Steuerung und die anschließende Verschmelzung zu einem

ausführbaren Modell - sei es mit den Hilfsmitteln der aspektorientierten Modellierung oder dem Einsatz spezieller Entwurfsmuster [13] – bietet hier einen Ausweg.

- Des Weiteren legen die bisher verwendeten Modellierungsansätze den Schwerpunkt auf die Beschreibung statischer Komponentenmodelle. Für fehlertolerante und dennoch kostengünstige X-by-Wire-Systeme außerordentlich wichtige dynamische Rekonfigurationsprozesse lassen sich allenfalls auf einer sehr implementierungsnahen Ebene erfassen und entziehen sich damit der modellbasierten Softwareentwicklung mit all ihren früher diskutierten Vorteilen. Hier sind neue regelbasierte visuelle Modellierungsansätze und deren Verschmelzung mit den Ausdrucksmitteln der UML gefragt, wie sie etwa von Graphtransformationssprachen zur Verfügung gestellt werden [14].

- Darüber hinaus ist die Integration datenflussorientierter Modellierungselemente, die bei der Entwicklung von Reglerprozessen in eingebetteter Software bevorzugt wird, in künftige Versionen der UML nicht in Sicht. Hier sind pragmatische Ansätze wie in [15] beschrieben oder weiter tragende Initiativen in Richtung Integration hybrider Modellierungsansätze in die UML gefragt, um so X-By-Wire-Systemen mit ihren einerseits kontinuierlichen Regelungsprozessen auf der einen Seite und diskreten Zustandsübergängen etwa in Folge dynamischer Rekonfigurationen gerecht zu werden.

- Schließlich gibt es noch viele offene Fragestellungen auf dem Gebiet des modellbasierten Tests von Software. So sind insbesondere die Definition modellbasierter Testüberdeckungsmaße für hochsicherheitskritische Software oder der Einsatz domänenspezifischen (X-By-Wire-)Wissens zur halbautomatischen und damit systematischeren Ableitung sinnvoller Testfälle aus erstellten Softwaremodellen aktuelle Forschungsthemen [16]. Gängige Forderungen für Testüberdeckungsmaße sicherheitskritischer Software im Eisenbahnwesen oder in der Luftfahrt orientieren sich ausschließlich an den Kontrollstrukturen imperativer Programmiersprachen und lassen sich damit kaum (unverändert) für die objektorientierte oder komponentenorientierte (modellorientierte) Softwareentwicklung einsetzen.

Mensch-Maschine-Interaktion

Die Gestaltung der Mensch-Maschine-Interaktion ist einerseits Herausforderung und bietet andererseits eine große Chance. Zunächst gilt es, die Bedienbarkeit und das Bediengefühl gegenüber heute gewohntem nicht zu verschlechtern. Andererseits bietet das X-by-Wire-Prinzip die erweiterten Möglichkeiten einer völlig neuen Bediencharakteristik wie sie in Forschungsprototypen mit Sidestick-Lenkung schon erprobt wurden [17]. Bisher ist aber noch offen, wie viel Änderung gegenüber heute gewohnter Charakteristik noch kompatibel ist mit der Mehrzahl der Fahrer, die von der herkömmlichen Art der Betätigung geprägt ist. Ein anderer Aspekt der Mensch-Maschine-Interaktion betrifft das Verhalten bei Funktionsdegradation, wie z.B. bei einem Teilausfall des Systems. Damit wird vor allem das Redun-

danzkonzept berührt, das die potenziellen Reaktionen des Fahrers auf die vorgesehenen Degradationsübergänge und –zustände mit zu berücksichtigen hat.

6. Technische Übergangslösungen

Gerade das als besonders kritisch angesehene Steer-by-Wire wird durch aktuelle Technikentwicklungen [18] stark gefördert. So ist mit der elektromechanischen Servolenkung (EPS) ein mechatronisches System im Einsatz, das zwar nicht fehlertolerant sein muss. Aber die Anforderungen bzgl. Absicherung gegen aktive Fehlfunktionen, wie sie durch Hard- und Softwarefehler ausgelöst werden könnten und zu unbeabsichtigten Lenkaktionen führen würden, sind vergleichbar mit Steer-by-Wire-Anforderungen. Allerdings sind diese EPS noch nicht so komplex wie Steer-by-Wire. Ähnliches gilt für die 2003 eingeführte Lenkwinkelüberlagerung. Das mit der Entwicklung dieser Systeme verbundene Know-how ist von kaum zu überschätzendem Wert für die Entwicklung von zuverlässigen Steer-by-Wire-Komponenten, denn die Felderfahrung mit diesen Komponenten ermöglicht eine erheblich leichtere Zuverlässigkeitsprognose und bietet Zugriff auf ausgereifte Komponenten.

In einem, wenn auch geringeren Umfang wie bei Full-X-by-Wire werden in den aktuellen und zukünftigen Brems- und Lenksystemen Funktionen verwirklicht, die sowohl Erfahrungen zur Wirkung auf den Nutzer liefern als auch auf X-by-Wire-Systeme übertragbare Kenntnisse über die mit den Funktionen verbundenen Algorithmen und Komponenten. Beispiele sind die aktive Beeinflussung des Lenkradmoments, die variable Lenkübersetzung oder weiterentwickelte Bremsassistentenfunktionen.

Am weitesten scheint die Entwicklung der für X-by-Wire geeigneten Datenbussysteme gediehen zu sein. Mitte bis Ende der neunziger Jahre mit Ziel eines X-by-Wire tauglichen Datenbusses angeschobene Entwicklungen stehen vor dem Abschluss, so dass voraussichtlich spätestens ab 2005 zwei von schwergewichtigen Konsortien getragene Time-Triggered-Datenbussysteme (TT-CAN [19], FleyRay [20]) zur Verfügung stehen.

Die allgemein bekannten, verallgemeinert *Elektronikprobleme* genannten Ausfälle hochkomplexer Fahrzeuge bewirken zurzeit ein Überdenken der Entwicklungsmethodik. Als Folge dieser (Rück-)Besinnung des Vorrangs von Zuverlässigkeit vor Funktionsumfang werden neue Methoden entwickelt und vor allem auch ausprobiert, die einem späteren Entwicklungseinstieg für Brake- und Steer-by-Wire erheblich erleichtern werden.

7. Ausblick

Die aktuelle Entwicklungspause gibt der Forschung eine große Chance, vor der hektischen, vom Time-to-Market-Gedanken geprägten Entwicklungsphase des zweiten Anlaufs, Grundlagen zu erarbeiten, die die besonderen mit X-by-Wire für Bremse und Lenkung verbundenen Herausforderungen leichter bestehen lassen. In einer Fachbereiche übergreifenden Zu-

sammenarbeit werden an der Technischen Universität Darmstadt Arbeiten zu X-by-Wire durchgeführt, die genau dieser Grundlagenlücke Rechnung tragen. Mit einer sowohl Methoden als auch beispielhafte Lösungen hervorbringenden Forschungsarbeit wird es, zusammen mit der forcierten Einführung von Fahrerassistenzsystemen, gelingen, X-by-Wire beim nächsten industriellen Anlauf erfolgreich zur Serie zu führen. Vorher schon werden aber einige Erkenntnisse auch in Übergangslösungen oder in ganz andere Technikbereiche einfließen.

8. Literatur

- [1] IEC 6: Normenentwurf IEC 61508, Part 1-7. Functional Safety of E/ E/ PES: (complex) Electrical/ (complex) Electronic/ Programmable Electronic Systems. Version 4.0. 1997
- [2] Isermann, R.: Fehlertolerante Komponenten für Drive-by-wire-Systeme. 10. Internationaler Kongress "Elektronik im Kraftfahrzeug" 27/28.09.2001, Baden-Baden. VDI-Bericht Nr. 1646, 2001
- [3] ESACS-Homepage: Enhanced Safety Assessment for Complex Systems, url: <http://www.cert.fr/esacs>
- [4] Isermann, R., Modellgestützte Diagnose im Kraftfahrzeug. MTZ/ATZ Autotomotive Electronics 2000, (Sonderheft), S. 92-99
- [5] Schunck, E.: Das Sicherheitskonzept einer elektrohydraulischen Bremse, in VDA Technischer Kongress 1999, Frankfurt, Germany
- [6] Reichart, G.: Sichere Elektronik im Kraftfahrzeug, Automatisierungstechnik, vol. 46, no. 2, pp. 78-83., 1998
- [7] Isermann, R., Schwarz, R., Stölzl, S. (2002): Fault tolerant Drive-by-Wire Systems, IEEE Control Systems Magazine, Oct. 2002, p.64-81,
- [8] Robert Bosch GmbH: Autoelektrik/Autoelektronik, 4. Auflage, Vieweg-Verlag, 2002.
- [9] Hellberg, C.; Kock, P.; Beineke, E.; Keutmair, J.: Test von Steuergerätenetzwerken in Nutzfahrzeugen, VDI Berichte Nr. 1504, Nutzfahrzeuge, 1999, S. 63-71
- [10] ETAS, ASCET-SD, http://www.etas.info/html/products/ec/ascetsd/de_products_ec_ascetsd_index.php, 2002
- [11] Mathworks, Matlab, <http://www.mathworks.com/products/matlab/>, 2002
- [12] Rational, Rose/Realtime, http://www.rational.com/products/rose/real_time/rtrrose.jsp, 2002
- [13] Bichler, L.; Schürr, A.: Objektorientierte Entwicklung eingebetteter (Echtzeit-)Systeme mit UML?, Proc. Ada Deutschland Tagung 2002 - Software für sicherheitskritische Systeme, Magdeburg, März 2002, 11-28

- [14] Blostein, D.; Schürr, A.: Computing with Graphs and Graph Rewriting , in: Software - Practice & Experience, Vol. 29, No. 3, Los Alamitos: IEEE Computer Society Press (1999), 1-21
- [15] Bichler, L.; Radermacher, A.; Schürr, A.: Integrating data flow equations with UML/ Realtime, erscheint in: Real-Time Systems - The International Journal of Time-Critical Computing Systems, Dordrecht: Kluwer Academic Publishers, 2004
- [16] Conrad, M.; Dörr, H.; Stürmer, I.; Schürr, A.: Graph Transformations for Model-Based Testing, Proc. Modellierung 2002, M. Glinz, G. Müller-Luschnat (Hrsg.), GI-Edition Lecture Notes in Informatics P-12, Tutzing, März 2002, Gesellschaft für Informatik (2002), 39-50
- [17] Eckstein, L.: Entwicklung und Überprüfung eines Bedienkonzepts und von Algorithmen zum Fahren eines Kraftfahrzeugs mit aktiven Sidesticks, Fortschritt-Berichte VDI Reihe 12/471, 2001
- [18] Fleck, R.: Methodische Entwicklung mechatronischer Lenksysteme mit Steer-by-Wire Funktionalität, Tagungsband fahrwerk.tech 2003, 11.-12.03.2003 München
- [19] Bosch CAN-Homepage: <http://www.can.bosch.com/>
- [20] FlexRay-Consortium Homepage: URL <http://www.flexray.com>