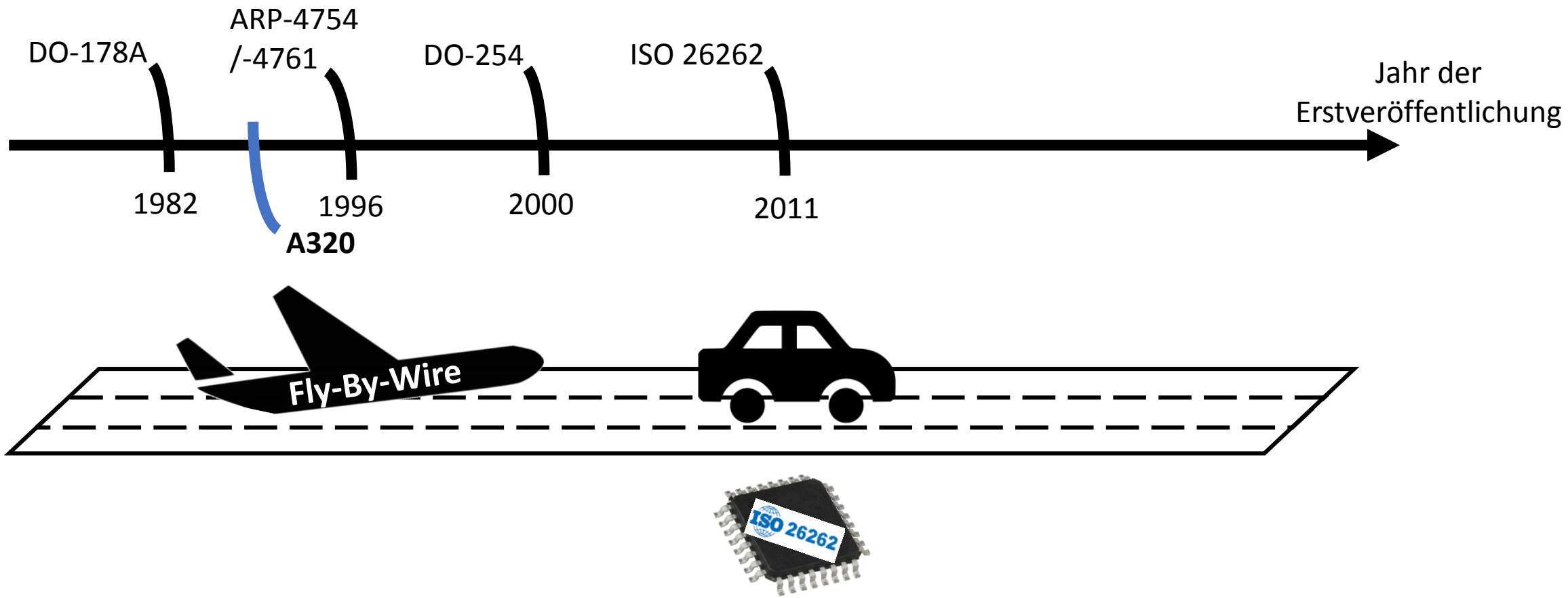
AIRBUS DEFENCE & SPACE

Technische Hochschule Ingolstadt

Funktionale Sicherheit in Automotive und Avionik: Ein Staffellauf

Andreas Schwierz, Georg Seifert und Sebastian Hiergeist

Historischer Verlauf

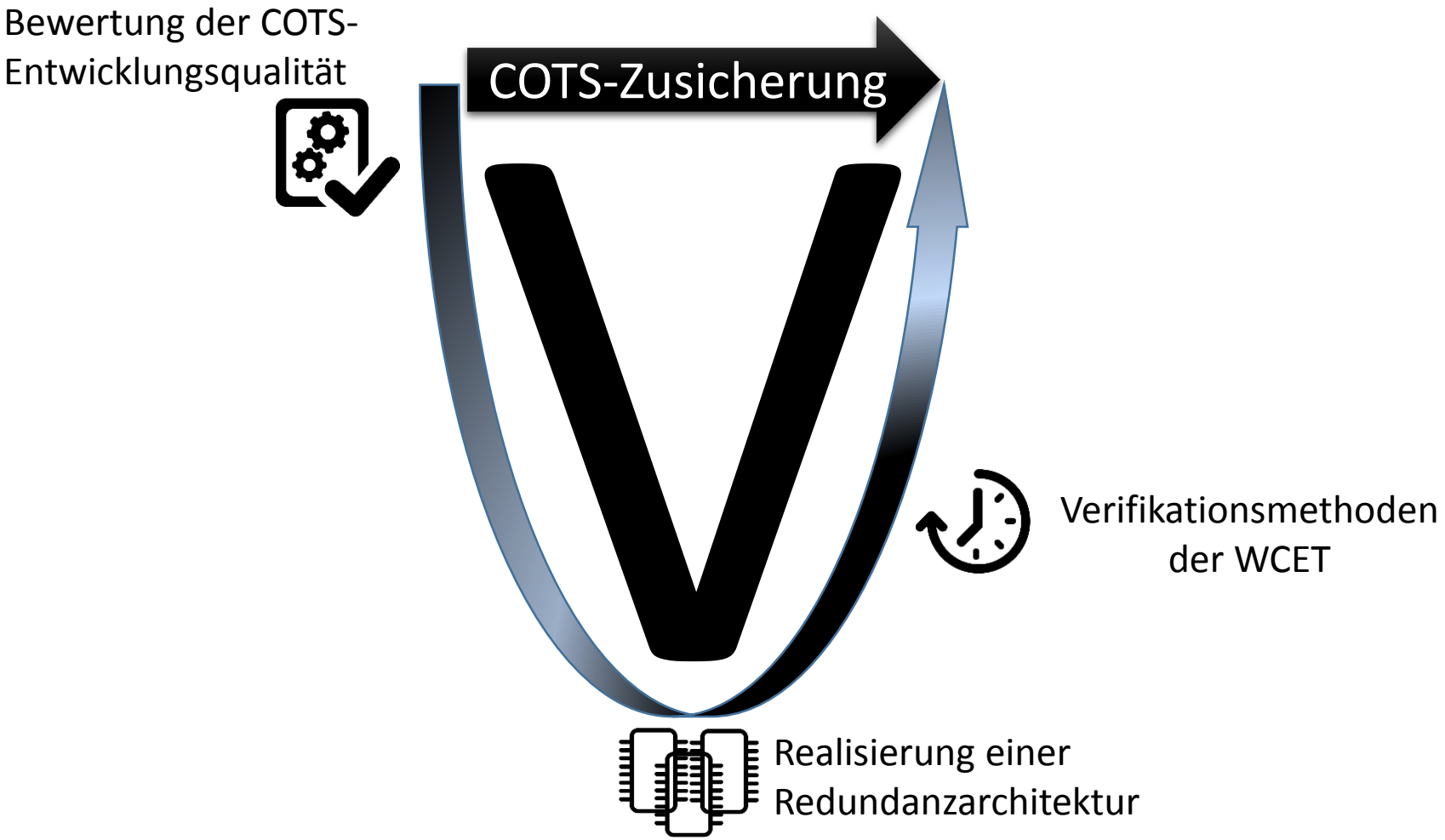


Motivation

- Entwicklung künftiger zulassbarer sicherheitskritischer Avionik?
- Funktionale/Technische Leistungsanforderungen steigen
- Verfügbarkeit von Recheneinheiten für bewährte Systemarchitekturen sinkt
- Technologiewechsel zu komplexen MCUs findet statt

Ziel: Nutzbarmachung dieser Technologie für sicherheitskritische Avionik

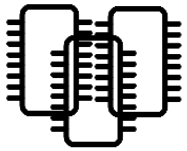
Avionik-Entwicklung



Forschungsziele

- Bewertung der COTS-Entwicklungsqualität
  - Entwicklungsqualität Automotive/Avionik

- Realisierung einer Redundanzarchitektur
  - Redundanznetzwerk mit MCU-Mittel



- Verifikationsmethoden der WCET
  - CPU und DMA zur effizienten E/A-Datenverarbeitung

Forschungsziele

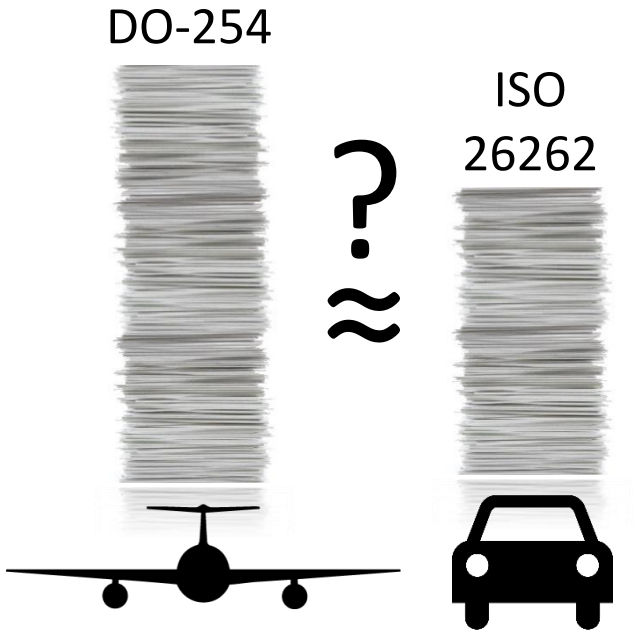
- Bewertung der COTS-Entwicklungsqualität
  - Entwicklungsqualität Automotive/Avionik

- Realisierung einer Redundanzarchitektur
  - Redundanznetzwerk mit MCU-Mittel

- Verifikationsmethoden der WCET
  - CPU und DMA zur effizienten E/A-Datenverarbeitung

Motivation

- Zulassungsbehörde fordert diese Ansätze für komplexe Hardware-Komponenten: Verifikation und Redundanz ersetzt dies nicht
- Systematische Fehler können durch einen disziplinierten und strukturierten Entwicklungsprozess vermieden werden



Herausforderung

- Domänenspezifische Standards unterscheiden sich in
  - Struktur und Nomenklatur
  - Aktualität und Realisierungsdetails

- Zulassungsbehörde erweitert die relevanten Standards um Handlungsempfehlungen und konkretisiert die Anwendbarkeit.
  →Dies steigert den Umfang des Vergleichs.

Herausforderung

- Evaluierung der gewonnen Erkenntnisse

“Because we cannot demonstrate how well we have done, we will show how hard we have tried.”
(John Rushby, 2006)

Zwischenfazit

- Konzept für den Domänen-Standard-Vergleich aufgestellt

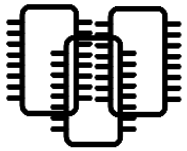
- Aktuell laufend:
  - Befüllen der Vergleichsmatrix und Definition eines qualitativen Bewertungsschema
  - Initiierung eines Kooperation zwischen TÜV Süd und EASA

- Weiteres Vorgehen:
  - Darstellung der Vergleichsergebnisse zur Verwertung innerhalb des Zulassungsverfahrens

Forschungsziele

- Bewertung der COTS-Entwicklungsqualität
  - Entwicklungsqualität Automotive/Avionik

- Realisierung einer Redundanzarchitektur
  - Redundanznetzwerk mit MCU-Mittel

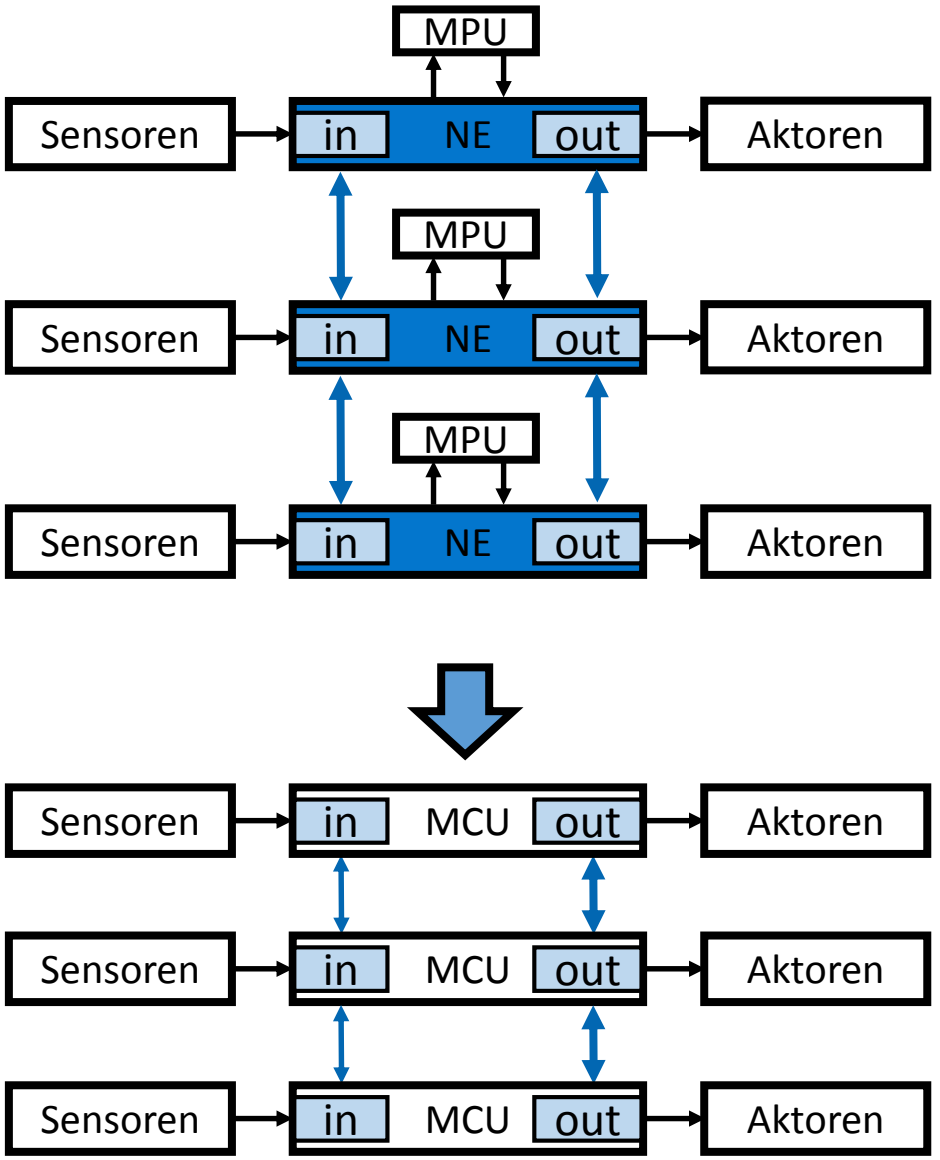


- Verifikationsmethoden der WCET
  - CPU und DMA zur effizienten E/A-Datenverarbeitung

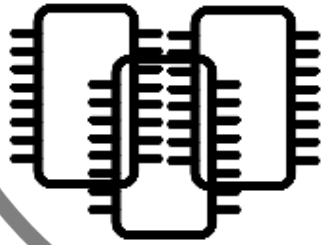
Motivation

- Wiederverwendung bewährter Redundanzarchitektur basierend auf proprietären NEs
- Ansatz für künftige UAV-Anwendungen ungeeignet

➢ Integration des Redundanznetzwerkes in MCUs



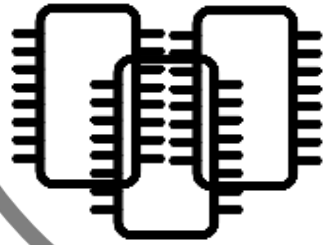
Herausforderungen



	Synchroner Betrieb	Daten-konsolidierung	Rückwirkungs-freiheit
Anforderungen	↓	↓	↓

Technische Herausforderungen:

- Rechenleistung des Redundanzansatzes
- Untersuchung der Einflussfaktoren auf Synchronität



Zwischenfazit

- Konzeption und Aufbau der Netzwerkarchitektur abgeschlossen

- Aktuell laufend:
  - Bewertungsschema für Auswahl eines Synchronisations-Algorithmus

Anregungen aus der Luftfahrtindustrie

- Weitere Steigerung des Vertrauens durch redundanten Einsatz nicht-baugleicher MCUs →Ausschluss von Design-Fehlern

Forschungsziele

- Bewertung der COTS-Entwicklungsqualität
  - Entwicklungsqualität Automotive/Avionik

- Realisierung einer Redundanzarchitektur
  - Redundanznetzwerk mit MCU-Mittel

- Verifikationsmethoden der WCET
  - CPU und DMA zur effizienten E/A-Datenverarbeitung

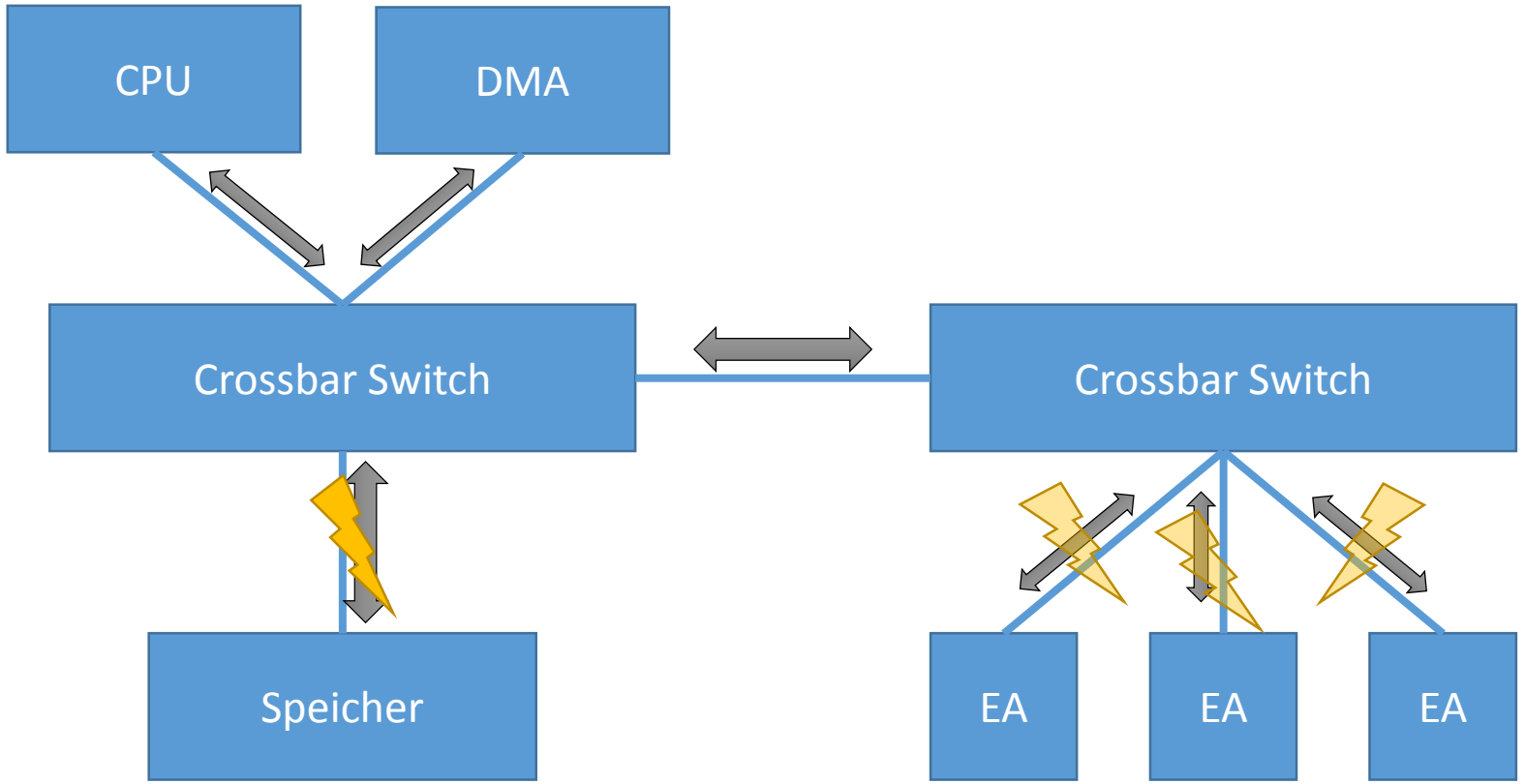
Motivation

- Betriebsstrategie: Ausschluss von gemeinsamen Ressourcen durch eingeschränkte Hardwarenutzung. DMA als **synchroner** Helfer.
  - Grund: Verfügbare WCET-Analysen erlauben keinen DMA als **asynchronen** Helfer.

- Ausschluss von gemeinsam genutzte Ressourcen ist nicht mehr praktikabel:
  - Nicht ausreichend Zwischenpuffer in MCU-EA-Controllern. CPU im Dauerstress.
  - Anstieg des MCU-internen Datenaufkommens (z.B. Redundanznetzwerk)

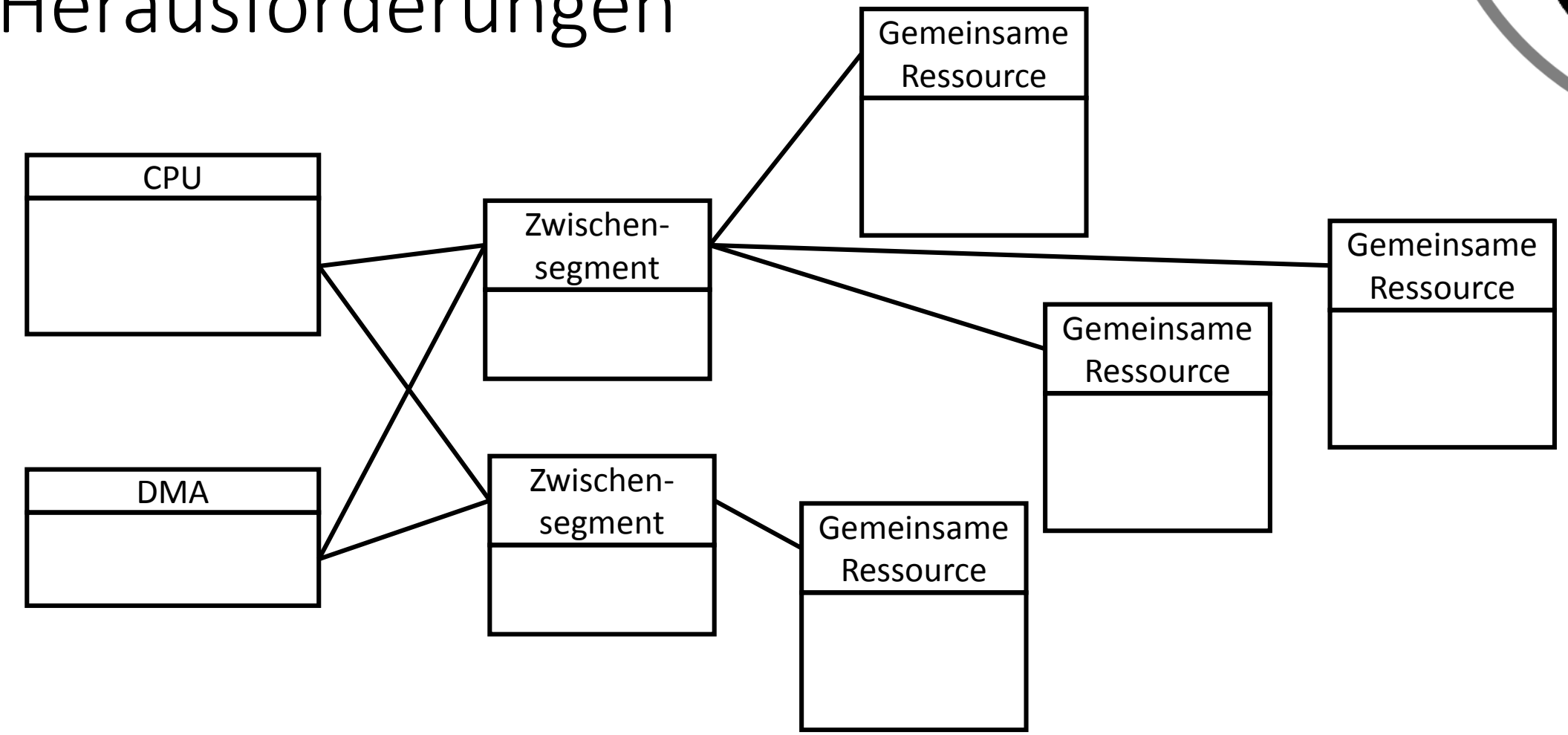
➢Neue Strategien: Erweiterung der statischen WCET-Analysen um DMA

Herausforderungen

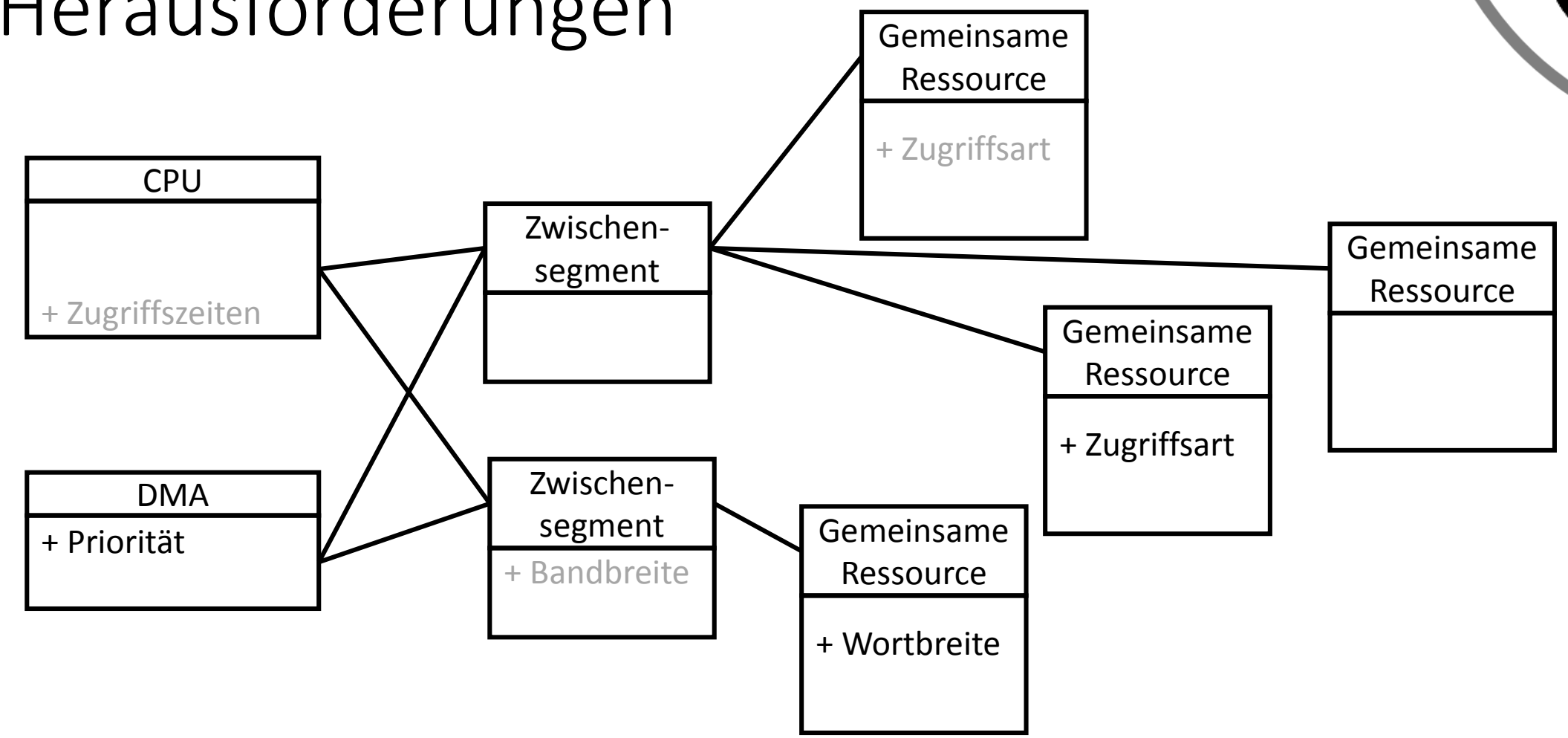


Datenbuch → **Stichproben** → **Integrität der WCET-Schätzung**

Herausforderungen

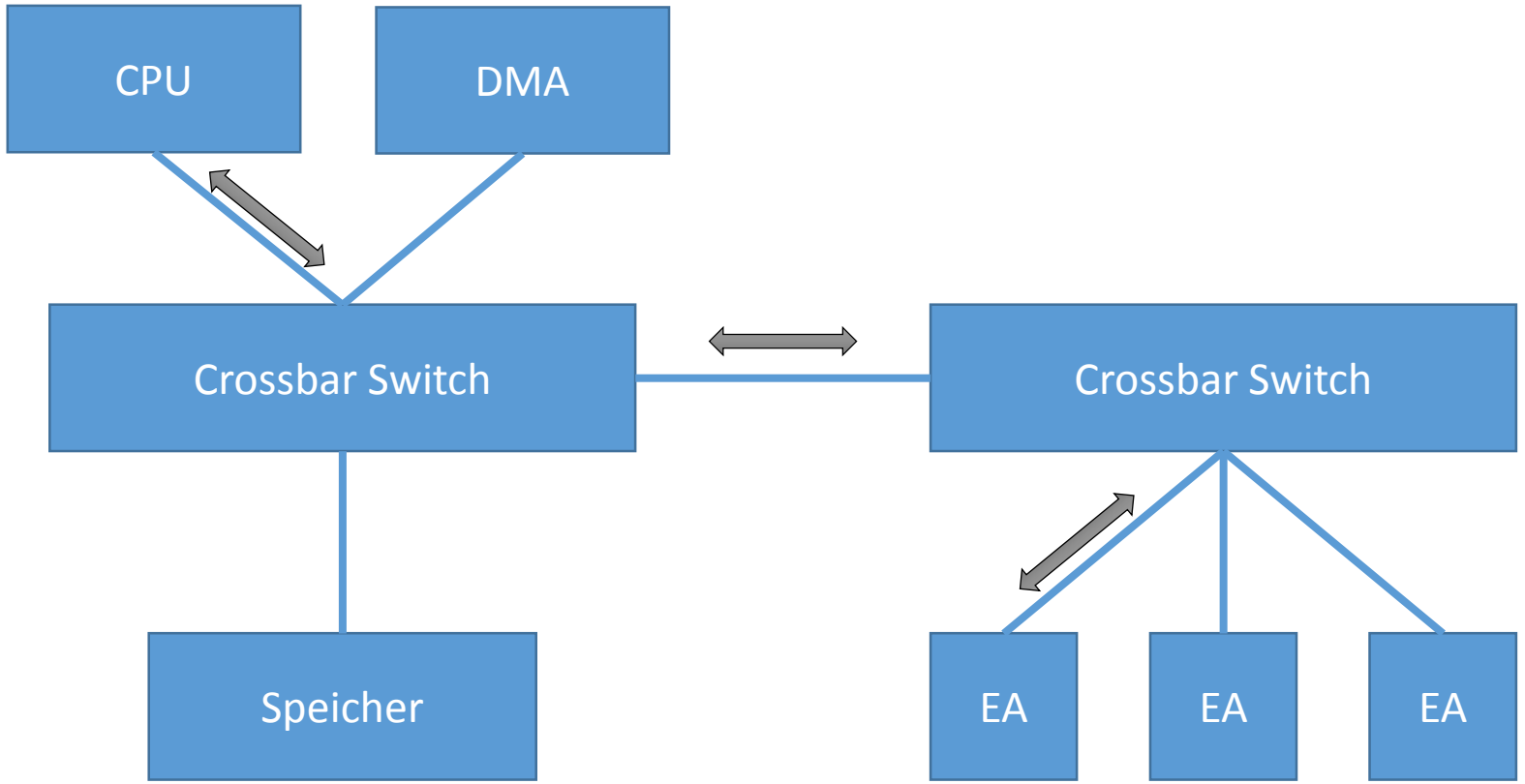


Herausforderungen

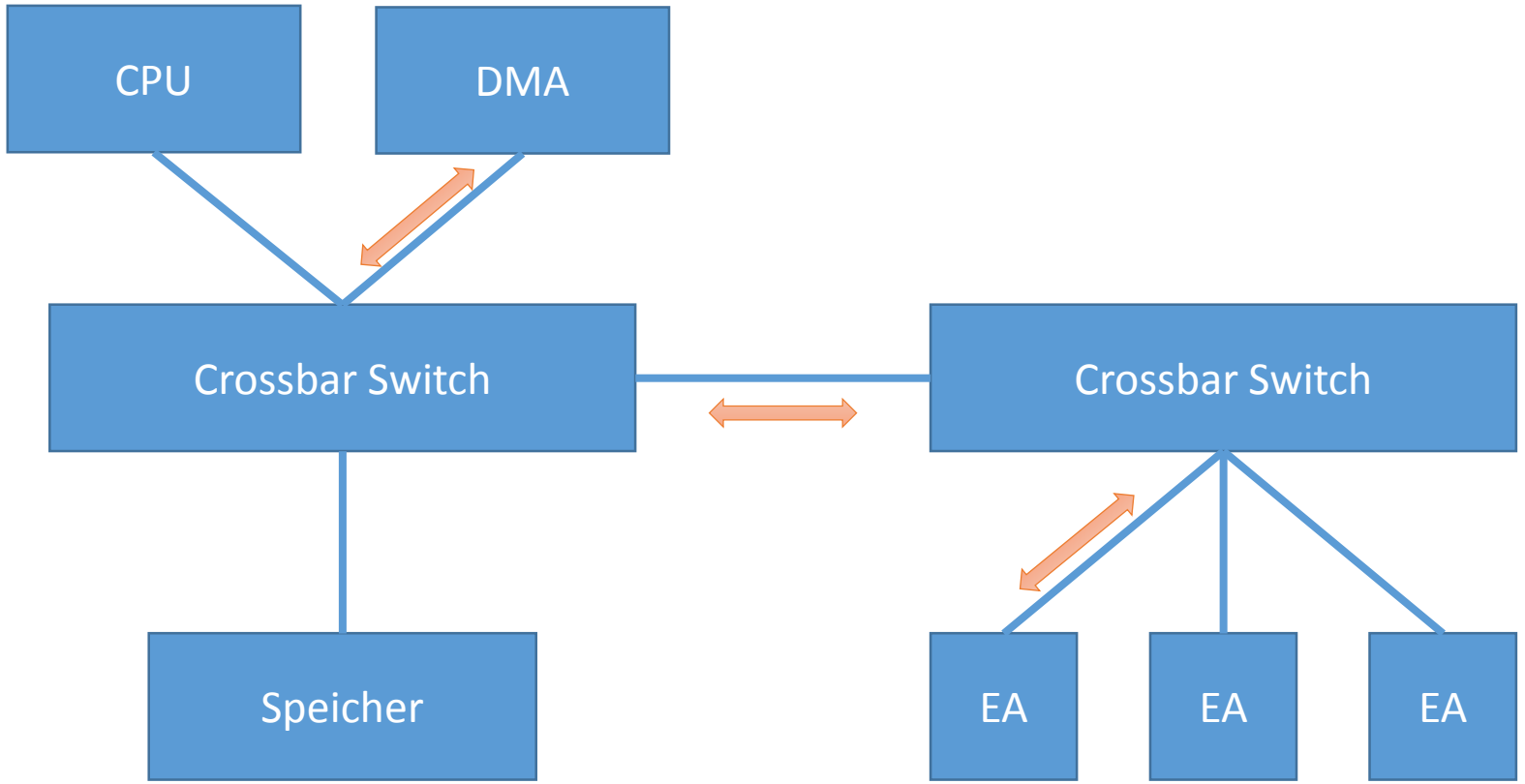


Integrität der WCET-Schätzung

Herausforderungen



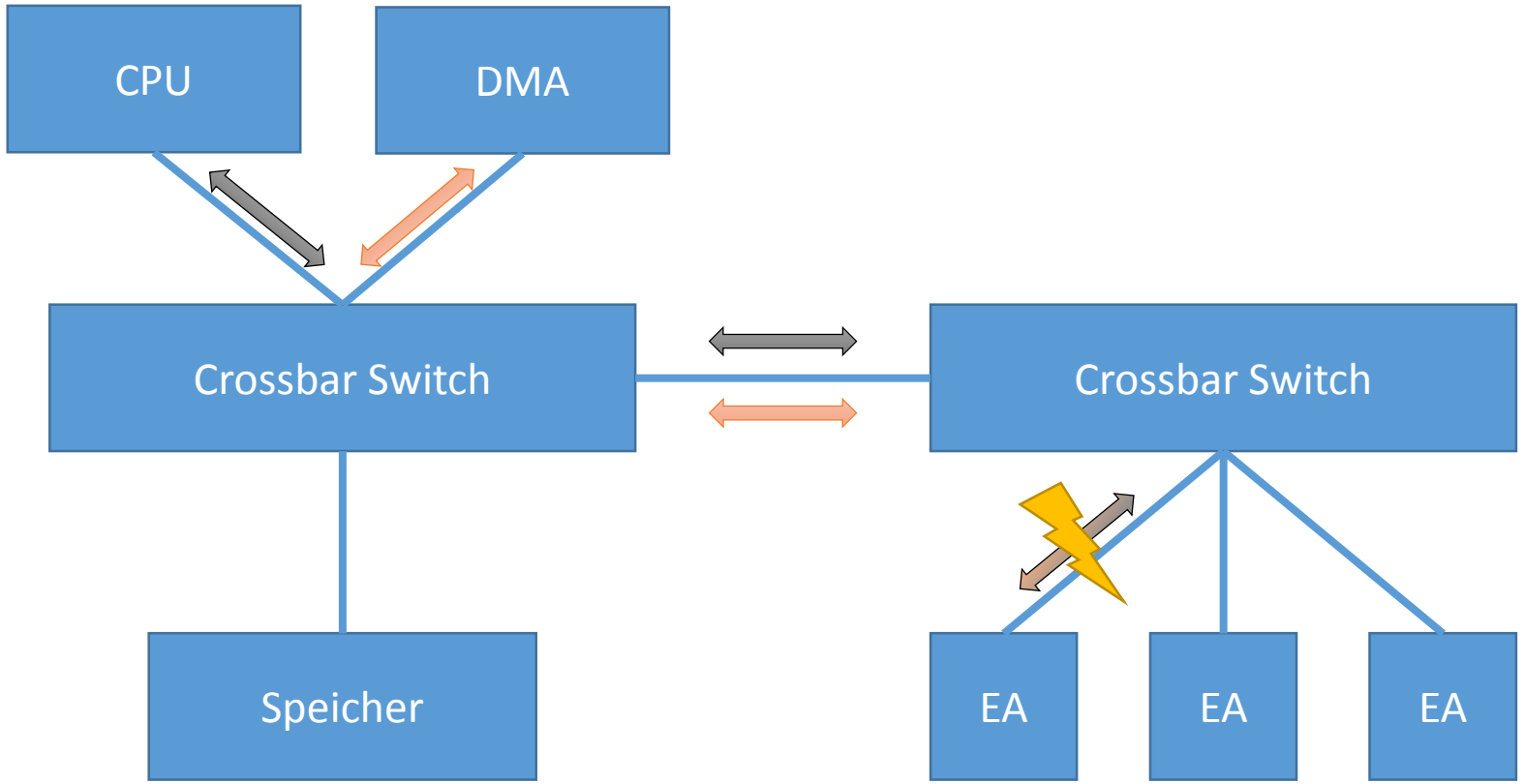
Herausforderungen



Datenbuch → **Stichproben** → **Modell** → **Integrität der WCET-Schätzung**

Mikrobenchmarks

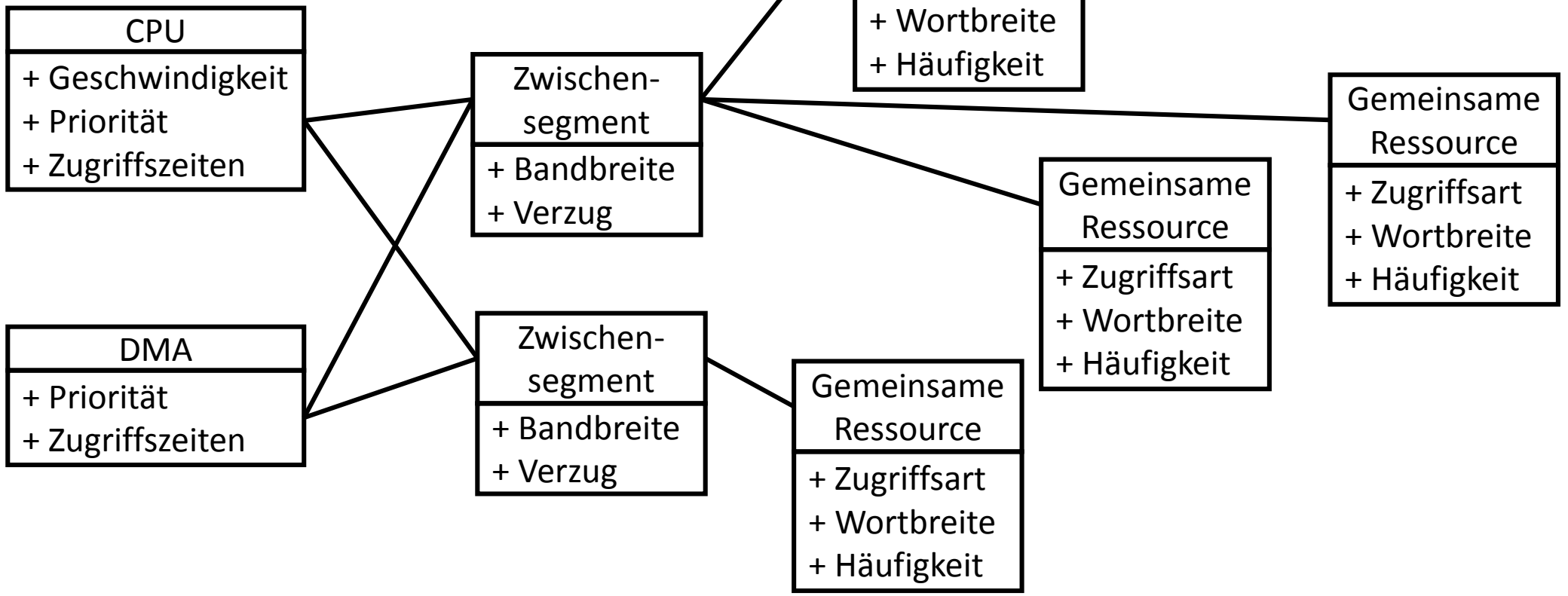
Herausforderungen



Datenbuch → Stichproben → Modell → **Integrität der WCET-Schätzung**

Mikrobenchmarks

Herausforderungen



Datenbuch → **Stichproben** → **Modell** → **Integrität der WCET-Schätzung**

Mikrobenchmarks

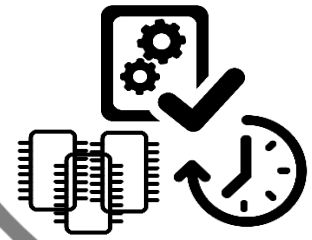
Zwischenfazit

- Datenbuchanalyse abgeschlossen und Testinfrastruktur realisiert

- Aktuell laufend:
  - Analyse des Systems mithilfe von Mikrobenchmarks
  - Ableiten von Modellen der MCU-Kommunikationsarchitektur

- Weiteres Vorgehen:
  - Modellvalidierung

Resümee: Synergiepotentiale



- Gegenüberstellung der Entwicklungsanforderungen beider Domänen erlaubt wechselseitige Akzeptanz und hat Einfluss auf den MCU-Markt
- Fail-Operational-Systemverhalten autonomer Systeme bedarf einer redundanten, synchron arbeitenden Rechnerarchitektur
- Modelle der MCU-internen Kommunikation ermöglichen den DMA als effizienten asynchroner Helfer zu verwenden



Resümee: Der Staffellauf