TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik und Fakultät Verkehrswissenschaften „Friedrich List“

Professur für VLSI-Entwurfssysteme, Diagnostik und Architektur
Professur für Verkehrssicherungstechnik

Zwischenpräsentation zur Diplomarbeit

Migration von Relaisschaltungen der Eisenbahnsicherungstechnik auf Programmierbare Schaltkreise

Stefan Wülfrath, 2013

Betreuer: Dr. Martin Zabel, Uwe Lehne
Betreuende Hochschullehrer: Prof. Spallek, Prof. Trinckauf

Dresden, 18.04.2013

Gliederung

1. Motivation und Zielstellung
2. Relaisstellwerkstechnik
   1. Einführung
   2. Sicherheitsrelevante Eigenschaften
   3. Sicherheitsprinzipien
3. PLD-basierte Systeme
   1. Einführung
   2. Sicherheitsrelevante Eigenschaften
   3. Gestaltung und Maßnahmen zur Ausfalloffenbarung
   4. Systemkonzept
4. Nächste Schritte
5. Quellenangaben und Literaturhinweise

1. Motivation und Zielstellung

Ausgangslage:

- viele bewährte Stellwerksbauformen (z.B. Relaisstellwerke, Elektronische Stellwerke)
- Problematik: Obsoleszenz
- Idee: Migrationsfähige Architekturen (z.B. PLD-basiert)

Zielstellung der Diplomarbeit:

- Entwicklung eines Verfahrens zur Migration von Relaisschaltungen auf Programmierbare Schaltkreise
- Konzeption einer PLD-basierten Systemarchitektur
- Transformation einer Relaisschaltung in eine äquivalente Hardwarebeschreibung (z.B. VHDL) für PLDs
- Bewertung anhand von Beispielschaltungen

2. Relaisstellwerkstechnik – Einführung (1)

- Geschichtlicher Abriss:
  - Beginn der Entwicklung (in Deutschland) ca. 1940
  - Seit ca. 1950 in großem Umfang eingesetzt
  - Hersteller: Siemens, Thales, WSSB (Deutsche Reichsbahn)
  - Seit ca. 1980 schrittweise Ersatz durch Elektronische Stellwerke (EStw)
- Über mehr als 50 Jahre bewährte Technik!
- Statistik der im Betrieb befindlichen Bauformen: [1]
  - 43,9% Mechanische / Elektromechanische Stellwerke
  - 42,5% Relaisstellwerke
  - 13,2% Elektronische Stellwerke

2. Relaisstellwerkstechnik – Einführung (2)

Normalrelais,
Bauform II (WSSB) [2]

Signalrelais (Eigenschaften)

- Hohe Ansprechschwelle
- Relativ hohe Anzugs- und Abfallzeiten
- Vorzugsausfallrichtung
- Selbstreinigende Kontakte, Große Kontaktabstände
- Zwangsführung der Kontakte
- Unverwechselbarkeitseinrichtung

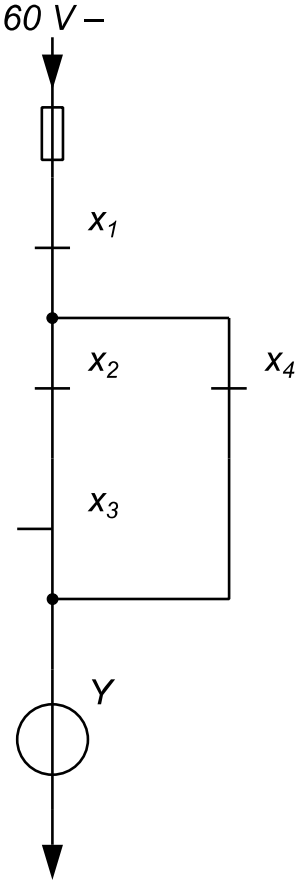
Prinzipielle Relaisbauarten:

- Monostabile Relais
  (Normalrelais, Kleinrelais)
- Bistabile Relais
  (Stützrelais, Kipprelais, Haftrelais)

2. Relaisstellwerkstechnik – Einführung (3)

- Elektrotechnische Realisierung von Booleschen Gleichungen
- Relaisschaltungen bestehen aus:
  - Spannungsversorgung (60 V Gleichspannung)
  - Stromkreis mit Schließer- und Öffner-Kontakten
  - Wicklungsanschlüssen eines (oder mehrerer) Relais
- Boolesche Gleichung ergibt sich aus den Bedingungen zur Ansteuerung des Relais

$$Y = x_1 \wedge ((x_2 \wedge \neg x_3) \vee x_4)$$



2. Relaisstellwerkstechnik – Sicherheitsrelevante Eigenschaften

- Ausfallverhalten der Relaistechnik sehr gut bekannt
- Betrachtung der Ausfallwirkungen
  → Zusammenfassung zu Ausfallarten
- Ausfallarten eines Signalrelais:
  - Anker zieht nicht an
  - Anker fällt nicht ab
  - Kontakt schließt nicht
  - Kontakt öffnet nicht
- Betätigungsbezogenes Ausfallverhalten
- Nach Frühausfällen: Konstante Ausfallrate λ
  → „Badewannenkurve“

2. Relaisstellwerkstechnik – Sicherheitsprinzipien

Sicherheitsprinzipien:

1. Ausschluss von bestimmten Ausfallarten
2. Einteilung in Ausfallklassen: Ausfälle I. und II. Ordnung
3. Ein Ausfall I. Ordnung darf nicht zu einem gefährlichen Zustand führen
4. Ein Ausfall I. Ordnung und ein gleichzeitiger Ausfall II. Ordnung dürfen zu keinem gefährlichen Zustand führen
5. Ausfalloffenbarung durch Hemmung der Anlage sofort oder spätestens bei der nächsten Betätigung
6. Aufheben der Hemmung nur durch Ausfallbeseitigung oder registrierte Hilfsbedienung

3. PLD-basierte Systeme – Einführung

- Programmierbare Schaltkreise:
  - Programmierbare Speicher (PROM, EEPROM, Flash)
  - Programmierbare Logikbausteine (PLD)
- PLD:
  - Aus Herstellungssicht: Generischer Standard-Schaltkreis
  - Bestimmung der Funktion durch den Anwender (Konfiguration)
- PLD-Typen: SPLD, CPLD, FPGA
- FPGA: Field-Programmable Gate Array
- PLD-basiertes System
  → elektronisches System mit PLD

Bildquelle: [3]

3. PLD-basierte Systeme – Sicherheitsrelevante Eigenschaften (1)

- Elektronische Schaltungen
  - Größere Anzahl an anzunehmenden Ausfallarten
  - Zeitbezogenes Ausfallverhalten
  - Zeitlicher Verlauf der Ausfallraten: „Badewannenkurve“
  - Relativ große Ausfallraten der elektronischen Bauelemente
- In komplexen Schaltungen oder integrierten Schaltkreisen: große Anzahl an Ausfallkombinationen

  → nicht beherrschbar
- Deshalb: Zusammenfassung zu Funktionseinheiten
- Anzunehmender Ausfall einer Funktionseinheit

  → Funktionsversagen

3. PLD-basierte Systeme – Sicherheitsrelevante Eigenschaften (2)

- Zusammenfassung der Ausfallarten zu Fehlermodellen
- Fehlermodelle für diskrete elektronische Schaltungen:
  - DC-Fehlermodell
  - Driftausfälle
  - Oszillation
- Partielle Verteilung der Ausfallrate eines Bauelementes auf Ausfallarten nur in besonderen Fällen möglich

  → Verwendung der Gesamtausfallrate
- Ausfallrate einer Funktionseinheit

  = Σ Ausfallraten aller Bauelemente
- Anwendung von speziellen Gestaltungsprinzipien

3. PLD-basierte Systeme – Gestaltung (1)

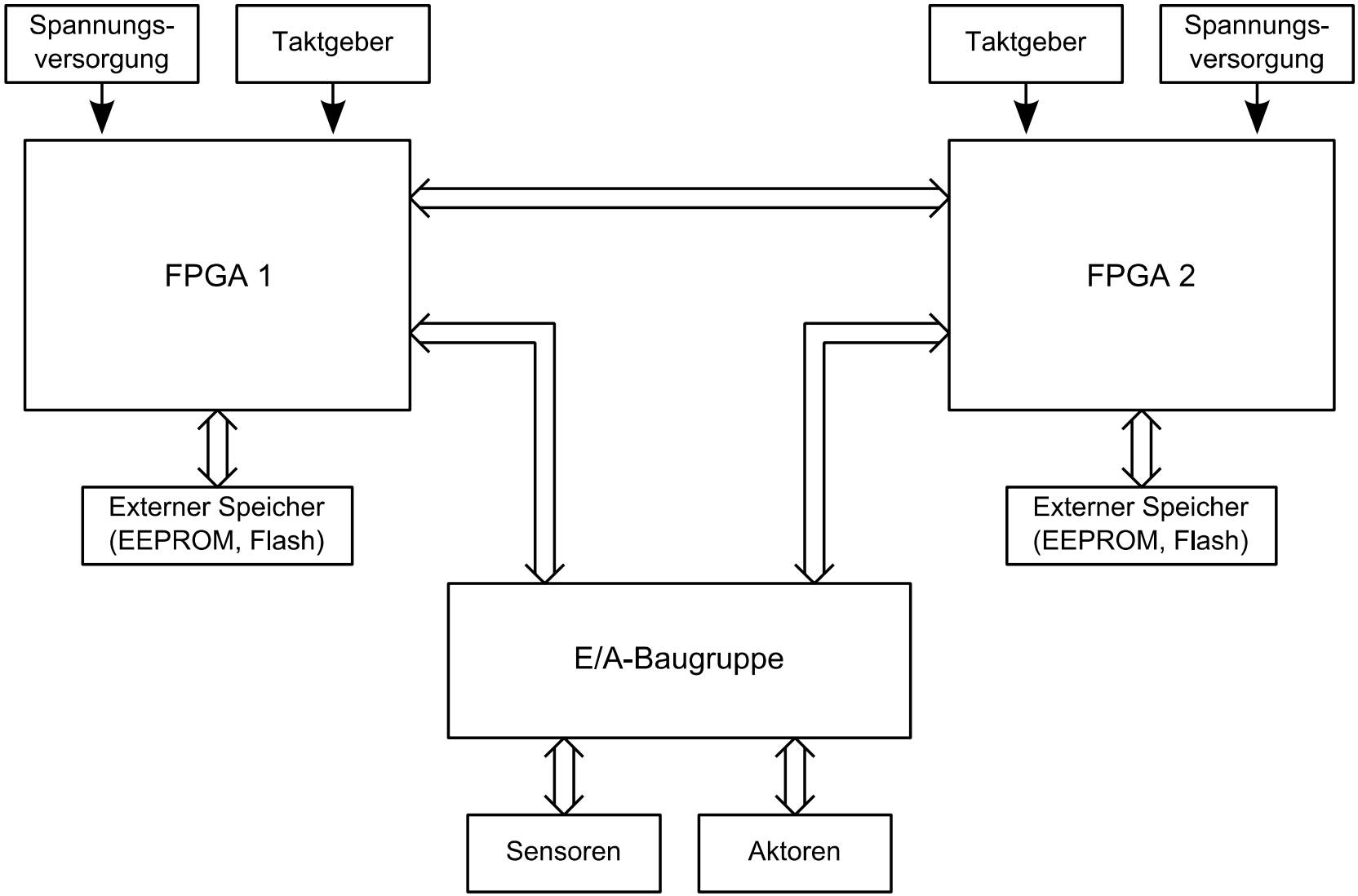
	Relaistechnik	PLD-basierte Systeme
Anzahl der Ausfallarten	Gering	Hoch
Vorzugsausfallrichtung	Ja	Nein
Aufwand für Schutzmaßnahmen	Gering	Hoch
Betrachtung von Mehrfachausfällen	Nur für Ausfälle II. Ordnung nötig	Immer
Gefährdungsrate eines (Teil-)Systems	Gering	Höher
Ausfallverhalten	Betätigungsbezogen	Zeitbezogen
Prüfungen (Selbsttest)	Datenflussabhängig	Datenflussunabhängig

Tabelle: Vergleich Relaistechnik vs. PLD-basierte Systeme

3. PLD-basierte Systeme – Gestaltung (2)

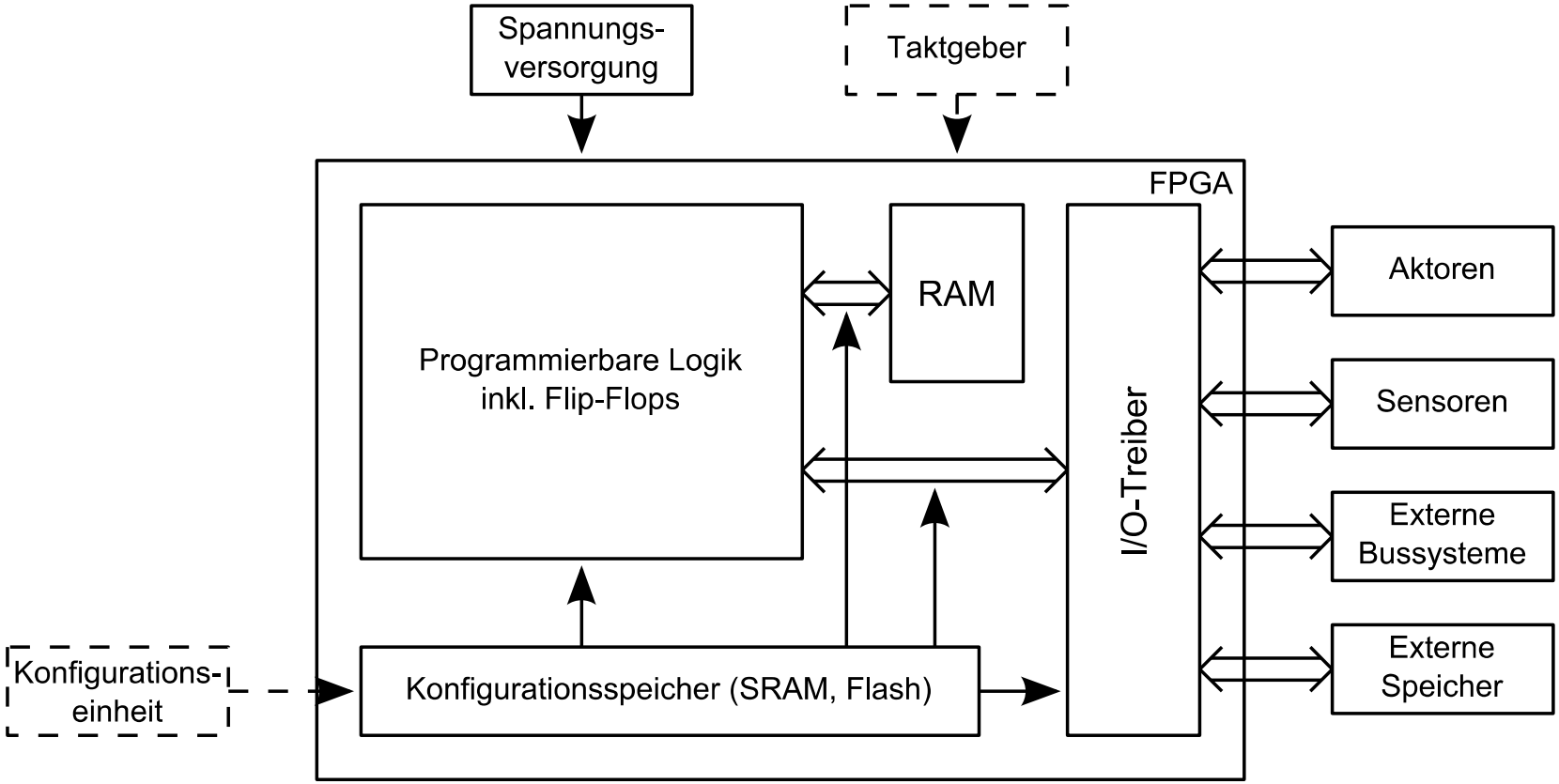
- Sicherheitsprinzipien
  - Composite fail-safety (Mehrkanalige Struktur)
  - Reactive fail-safety (Überwachung der Ausgaben)
  - Inherent fail-safety (Eigensicher)
- Bei Erkennung eines Ausfalls

  → Sicherheitsgerichtete Reaktion
- Stand der Technik: Anwendung von Redundanz
  - Mehrkanaligkeit
  - Unabhängige Überwachung
  - Codierung
- Voraussetzung: Unabhängigkeit der redundanten Einheiten
- Beachte: Common-Cause-Failure (CCF)



Beispiel für ein zweikanaliges FPGA-basiertes System

3. PLD-basierte Systeme – Maßnahmen zur Ausfalloffenbarung (2)



Logische Struktur eines FPGA

3. PLD-basierte Systeme – Maßnahmen zur Ausfalloffenbarung (3)

- JTAG-Schnittstelle
  - Integrierte Konfigurations-, Test- und Diagnoseschnittstelle
  - Test des Chips nach dem Einbau in das System
  - Für Test während des Betriebs nicht geeignet
- Konfigurationsspeicher
  - zyklische Berechnung und Prüfung der CRC-Summe der Konfigurationsdaten
  - Zusätzlich: Gegenseitiger Vergleich mit redundantem Kanal
- Programmierbare Logik
  - Selbsttests (z.B. Scan-Path, Boundary-Scan)
  - Gegenseitiger Vergleich d. Zustandsvektoren
  - Zeitliche und logische Überwachung durch Watchdogs

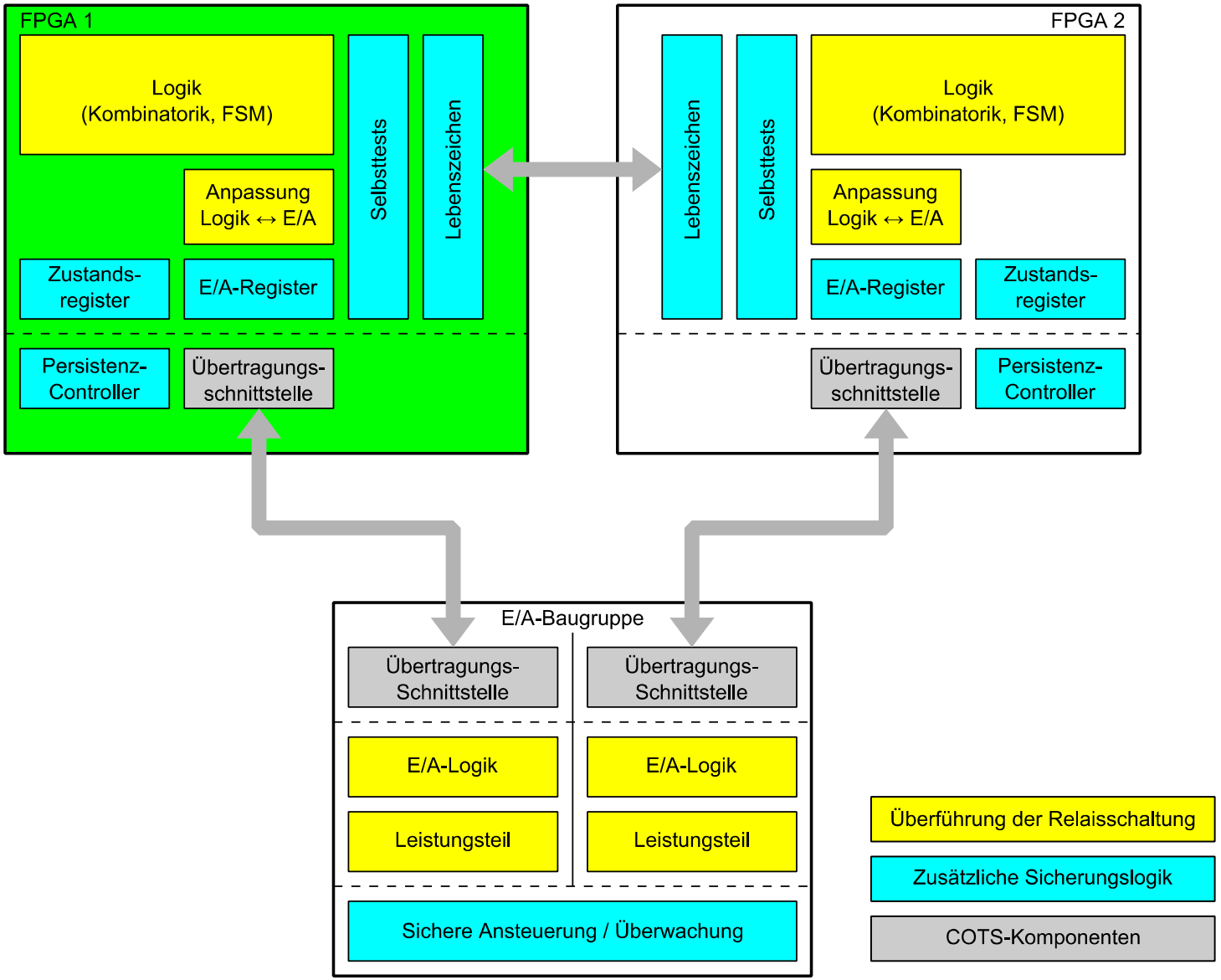
3. PLD-basierte Systeme – Maßnahmen zur Ausfalloffenbarung (4)

- RAM
  - Permanente Fehler: RAM-Tests (z.B. Galpat)
  - Erkennung von Soft-Errors: Antivalente redundante Speicherung
- I/O-Einheiten
  - Fehlerhafte Ausgabe: Sicherer Vergleich durch E/A-Baugruppe
  - Fehlerhafte Eingangspins: Redundante, antivalente Eingänge
  - Stuck-At-X: Getaktete Ein-/Ausgänge
  - Busschnittstellen: Erkennung durch Busprotokoll
  - Zusätzlich: gegenseitiger Vergleich der Eingangsabbilder
- Spannungsversorgung
  - Überwachung auf Über- und Unterspannung
  - Redundante Spannungsversorgungen
  - Externe Sicherung relevanter Daten
- Taktgeber
  - Generierung und Überwachung eines Lebenszeichens

3. PLD-basierte Systeme – Maßnahmen zur Ausfalloffenbarung (5)

Komponente	**Interne Maßnahmen**	**Externe Maßnahmen**
Konfigurations-speicher	CRC-Prüfsummen	Vergleich CRC-Prüfsummen
Programmierbare Logik	Selbsttests, Watchdog, Generierung Lebenszeichen	Vergleich Zustandsvektoren, Austausch und Überwachung Lebenszeichen
RAM	RAM-Tests (Galpat), Schreib-/Lesetests, Redundante antivalente Speicherung	
I/O-Treiber	Redundante antivalente Eingänge, Überwachung Busprotokoll, Taktung Ein- und Ausgänge	Vergleich Eingangsvektoren, Überwachung Busprotokoll
Spannungs-versorgung		Überwachung Über-/ Unterspannung, Redundante Versorgung, Sicherung relevanter Daten
Taktgeber	Generierung Lebenszeichen	Austausch und Überwachung Lebenszeichen

3. PLD-basierte Systeme – Systemkonzept



4. Nächste Schritte

- Konzeption einer Systemarchitektur
- Entwurf eines Regelwerkes zur Modularisierung der Originalschaltungen
- Entwurf eines Regelwerkes zur Aufteilung einer Relaisschaltung in Logik- und Leistungsteil
  - Trennung von Innen- und Außenanlage
  - Beibehaltung der Sicherheitsprinzipien der Originalschaltung
- Entwurf eines Regelwerkes zur Transformation des Logikanteiles in eine äquivalente PLD-Programmierung
  - (VHDL-) Zustandsmodelle der Relais entwickeln
  - Überführung Ansteuerbedingungen (Kombinatorik)
  - Schnittstellen zwischen Logik und Leistungsteil
  - Ansteuerung und Überwachung E/A-Baugruppe

5. Quellenangaben und Literaturhinweise

Quellen:

[1] http://www.stellwerke.de/liste/seite3_s.html

[2] http://commons.wikimedia.org/wiki/File:Bauform_II_Normalrelais.jpg

[3] http://commons.wikimedia.org/wiki/File:Altera_StratixIVGX_FPGA.jpg

Literaturhinweise:

- Kusche, W.: Gleisbildstellwerke. transpress Berlin, 1984
- Fenner, W.; Naumann, P.; Trinckauf, J.: Bahnsicherungstechnik. Publicis Corporate Publishing Erlangen, 2003
- Kesel, F.; Bartholomä, R.: Entwurf von digitalen Schaltungen und Systemen mit HDLs und FPGAs, Oldenbourg Verlag München, 2009

Relevante Normen: DIN EN 50129, DIN EN 61508, DIN 50128

Eisenbahnsicherungstechnik für Informatiker:

- Stefan Katzenbeisser: Can trains be hacked? (Vortrag beim CCC)
  → http://www.youtube.com/watch?v=bMEejX4uANw