Sicherheitskritische Kommunikationssysteme auf dem Prüfstand – ein Zwischenbericht

Klaus Echtle

Verlässlichkeit von Rechensystemen

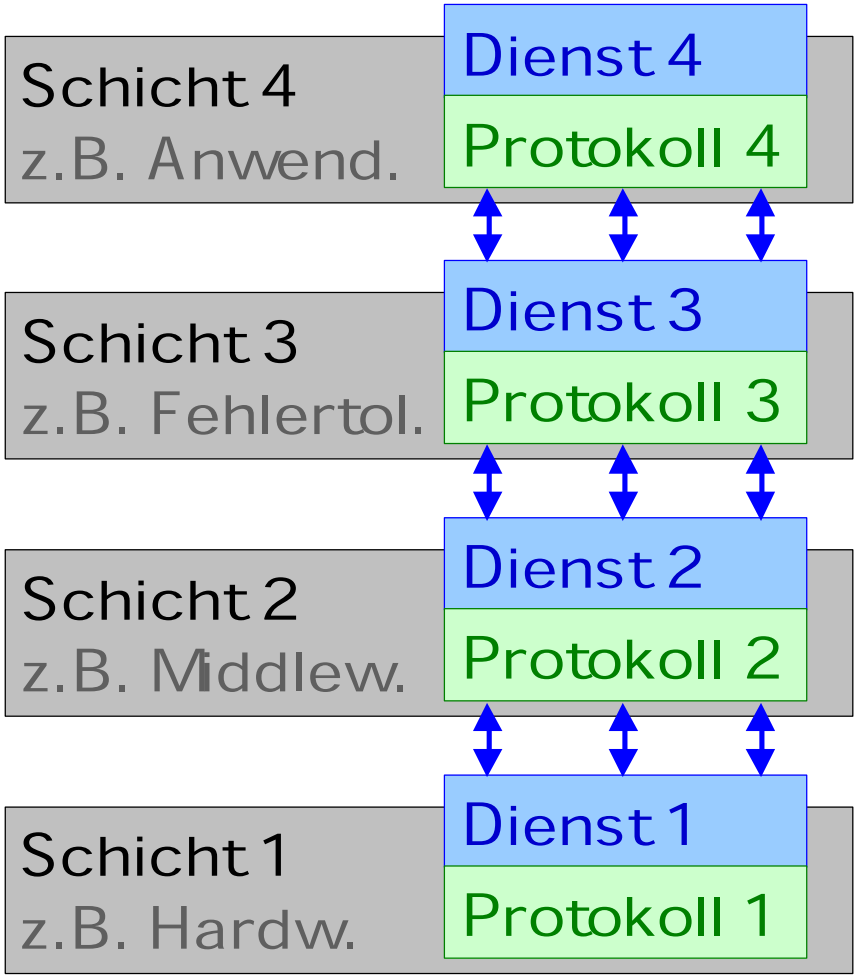
ICB, Universität Duisburg-Essen

Wolfgang Mickisch

Institut für Fahrzeugtechnik

RWTÜV Essen

Schichtenstrukturierte Kommunikation



Wichtig für den Systementwurf:

korrekte Interaktion ?

korrekt auch im Fehlerfall ?

Test ?
Verifikation ?

Überblick

- Projekt FlexBeam
  Institut für Fahrzeugtechnik, RWTÜV, Essen
  Gruppe VR, ICB, Uni Duisburg-Essen
- Simulationsmodell mit Fehlerinjektion
  Verwendung von Entwurfstools
  Test unter Fehlerinjektion
- Modell zur Analyse des Zustandsraums
  Anwendung auf komplexe Protokolle
- Unterstützung des Protokollentwurfs
  Konformität

Projekt FlexBeam

FlexRay Behaviour Model

Institut für Fahrzeugtechnik
RWTÜV, Essen

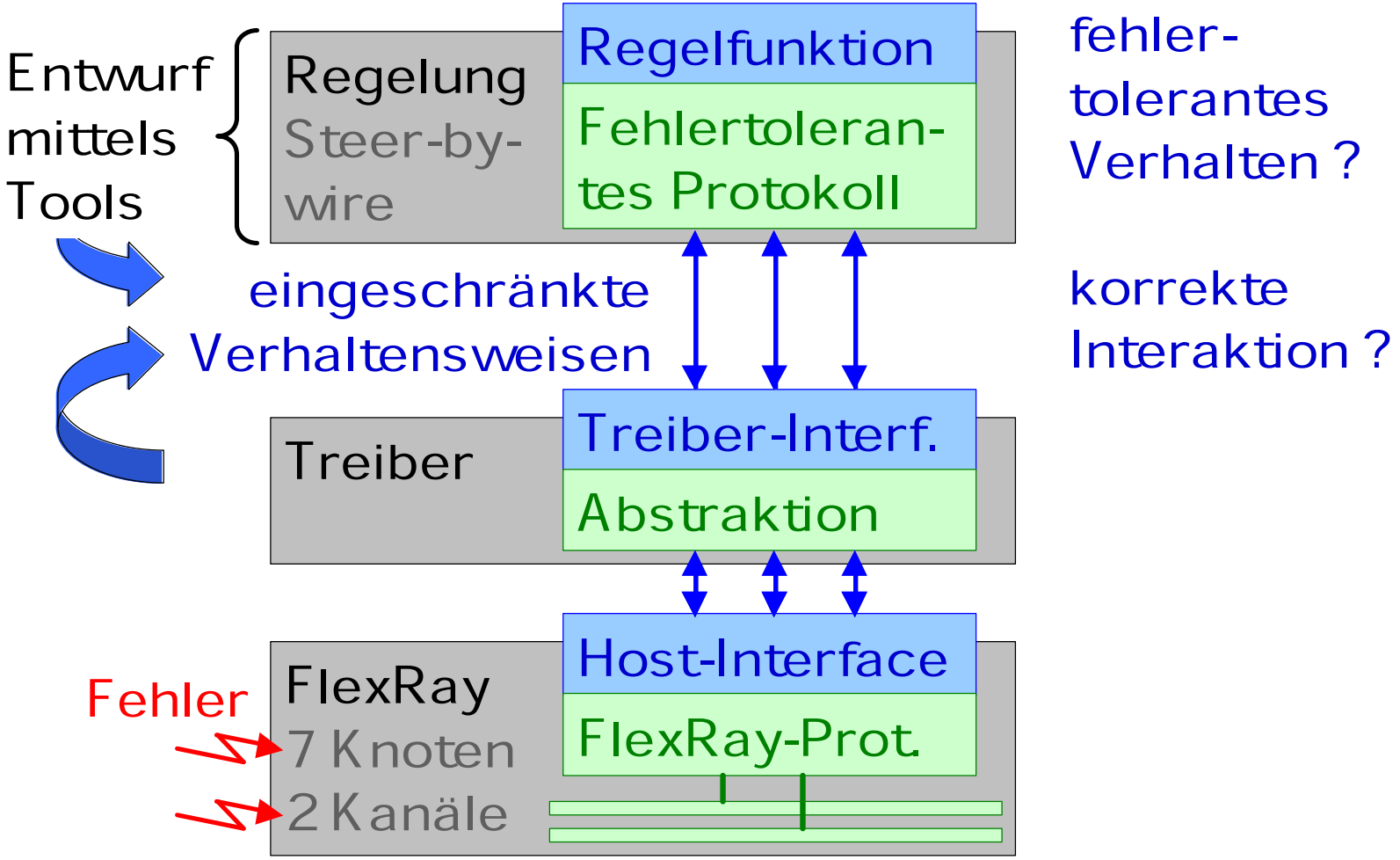
Gruppe „Verlässlichkeit von Rechensystemen“, ICB

Unterstützung für den Entwurf:

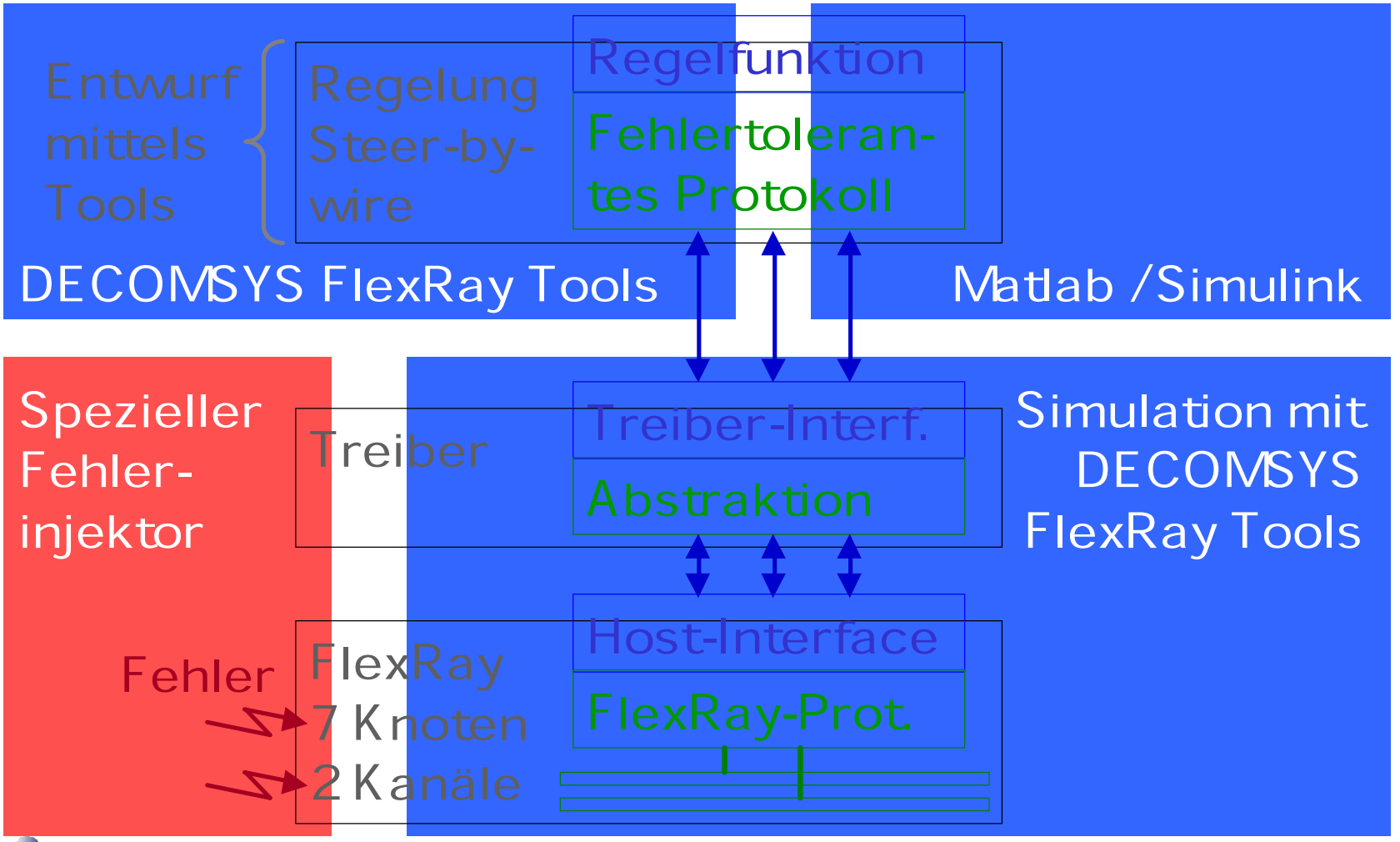
Konformität zwischen kommunizierenden Schichten

Methode 1:	Methode 2:	Methode 3:
Konsistenz-prüfungen, Inspektion	Modell-basierte Analyse	Tool-basierter Entwurf

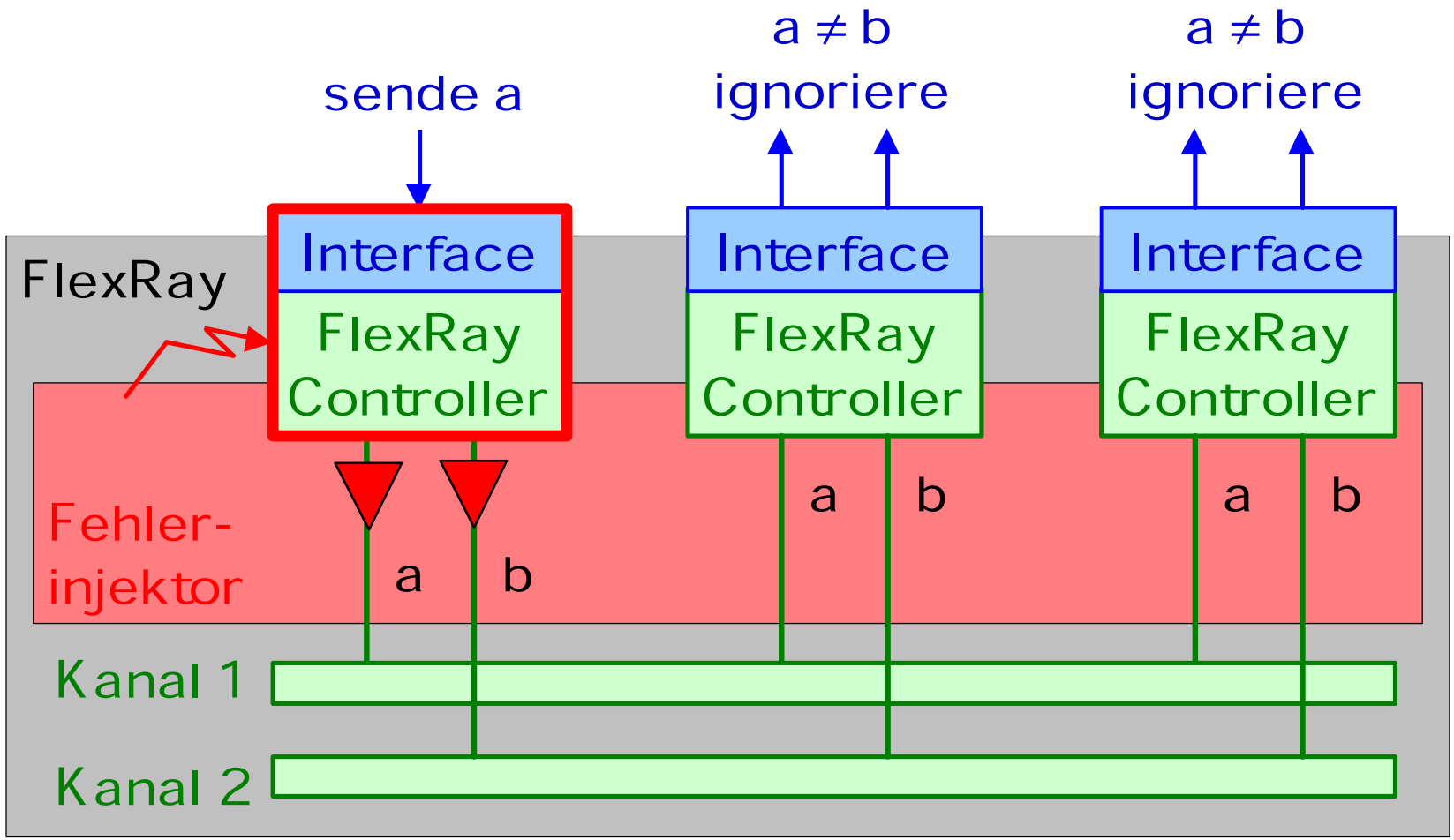
Simulationsmodell mit Fehlerinjektion



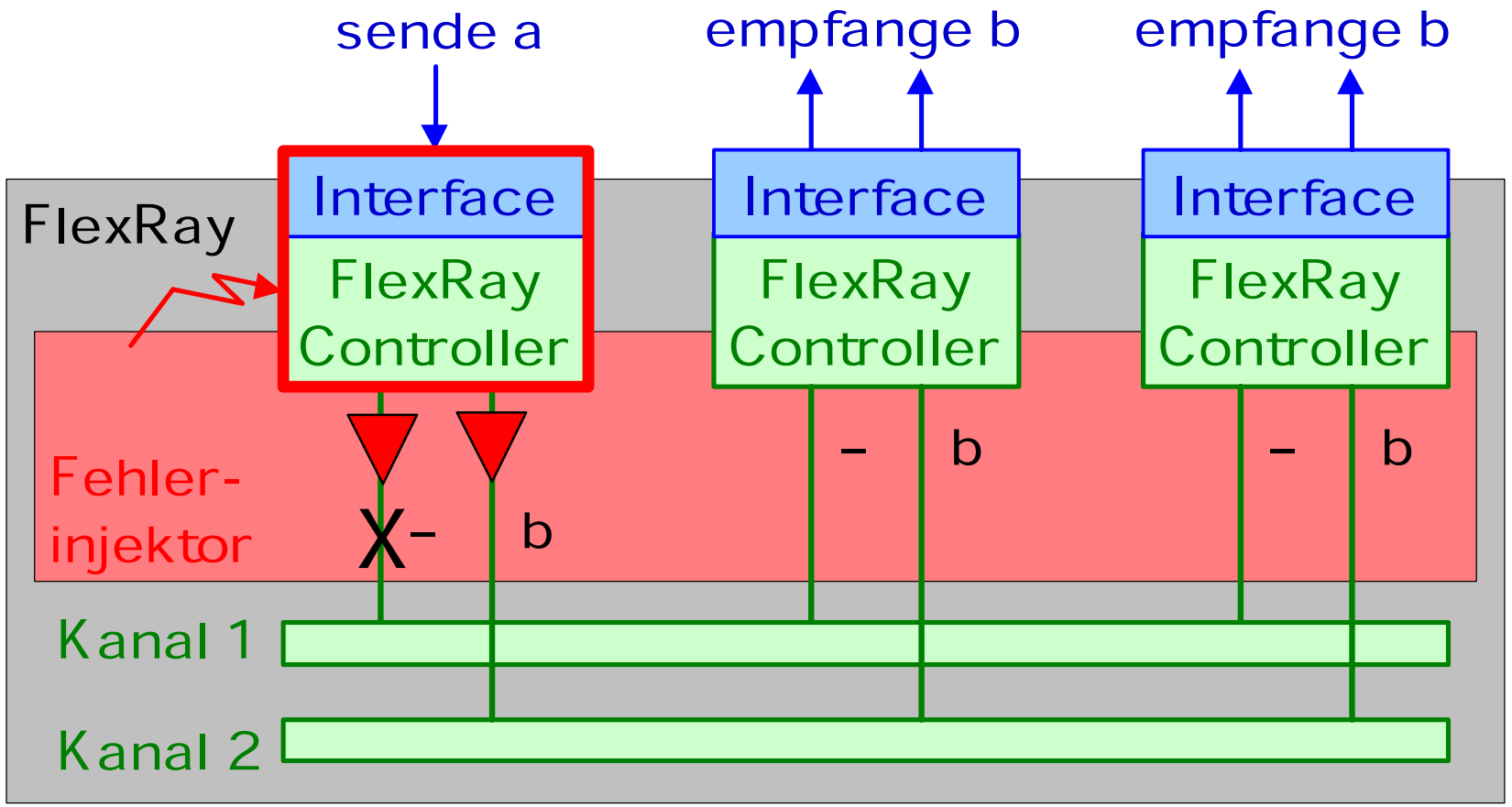
Eingesetzte Tools



Injektion von Knotenfehlern

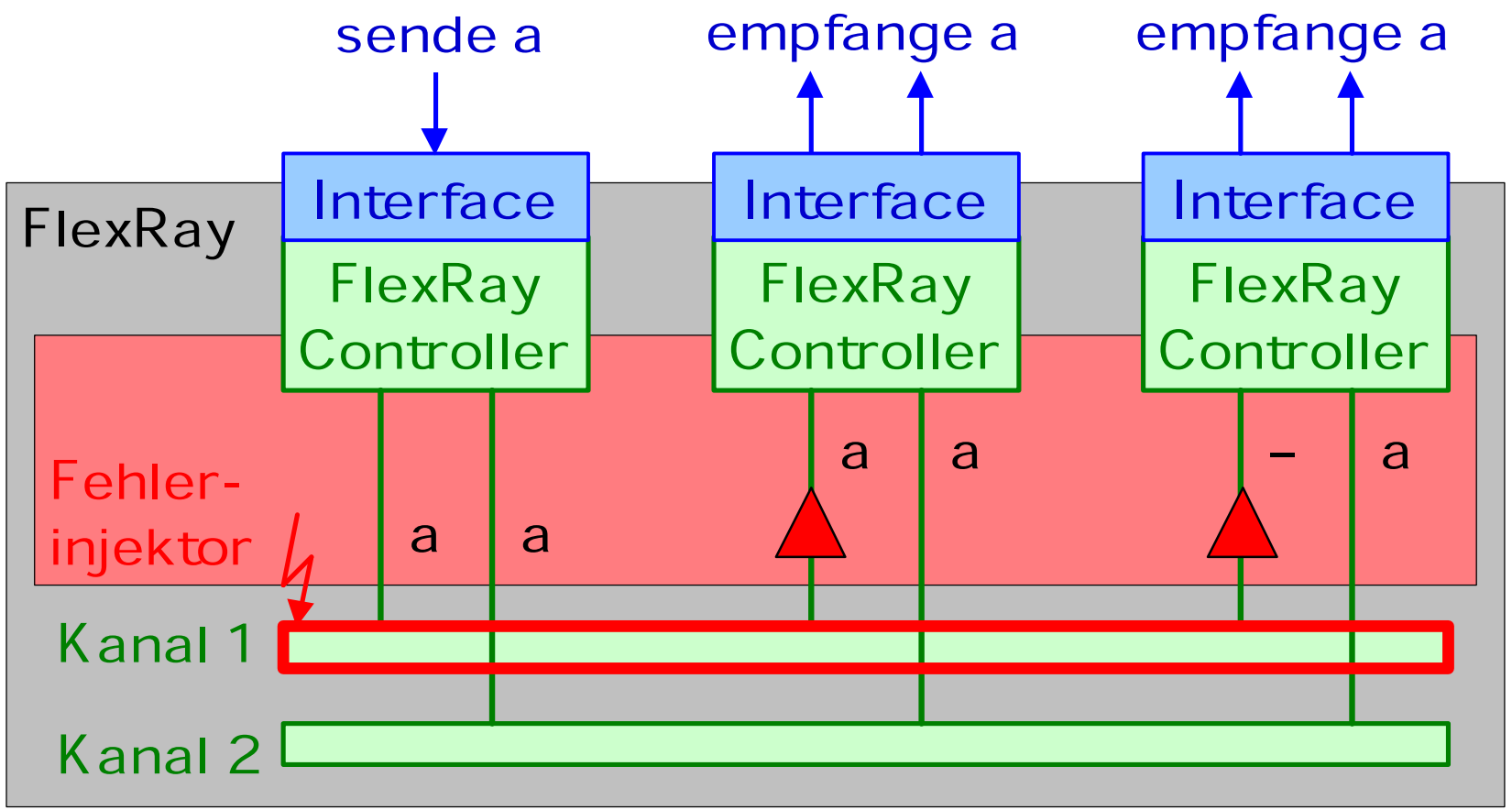


Injektion von Knotenfehlern

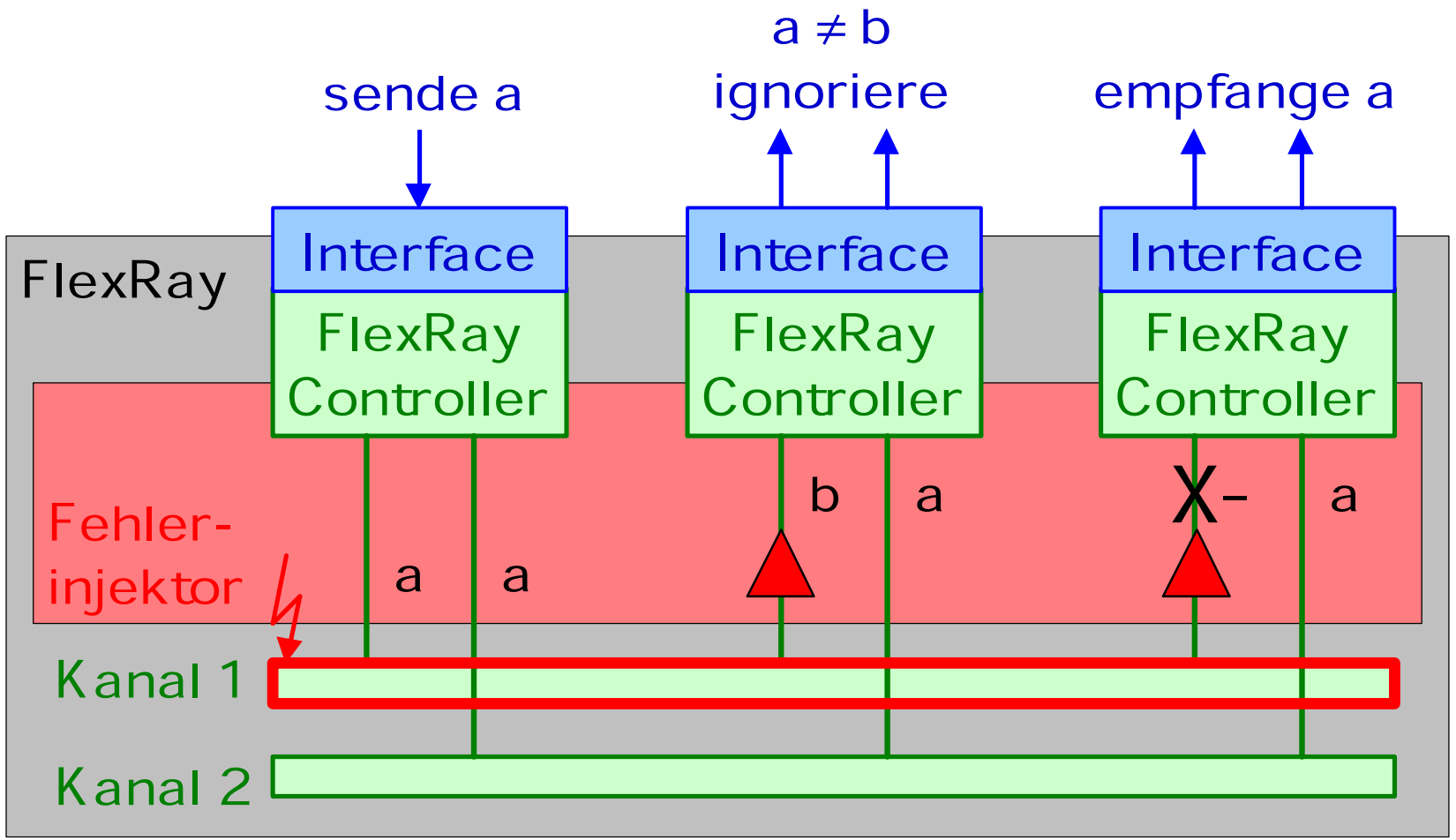


aber keine Verfälschung von fremdsignierten Nachrichten

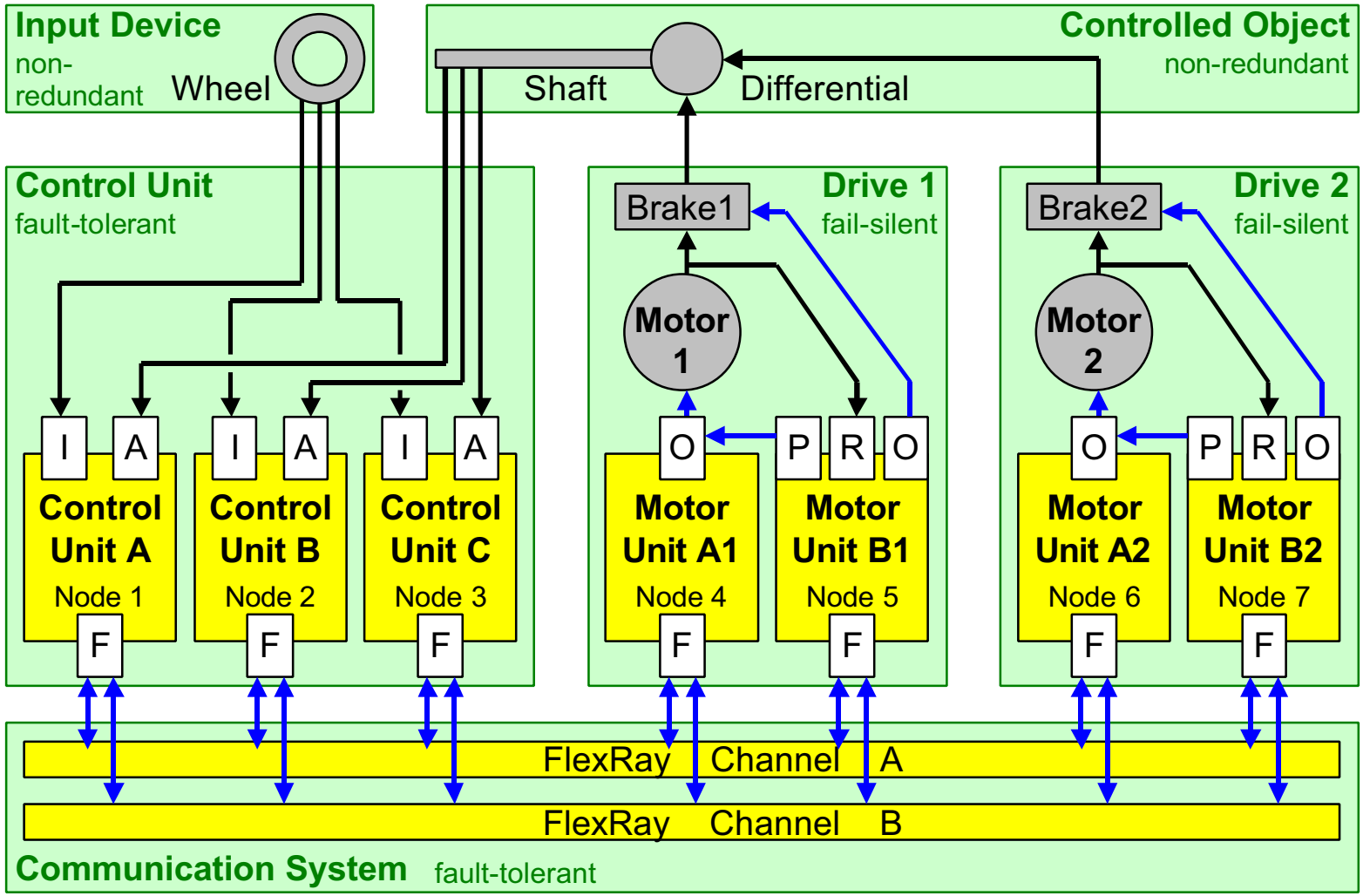
Injektion von Kanalfehlern



zu vernachlässigen, weil extrem selten



Beispielsystem: Steer-by-Wire

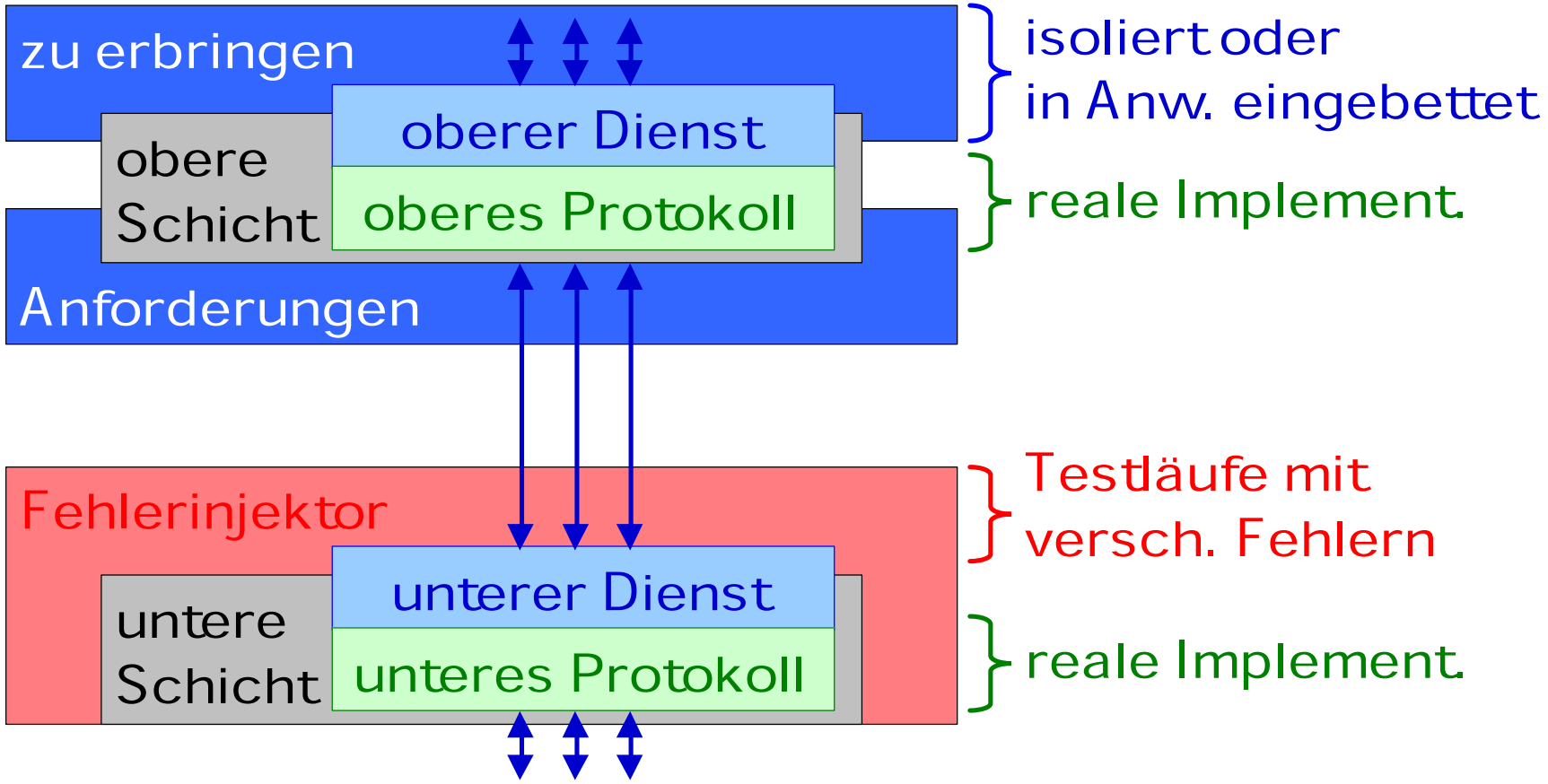


Übergang zu einem realen FlexRay-System

- FlexRay-Hardware
  Controller, Channels
- Steuergeräte als Knoten
  automobiltypisch: Hardware, Betriebssystem
- Beispiel-Anwendung
  X-by-Wire, Lesen von Sensoren,
  Ansteuern von Aktuatoren
- Fehlerinjektor
  implementiert durch Software,
  Injektion jeweils unterhalb der Schichtengrenze,
  deren Interaktionen zu bewerten sind

Test durch Fehlerinjektion

Prüfstand: Wird oberer Dienst korrekt erbracht?



Komplexes Protokollverhalten

- Inhalte aufeinanderfolgender Nachrichten in einem Zyklus hängen voneinander ab (z.B. für Fehlertoleranz-Funktionen)
- Nachrichten zum Exception Handling mit situationsabhängigem Inhalt
- Piggybacking von Information über mehrere Zyklen hinweg
- Ketten von (evtl. signierten) Nachrichten über mehrere Knoten (z.B. verteilte Entscheidung)

Bei Vielzahl von Fehlerfällen:
schwierig Korrektheit zu garantieren,
Tests oft nicht ausreichend.

Exploration des Zustandsraums

Anforderungen: oberes Protokoll

Anford. formalisiert

Ver-gleich

Verhalten der Anw.: nicht determin. allgem. Modell des Kommuni-kationsmusters

Verh. des Dienstes: nicht determin. Modell des externes Verhal-tens inkl. Fehler

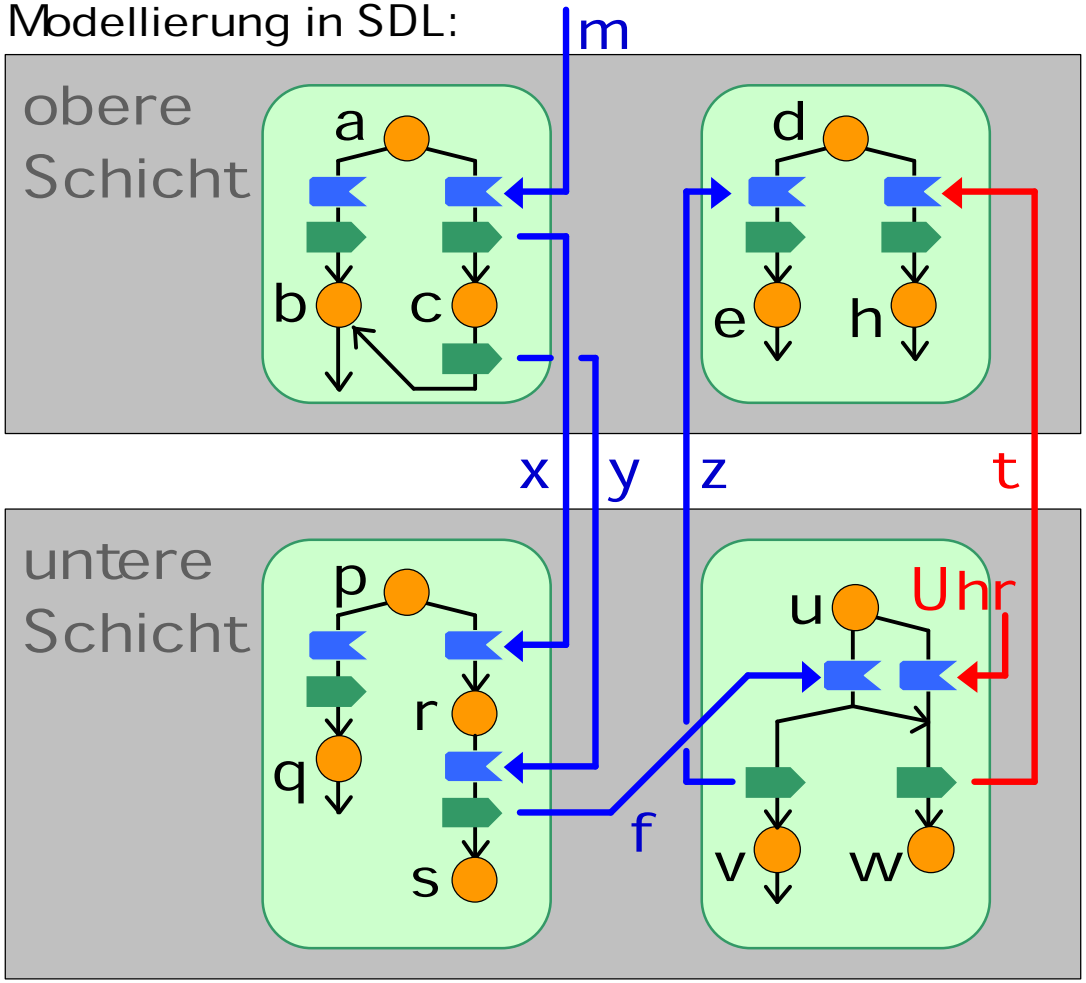
Erreich-barkeits-analyse

Zustands-raum

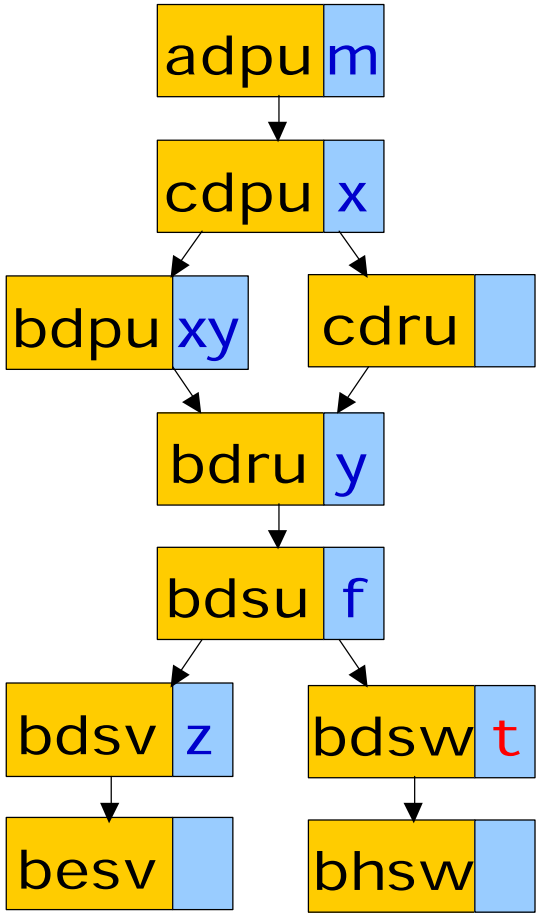
Verhalten: unterer Dienst

Zustands-Transitions-Systeme

Modellierung in SDL:



Erreichbarkeitsanalyse:

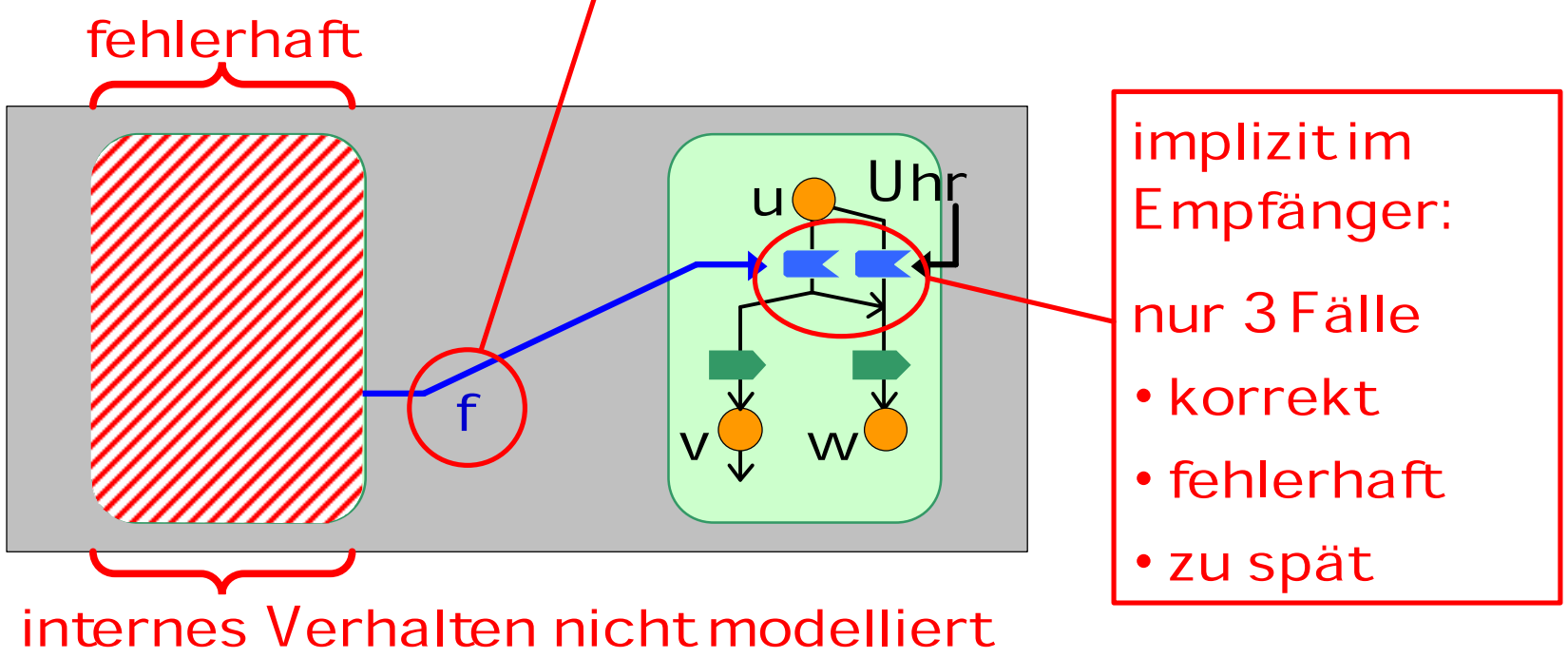


Modellierung von Fehlern

Nicht: Explizite Modellierung bestimmter Fehlerfälle.

Sondern: Allgemeines Fehlverhalten

„beliebige Information zu einem beliebigen Zeitpunkt".

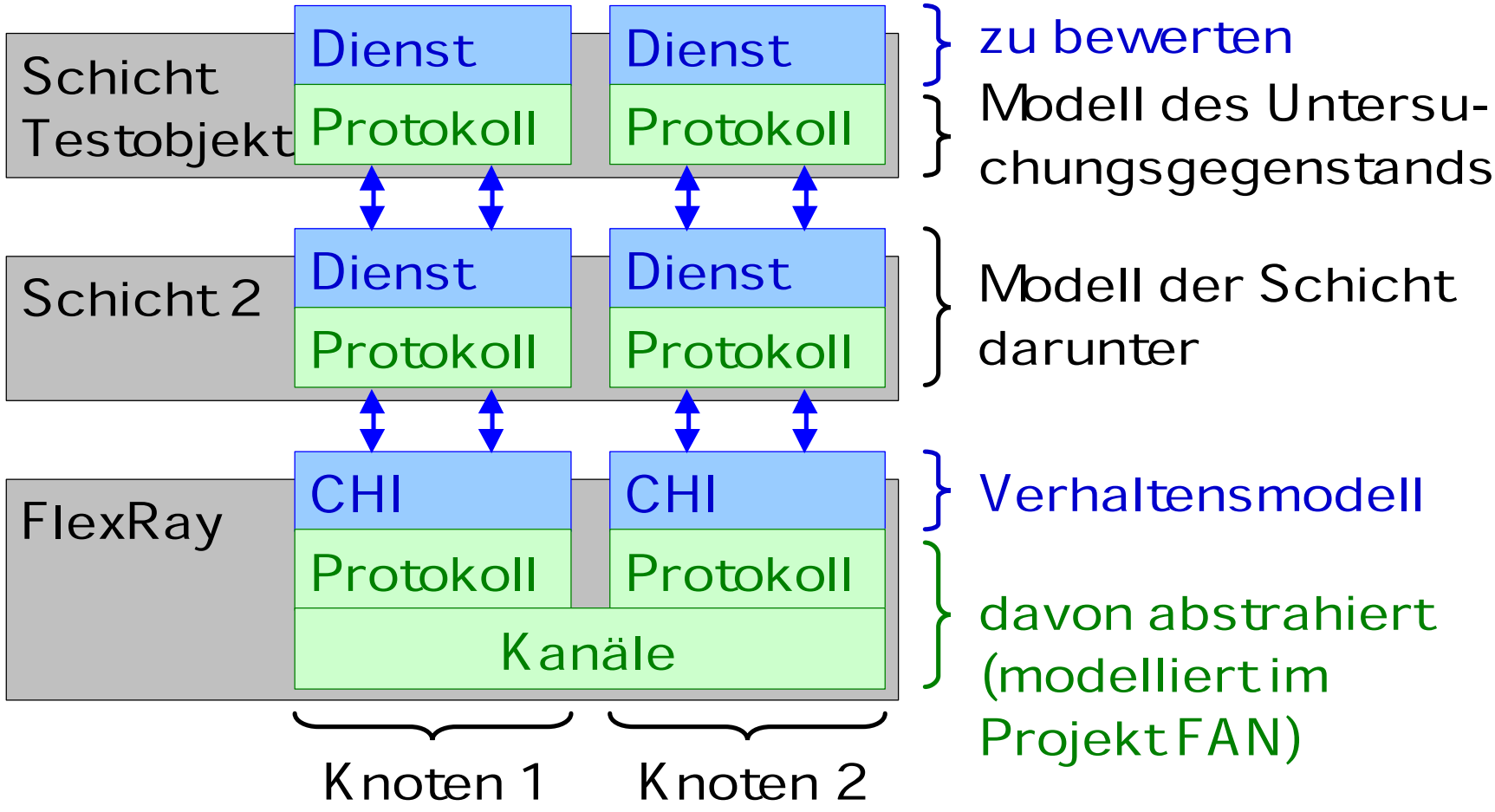


implizit im Empfänger:

nur 3 Fälle

- korrekt
- fehlerhaft
- zu spät

Verhaltensmodell von FlexRay



Zusammenfassung

Anforderungen

- geringe Kosten
- und zugleich hohe Kommunikationsleistung
- und zugleich hohe Sicherheit mittels Fehlertoleranz

führen oft zu komplizierten Lösungen.

Vielfalt der Fehlerfälle $\Rightarrow$ Schwierig, sicheres Verhalten in jedem Fehlerfall zu garantieren.

Frühzeitiges Aufdecken von Entwurfsschwächen:

- Simulation unter Fehlerinjektion
- Exploration des Zustandsraums

Unterstützung des Protokollentwurfs

Projekt FlexBeam:

Methoden zum frühzeitigen Aufdecken von Entwurfsschwächen

- „Übersehen" von Fehlerfällen
- falsche /unerwartete Reaktion in Ausnahmesituationen
- Verletzung von Echtzeitbedingungen
- falsche /ungünstige Parametrisierung