



Funktionale Sicherheit in der Entwicklung von Fahrwerks- und Fahrerassistenz-Systemen: Fokus Systemarchitektur

Dr. Jochen Koepnik, Daimler AG

Dr. Simon Burton, Vector Consulting Services GmbH

Vector Congress, 7./8. Oktober 2008, Stuttgart

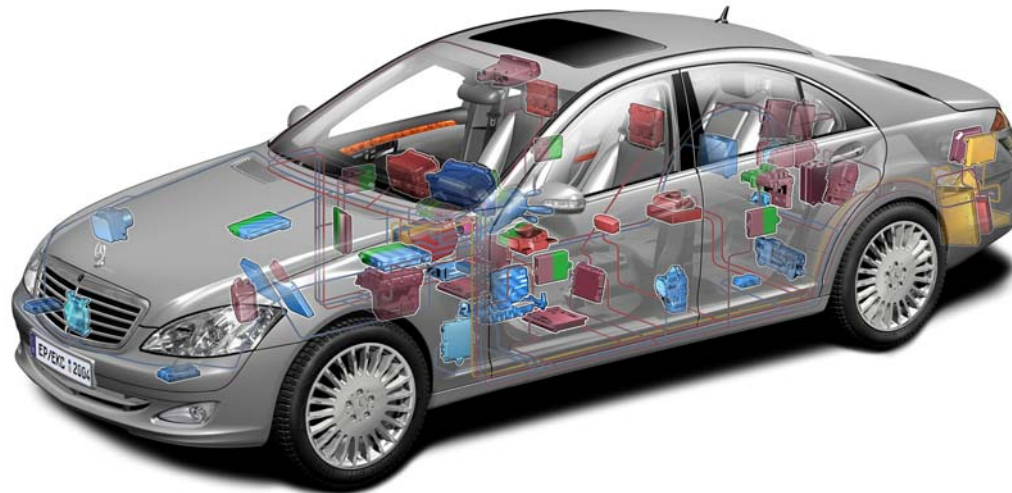
Ziel des Vortrags

- Darstellung, welchen Beitrag Architekturmaßnahmen bei der Umsetzung der Funktionalen Sicherheit leisten können.
- Dabei geht es um die Betrachtung von Architekturaspekten sowohl auf System- als auch Komponentenebene.
- Diskutiert werden Vorgehensweisen, Realisierungs- und Optimierungsmöglichkeiten.

Beispiele für Fahrwerks- und Fahrerassistenz-Systeme

ESP
Elektronische Parkbremse
Aktive Federung/Dämpfung
Elektrische Lenkung

Abstandsregeltempomat
Crash-Bremse
Einparken mit Querführung
Spurhalteassistent



Fahrwerks- und Fahrerassistenzsysteme greifen immer stärker in die aktive Steuerung des Fahrzeugs ein!

Neue Funktionen - neue Gefahren?

- Jede Funktion kann Fehlfunktionen aufweisen, die abzusichern sind.
- Je stärker Funktionen aktorisch eingreifen (Bremse, Lenkung, Antrieb), und je komplexer deren Vernetzung ist, desto größer ist das Potenzial für fehlerhafte gefährliche Eingriffe.

Beispiele für Fehlfunktionen:

Elektrische Lenkung:
Unmotiviertes Lenkmoment bei Fahrt



Spurhalteassistent:
Falsche Eingriffe beim Spurführen



ESP:
Unmotivierter Bremseneingriff bei Fahrt



Einparken mit Querführung:
Falsche Lenkansteuerung beim Parken



Elektronische Parkbremse:
Unmotivierte Aktivierung bei Fahrt



Crash-Bremse:
Unmotivierter Bremseneingriffe bei Fahrt



Die Sicherheitsintegrität von Systemen muss so hoch sein, dass gefährliche Eingriffe in die Fahrzeugführung mit ausreichend hoher Wahrscheinlichkeit vermieden werden.

Funktionale Sicherheit (frei nach ISO 26262)

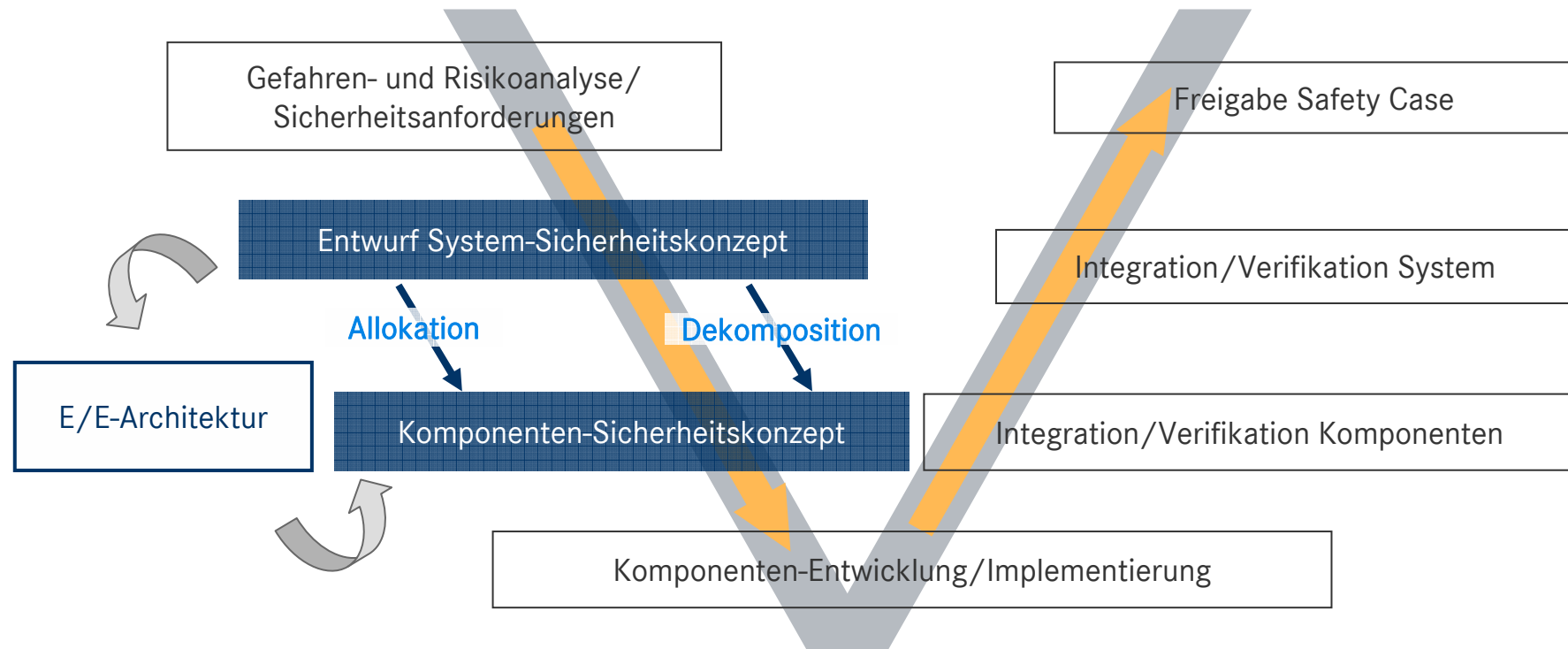
Funktionale Sicherheit zielt auf die korrekte Funktion eines sicherheitsrelevanten E/E-Systems ab. Ziel ist die Vermeidung oder Begrenzung der Auswirkung von gefährlichen systematischen und zufälligen Fehlern in SW bzw. HW.

- Funktionale Sicherheit ist eine Systemeigenschaft und kann nicht allein auf Komponentenebene erzeugt werden.
- Funktionale Sicherheit kann man nur entlang der Wirkketten von potentiellen Hazards diskutieren. Relevant ist das Zusammenwirken der zum System gehörenden Sensoren, Aktoren und Steuergeräte.

Abgrenzung im Vortrag:

Schwerpunkt im Vortrag ist die Behandlung von elektrischen systematischen bzw. zufälligen Fehlern. Eine ggf. vorhandene Unzulänglichkeit in der Spezifikation der Sollfunktion wird hier nicht betrachtet.

Sicherheitskonzept und E/E-Architektur

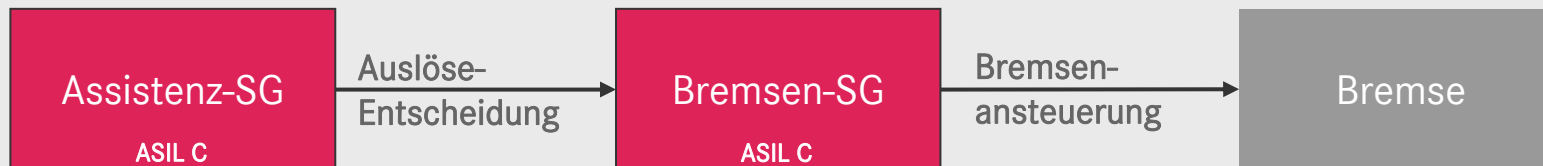


➤ Je nach gewählter E/E-Architektur können sich unterschiedliche Sicherheitskonzepte ergeben .

Der Aufwand für das Erreichen der Sicherheitsziele läßt sich durch ein optimiertes Zusammenspiel von E/E-Architektur und Sicherheitskonzept begrenzen.

Beispiel: Assistenzfunktion mit Bremseingriff

Hazard H1: Unbegrenzte fehlerhafte Vollbremsung bis zum Stillstand: ASIL C



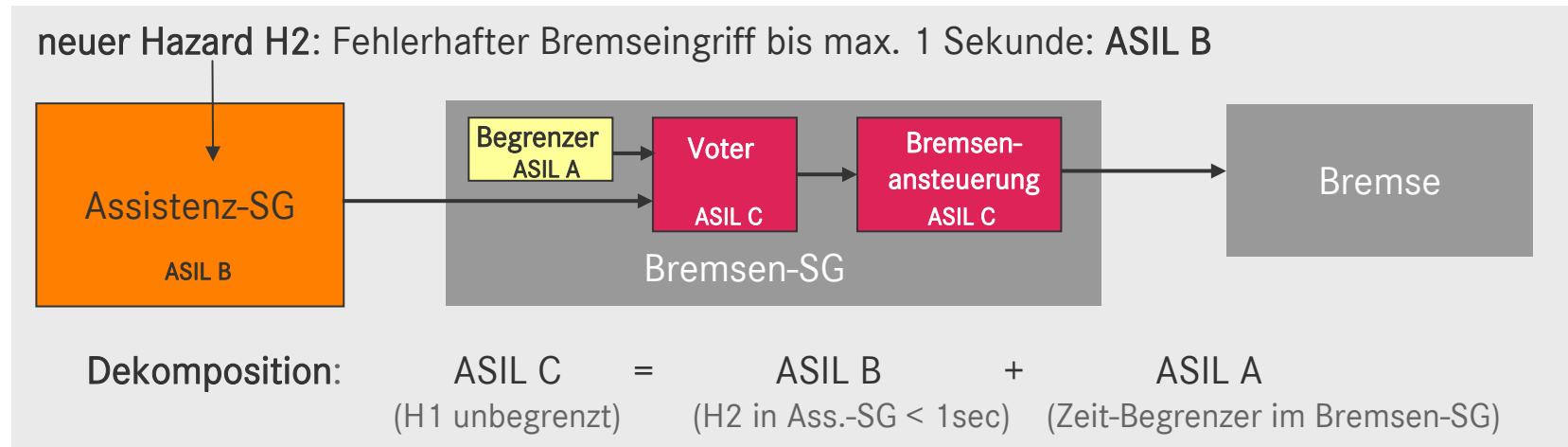
beide SG könnten H1 auslösen: → beide ASIL C

Ziel: möglichst Reduktion des ASIL-Levels des Assistenz-SGs (da neues SG) unter Verwendung der bereits vorhandenen hohen ASIL-Tauglichkeit des Bremsen-SGs.

Lösungsweg:

- Assistenzfunktion in der Eingriffsdauer zeitlich begrenzen, ohne Kundennutzen zu verlieren (z.B. Bremseingriffe begrenzen auf < 1 sec).
- Nachweis, dass für Fehleingriffe < 1 sec die Beherrschbarkeit durch den Fahrer besser wird.
- Falls ja, darf die Assistenz-Logik mit ASIL-B dargestellt werden.
- Die fehlende Integrität zu ASIL C muss durch die Architekturmaßnahme „Zeitbegrenzer“ (auf z.B. 1 sec) abgesichert werden.
- Aufteilen der Funktionalität in Assistenz-Logik und Zeitbegrenzung des Eingriffs.

Beispiel: Assistenzfunktion mit Bremseneingriff



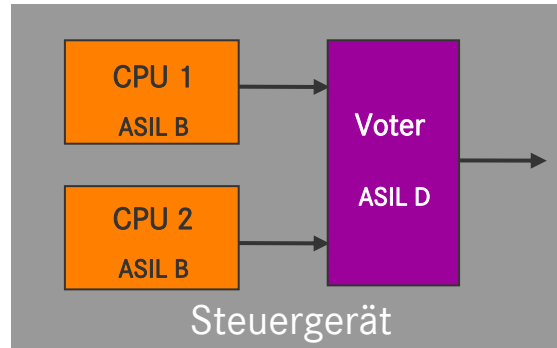
Das Assistenz-SG kann mit ASIL B realisiert werden, während das Bremsen-SG die ASIL-C- Anteile aufnehmen muss und auch kann.

Sinnvolle Funktionseinschränkungen können helfen, den ASIL für einzelne Komponenten zu reduzieren.
 Verteilung der Sicherheitsanforderungen auf Komponenten derart, daß hohe ASIL-Level von neuen Funktionen in Steuergeräten mit bereits hohem ASIL landen.

Homogene Redundanz

- Duplikation einer Sicherheitsanforderung auf ein identisches System
 - Reduktion des ASIL bezüglich zufälliger HW-Ausfälle wird erreicht
 - Der ASIL für systematische Fehler darf nicht reduziert werden (z.B. SW-Entw.-Prozess der Applikation, HW-Entw.-Prozess der Prozessoren)
- Anwendung z.B. bei Dual-Core-Prozessoren,
ansonsten in dieser Reinform im Automotive-Bereich eher selten.

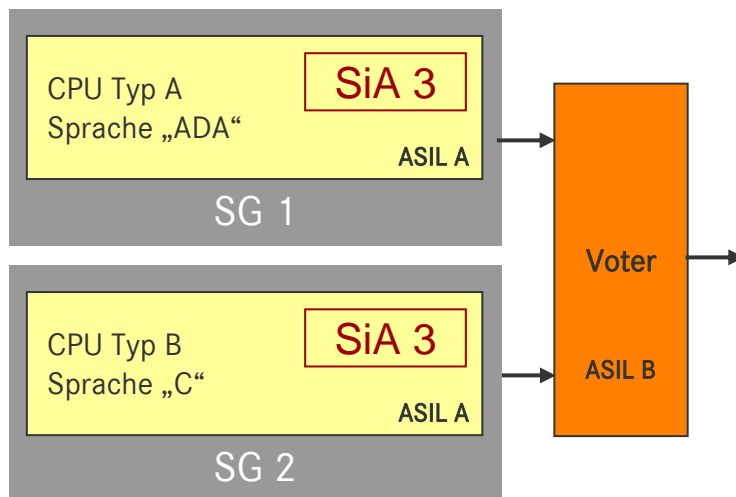
Beispiel:



- Beide CPUs sind identisch.
- Auf beiden CPUs läuft die gleiche Software.
- Der Voter gibt Stellbefehle nur bei identischem CPU-Ergebnis weiter.

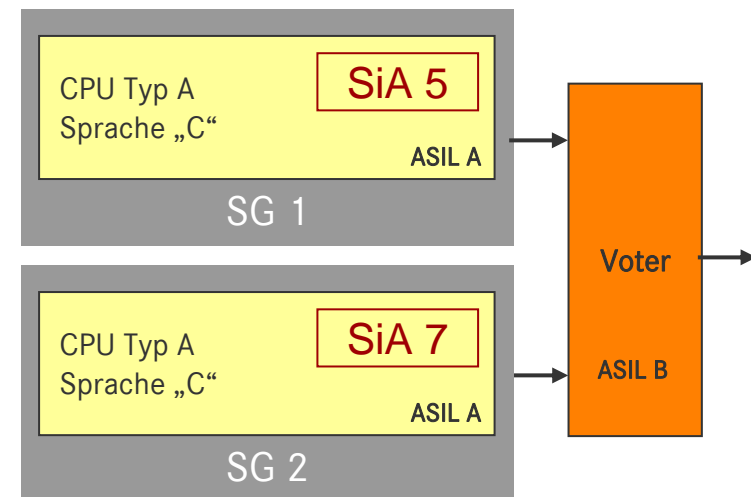
Diversitäre Redundanz

1. Implementierung der gleichen Sicherheitsanforderung auf diversitären Komponenten.



2. Implementierung diversitärer Sicherheitsanforderungen auf gleichartigen Komponenten.

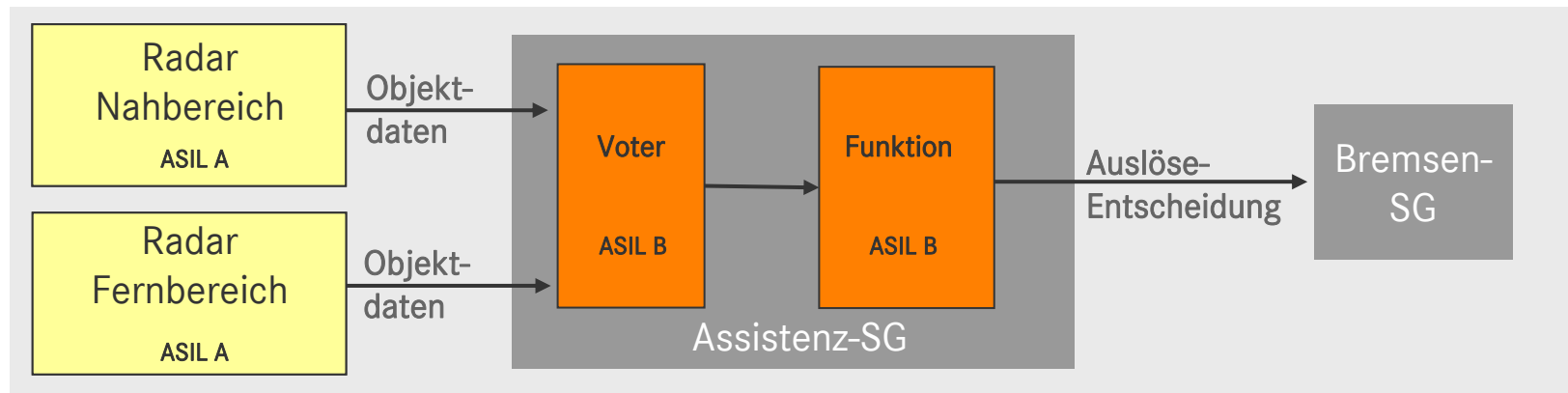
(SiA 5 und 7 müssen dasselbe Si-Ziel erfüllen)



Bei diversitärer Redundanz wird eine Reduktion des ASIL in Bezug auf zufällige HW-Ausfälle und systematische Fehler erreicht.

Beispiel: Sensorik für Assistenzfunktionen

Objekterkennung: Ziel: ASIL-Reduktion für die E/E-Implementierung der Sensoren



Vorgehen zur diversitären Redundanz:

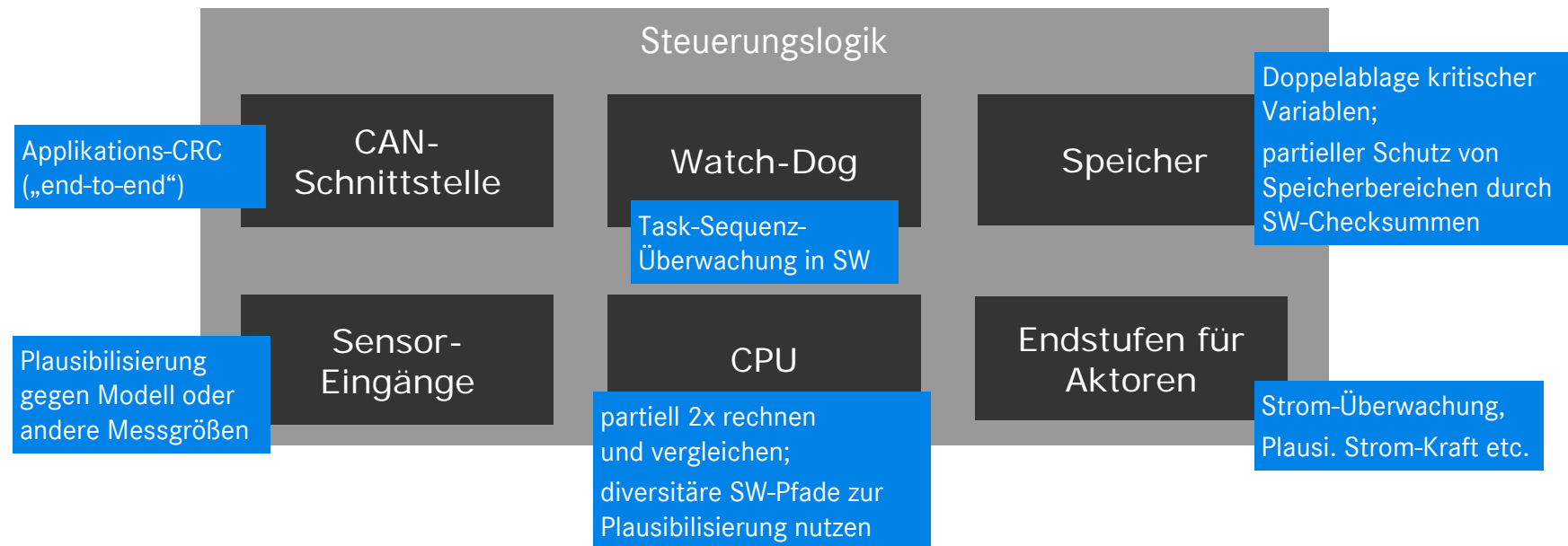
- Redundante Sensoren können aus Funktionssicht für sichere Objekterkennung notwendig sein. Beide Sensoren müssen ein Objekt erkannt haben.
- Dann Nutzung dieser Architektur für die Senkung des Integritätslevels der E/E-Implementierung.
- Beide Sensoren haben ein verschiedenes HW/SW-Konzept und sind in diesem Sinne diversitär.

Einsatz von Redundanzen bei der Dekomposition so wählen, dass vorhandene Komponenten, Übertragungswege und Ressourcen optimal genutzt werden und gleichzeitig die ASIL-Level der Komponenten und Module begrenzt werden.

Absicherung gegen zufällige HW-Fehler innerhalb einer Komponente

Funktionsspezifische Absicherung kritischer Pfade:

- Identifikation kritischer Wirkpfade und Absicherung derselben gegen Fehler.

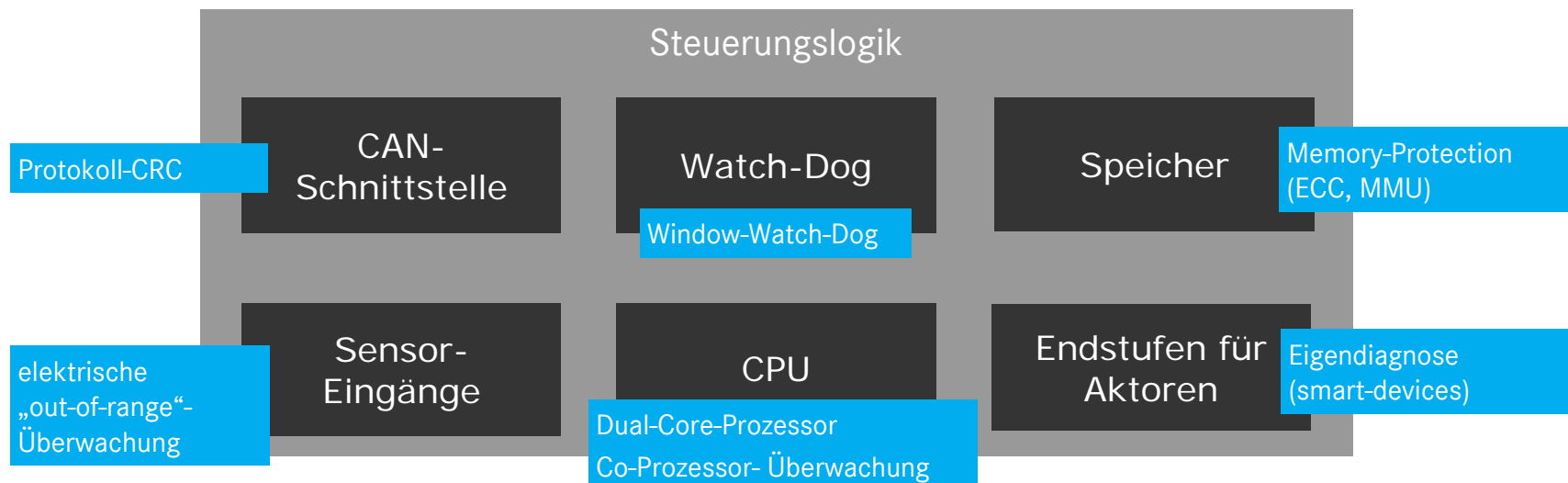


- Vorteil: Preisgünstige Standard-Bauelemente und Prozessoren verwendbar.
- Nachteil: Höherer Aufwand für pfadspezifische SI-Analysen und Absicherungsmaßnahmen.

Absicherung gegen zufällige HW-Fehler innerhalb einer Komponente

Generische Maßnahmen:

- Funktionsunabhängige Absicherung der Hardware gegen gefährliche Ausfälle.

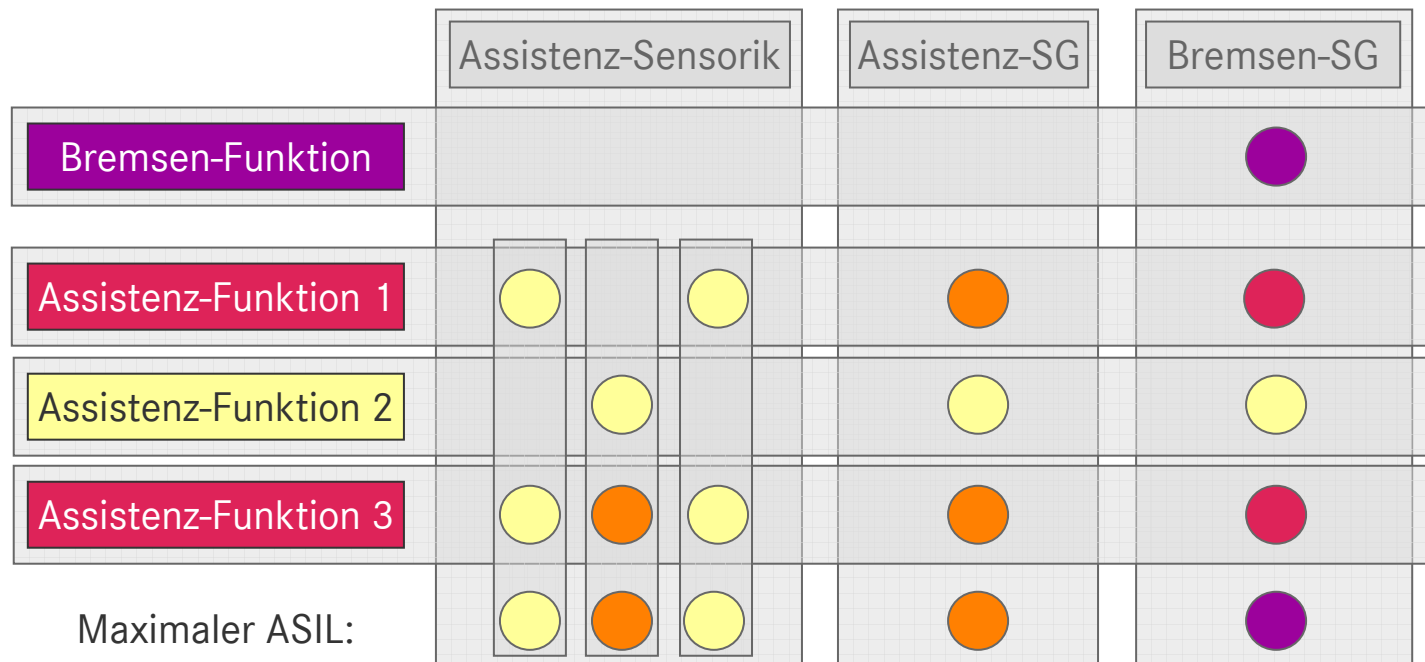


- Vorteil: Einfachere Implementierung komplexer Sicherheitsfunktionen.
- Nachteil: Höhere Kosten von Bauelementen mit generischen Sicherheitseigenschaften.

Trade-off notwendig zwischen generischer und funktionspezifischer Absicherung. Systeme mit hohem ASIL tendieren zu größerem Anteil an generischen Maßnahmen. Ebenso Systeme mit vielen verschiedenen sicherheitsrelevanten Funktionen.

Optimierte Dekomposition und E/E-Architektur

Die Dekomposition neuer Funktionen auf eine vorhandene E/E-Architektur sollte wenn möglich derart sein, daß neue Funktionen die ASIL-Level vorhandener Komponenten nicht erhöhen.



Funktionale Sicherheit kann durch geeignete Architekturmaßnahmen effizient unterstützt werden. Die ASIL-Verteilung im Fahrzeug ist ohne SI-Verlust optimierbar.