TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik und Fakultät Verkehrswissenschaften „Friedrich List“

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

Verteidigung der 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, 02.09.2013

Gliederung

1. Motivation
2. Sichere Stellwerksplattform
3. Transformationsverfahren
4. Ergebnisse und Ausblick

Quellen und Literaturhinweise

1. Motivation – Ausgangslage und Idee

Ausgangslage:

- Anteile der Stellwerksbauformen im Netz der DB AG (2012) [1]
  - 44 % Mechanische / Elektromechanische Stellwerke
  - **42 % Relaisstellwerke (ca. 1700)**
  - 13 % Elektronische Stellwerke
- kurz- bis mittelfristiger Ersatz aufgrund Bauelementalterung
- Suche nach einer kostengünstigen Alternative zu elektronischen Stellwerken

Idee:

- Ersatz durch funktionsidentische elektronische Lösung
- Verwendung einer industriellen Standardlösung (→ FPGA)

1. Motivation – Resultierende Zielstellung

Zielstellung

Entwicklung eines Verfahrens zur Transformation einer Relaisschaltung in eine äquivalente Hardwarebeschreibung

Resultierende Aufgaben

a) Analyse und Vergleich der Eigenschaften von Relaisstellwerkstechnik und programmierbaren Schaltkreisen

b) Konzeption einer generischen FPGA-basierten Stellwerksplattform

c) Entwicklung eines Transformationsverfahrens

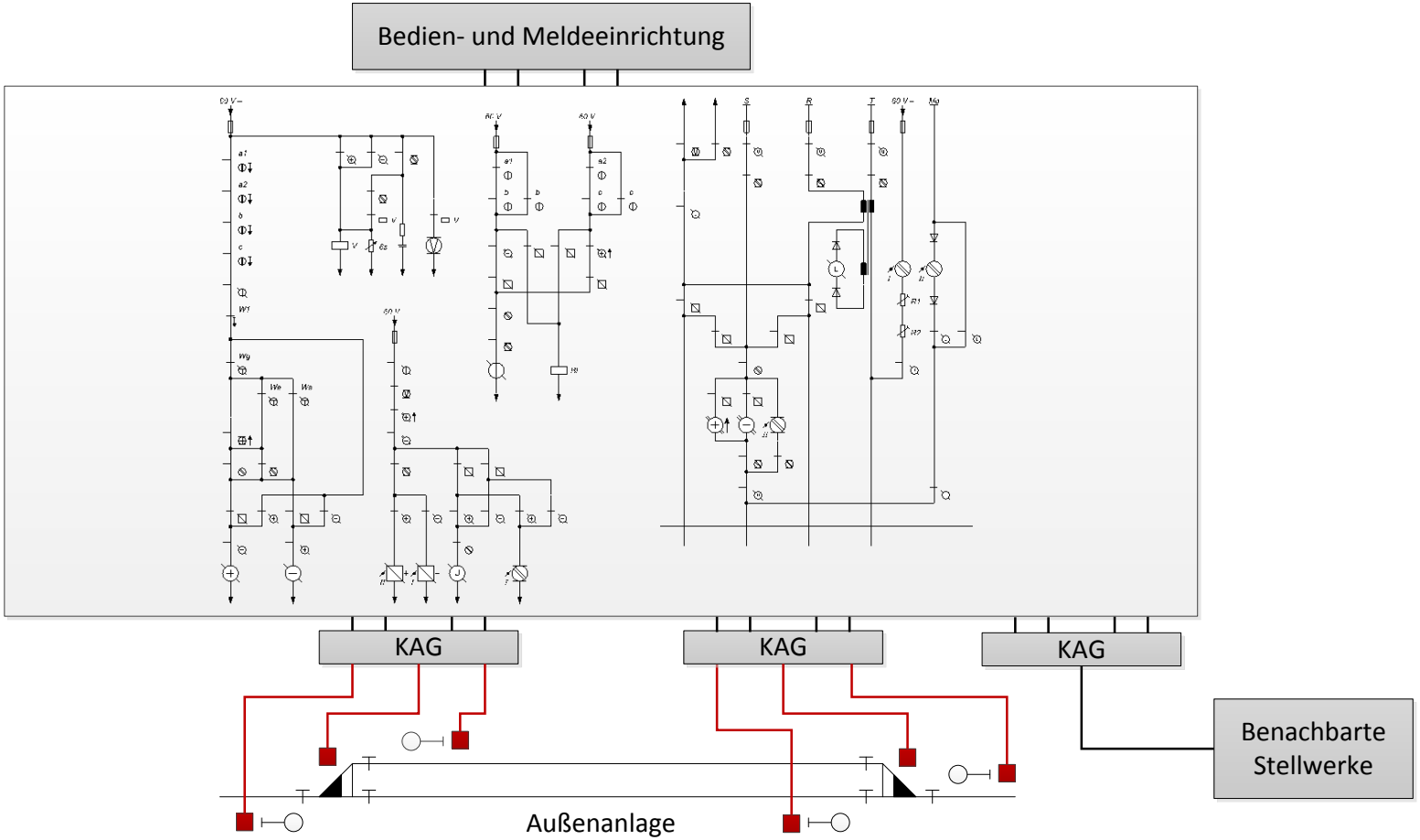
d) Prototypische Realisierung eines Anwendungsbeispiels

Gliederung

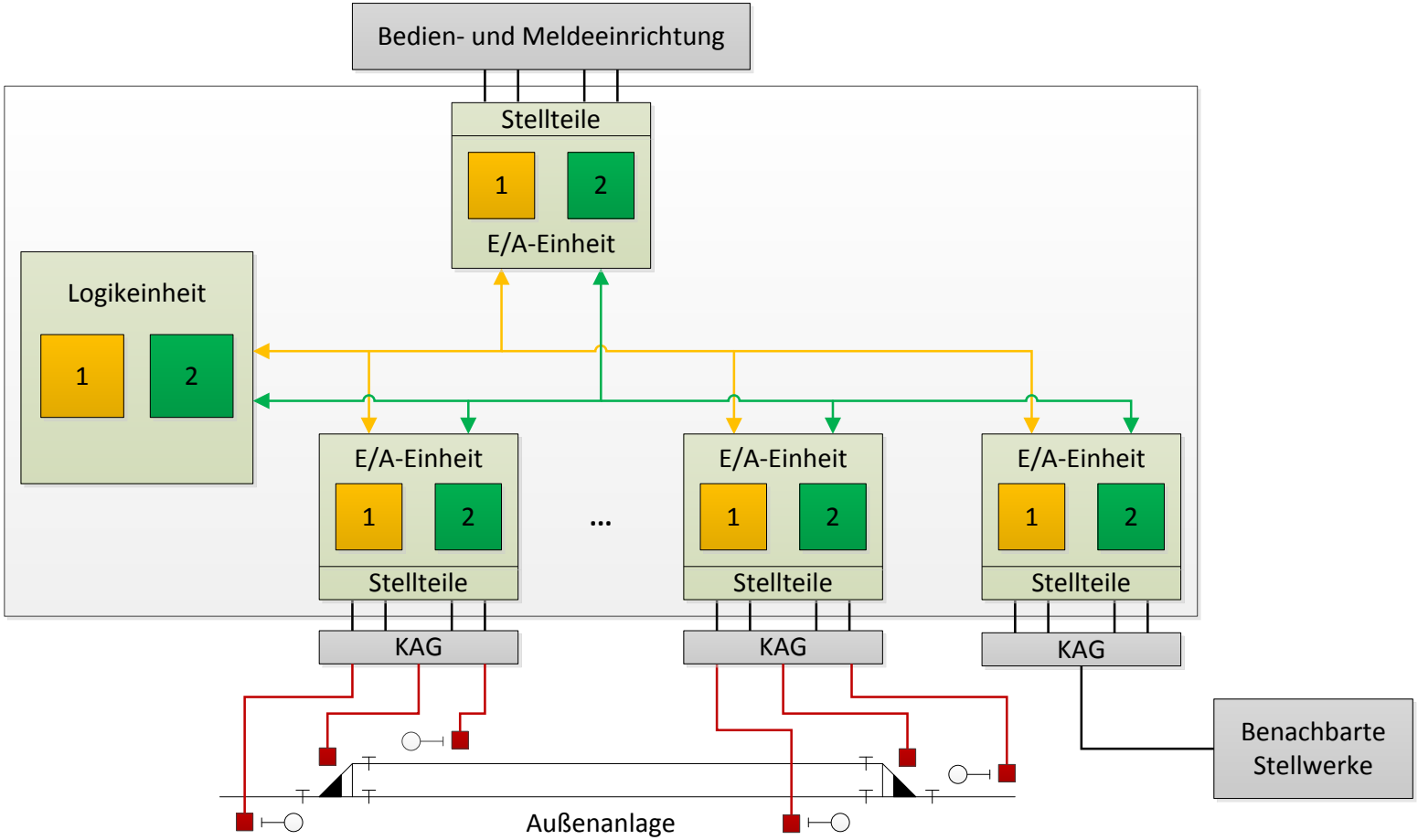
1. Motivation
2. **Sichere Stellwerksplattform**
3. Transformationsverfahren
4. Ergebnisse und Ausblick

Quellen und Literaturhinweise

2. Sichere Stellwerksplattform – Architektur



2. Sichere Stellwerksplattform – Architektur



2. Sichere Stellwerksplattform – Sicherheit

a) 2-aus-2-System mit sicherem Vergleicher

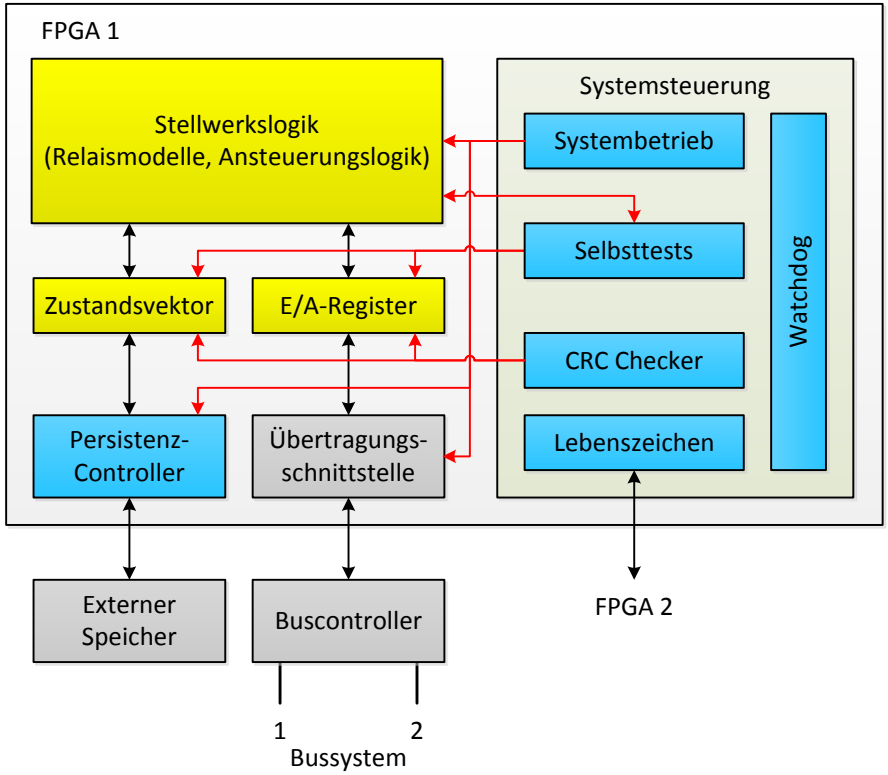
- Datenflussabhängige Ausfalloffenbarung
- Vergleich der Prozessausgaben
- Offenbarung von Ausfällen, die Prozessausgabe verfälschen
- Ausfalloffenbarungszeit ca. 30 Tage

  → Gleichgerichtete Ausfälle möglich !

b) Zusätzliche Prüfungen und Tests

- Datenflussunabhängige Ausfalloffenbarung
- zyklische Prüfung der konfigurierten Logik
- Erkennung von FPGA-internen Ausfällen (Stuck-At-X, Bridging)
- Ausfalloffenbarungszeit ca. 1 Minute

2. Sichere Stellwerksplattform – FPGA-Logik



Logische Trennung

- Systemsteuerung (anwendungsunabhängig)
- Stellwerkslogik (anwendungsspezifisch)

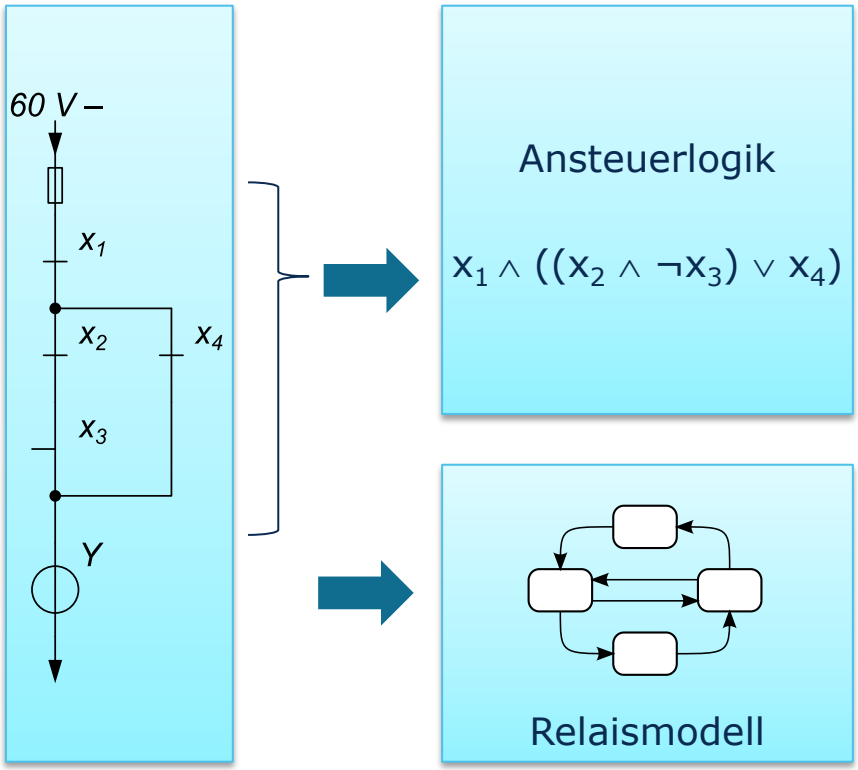
Ausfalloffenbarung

- gegenseitiger Vergleich der Zustandsvektoren
- CRC-Überwachung
- Selbsttests
- Lebenszeichenaustausch
- Watchdog

Permanente Zustandsdaten

- Externer Speicher (Flash)

2. Sichere Stellwerksplattform – Stw-Logik



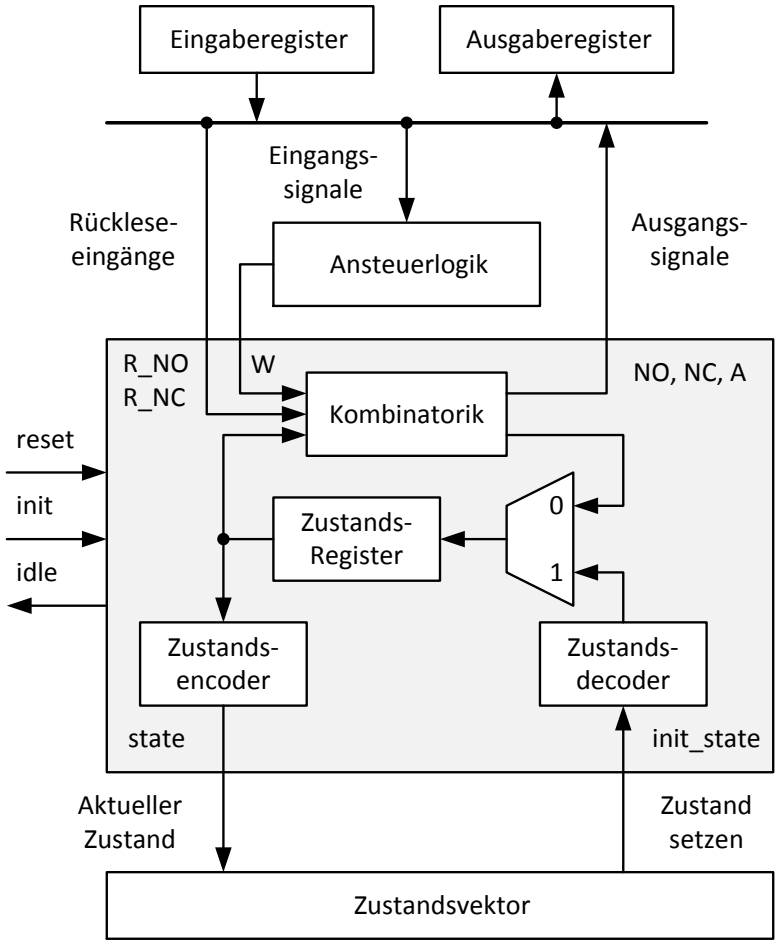
Ansteuerlogik

- kombinatorische Ansteuerung der Eingänge (Wicklungen) des Relaismodells
- Ergebnis des Transformationsverfahrens

Relaismodell

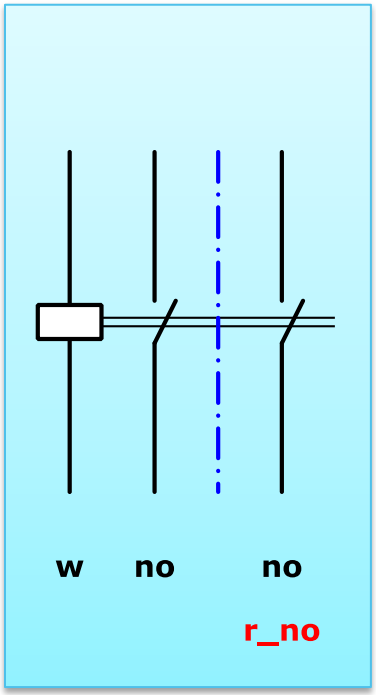
- generische VHDL-Module
  → als Bibliothek
- Nachbildung des Schaltverhaltens
- logische Ansteuerung des Leistungsteils

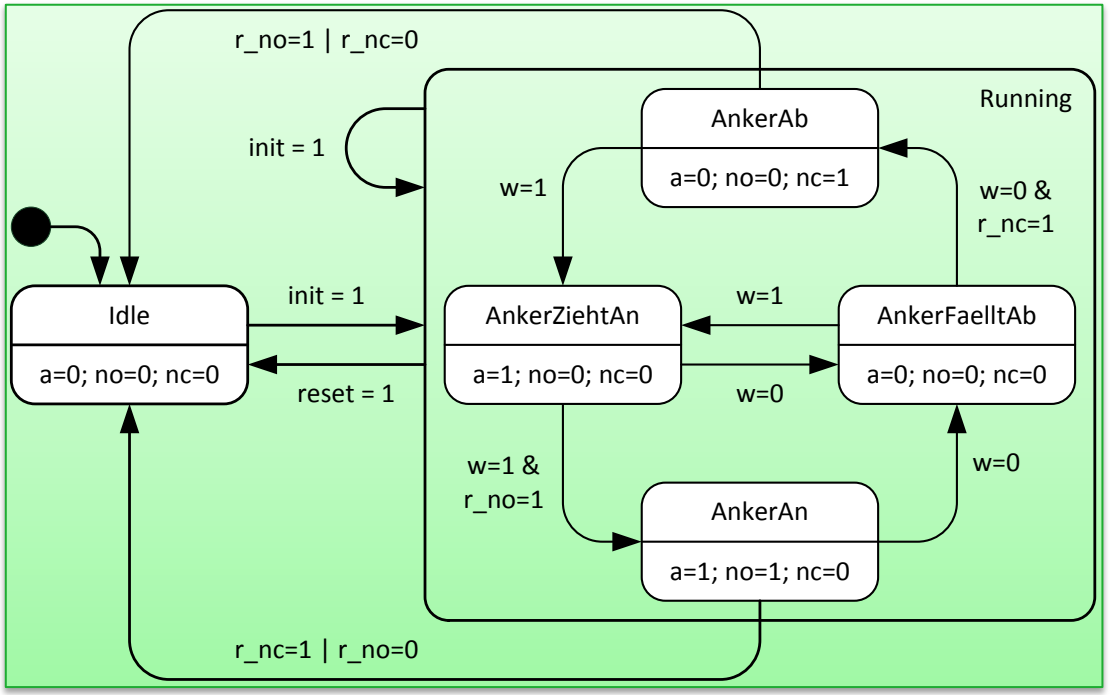
2. Sichere Stellwerksplattform – Relaismodul



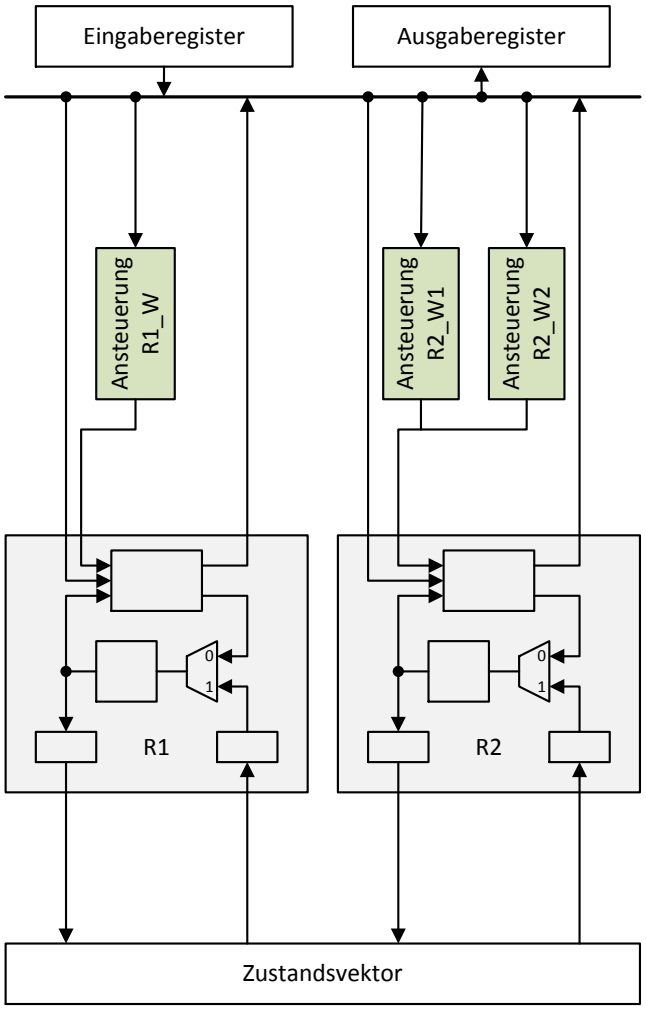
- Endliche Zustandsmaschine
- Steuereingänge
  - Setzen / Rücksetzen
- Steuerausgänge
  - aktueller Zustand
- Dateneingänge
  - Wicklungsansteuerung
  - Rückleseeingänge
- Datenausgänge
  - Kontaktstellung (Schließer, Öffner)
  - Ansteuerung des Stellteils

2. Sichere Stellwerksplattform – Zustandsmodell



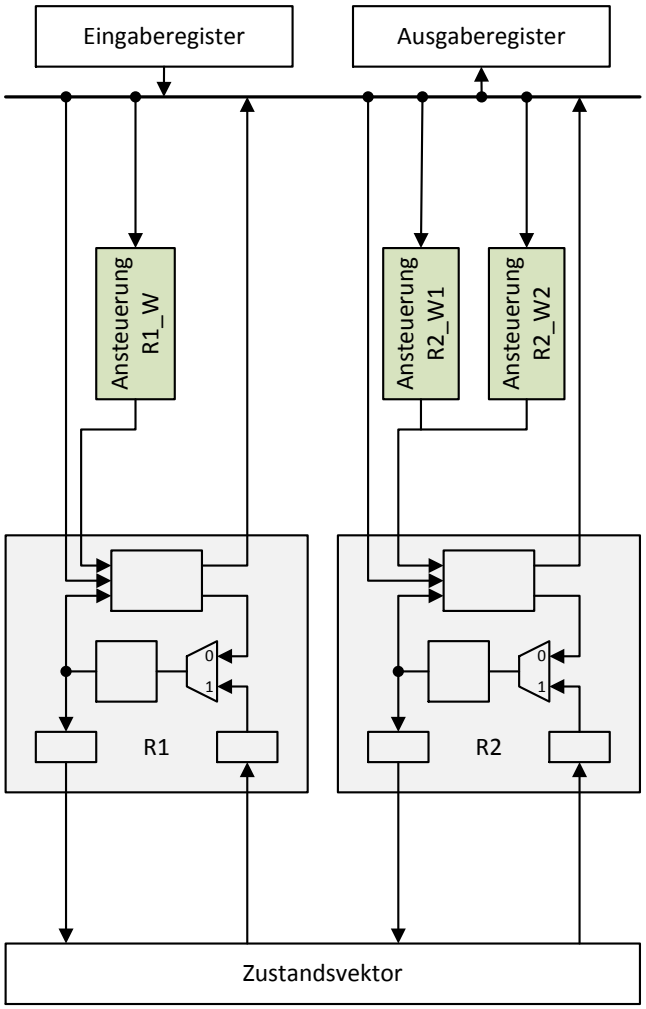


$$(no \wedge nc = 0) \wedge (r\_no \wedge r\_nc = 0) \wedge (no \wedge r\_nc = 0) \wedge (r\_no \wedge nc = 0)$$



Stellwerkslogik

- Relaismodule
- Ansteuerlogik
- E/A-Register
- Zustandsvektor

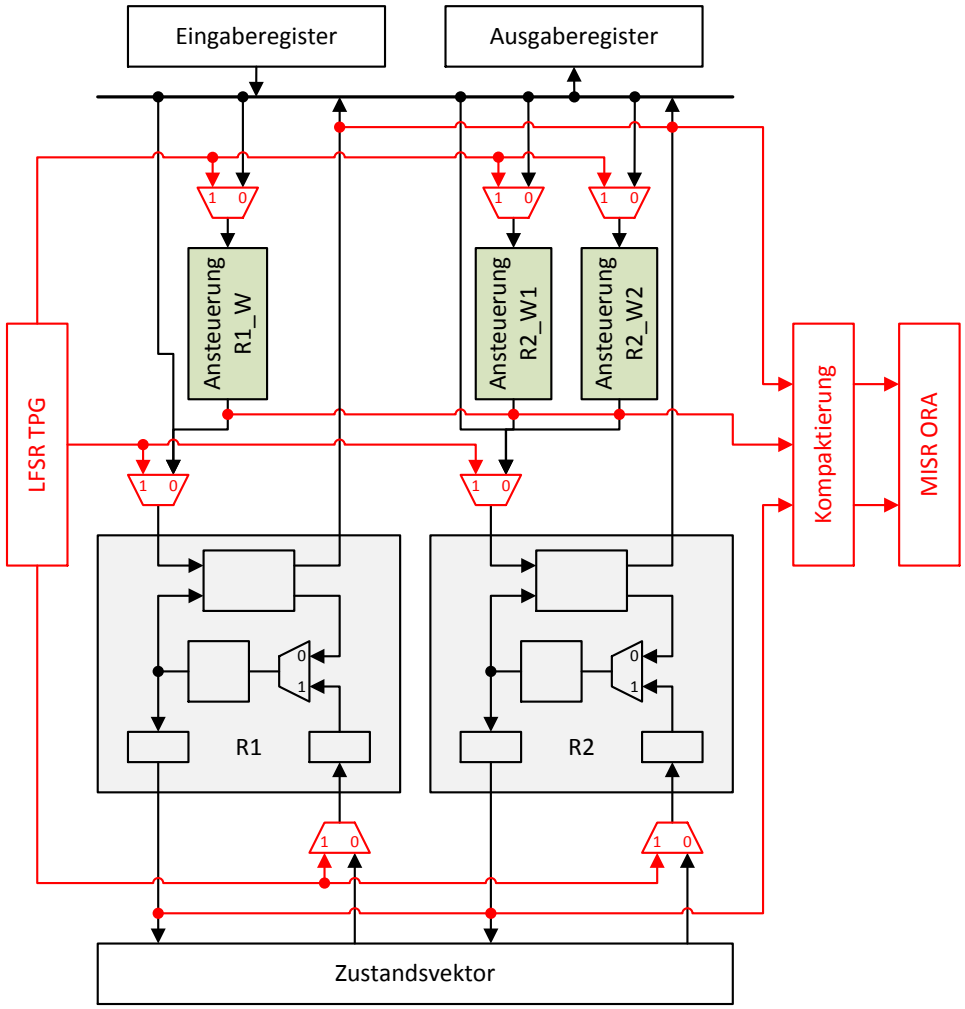


Stellwerkslogik

- Relaismodule
- Ansteuerlogik
- E/A-Register
- Zustandsvektor

Selbsttestkonzept

- generische Testmuster
- Partitioned Autonomous Test



Stellwerkslogik

- Relaismodule
- Ansteuerlogik
- E/A-Register
- Zustandsvektor

Selbsttestkonzept

- generische Testmuster
- Partitioned Autonomous Test

Selbsttestlogik

- Testmustergenerator
- Test-Multiplexer
- Kompaktierung
- Signaturregister

Gliederung

1. Motivation
2. Sichere Stellwerksplattform
3. **Transformationsverfahren**
4. Ergebnisse und Ausblick

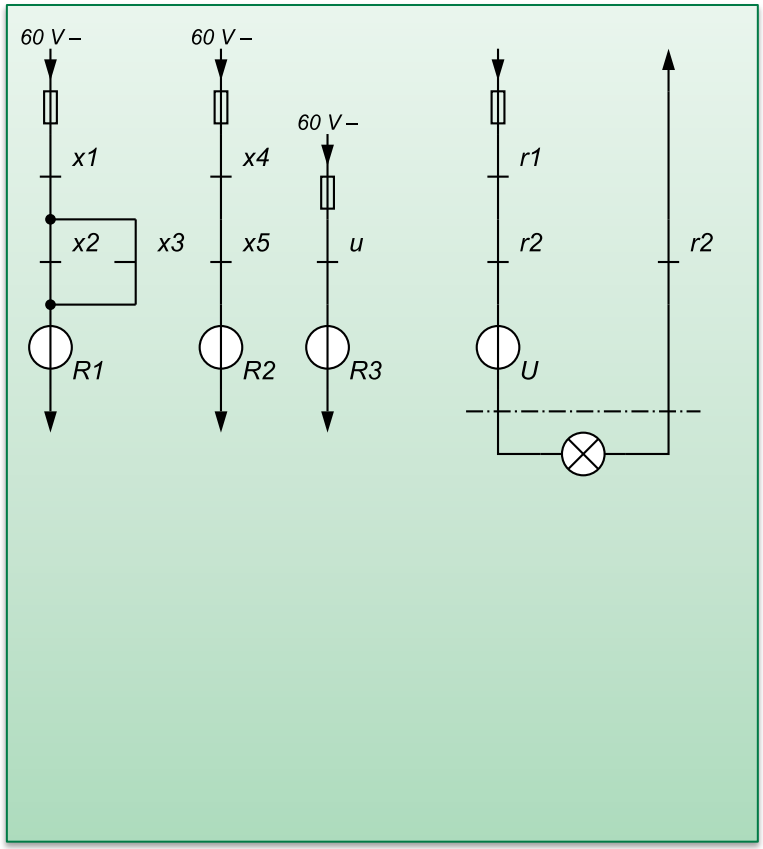
Quellen und Literaturhinweise

3. Transformationsverfahren

1. Auswahl und Aufteilung der Originalschaltungen
   a) Identifizierung und Modularisierung der Originalschaltungen
   b) Aufteilung der Relaisschaltung in Logik- und Leistungsteil
   c) Definition der Schnittstellen zwischen Logik- und Leistungsteil
2. Überführung des Logikteils
   a) Abbildung des Logikteils auf das Transformationsmodell
   b) Transformation der Ansteuerlogik
3. Integration in die Stellwerksplattform
4. Verifikation und Validierung

3. Transformation – Auswahl und Aufteilung (1)

Identifizierung / Modularisierung der Originalschaltungen



Ausgangspunkt

- Schaltpläne in gedruckter / elektronischer Form

Auswahl der Schaltungen

- alle projektierten Schaltungen eines Stellwerks
- nur einzelne Relaisgruppen

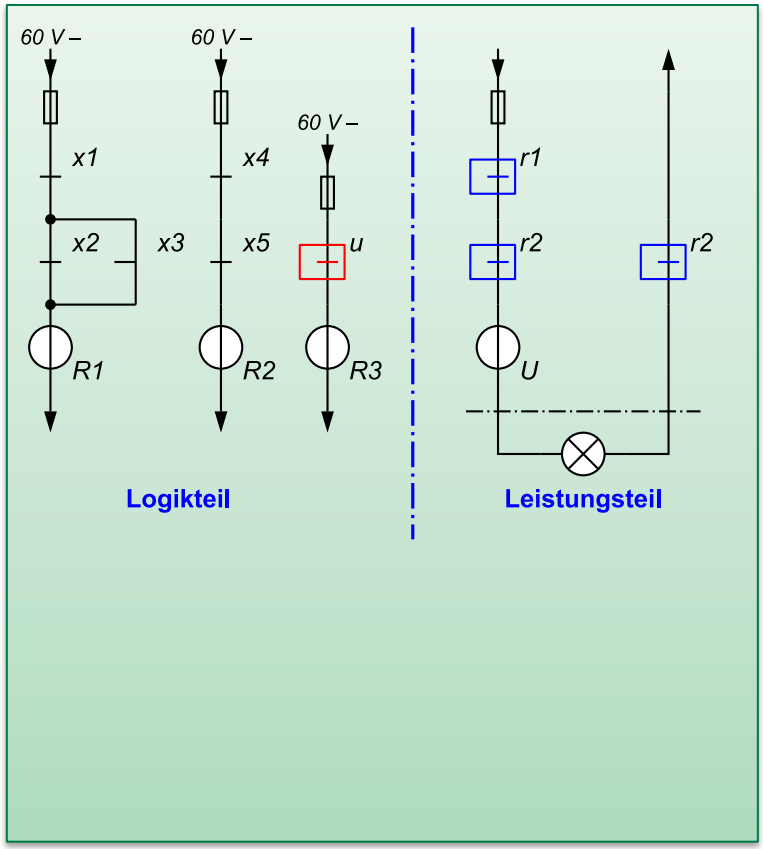
→ flexibel wählbar

Konfiguration der generischen Systemarchitektur

- Anzahl E/A-Einheiten
- Zuordnung zu Elementen

3. Transformation – Auswahl und Aufteilung (2)

Aufteilung der Relaisschaltung in Logik- und Leistungsteil



Logikteil

- logische Verknüpfungen in der Relaisinnenanlage

→ FPGA

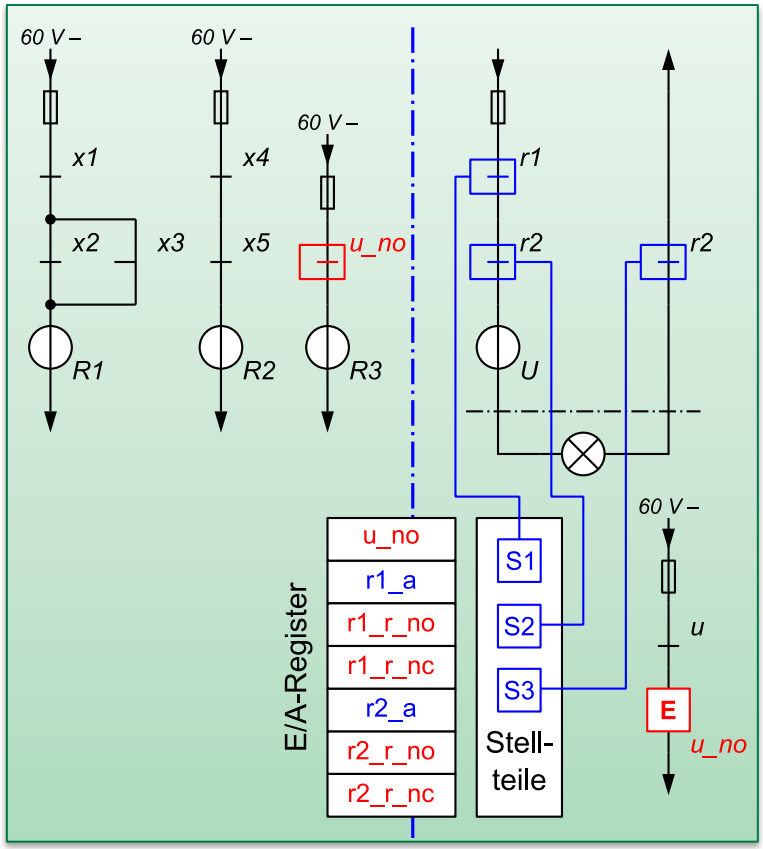
Leistungsteil

- Überwachung / Ansteuerung der Außenanlage
- Schnittstelle zur Bedien- und Meldeeinrichtung

→ Schnittstelle: E/A-Einheiten

3. Transformation – Auswahl und Aufteilung (3)

Schnittstellen zwischen Logik- und Leistungsteil



Eingangssignale

- Einlesen durch sichere Eingänge

Ausgangssignale

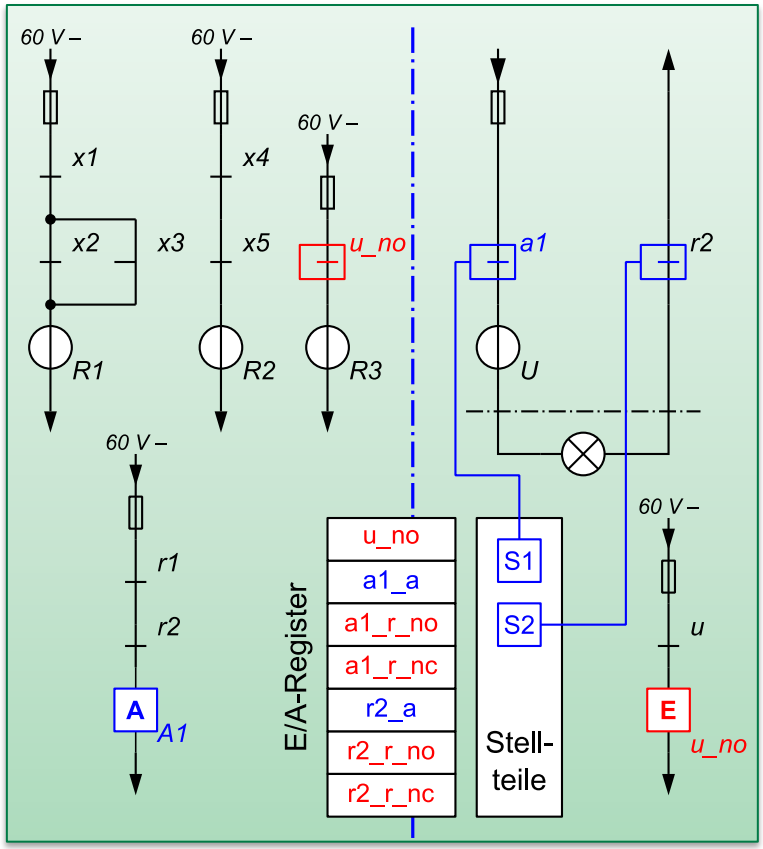
- sichere Stellteile inkl. Rückleseeingängen

Definition der Schnittstelle

- Ein- und Ausgangssignale
- Abbildung auf E/A-Register

3. Transformation – Auswahl und Aufteilung (4)

Zusammenfassung von externen Schaltern



Problem

- hohe Anzahl an benötigten Stellteilen / Schaltern

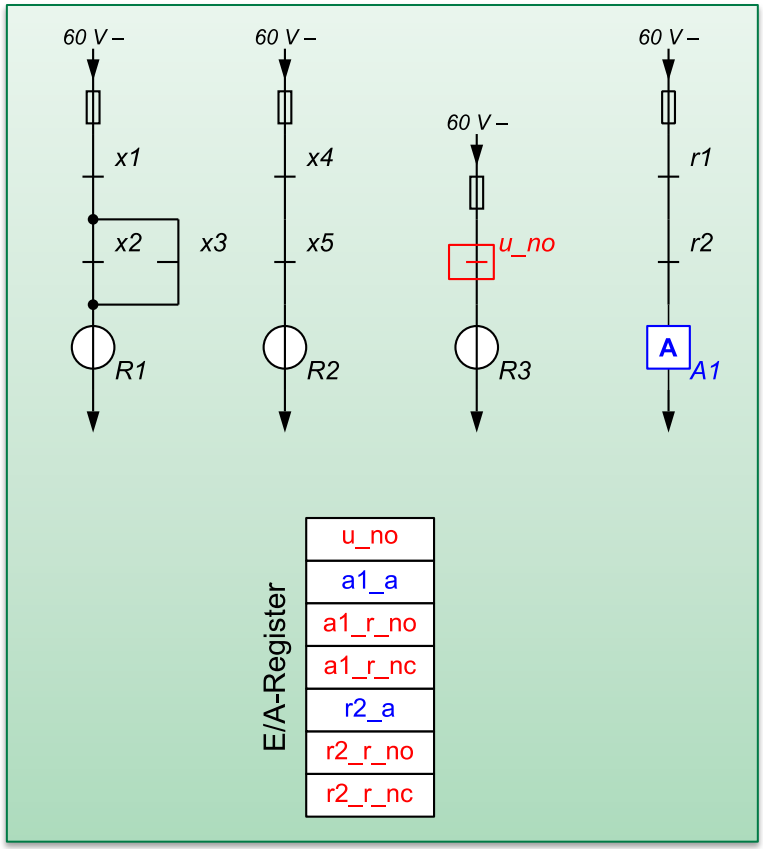
→ logische Zusammenfassung sinnvoll

Lösung

- Realisierung der logischen Verknüpfung in FPGA-Logik

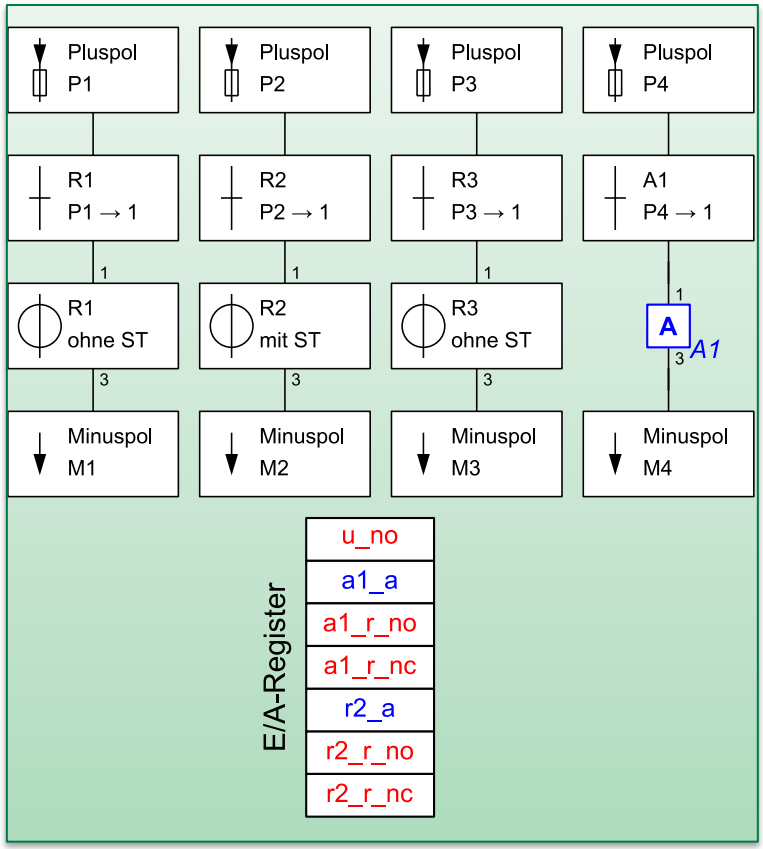
3. Transformation – Überführung (1)

Abbildung des Logikteils auf das Transformationsmodell



3. Transformation – Überführung (2)

Abbildung des Logikteils auf das Transformationsmodell



Überführung der Schaltungen in Moduldarstellung

- Pluspole, Minuspole
- Teilnetzwerke (Kombinatorik)
- Relaismodule
- Verzögerungsbausteine

Getrennte Überführung

- Kombinatorik (Ansteuerlogik)
- Relais (Zustandsmodelle)

Ansteuerlogik

- logische Verknüpfung der Teilnetzwerke im Ansteuerpfad

3. Transformation – Überführung (3)

Transformation der Ansteuerlogik

$$
\begin{aligned}
r1\_w &:= (x1\_no \wedge x2\_no) \vee \\
&\quad\ (x1\_no \wedge x3\_nc) \\
r2\_w &:= x4\_no \wedge x5\_no \\
r3\_w &:= u\_no \\
a1\_w &:= r1\_no \wedge r2\_no
\end{aligned}
$$

Analyse der Teilnetzwerke

- Überführung in Boolesche Gleichungen
- Backtracking-Algorithmus

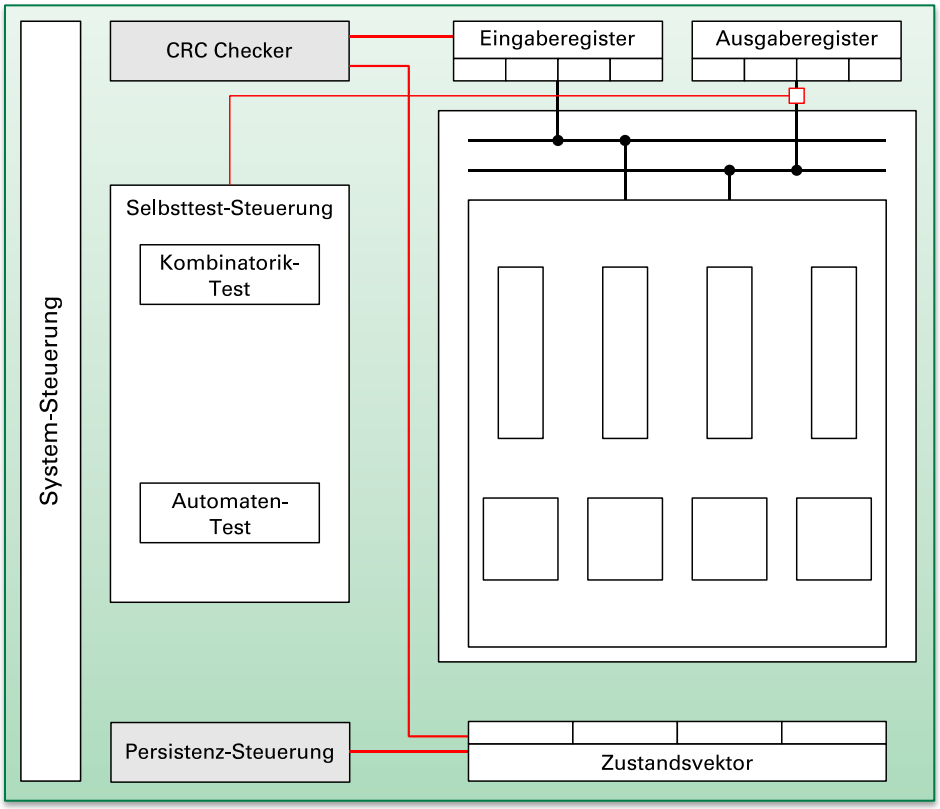
VHDL-Module

- ein Ansteuerlogik-Modul je Relaiswicklung

→ Boolesche Gleichungen

3. Transformation – Integration (1)

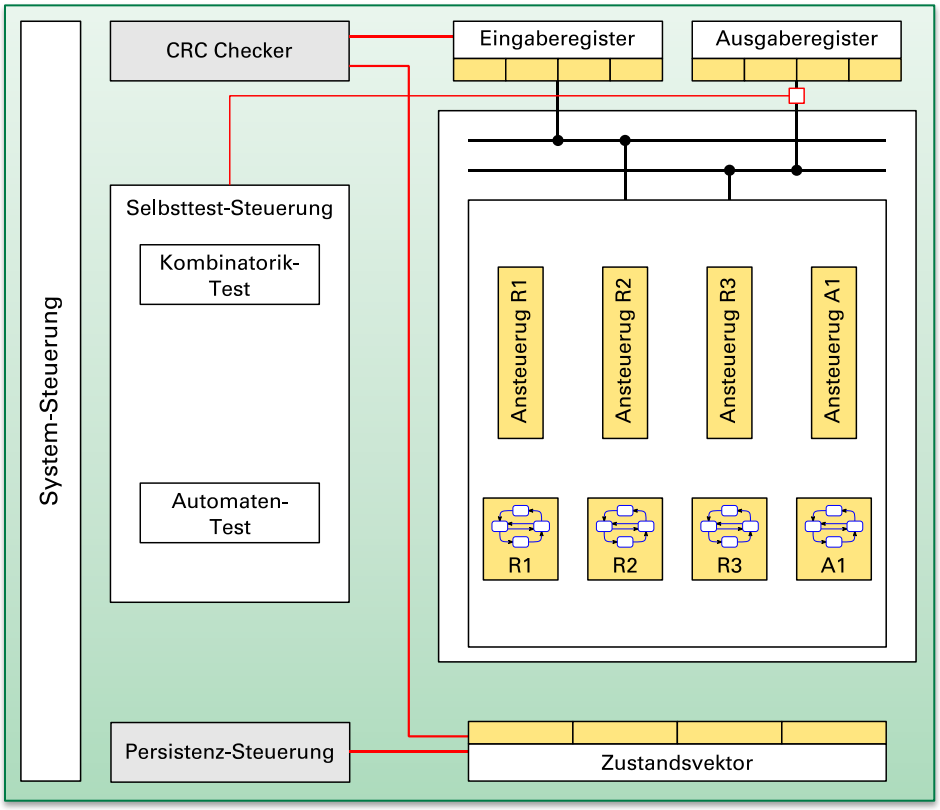
Integration in die Stellwerksplattform



- Generische FPGA-Logik
  - System-Steuerung
  - Selbsttest-Steuerung
  - Schnittstellen

3. Transformation – Integration (2)

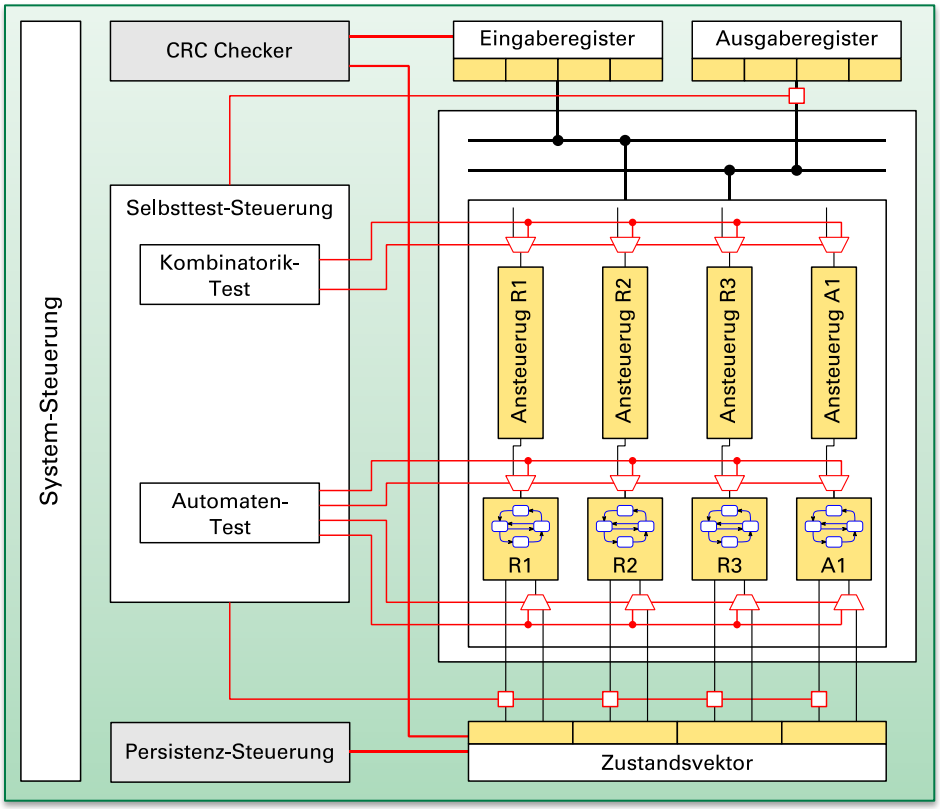
Integration in die Stellwerksplattform



- Generische FPGA-Logik
- Stellwerkslogik
  - Ansteuerlogik
  - Instanzen der Relaismodule
  - E/A-Register
  - Zustandsvektor
  - Definition permanent zu speichernder Zustände

3. Transformation – Integration (3)

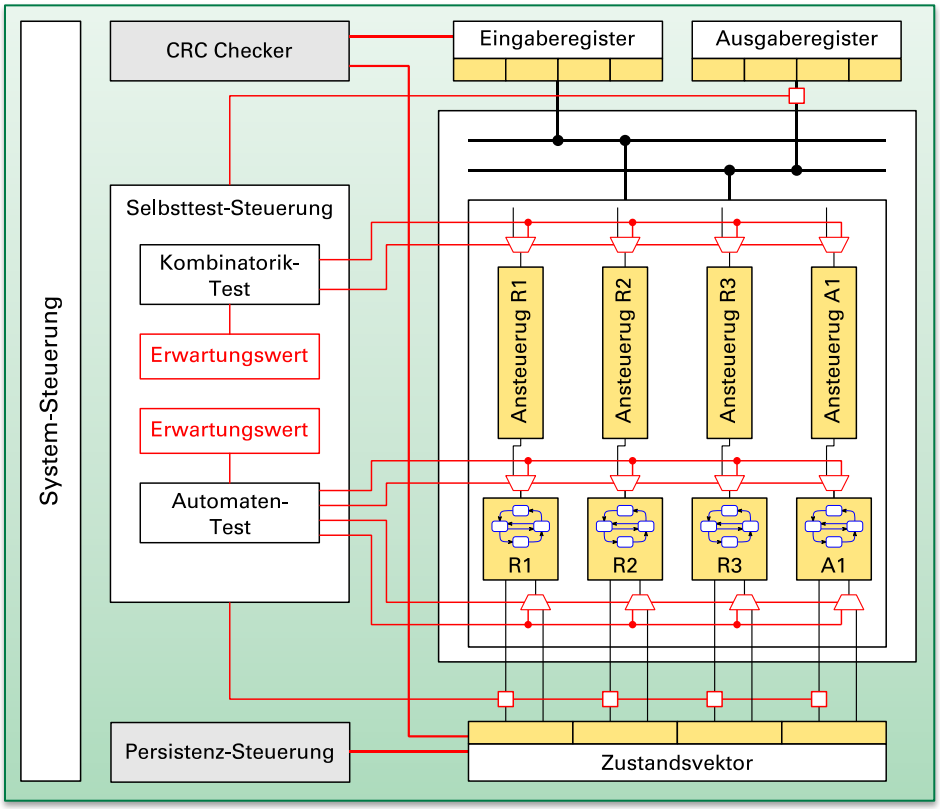
Integration in die Stellwerksplattform



- Generische FPGA-Logik
- Stellwerkslogik
- Selbsttest-Logik
  - Eingänge: Multiplexer zum Anlegen von Testmustern (TPG)
  - Ausgänge: Anschluss an Ausgabeanalysator (ORA)
  - getrennt für Ansteuerlogik und Relaisinstanzen

3. Transformation – Integration (4)

Integration in die Stellwerksplattform



- Generische FPGA-Logik
- Stellwerkslogik
- Selbsttest-Logik
- Erwartungswerte der Selbsttests
  - Ermittlung durch Simulation
- Synthese des VHDL-Code
  - Konfigurationsdatei
  - Übertragung auf FPGA

Gliederung

1. Motivation
2. Sichere Stellwerksplattform
3. Transformationsverfahren
4. **Ergebnisse und Ausblick**

Quellen und Literaturhinweise

4. Ergebnisse und Ausblick (1)

Ergebnisse

- Analyse und Vergleich der Sicherheitsprinzipien
- Konzeption einer sicheren Stellwerksplattform
- Entwicklung des Transformationsverfahrens
- Anwendung am Beispiel der Weichengruppe GS II DR

Sichere Stellwerksplattform

- Beibehaltung der bisherigen Schnittstellen
- Entwicklung der Ausfalloffenbarungsmechanismen
- Sicherheitsmechanismen unabhängig vom FPGA-Typ
  → einfache Migration
- Nachweis der Eignung unter worst-case Annahmen:
  → HR < 10^{-8} h^{-1} < THR (SIL 4)

4. Ergebnisse und Ausblick (2)

Regelwerk der Transformation

- Vorverarbeitung mit Planprüfung
- Realisierung generischer Relaismodule
- Transformation der kombinatorischen Ansteuerlogik
- Integration generischer Selbsttestmechanismen
- Konzept zur Verifikation und Validierung

Weitere Schritte

- vollständige Entwicklung und Realisierung der Plattform
- Umsetzung des Regelwerks in ein Transformationswerkzeug
- Führung der Sicherheitsnachweise für die generische Plattform und das Transformationswerkzeug

Quellen und Literaturhinweise

Quellen

[1] Kötting, Holger: Liste Deutscher Stellwerke. Oktober 2012. http://www.stellwerke.de/liste/seite3_s.html

[2] Stroud, Charles E.: A Designer‘s Guide to Built-In Self-Test. Boston: Kluwer Academic Publishers, 2002.

Literaturhinweise

- Kusche, Wolfgang: Gleisbildstellwerke. Berlin: transpress, Verlag für Verkehrswesen, 1984.
- Kesel, Frank; Bartholomä, Ruben: Entwurf von digitalen Schaltungen und Systemen mit HDLs und FPGAs. München: Oldenbourg, 2009.
- Fenner, Wolfgang; Naumann, Peter; Trinckauf, Jochen: Bahnsicherungstechnik. Erlangen: Publicis Corporate Publishing, 2003.
- DIN EN-Normen: 61508, 50129, 50128, 13849