

Fehlerredundante Computerarchitektur zur Flugzeugsteuerung



Prof. Dr. Anton Gunzinger
CEO

Supercomputing Systems AG
Technoparkstrasse 1
8005 Zürich

Tel: 01/445 16 00
Fax: 01/445 16 10
e-mail: gunzinger@scs.ch
www: <http://www.scs.ch>

Übersicht

Supercomputing Systems

1. Übersicht Flugzeug
2. Anforderungen
3. Lösungsansatz
4. Umsetzung
5. Teststrategie
6. Zusammenfassung

1.1 Das Flugzeug

Supercomputing Systems

- ❖ Kleinmaschine
- ❖ 4-12 Passagiere

1.2 Steuerung

Supercomputing Systems

❖ Flugzeug: Power Vector Controlled

- Keine Control Surfaces wie Klappen

❖ 12 Jets

- Leistung
- Anstellwinkel

→ Avionik: Fly By Wire nötig

→ Ausfall der Avionik: 

2.1 Anforderungen

Supercomputing Systems

- ❖ Steuerung (Primary Flight Computer, PFC) muss immer funktionieren
- ❖ Kompletter System-Restart in ca. 100ms (z.B. nach Blitzschlag)

2.2 Anforderungen Gesetzgeber

Supercomputing Systems

❖ Wahrscheinlichkeit eines schwerwiegenden Unfalls

- Klasse I (SEP, <2.7t): $<10^{-6}/h$
- Klasse II (MEP, SET, <2.7t): $<10^{-7}/h$
- Klasse III (SEP, MEP, SET, MET, >2.7t): $<10^{-8}/h$
- Klasse IV (Commuter): $<10^{-9}/h$
- SEP/MEP: Single/Multi Engine Piston
- SET/MET: Single/Multi Engine Turbine

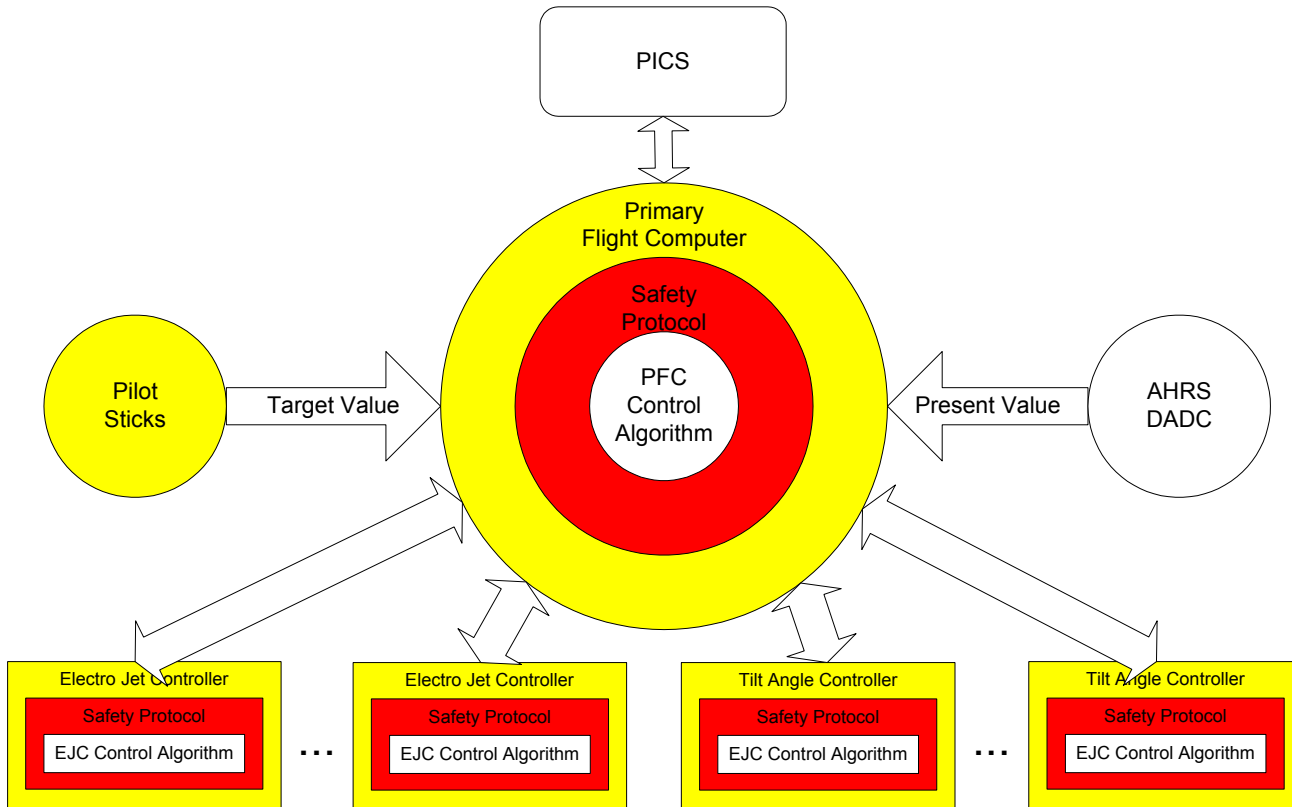
2.3 Zuverlässigkeit Bauteile

Supercomputing Systems

- ❖ Passive Bauteile (R, L): $10^{-7} \dots 10^{-8}/h$
- ❖ Halbleiter: $\approx 10^{-6}/h$
- ❖ Elko: $\approx 10^{-5}/h$
- Zuverlässigkeit Board: $\approx 10^{-4}/h$
- Anforderung Behörden: $10^{-8} \dots 10^{-9}/h$
- Anforderung nicht mit einem Rechner erfüllbar, **Redundanz nötig!**

3.1 Gesamtkonzept Regelung I

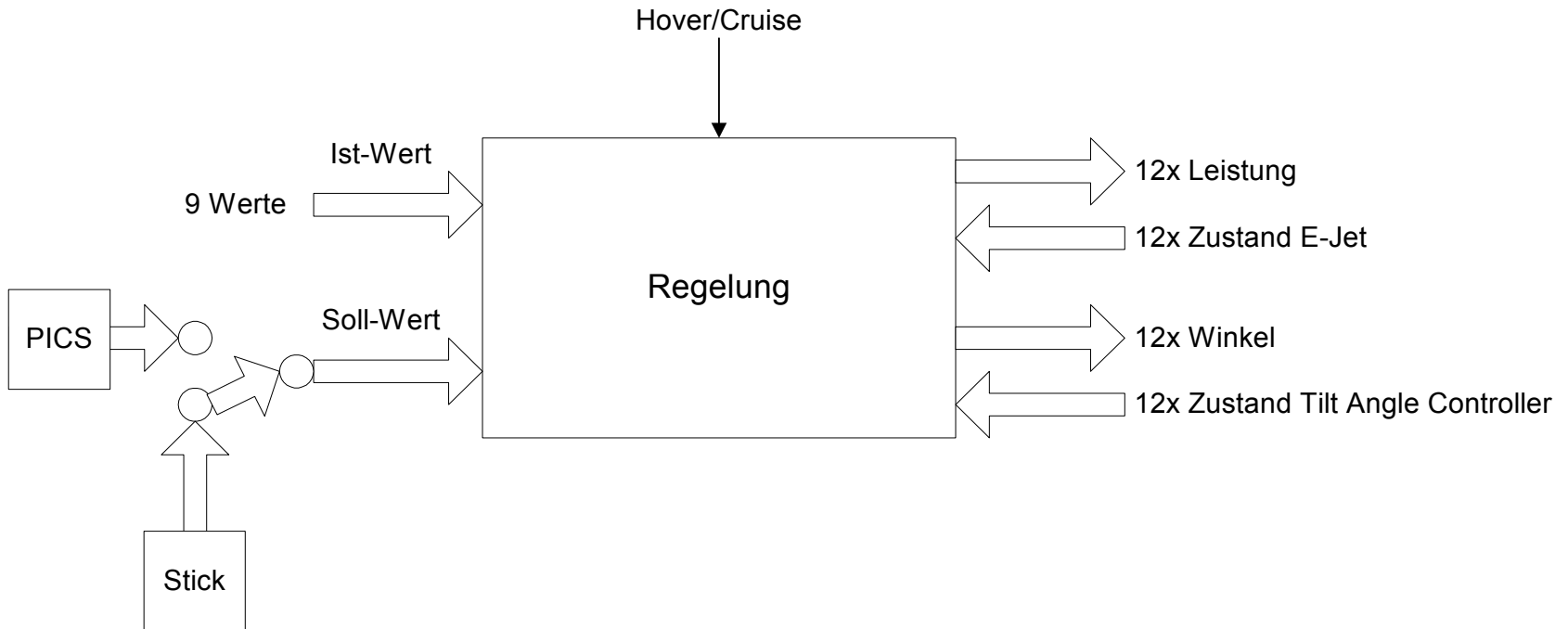
S Supercomputing Systems



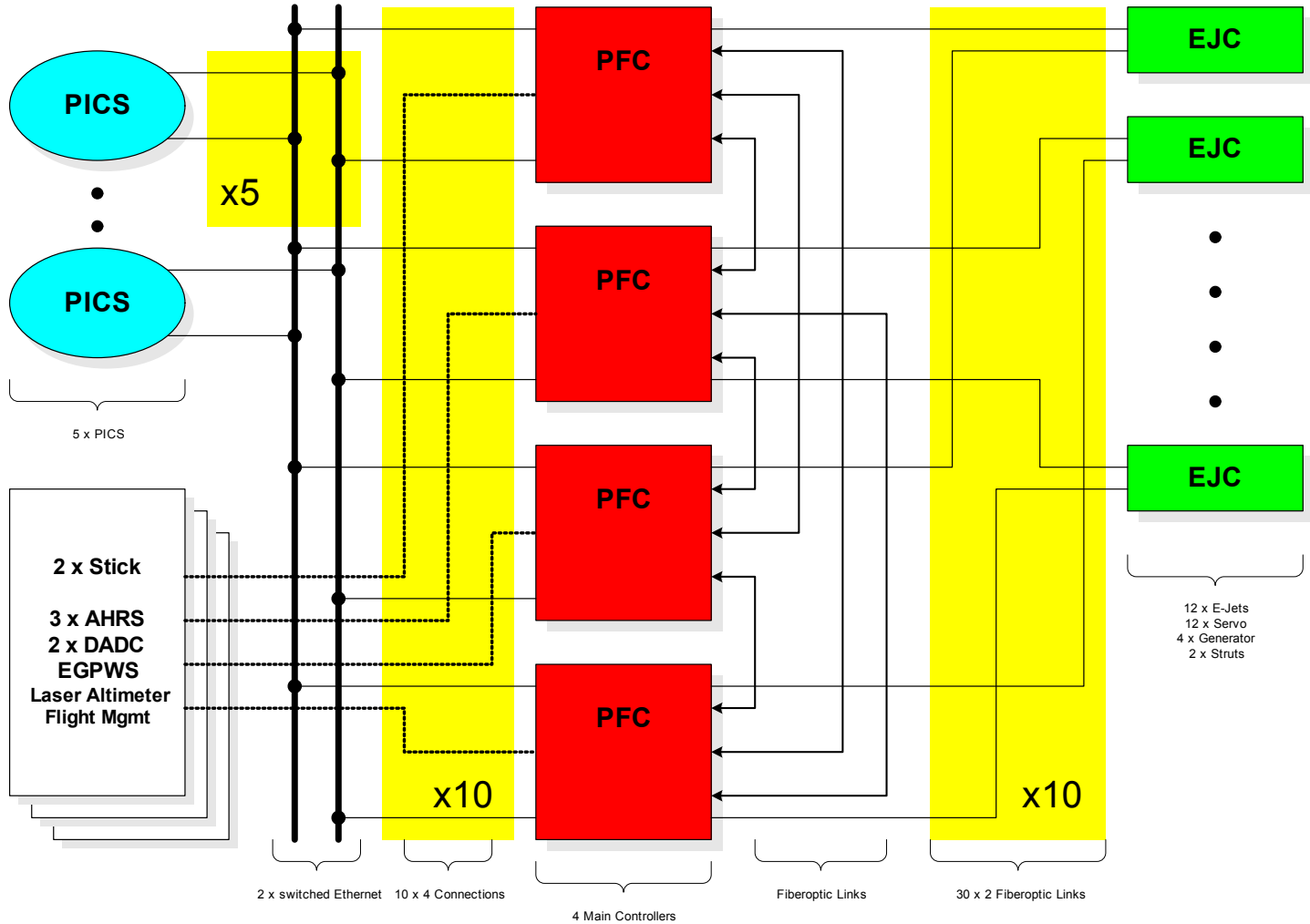
3.2 Gesamtkonzept Regelung II

Supercomputing Systems

❖ Samplingrate Regler: 50 Hz

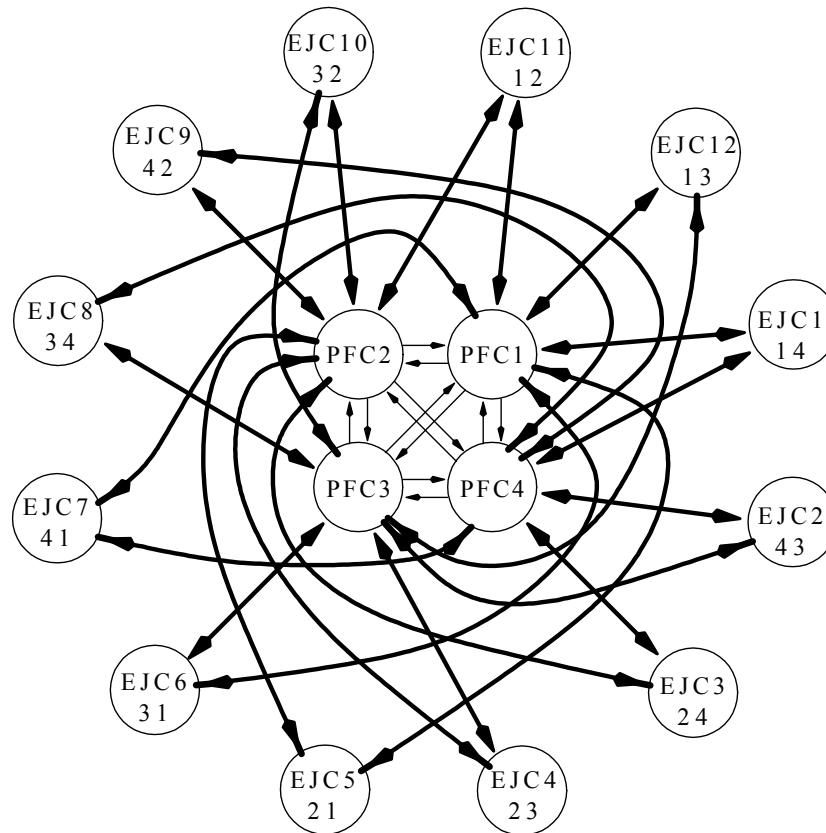


3.3 Übersicht Steuerung



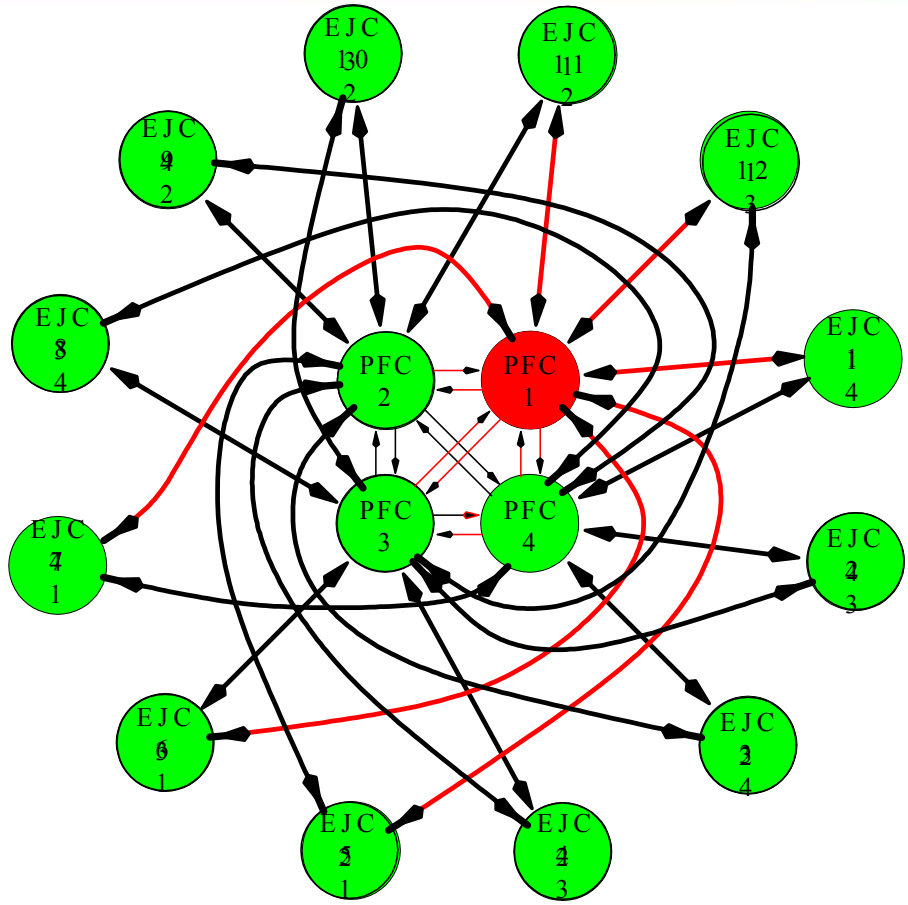
3.4 Verkabelung des Systems I

Supercomputing Systems



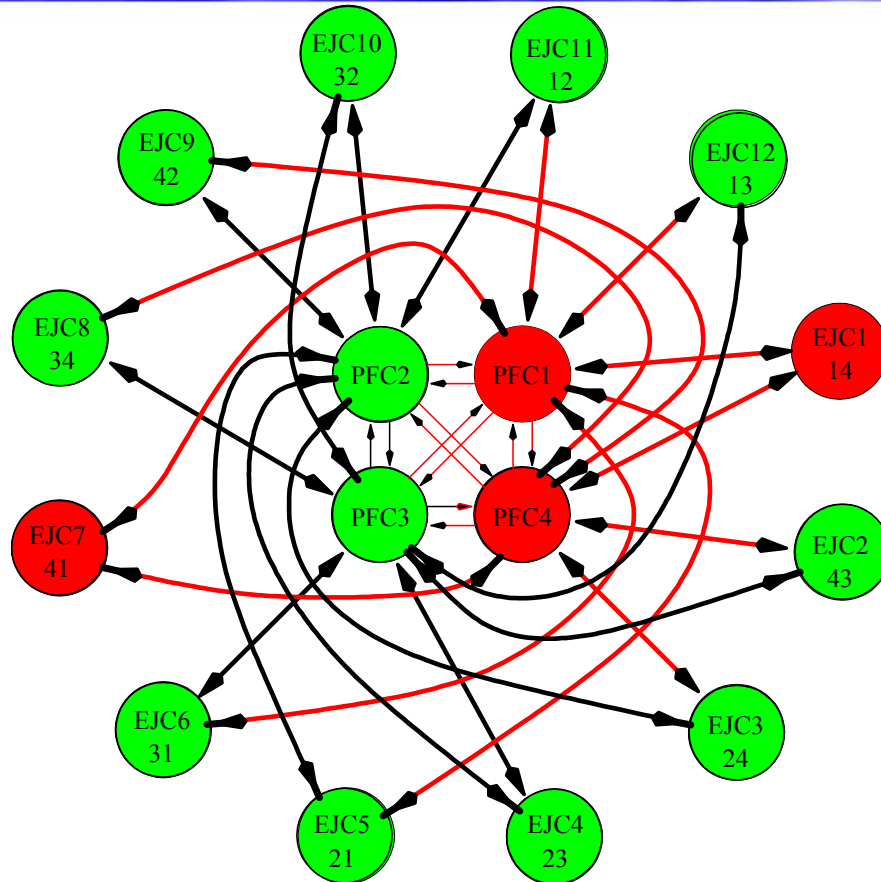
3.5 PFC1 tot

Supercomputing Systems



3.6 PFC1 tot, PFC4 tot

Supercomputing Systems



3.7 Fehlerunterscheidung

Supercomputing Systems

❖ Benign

- Rechner/Sensor liefert keine oder einfach als ungültig erkennbare Daten

❖ Byzantine

- Rechner/Sensor liefert plausible jedoch falsche Daten

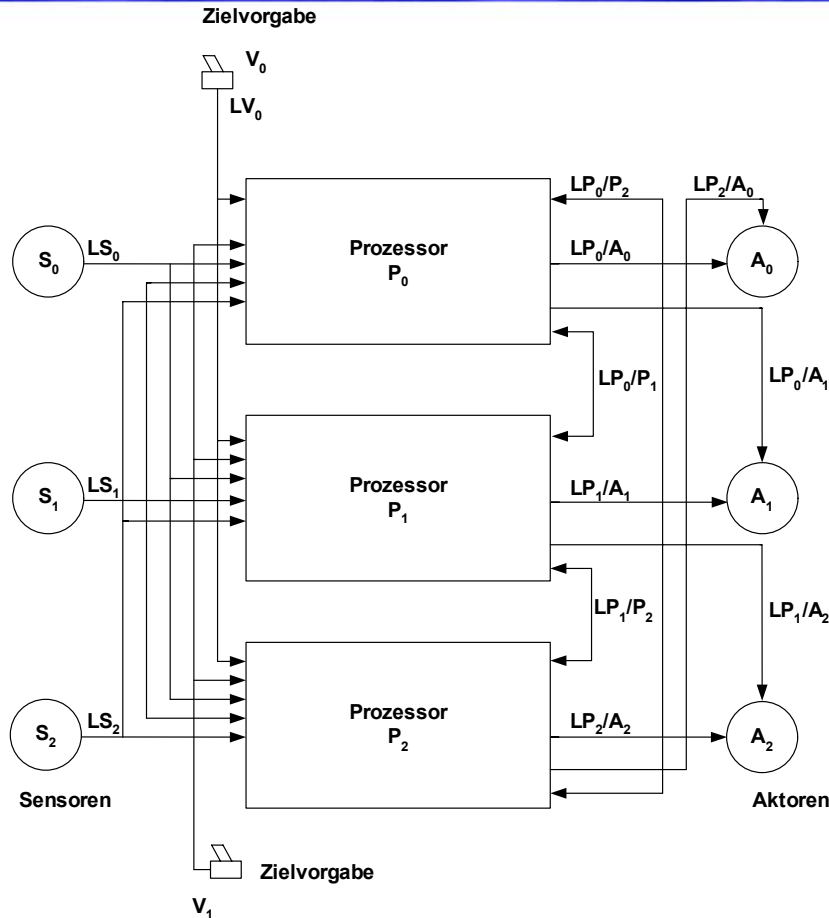
3.8 Redundante PFC

Supercomputing Systems

- ❖ Alle 4 PFC-Rechner rechnen synchron dasselbe
 - Keine Rekonfiguration im Fehlerfall
 - Synchrone, Zeitgesteuerte Kommunikation
 - ❖ Einfach beweisbar korrekt
 - ❖ Globale zuverlässige synchronisierte Zeit nötig
 - Verteilung/Auswahl des gültigen Werts durch Byzantine Agreement

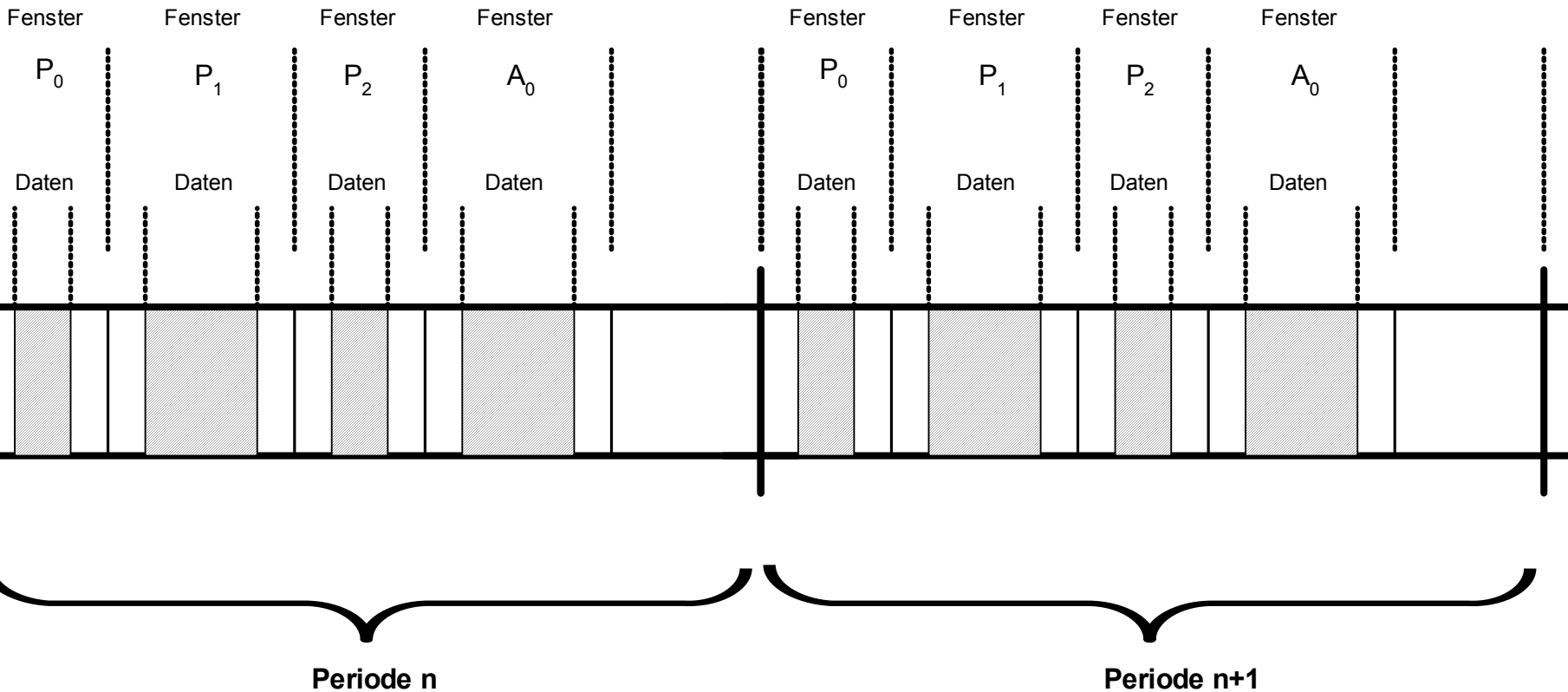
3.9 Detailiertes Blockschaftbild

S Supercomputing Systems



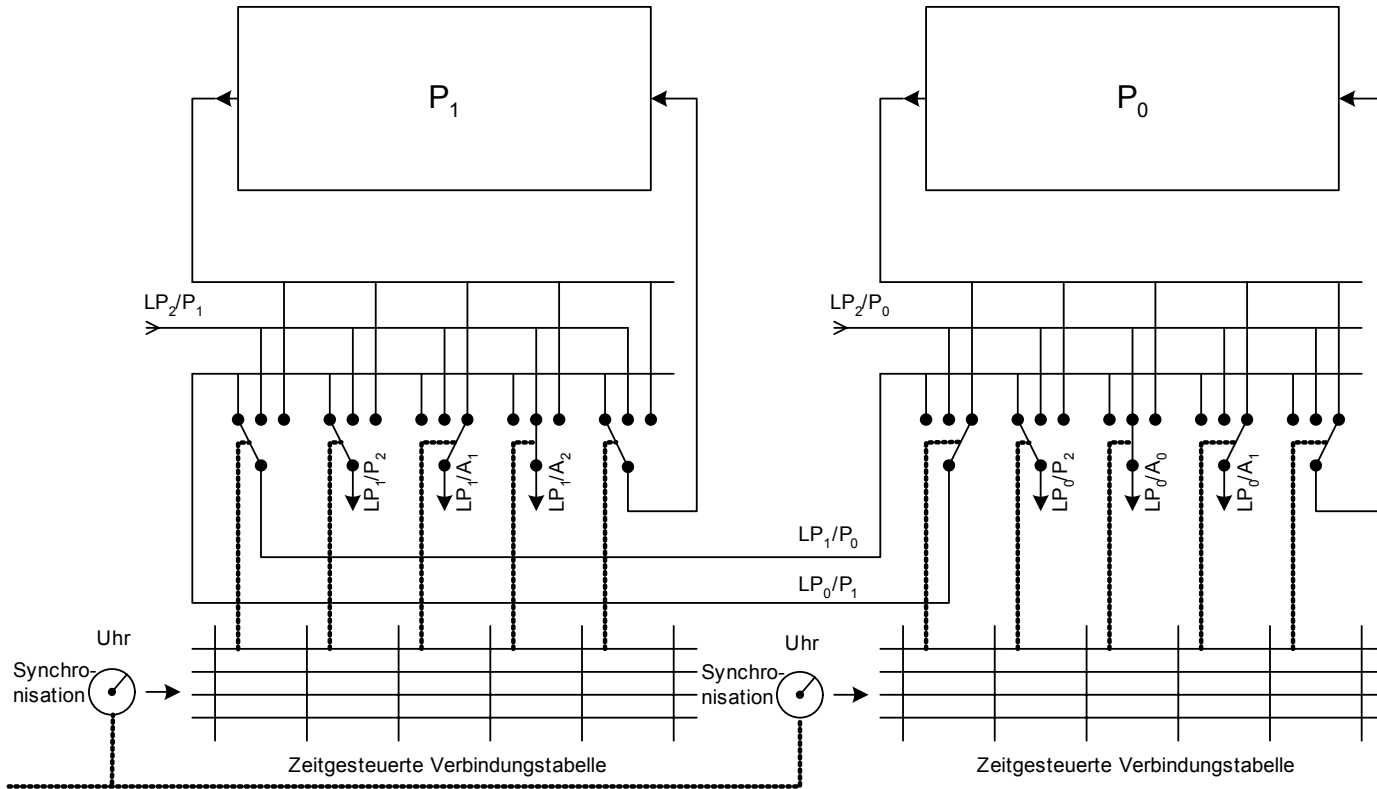
3.10 Zeitmultiplexverfahren

Supercomputing Systems



3.11 Verteiltes Steuerwerk für die Kommunikation

Supercomputing Systems



3.12 Kommunikation im Fehlerfall

Supercomputing Systems

	LP ₀ /A ₀	LP ₂ /A ₀
P ₀		
P ₁		
P ₂		

Figur 3

Empfangene Daten im Aktor A₀; Normalbetrieb

	LP ₀ /A ₀	LP ₂ /A ₀
P ₀		
P ₁		
P ₂		

Figur 3A

Empfangene Daten im Aktor A₀; LP₂/A₂ defekt

	LP ₀ /A ₀	LP ₂ /A ₀
P ₀		
P ₁		
P ₂		

Figur 3B

Empfangene Daten im Aktor A₀; LP₀/P₁ defekt

	LP ₀ /A ₀	LP ₂ /A ₀

Figur 3C

 Daten ungültig

 Daten ungültig

	LP ₀ /A ₀	LP ₂ /A ₀

Figur 3D

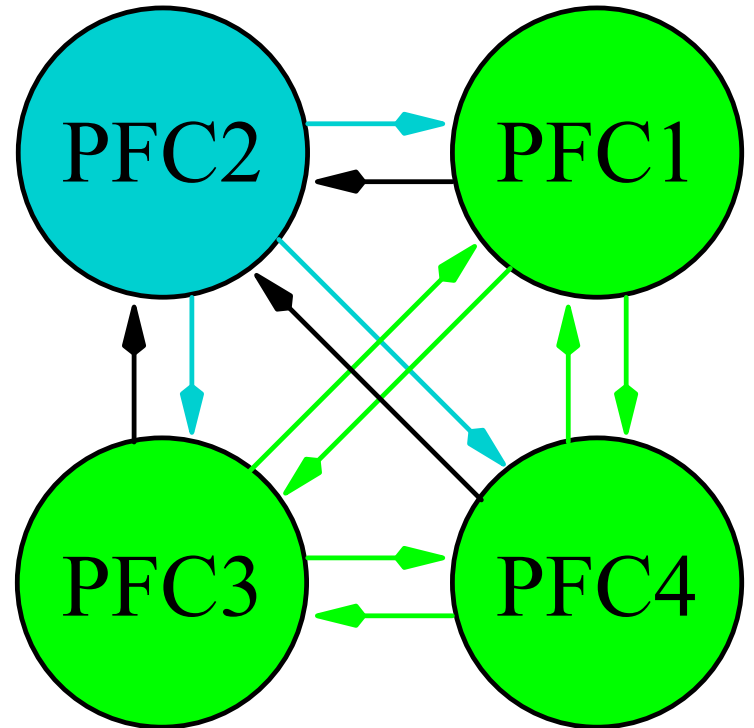
 Daten ungültig

 Daten ungültig

3.13 Byzantine General's Problem

Supercomputing Systems

- ❖ PFC2 General
- ❖ PFC1,3,4 Lieutenant
- ❖ Lieutenants untereinander verifizieren, dass der General nicht korrupt ist



3.14 Oral vs. Signed Messages

Supercomputing Systems

❖ Oral Messages (OM)

- Können von korrupten Teilnehmern gefälscht werden
- Einfach implementierbar
- Aufwändigeres Protokoll, weniger korrupte Teilnehmer tolerierbar (<33%)

❖ Signed Messages (SM)

- Können von korrupten Teilnehmern nicht gefälscht, nur unterdrückt werden
- Kompliziertere Implementation (Public Key Cryptography)
- Weniger ausgetauschte Messages (insbes. bei nichtvollständigem Kommunikationsgraph), mehr korrupte Teilnehmer tolerierbar (<50%, wenn Erreichbarkeit gewährleistet bleibt)

4. Teststrategie

Supercomputing Systems

Design-Verifikation:

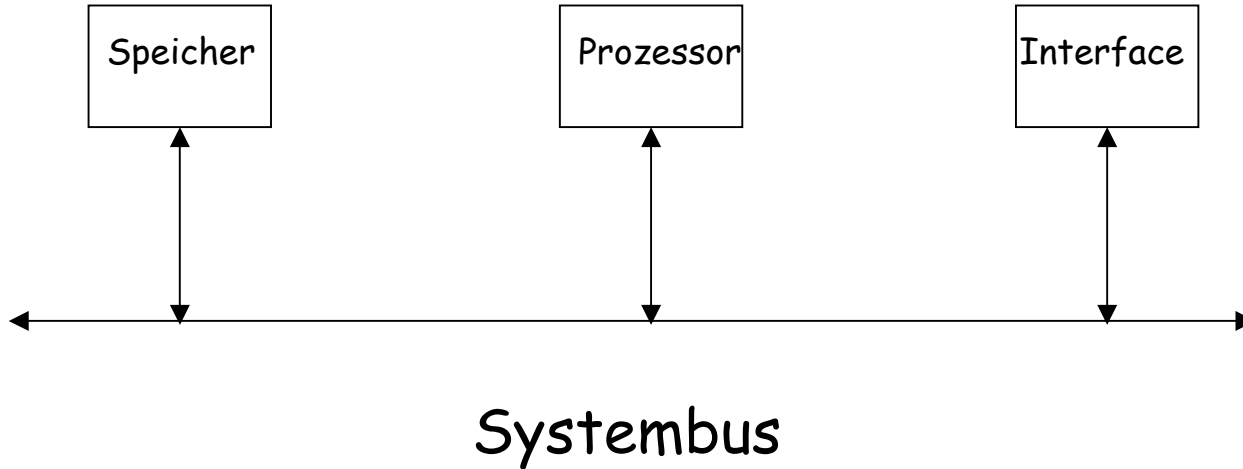
- ❖ Überprüfen von Programmen und Schaltungen gegenüber den Spezifikationen
- ❖ Test des Zusammen-spiels der Komponenten inkl. Fehlerfällen

Pre- & Inflight Tests:

- ❖ Sicherstellen der korrekten Funktion vor und während des Betriebs
- ❖ Frühzeitiges Erkennen von potentiellen Problemen

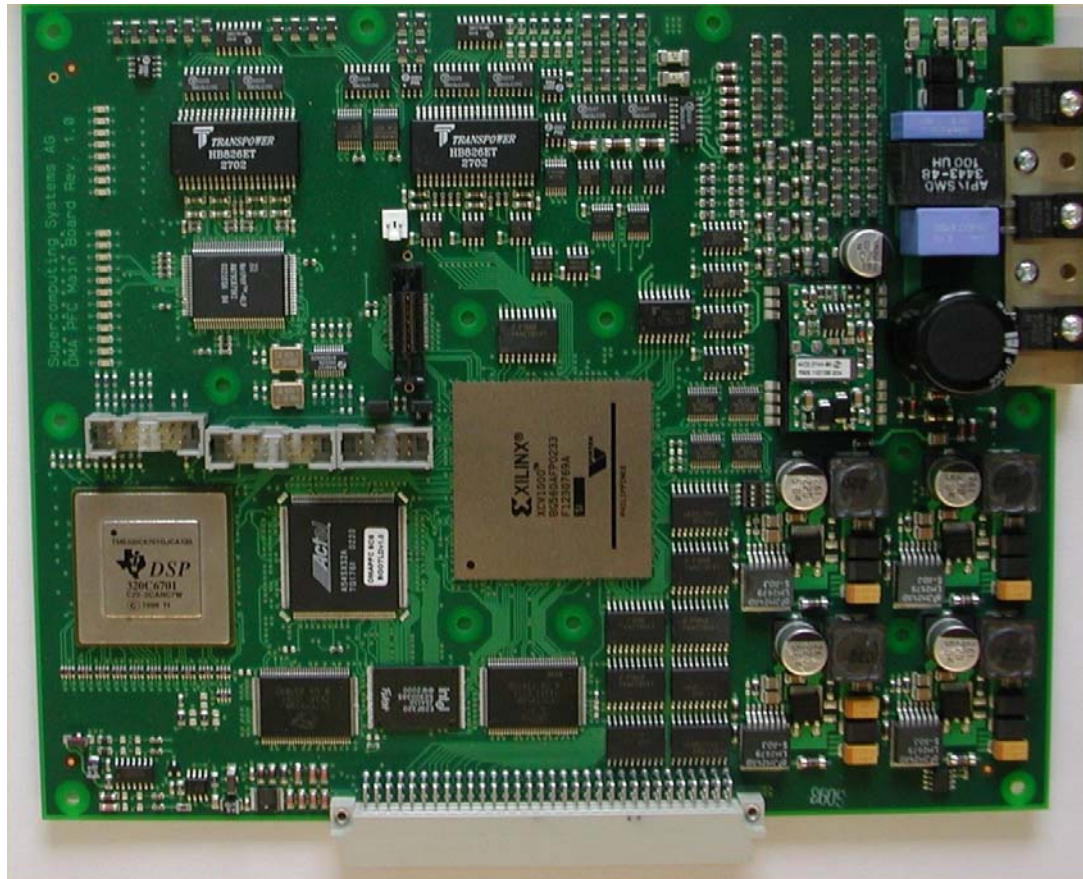
4.1 Blockschaltbild PFC

Supercomputing Systems



4.2 Realisation

Supercomputing Systems



5.1 Design Verifikation

Supercomputing Systems

- ❖ Jede Komponente (HW-Karte, SW-Modul) wird nach der Entwicklung getestet
 - ❖ Das Zusammenspiel sämtlicher Komponenten wird vor dem ersten Flug im Simulator getestet
→ Störungsfälle können auf sicherem Boden durchgespielt werden
- Verifikation ist als wichtigster Projektschritt zu betrachten, entsprechende Features sind von Anfang an einzuplanen

5.2 Pre- & Inflight Tests

Supercomputing Systems

- ❖ Sämtliche Datenspeicher (SRAM, DSP, FPGA) sowie Kommunikationsleitungen werden durch Prüfsummen gesichert
 - ❖ Komponenten überwachen sich selbst und gegenseitig
 - ❖ Watchdog in höchst zuverlässigem Antifuse-FPGA
- Testbarkeit ist das zentralste Feature und muss schon im Design eingeplant werden

6. Zusammenfassung

Supercomputing Systems

- ❖ Es wurde ein Konzept für ein fehlerredundanten Rechner vorgestellt
- ❖ Dieses Konzept garantiert, dass im Fehlerfall keine andere Verarbeitung als im Normalbetrieb vorkommt
- ❖ Es lässt sich beweisen, dass auch mehrere gleichzeitig auftretende Fehler ein korrektes Arbeiten des Rechners garantieren.