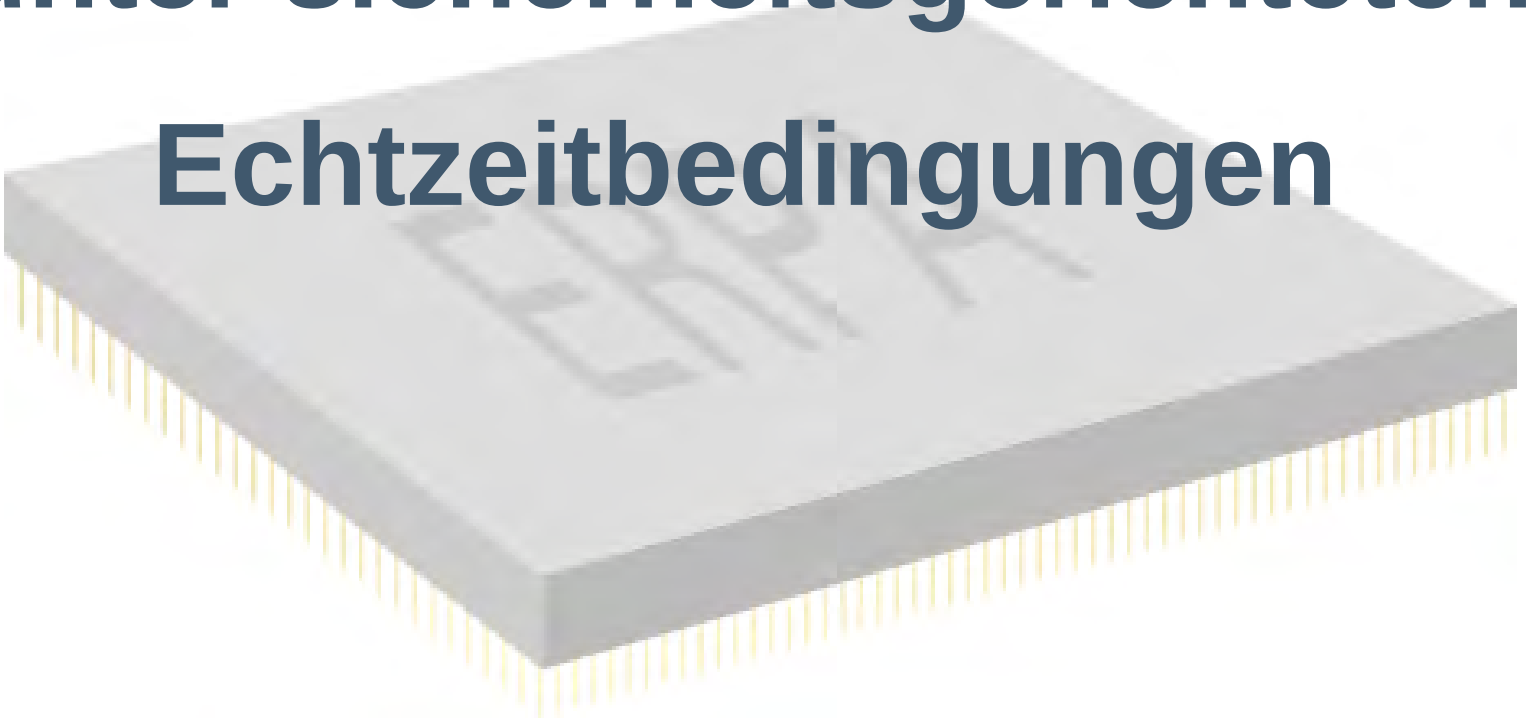
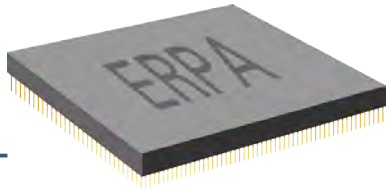
Prozessorarchitektur zum Einsatz unter sicherheitsgerichteten Echtzeitbedingungen



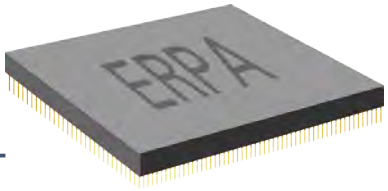
Dipl.-Ing. (FH) Daniel Koß

Inhalt



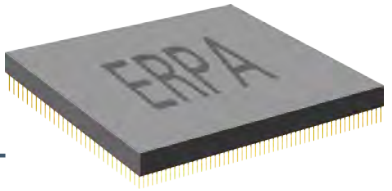
- Grundlagen
- Stand der Technik
- Anforderungen
- Konzeptentwurf
- Bewertung
- Fazit und Ausblick

Übersicht



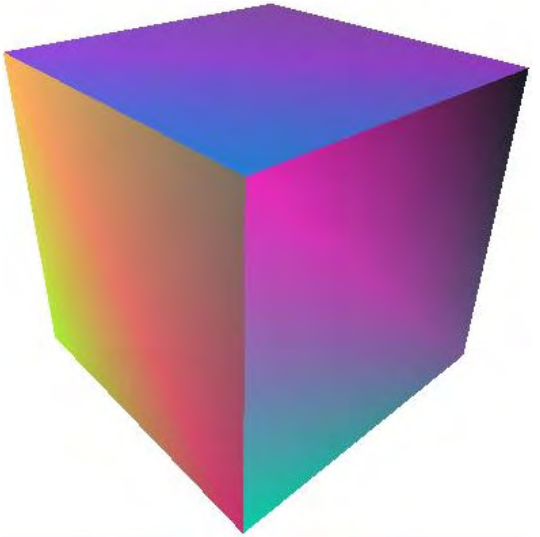
- Grundlagen
- Stand der Technik
- Anforderungen
- Konzeptentwurf
- Bewertung
- Fazit und Ausblick

Grundlagen



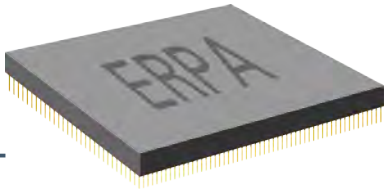
Technologietreiber

3D-Technologien



Multimedia

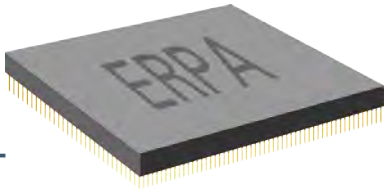
Grundlagen



Herausforderungen der Prozessautomatisierung

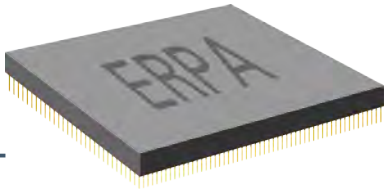
- Echtzeitbedingungen
  - Garantierte Einhaltung definierter Zeitschranken
  - Vorhersehbarkeit von Verhalten & Ausführungszeit
- Sicherheit
  - Ausschluss der Gefährdung von Mensch & Umwelt

Übersicht



- Grundlagen
- Stand der Technik
- Anforderungen
- Konzeptentwurf
- Bewertung
- Fazit und Ausblick

Stand der Technik

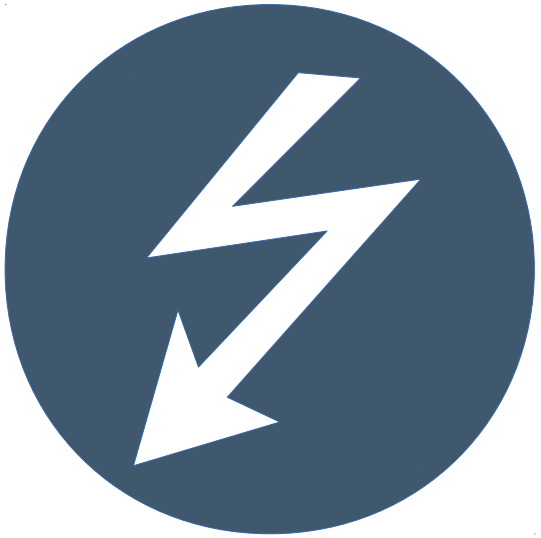


Problematische Technologien

Unterbrechungen

Ausfallsicherheit

Prioritäten



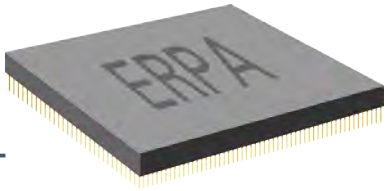
Pipelines

Prozessorspeicher

RISC vs. CISC

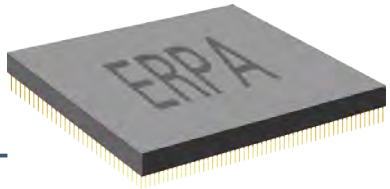
Superskalarität

Übersicht



- Grundlagen
- Stand der Technik
- Anforderungen
- Konzeptentwurf
- Bewertung
- Fazit und Ausblick

Anforderungen



Allgemeine Anforderungen

Fehler- und Ausfallerkennung

Vorhersehbarkeit

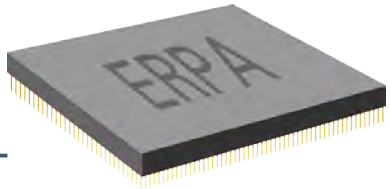
Rechtzeitigkeit

Fehlertoleranz

Sicherer Zustand

Einsatz nach SIL 4 (DIN EN 61508)

Anforderungen



Konkrete Anforderungen aus der DIN EN 61508

Trennung von sicheren & unsicheren Funktionen

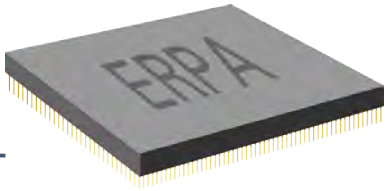
Besondere Behandlung von Halbleiter-Redundanz

Vermeidung asynchroner Konstrukte

Unentdeckte, unsichere Ausfälle < 10%

Logik simplifizieren

Anforderungen



Anforderungen der DIN EN 61508 an die Programmierbarkeit

Diversitäre Überwachungseinrichtungen

Statische Betriebsmittelzuteilung

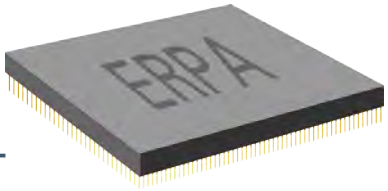
Abgestufte Funktions-einschränkung

Vermeidung von Unterbrechungen

Zyklische Abarbeitung empfohlen

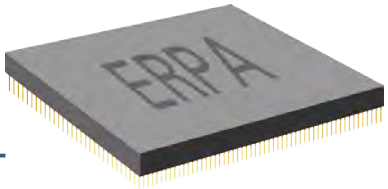
Statische Zugriffsynchronisation auf gemeinsam genutzte Ressourcen

Übersicht



- Grundlagen
- Stand der Technik
- Anforderungen
- Konzeptentwurf
- Bewertung
- Fazit und Ausblick

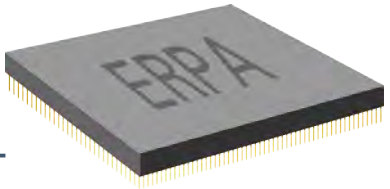
Konzeptentwurf



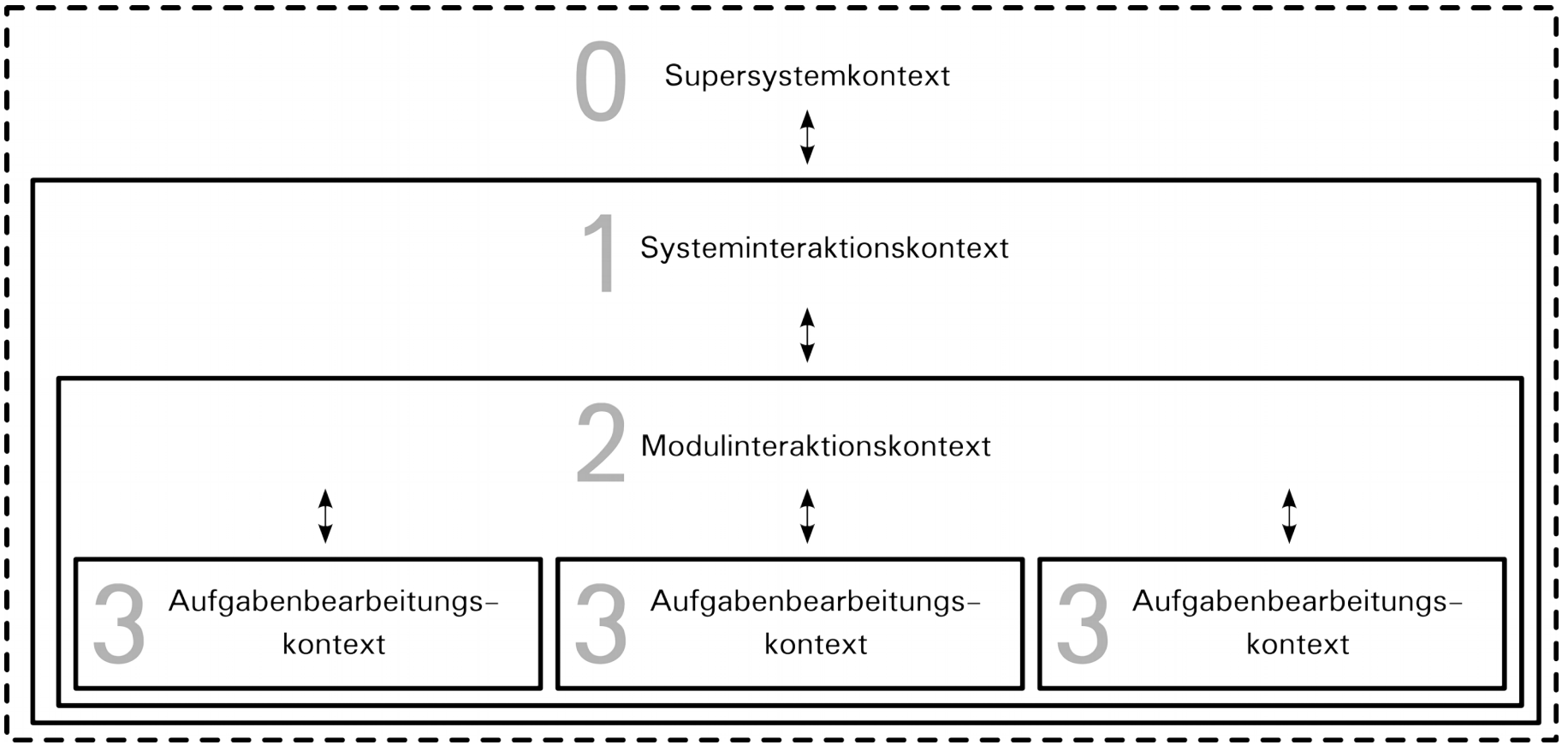
„[...] von sicherheitsgerichteten Automatisierungssystemen zu erfüllende Bedingungen und Ziele können nur erreicht werden, wenn Einfachheit als fundamentales Entwurfsprinzip gewählt [wird]“

Halang, Konakovsky (2013)

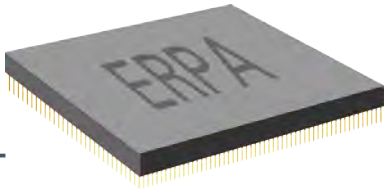
Konzeptentwurf



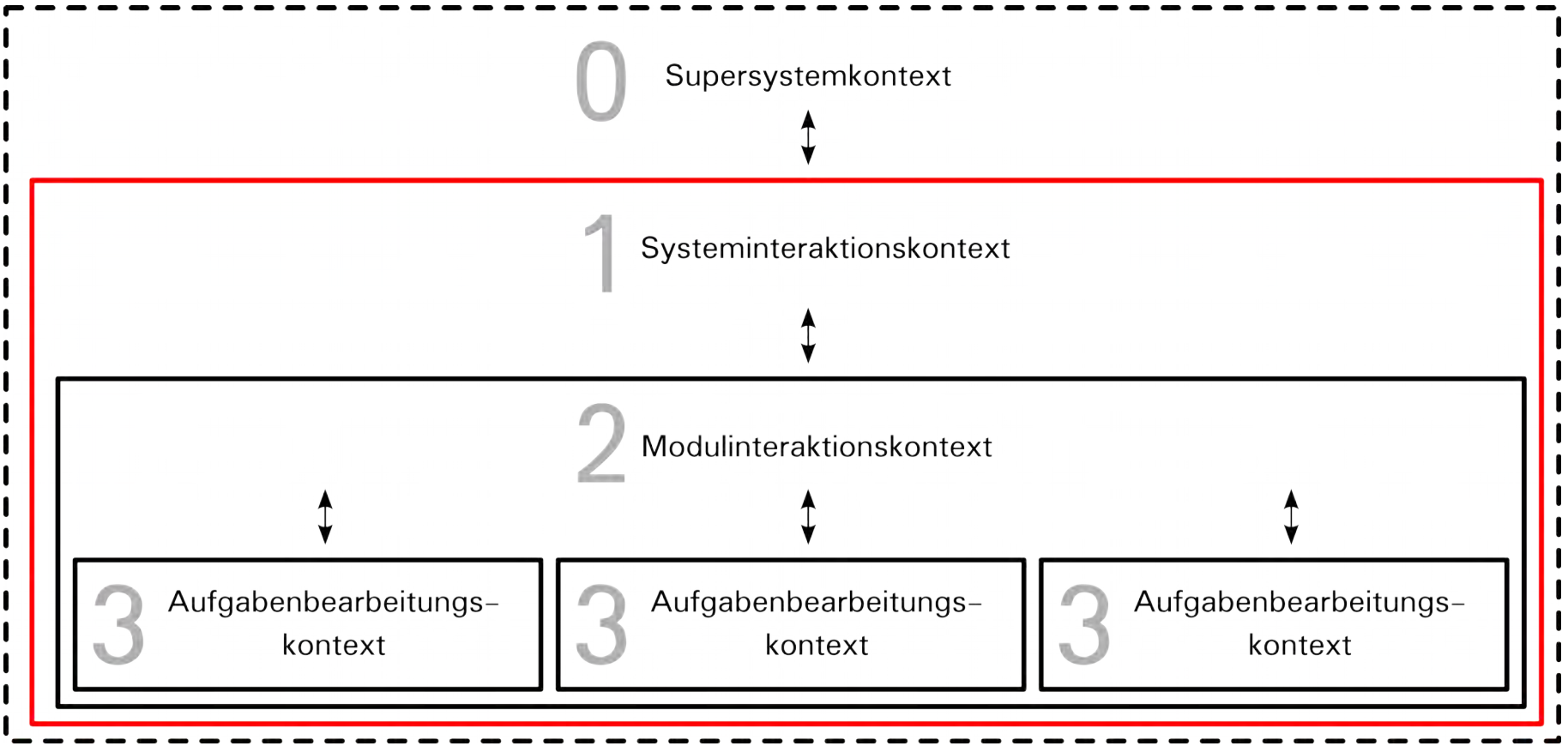
Abstraktionsebenen



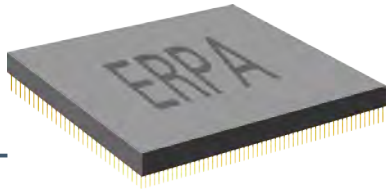
Konzeptentwurf



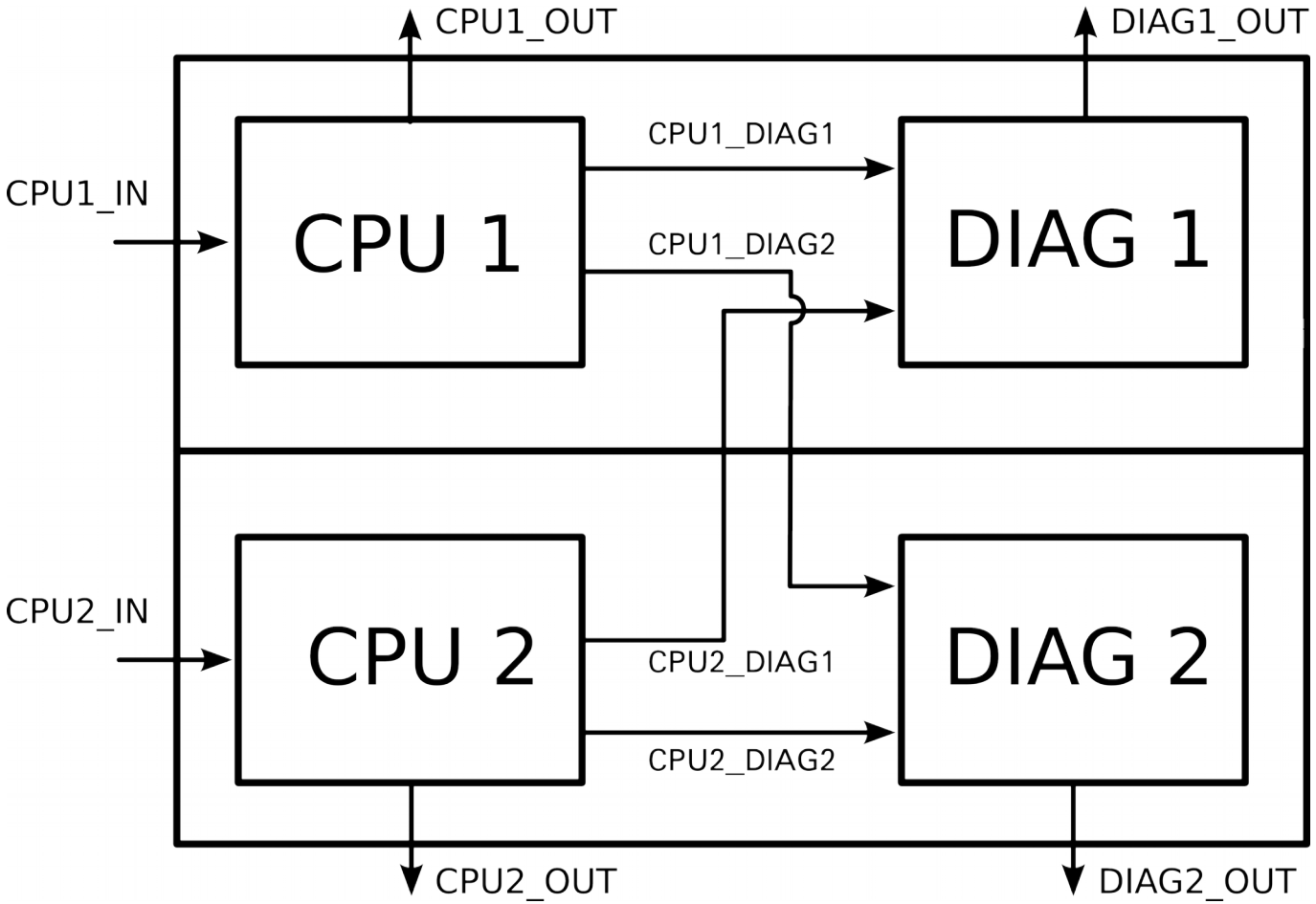
Systeminteraktionskontext



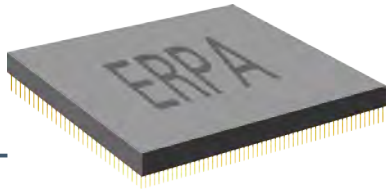
Konzeptentwurf



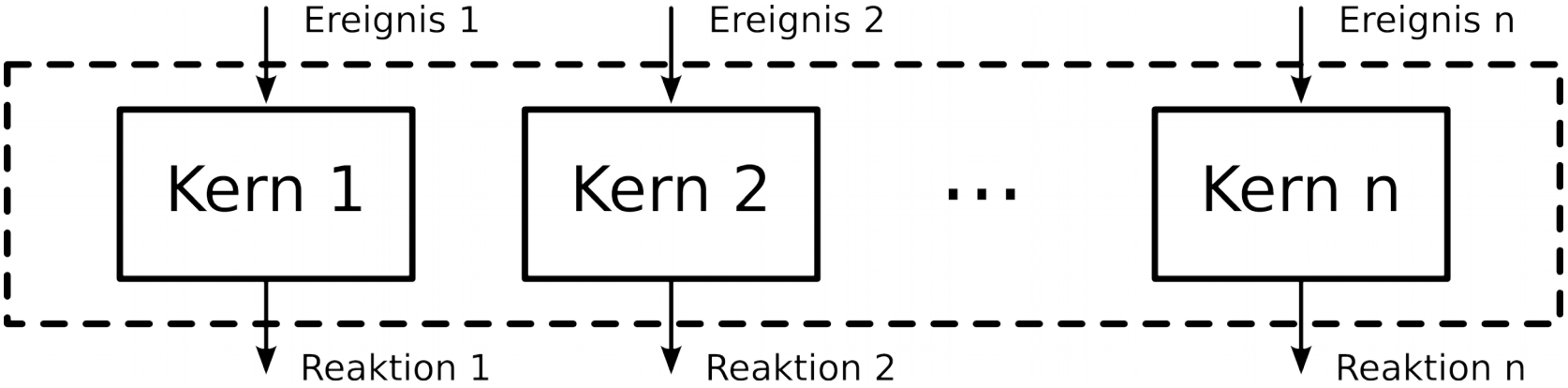
Systeminteraktionskontext



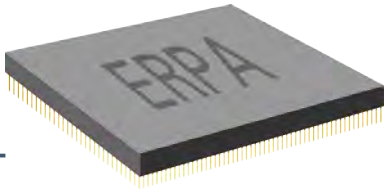
Konzeptentwurf



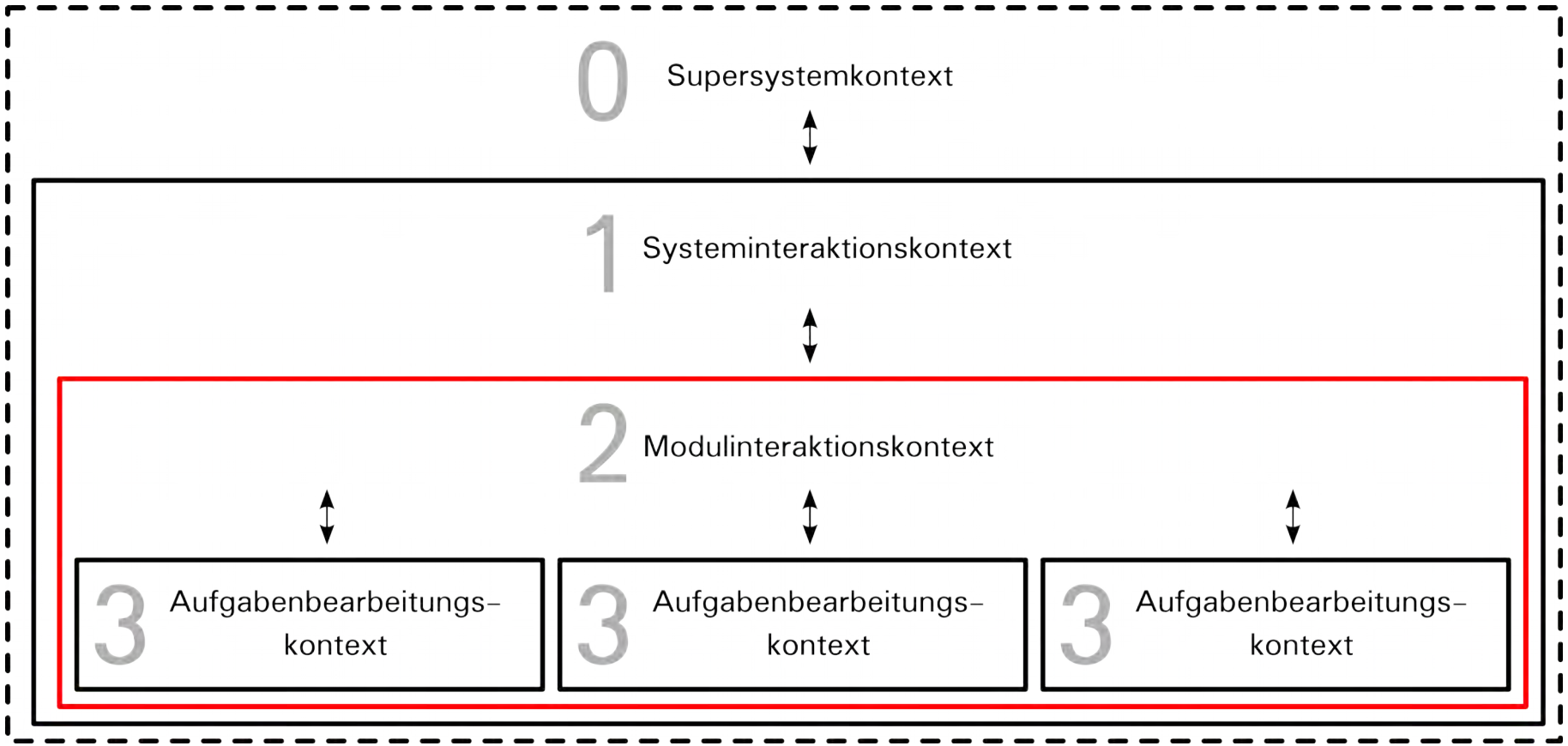
Systeminteraktionskontext



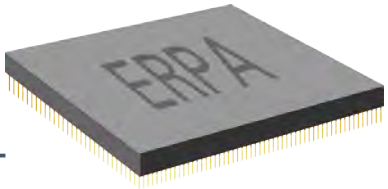
Konzeptentwurf



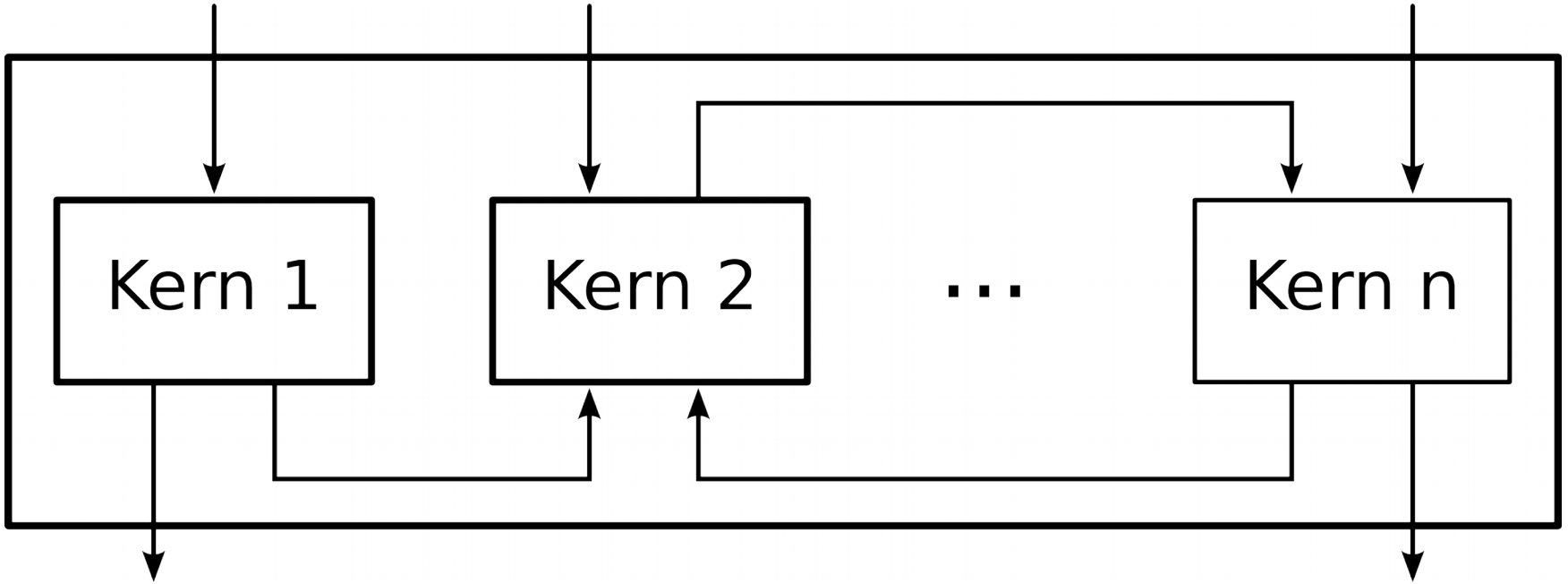
Modulinteraktionskontext



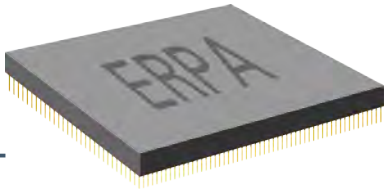
Konzeptentwurf



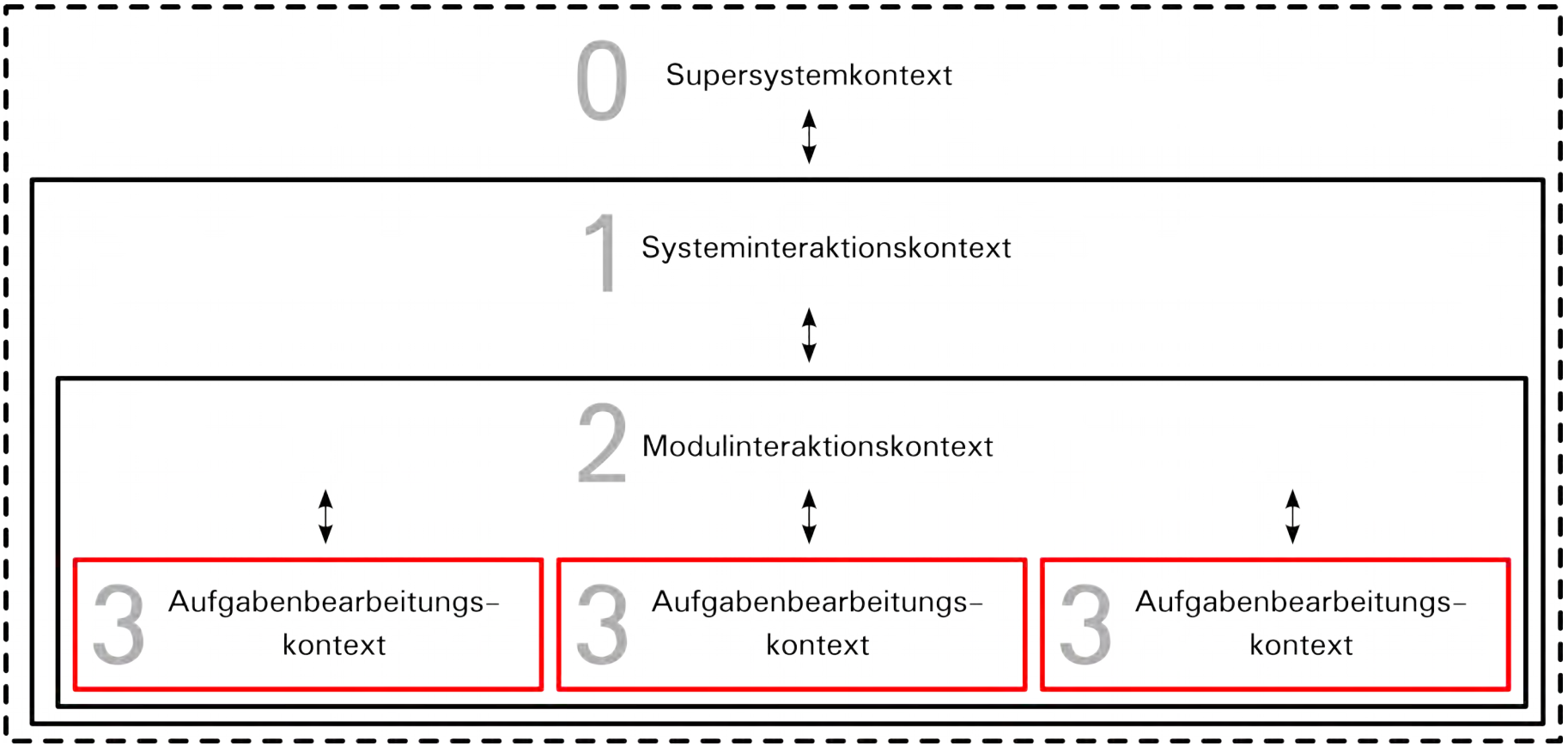
Modulinteraktionskontext



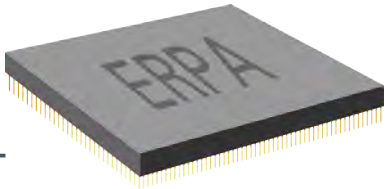
Konzeptentwurf



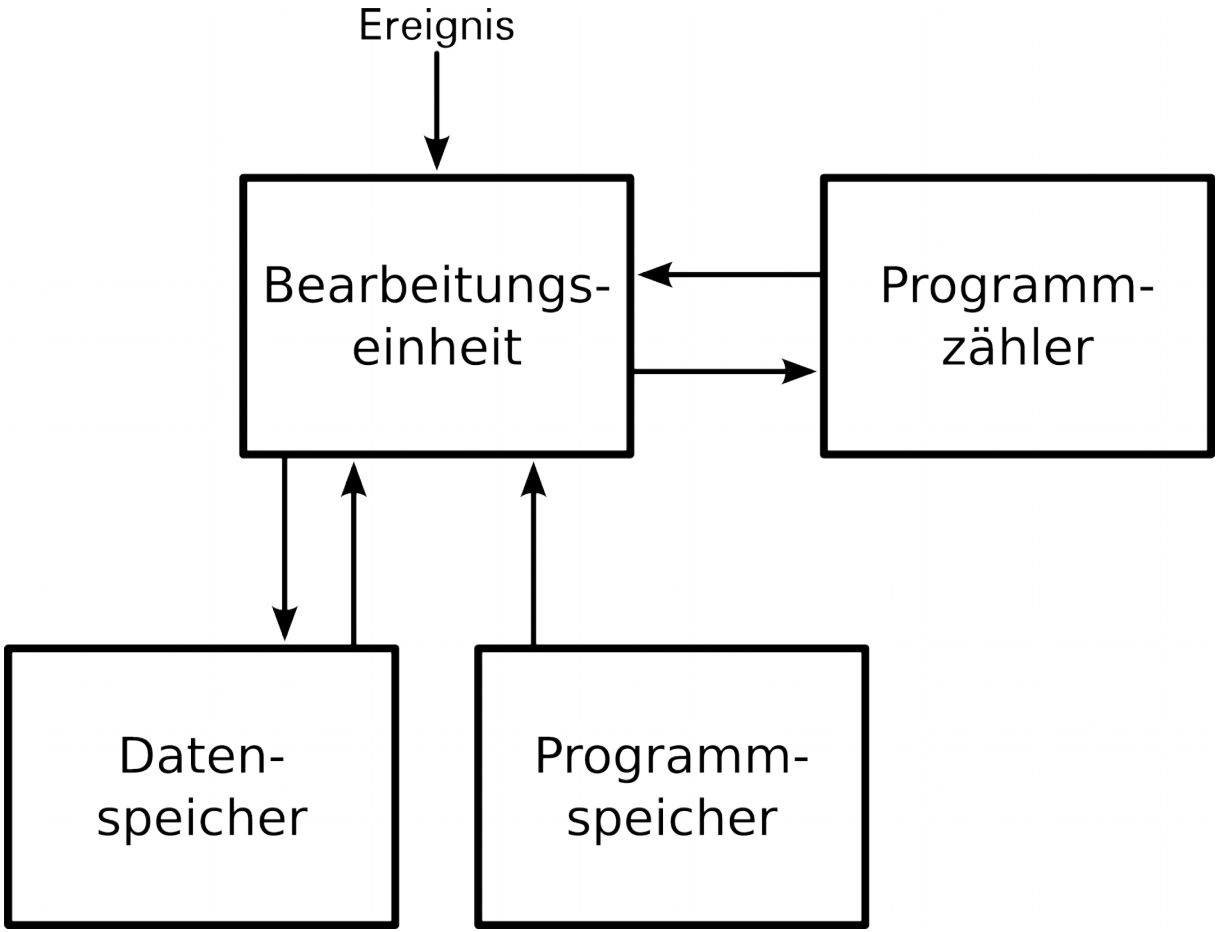
Modulinteraktionskontext



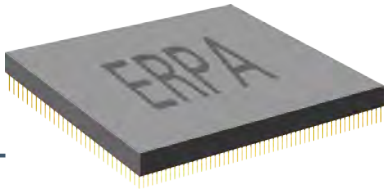
Konzeptentwurf



Aufgabenbearbeitungskontext

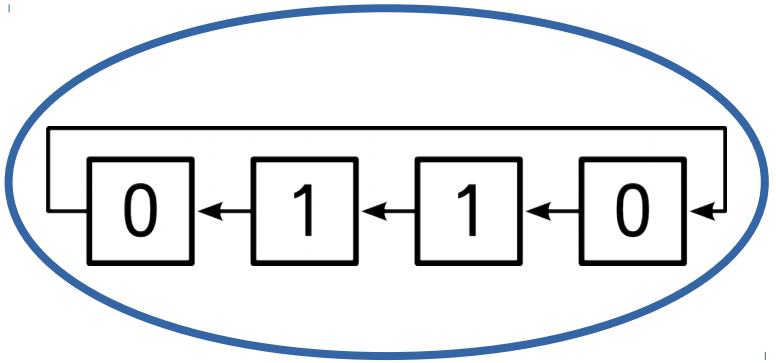


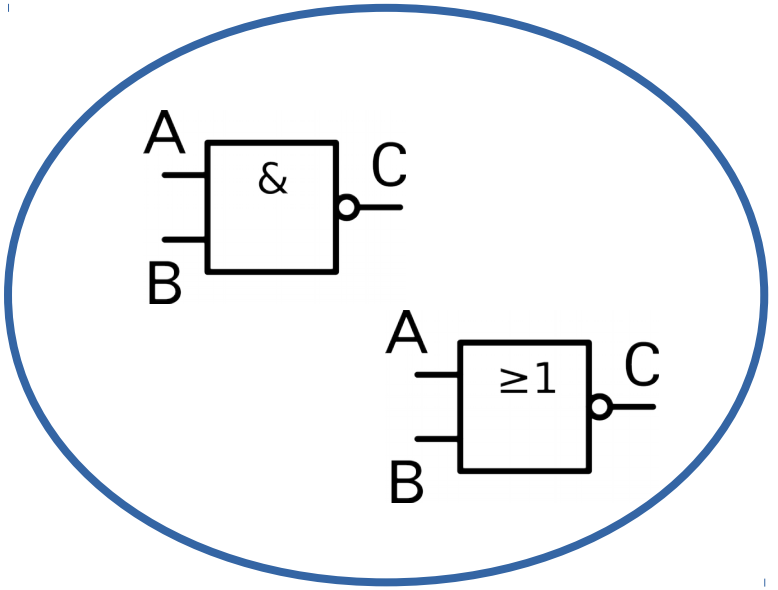
Konzeptentwurf

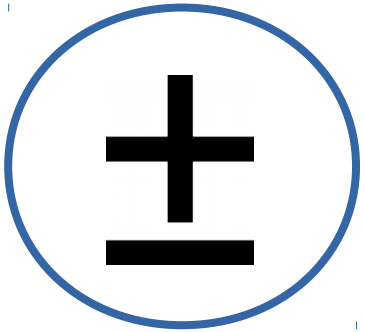


Aufgabenbearbeitungskontext

Minimaler Befehlssatz:

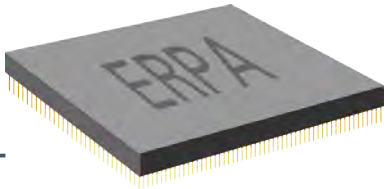




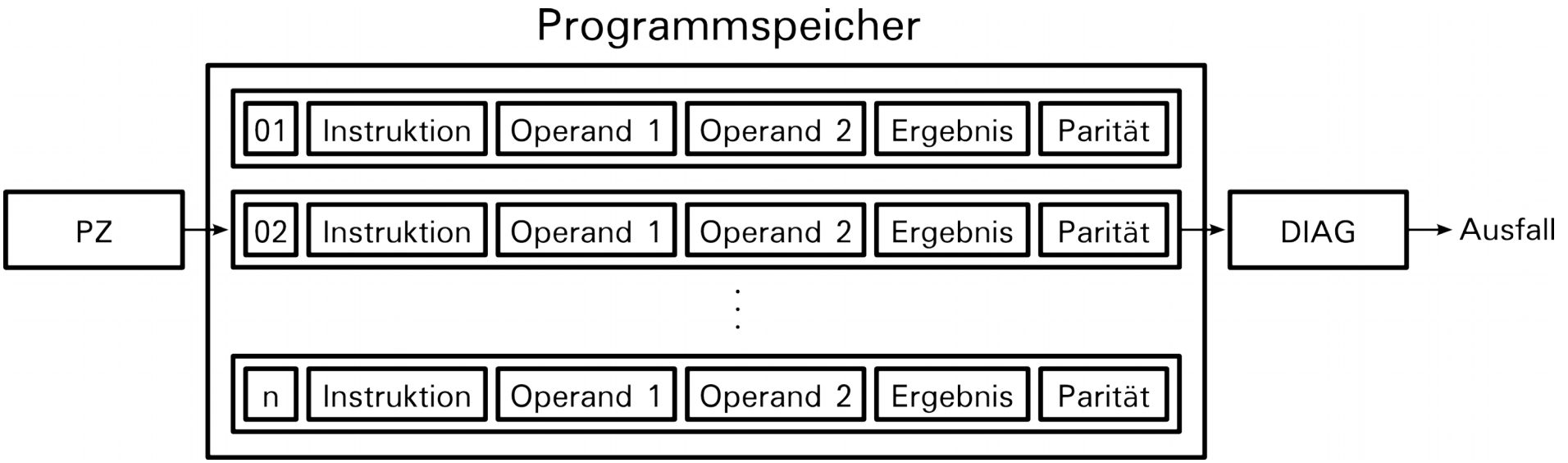


SPRUNG_K

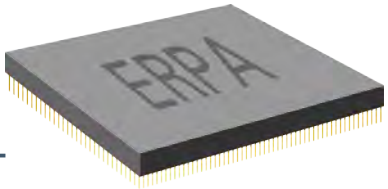
Konzeptentwurf



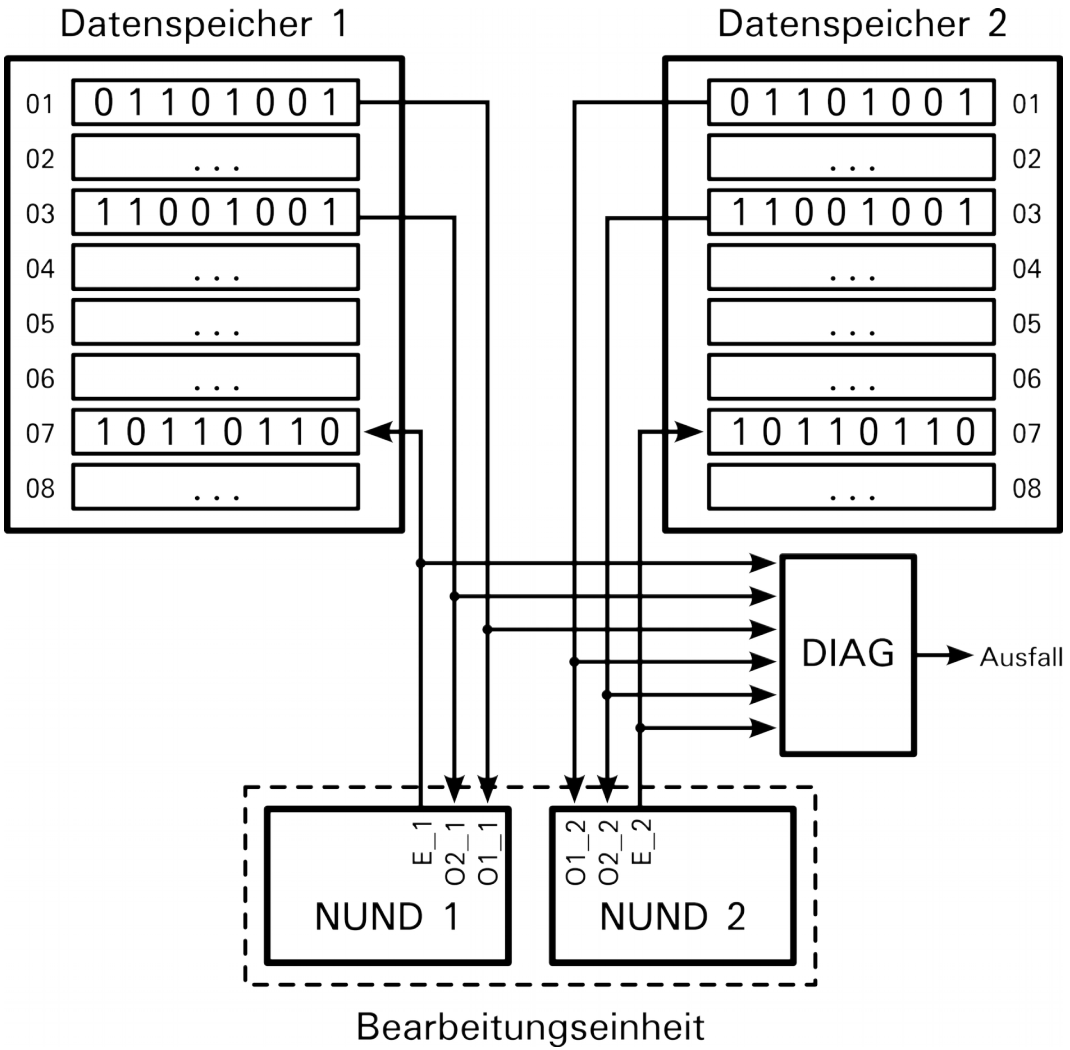
Programmspeichersicherung



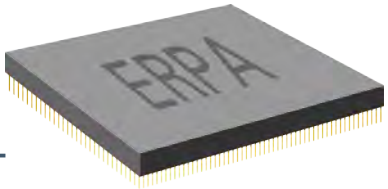
Konzeptentwurf



Datenspeichersicherung



Konzeptentwurf

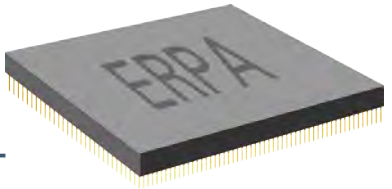


Diagnoseinstanzen

Passive Überwachung:

- Datenspeicher: lesen, schreiben
- Programmspeicher: lesen
- Kommunikation: sämtliche Kanäle
- Kerne: Programmabarbeitung
- Kerne: Programmablauf (Herzschlag)

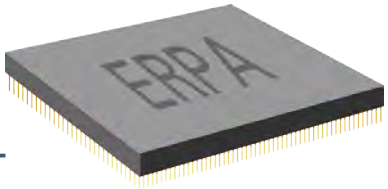
Konzeptentwurf

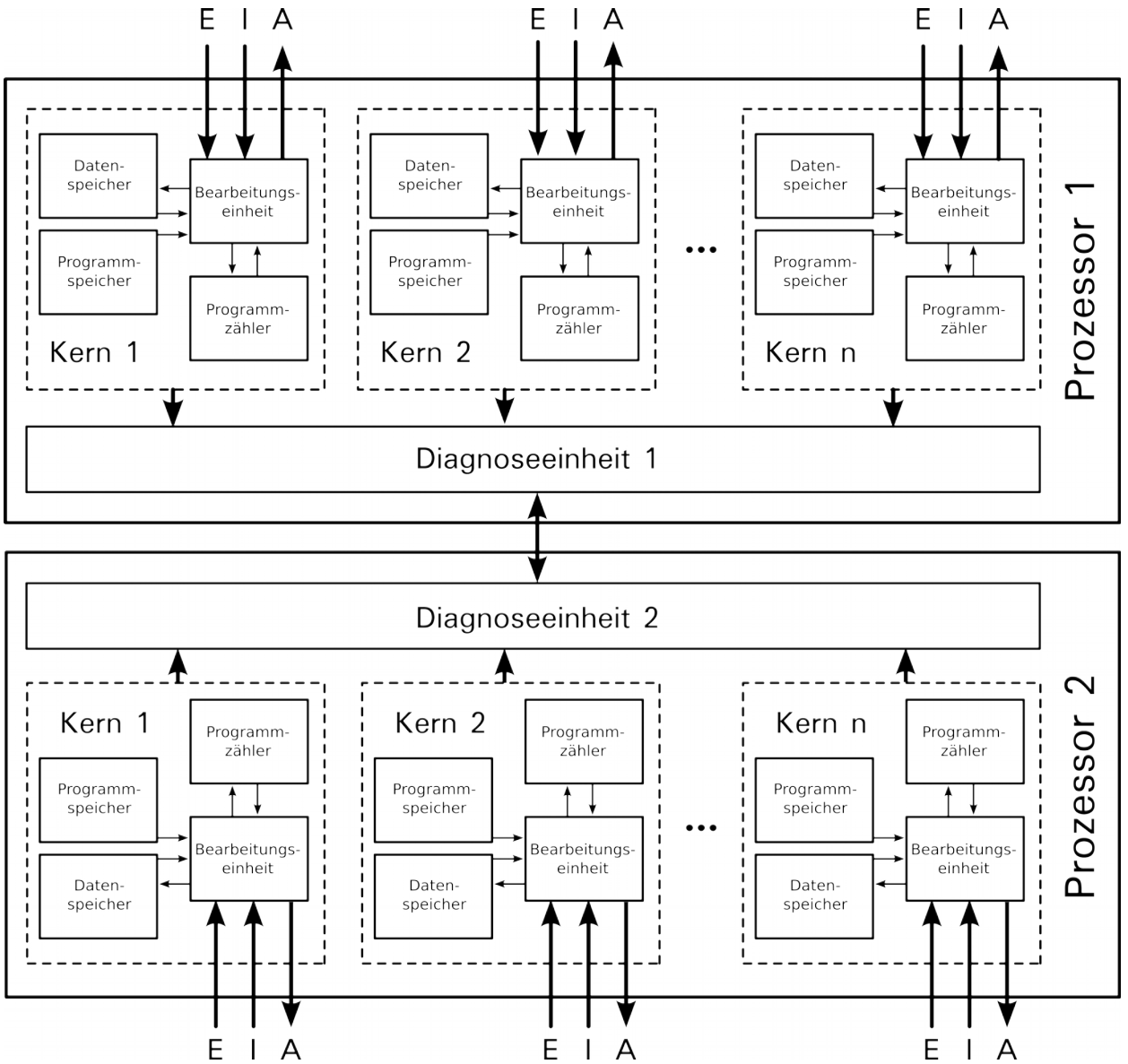


Gesamtarchitektur

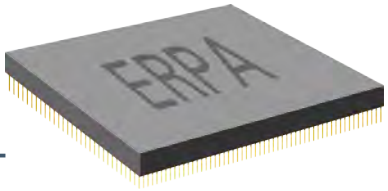
- ERPA – ereignis-reaktive Prozessorarchitektur
- 4-fache Redundanz aller Rechenkerne
- Einfachfehler erkennbar und tolerierbar
- Zweifachfehler erkennbar, > 90% tolerierbar

Konzeptentwurf



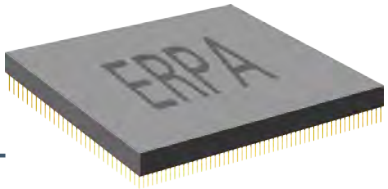


Übersicht

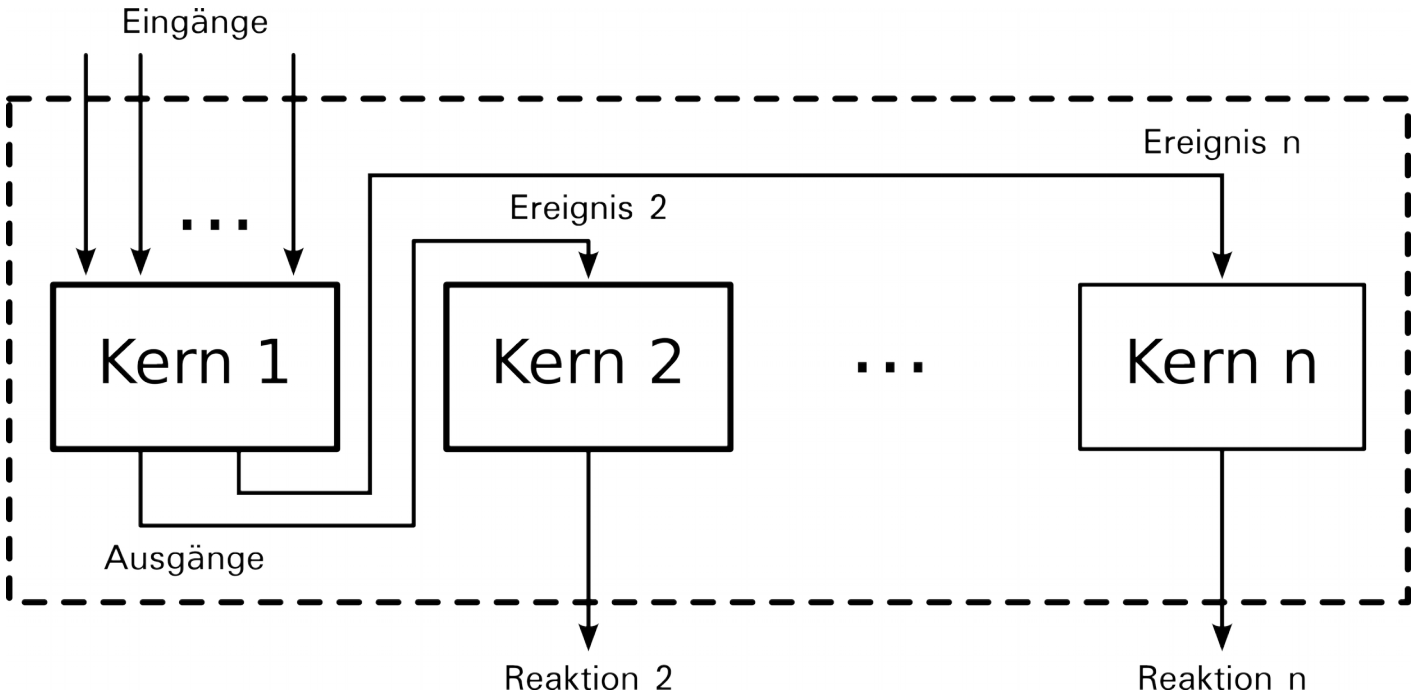


- Grundlagen
- Stand der Technik
- Anforderungen
- Konzeptentwurf
- Bewertung
- Fazit und Ausblick

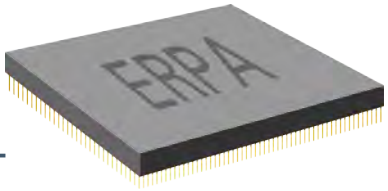
Bewertung



- Erfüllung aller relevanten Anforderungen der DIN EN 61508
- Sogar zyklische/zeitgesteuerte Abarbeitung ist innerhalb der reaktiven Architektur möglich:

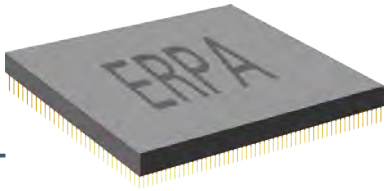


Übersicht



- Grundlagen
- Stand der Technik
- Anforderungen
- Konzeptentwurf
- Bewertung
- Fazit und Ausblick

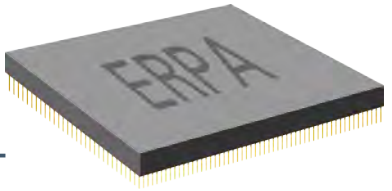
Fazit und Ausblick



“Einfachheit ist das Resultat der Reife.“

Johann Christoph Friedrich von Schiller

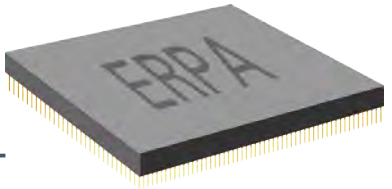
Fazit und Ausblick



Fazit:

- 4-fache Redundanz: Tolerierung aller Einfachfehler
- Diagnosedeckungsgrad 100%
- Überwachung des Programmablaufs
- Alle relevanten Anforderungen der DIN EN 61508 erfüllt
- Keine problematische Technologie benötigt
- Skalierbarkeit unbegrenzt möglich
- Leichte Nachvollziehbarkeit

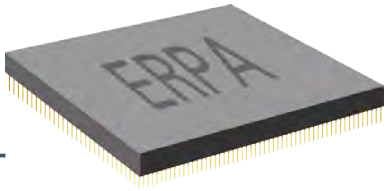
Fazit und Ausblick



Ausblick Implementierung:

- Programmierung vielfältig realisierbar
- Diversitäre Rückwärtsanalyse leicht möglich
- Verwendung von Hochsprachen:
  - Verwendung von Sprachteilmenge
  - Strenge Typisierung
  - Entwurfs- & Programmierrichtlinien

Fazit und Ausblick

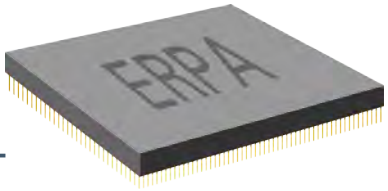


Ausblick Zukunft:

- ERPA im Software-Entwicklungsprozess
  - Programmgröße steht bei Implementierung fest
  - Datenspeichergröße steht bei Implementierung fest
  - Anzahl Rechenkerne = Anzahl Ereignisse
  - Kommunikationsschnittstellen nach Bedarf

→ tiefergehende Anstrengungen vonnöten

Ende



Vielen Dank für Ihre Aufmerksamkeit!

Fragen und Anregungen jetzt, später oder an

danielkoss@web.de