

Sicherheitsrelevante Systembeurteilung bei einer Neuentwicklung - Am Beispiel: Aktivlenkung-



BMW Group



Systembeurteilung

Überblick



- Neuentwicklung am Beispiel Aktivlenkung
- Risikoanalyse
- Systembeurteilung
- Probandenversuch

Aktivlenkung

Motivation



- Konventionelle Lenksysteme sind ausgereizt; das Potential durch Variation der Handmomente (Servotronic) ist weitgehend erschöpft.
- Fahrleistungspotentiale steigen kontinuierlich; der Zielkonflikt zwischen Fahr- und Geradeauslaufstabilität sowie Handlichkeit lässt sich mit **einer** festen Lenkungsauslegung nur schwer lösen.
- Die Fahrstabilisierung über radindividuelle Bremsen eingriffe wird zunehmend als unkomfortabel empfunden.



Die Überlagerungslenkung verbindet die Vorteile konventioneller Lenkungen mit den Funktionen der by-wire-Systeme.



- Reine by-wire-Systeme sind (noch?) zu komplex, zu teuer und weisen ein synthetisches Lenkmoment auf. Ihre Akzeptanz im Markt ist fraglich.

Aktivlenkung

Funktion



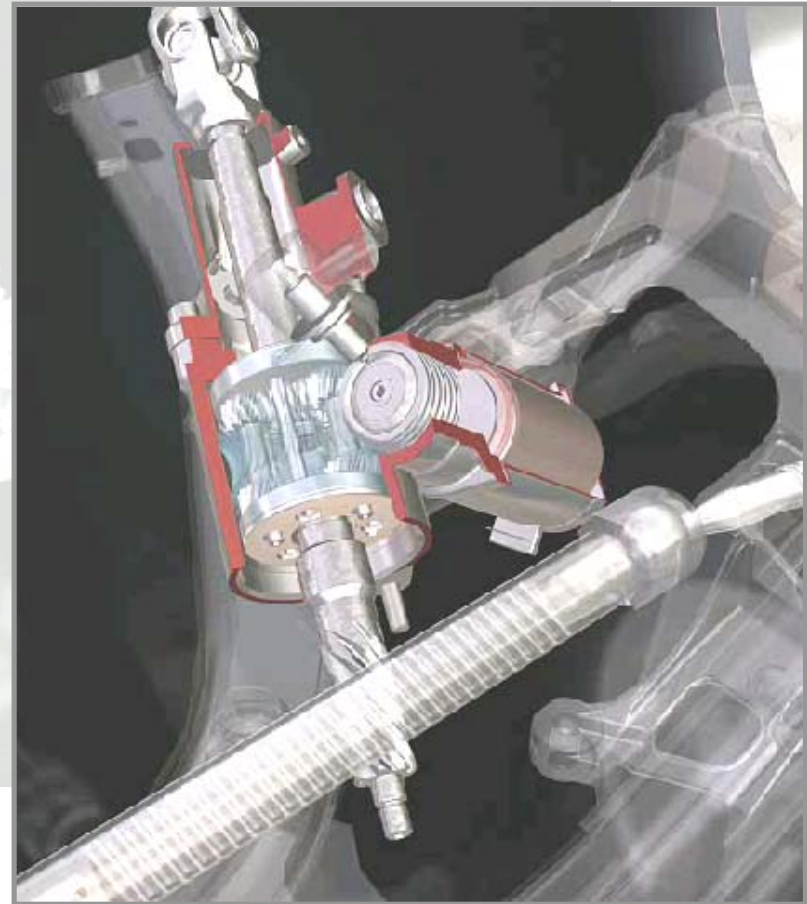
Einführung neuer kundenwertiger Funktionen, um das Handling, die Fahrzeugdynamik und die Stabilität zu optimieren:

Variable Lenkübersetzung

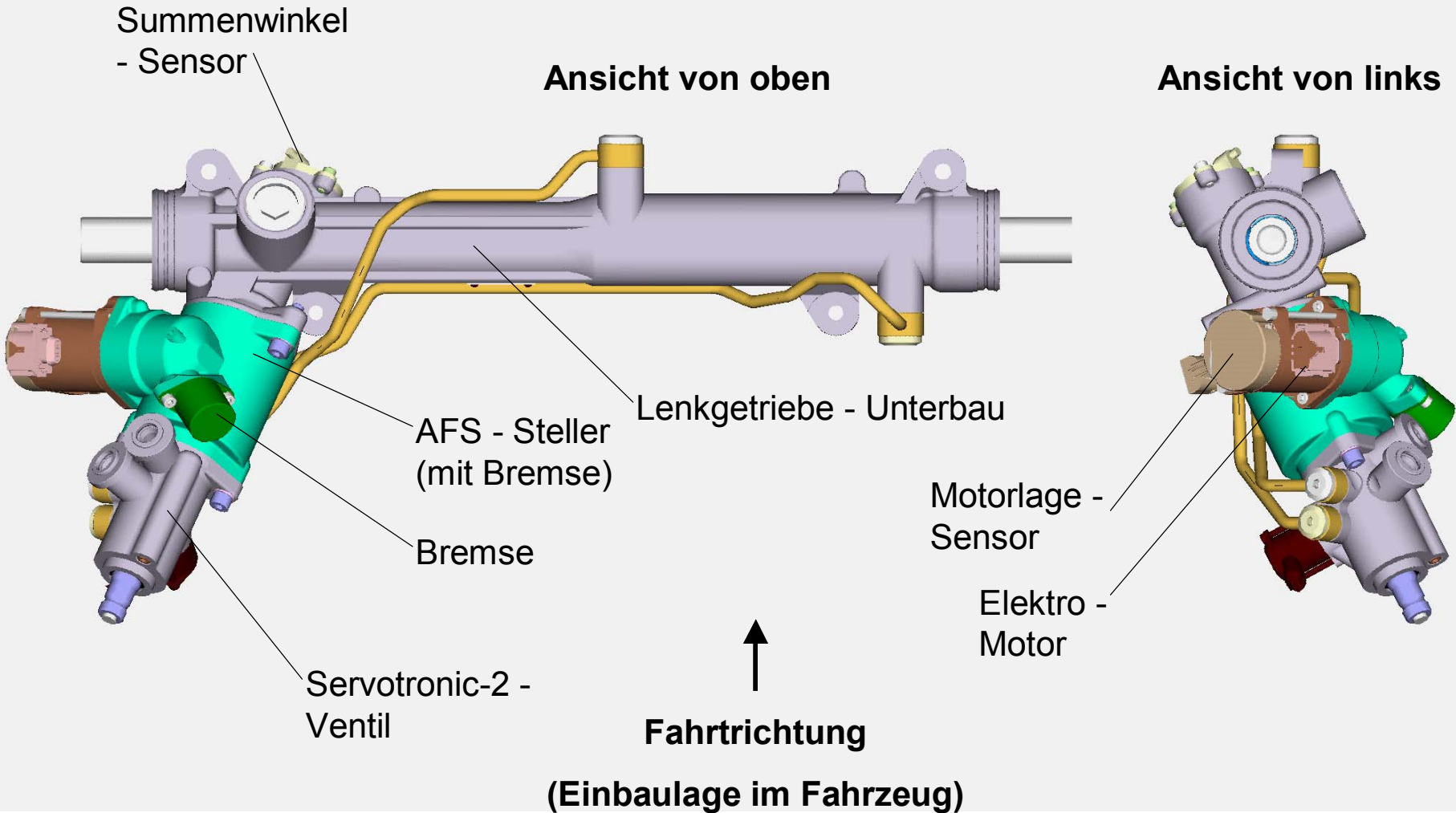
Überlagerter Lenkwinkel =
 $f(\text{Lenkwinkel, Geschwindigkeit})$

Gierratenregelung

Überlagerter Lenkwinkel =
 $f(\text{Lenkwinkel, Geschwindigkeit, Gierrate, Querbesehleunigung})$



Aktivlenkung Mechanisches Layout



Aktivlenkung

Film



Aktivlenkung

Sicherheitskonzept



- Die Aktivlenkung kann konzeptbedingt *fail-silent* ausgelegt werden; d. h., bei einem schwerwiegenden Fehler wird das System abgeschaltet.
- Redundante Signalpfade dienen zur Erhöhung der Verfügbarkeit oder zur schnelleren Erkennung von Signalfehlern.
- Die Systemverfügbarkeit wird durch diverse Funktionsdegradationen erhöht.
- Bei einer Totalabschaltung fällt die Übersetzung auf einen (mechanisch definierten) Mittelwert zurück. U. U. verbleibt ein Lenkradschiefstand.
- Das bei einem Systemausfall veränderte Lenkverhalten wurde von unabhängigen Instituten mit einer repräsentativen Anzahl von Probanden bewertet.
Fahrstabilität und Kursführung wurden dabei nicht bzw. nicht wesentlich beeinflusst. Insbesondere sind die ermittelten Auswirkungen geringer als andere bekannte und akzeptierte Kursstörungen.

Neuentwicklung

Gefahrenanalyse



Gefahrenanalyse und Risikobewertung:

Beschreibung möglicher Fehlfunktionen auf Systemebene

Bewertung der Aufenthaltswahrscheinlichkeit

Bewertung der Kontrollierbarkeit

Bewertung des Schadensausmaßes

Neuentwicklung

Systembeurteilung



Sicherheitsrelevante Systembeurteilung:

Risikobeurteilung bei Ausfall des Systems

Risikobeurteilung bei Ausfall von Eingangssignalen

Tolerierbare Fehlerschwellen

Zustandsübergänge

Systembeurteilung

Risikobeurteilung bei Ausfall des Systems



Wie kritisch ist der Ausfall des Systems?

Wie reagiert das Fahrzeug?

Muss der Fahrer gewarnt werden?

Ist eine Reaktion des Fahrers notwendig?

Wie muss der Fahrer reagieren?

Welche Systeme sind davon noch betroffen?

Systembeurteilung

Risikobeurteilung bei Ausfall von Eingangssignalen



Welche Eingangssignale gibt es?

Welche Auswirkungen haben die Eingangssignale auf die Ausgangssignale?

Welche Auswirkungen haben die Eingangssignale auf Aktuatoren?

Gibt es „sichere“ Ersatzwerte?

Welche Plausibilisierungen sind notwendig?

Systembeurteilung

Fehlerschwellen



Risikobeurteilung bei Fehlaktivierung

Wie kritisch sind einzelne Fehler?

Welche Fehler dürfen wie lange anliegen?

Wie groß dürfen irreversible Fehler sein?

Wie lange dürfen reversible Fehler vorhanden sein.

Wann muss abgeschaltet werden (Latenzzeit)?

Wann muss degradiert werden?

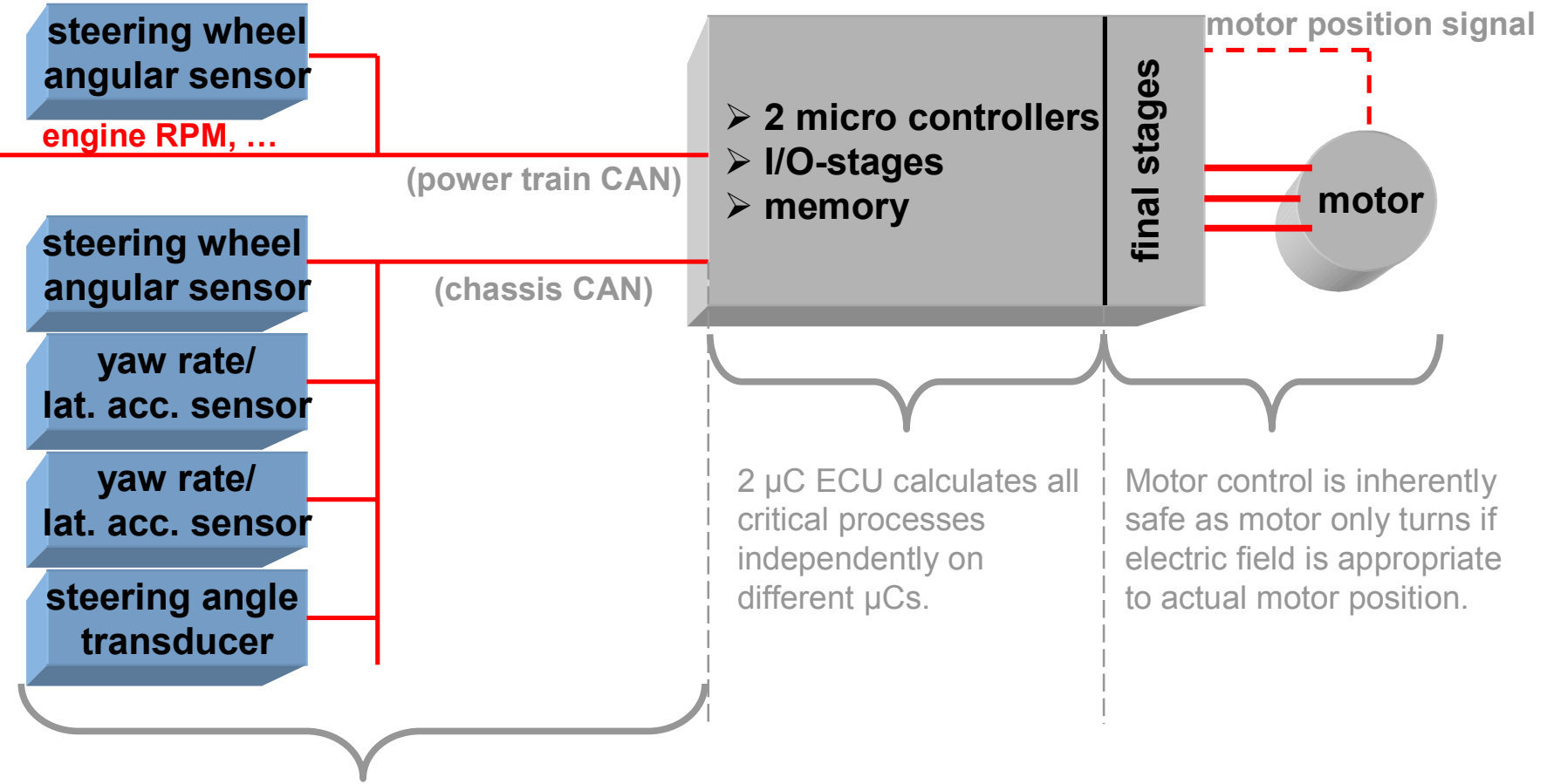
Wie muss degradiert werden?

Systembeurteilung

Zustandsübergänge



Aktivlenkung Sicherheitskonzept



Redundant input signals and independent signal transmission paths ensure fast signal failure detection.

2 μ C ECU calculates all critical processes independently on different μ Cs.

Motor control is inherently safe as motor only turns if electric field is appropriate to actual motor position.

Aktivlenkung Test



Ergebnisse des Probandenversuches:
(In Kooperation mit dem Interdisziplinären Zentrum für
Verkehrswissenschaften an der Uni Würzburg)

- Nachweis des Fail Silent Konzeptes
- Nachweis der Zustandsübergänge
- Nachweis der Fehlerschwellen

Aktivlenkung

Probandenversuch



Aktivlenkung Probandenversuch



Aktivlenkung Probandenversuch



Aktivlenkung Probandenversuch



Aktivlenkung

Probandenversuch



Vielen Dank für ihre Aufmerksamkeit.

