ENTWICKLUNGSPROZESSE I WERKZEUGE I PLATTFORMEN
FÜR SICHERHEITSKRITISCHE MULTICORESYSTEME

ARAMiS II Abschlussveranstaltung
20.09.2019 Stuttgart

Verwertung in der Automotive Domäne

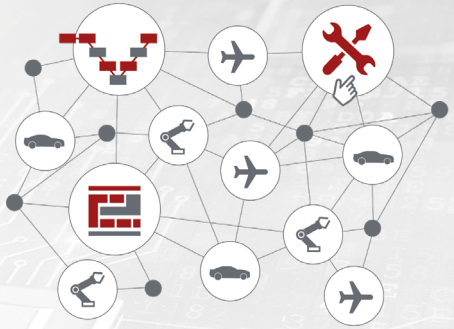
Hatem Miled, Audi AG

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Automotive Partner

aramis II
ENTWICKLUNGSPROZESSE I WERKZEUGE I PLATTFORMEN
FÜR SICHERHEITSKRITISCHE MULTICORESYSTEME

Automotive



Audi

Continental

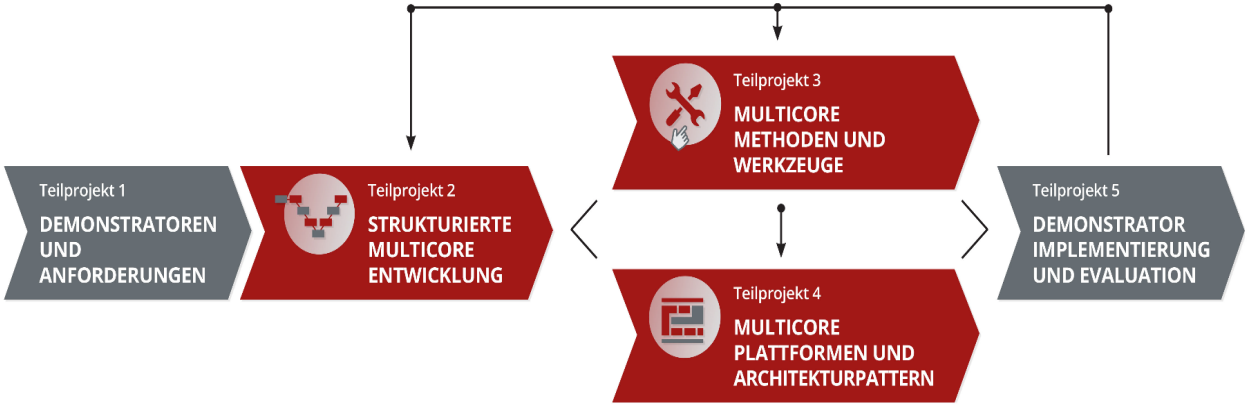
DENSO

BOSCH

SCHAEFFLER

LuK INA FAG

Ziele der Automotive Domäne



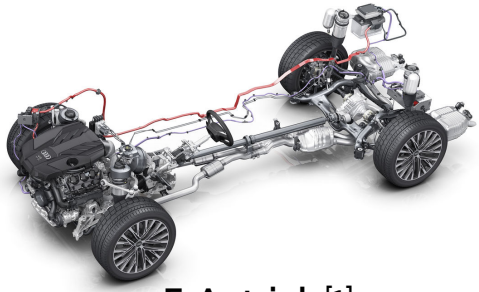
- Optimierung der Entwicklungsprozesse
- Migration von Single auf Multicore-Plattform
- Methoden und Werkzeuge
- Fail Operational Konzepte
- Methodologie

Automotive Entwicklungsplattformen

Fahrwerk [1]

Automotive Demonstratoren

Powertrain [2]

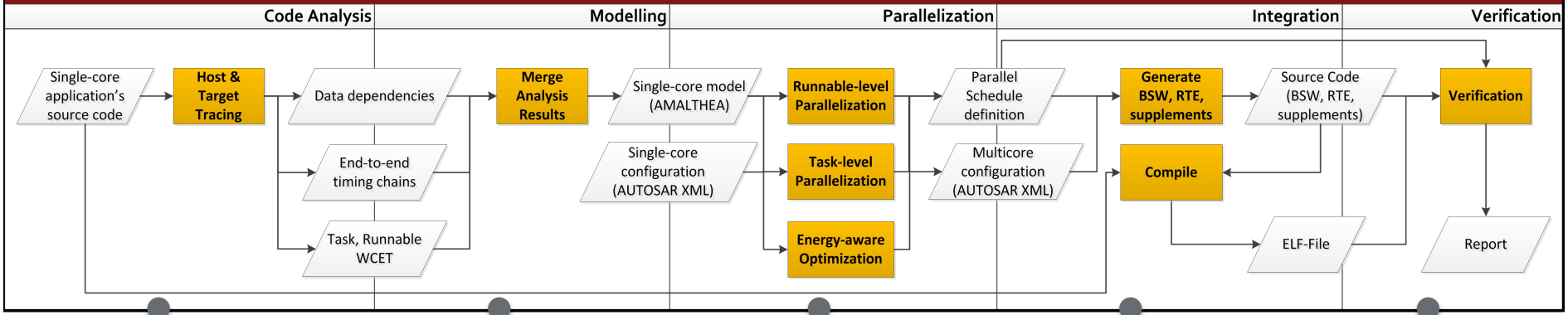


E-Antrieb [1]

[1] https://www.audi-mediacenter.com/
[2] https://www.autoguide.com/

Optimierung der Entwicklungsprozesse

Workflow for Multicore Migration in UC5.2



- Host Tracing
  - Silexica (Automotive Flow: Analyze)
  - Elektrobit (Tresos Studio / AutoCore)
- Target Tracing
  - AbsInt (TimingProfiler + TimeWeaver)
  - Symtavision

- AbsInt / Timing Architects (APP4MC)

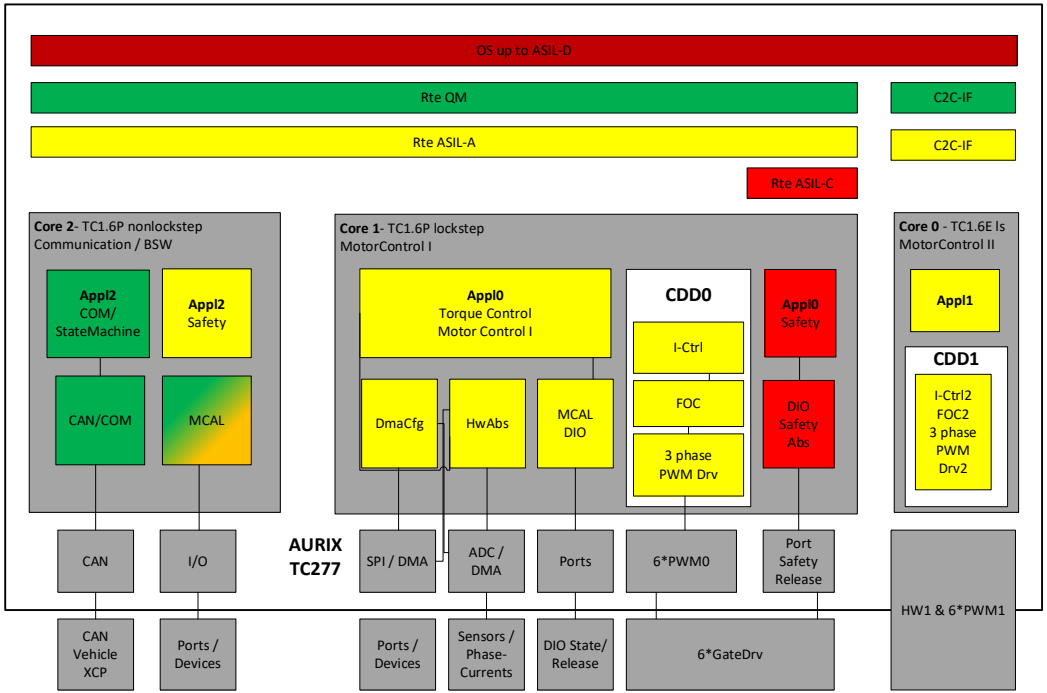
- Silexica (Automotive Flow: Optimize)
- Timing Architects (TA Simulator, TA Optimizer)
- Denso (Parcus)

- Elektrobit (Tresos Studio / AutoCore)
- Silexica (Automotive Flow: Implement)
- TU Braunschweig

- Uni Kiel (Gropius/Lodin)
- Accemic (CEDAR)
- Uni Lübeck (TeSSLa)
- Fraunhofer IESE (FERAL framework)

Migration von Single auf Multicore-Plattform

Triple Core – Dual PMSM Configuration

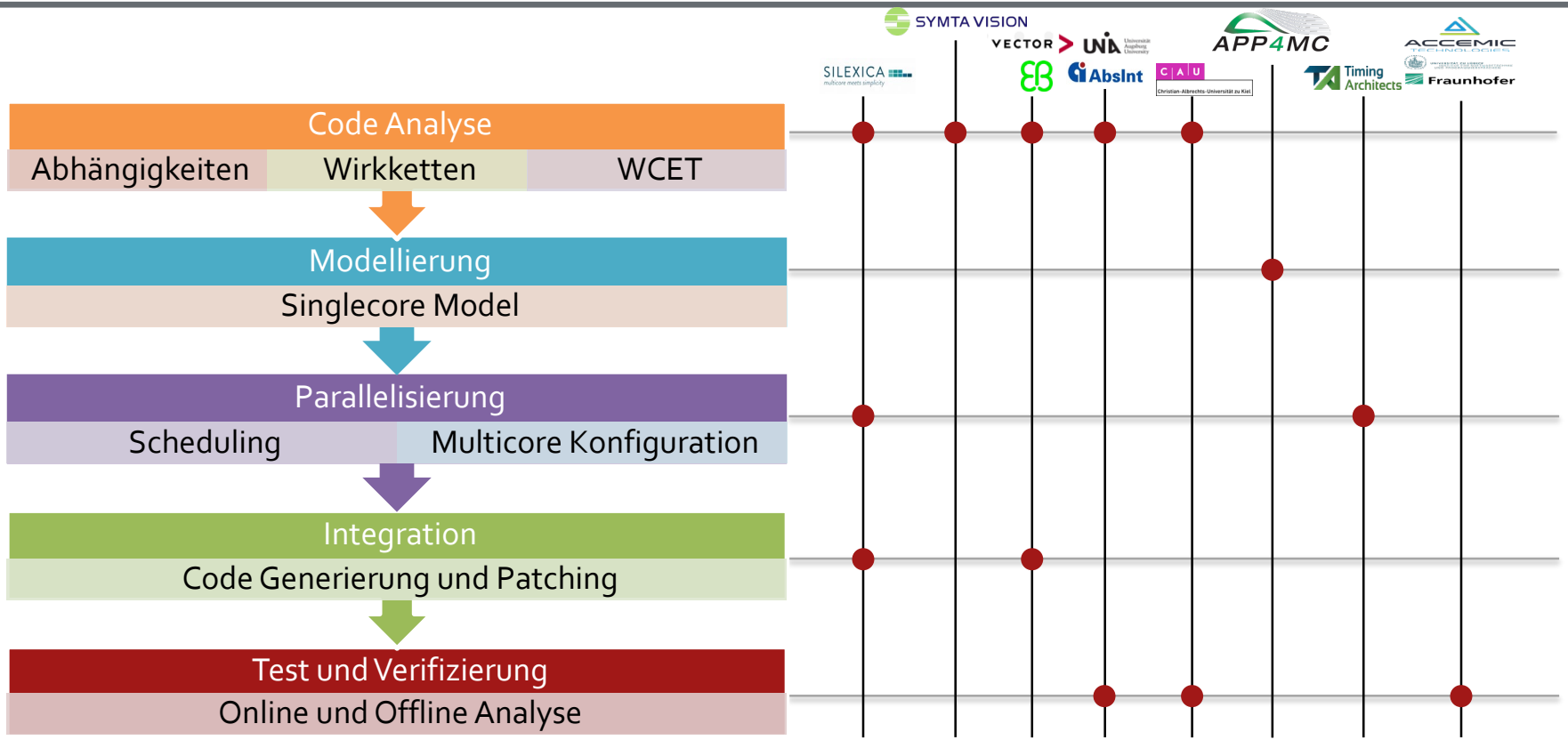


Color Table:

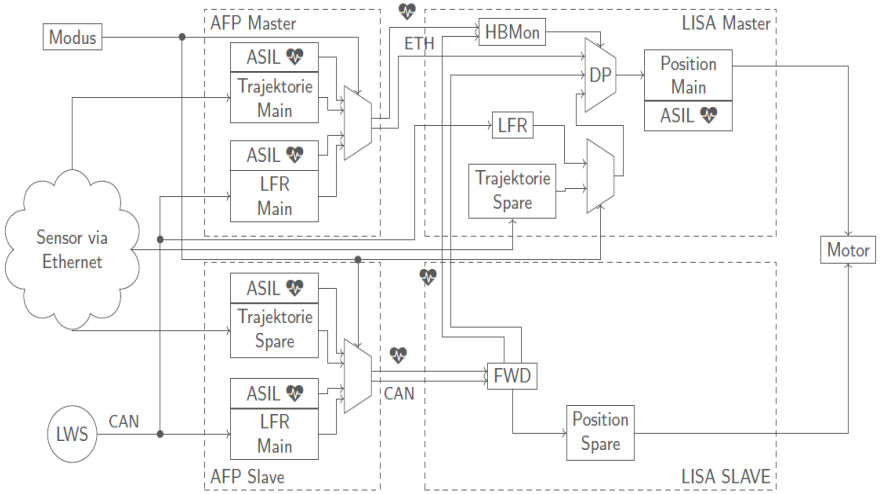
- Instruction Rate und Cache Nutzung
- RTE Spinlocks
- WCET von Spinlocks
- Task und Interrupt Laufzeiten
- Interrupt Jitter und Echtzeitsfähigkeiten

Abkürzungen:
PMSM: Permanent magnet synchronous motor
RTE: Runtime Environment
SPI: Serial Peripheral Interface
DMA: Direct Memory Access
ASIL: Automotive Safety Integrity Level
MCAL: Microcontroller Abstraction Layer
CAN: Controller Area Network
COM: Communication
DIO: Digital Input Output
ADC: Analog Digital Converter
PWM: Pulsweitenmodulation
QM: Quality Management

Methoden und Werkzeuge

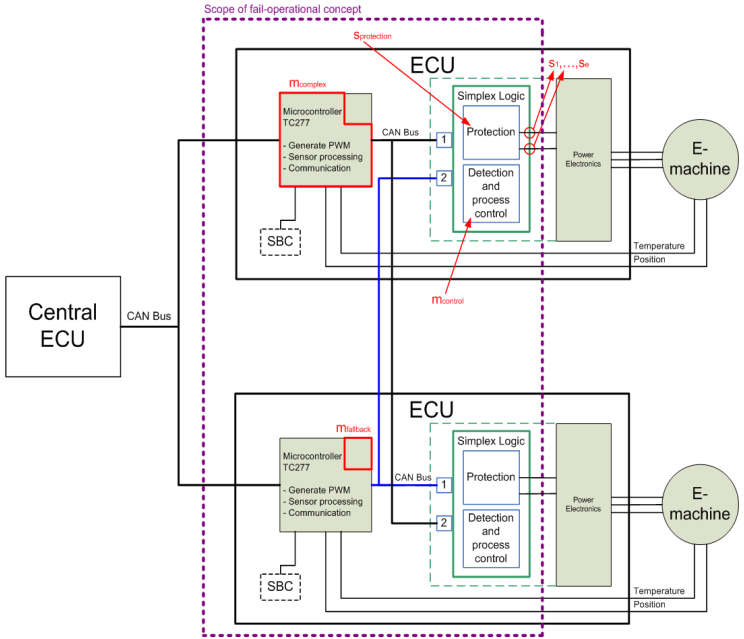


Fail Operational Konzepte
Erhöhung der Verfügbarkeit



Hot Standby Fail Operational Konzept

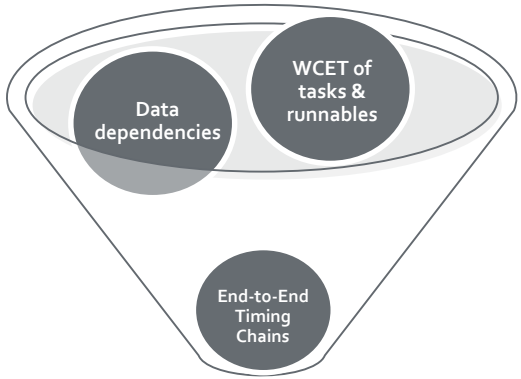
Abkürzungen:
HBMon: Heartbeat Monitoring
LFR: Lenkfolgeregler
ASIL: Automotive Safety Integrity Level
LWS: Lenkwinkelsensor
AFP: Audi Fahrwerk Plattform
LISA: Leistungs- und Integrationssteuergerät
FWD: ForWarD
DP: Data Proxy

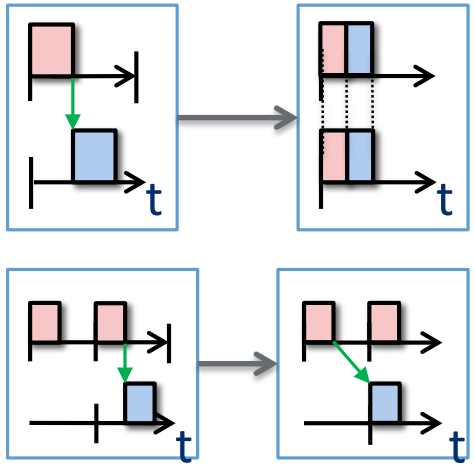


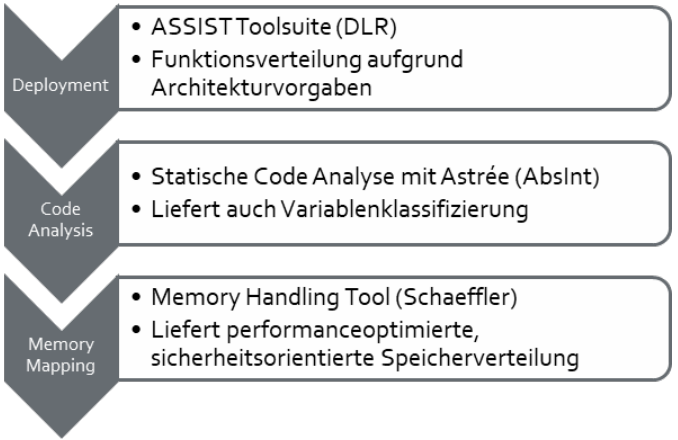
Mapped simplex Architecture

Abkürzungen:
CAN: Controller Area Network
ECU: Electronic Control Unit
PWM: Pulsweitenmodulation
SBC: System basis chip

Methodologie 1





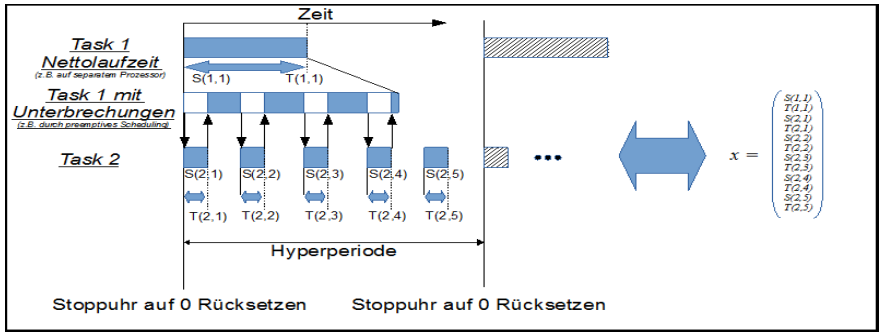


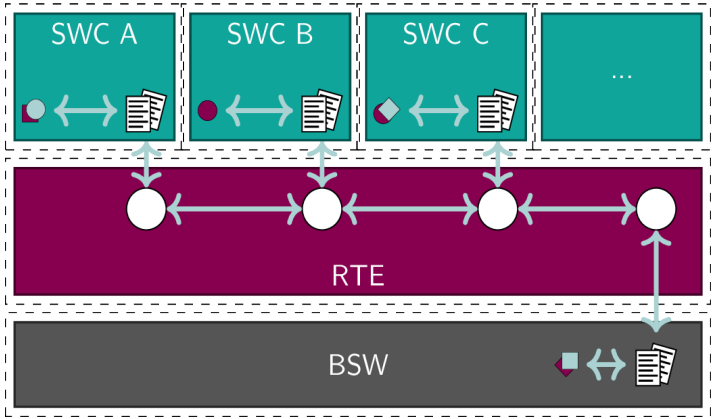
AMALTHEA Model

Logical Execution Time
LET@AUTOSAR

Memory Mapping Toolflow

Methodologie 2





Timingmessung

parametrisierbare RTE (paRTE)

Zusammenfassung und Ergebnisse

- Optimierung der Entwicklungsprozesse
- Migration von Single auf Multicore-Plattform
- Methoden und Werkzeuge
- Fail Operational Konzepte
- Methodologie

- Reduzierung der Migrationsaufwände in Multicore-Plattformen um 50 %
- Performancevergleich (Benchmark) zwischen Singlecore und Multicore-Lösung
- Erfolgreicher Einsatz von Methoden und Werkzeugen für die spätere Serienentwicklung
- Fail Operational Konzepte für vollautomatisiertem Fahren
- Neue Methodologie zur Vereinfachung der Entwicklungsarbeit

aramis II

ENTWICKLUNGSPROZESSE I WERKZEUGE I PLATTFORMEN
FÜR SICHERHEITSKRITISCHE MULTICORESYSTEME

ARAMiS II Abschlussveranstaltung
20.09.2019 Stuttgart

Verwertung in der Avionik-Domäne

Andreas Schacht, Hensoldt

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Inhalt

- ARAMiS-II - Ziele
- Multicore Herausforderungen - Recall
- Lösungsfelder
- Prozess
- Methodik
- Werkzeuge
- Problemfelder

ARAMiS-II - Ziele

- Entwicklungsprozesse,
  Methoden,
  Werkzeuge und
  Plattformen für
  sicherheitskritische Multicore Systeme

Multicore Herausforderungen - Recall

- Interferenzen
  - Internal Core (CoreNet)
  - External (IO, Shared Memory, Shared Caches)
  - Echte Parallelität)
- Determinismus
  - Segregation (Space & Time)
  - WCET, WCRT
- Verification
  - Aufwand steigt nichtlinear mit DAL (D, C, B, A) auf dem V-Pfad
  - Einsatz von Tools bringt hier größten Benefit

Lösungsfelder

- Entwicklungsprozesse (AP2.2)
- Methoden (TP3.x)
- Werkzeuge (TP3.x)
- Plattformen (AP2.3, TP4.x)

Prozess

- Schwerpunkt Avionik
  - AP2.2 Generischer Entwicklungsprozess
    - System
    - Requirements
    - Design
    - Implementation
    - Integration
    - Verification

Methodik

- Voraussetzung für Einsatz von Werkzeugen
  - Modellbasierte Entwicklung
- System Architecture & Design
  - Partitioning (AP3.1)
  - Deployment (AP3.5)
  - Schedule (AP3.5)
  - Design Space Exploration (AP3.2)
  - Parallelization (AP3.4)

Methodik

- Verifikation
  - Zuverlässige Ermittlung des WCET
  - Zuverlässige Ermittlung der realen WCRT
  - Verifikation der Lastverteilung (Deployement)
  - Verifikation des Schedules
  - Test Case Generierung aus Requirements
  - Automatische Erstellung von Test Prozeduren
  - Erkennung von Interferenzen
    - Zugriff auf gemeinsam genutzte Ressourcen
    - Konflikte aus parallelen Abläufen

Plattform

- Haupteinsatzgebiete
  - Flight Control Computer (harte Echtzeit)
  - Mission / Data Management Computer (hohe Datenmengen)
- Mindestanforderungen: Fehler müssen erkannt werden und das System in einen sicheren funktionalen Zustand gebracht werden (Fail Operational)
- Mitigation Concepts
  - Safety Net
  - Monitoring

Werkzeuge

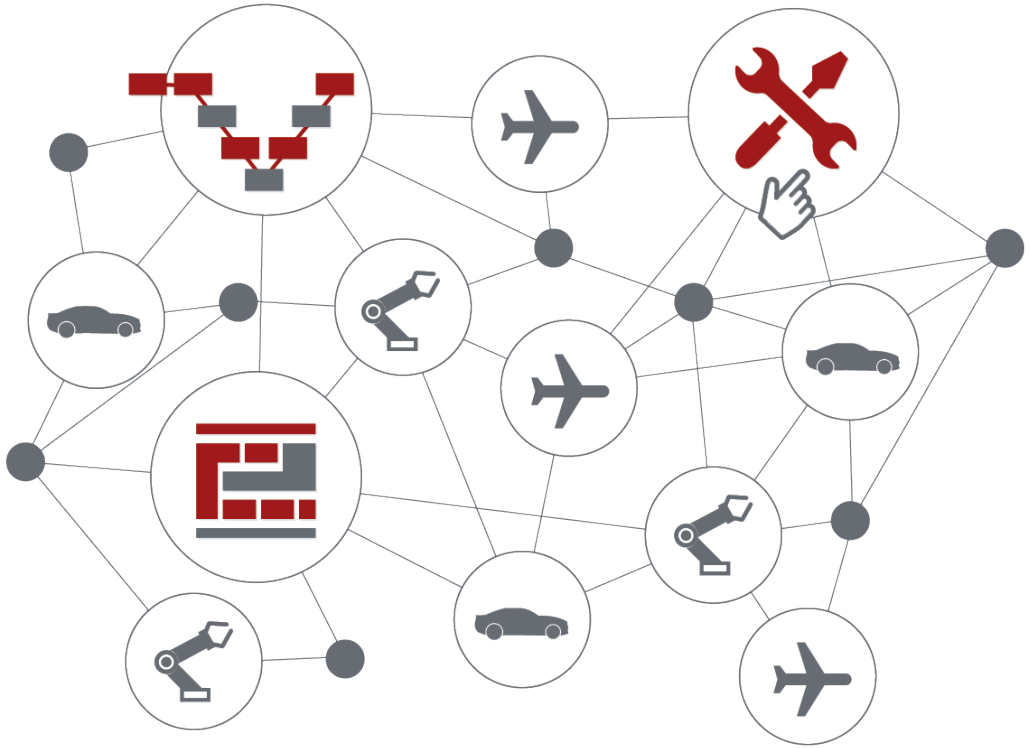
- Entwicklung
  - Modellbasierte Entwicklung mit ARAMiS Tool-Box
- Verification
  - WCET, WCRT
  - Coverage
  - Laufzeitanalysen (Demonstratoren)

Problemfelder

- Durchgängigkeit der Werkzeuge
  - Interoperabilität zwischen Werkzeugen unterschiedlicher Hersteller
  - FOCUS der Werkzeuge -> AUTOSAR (Automotive)
  - Qualification der Tools

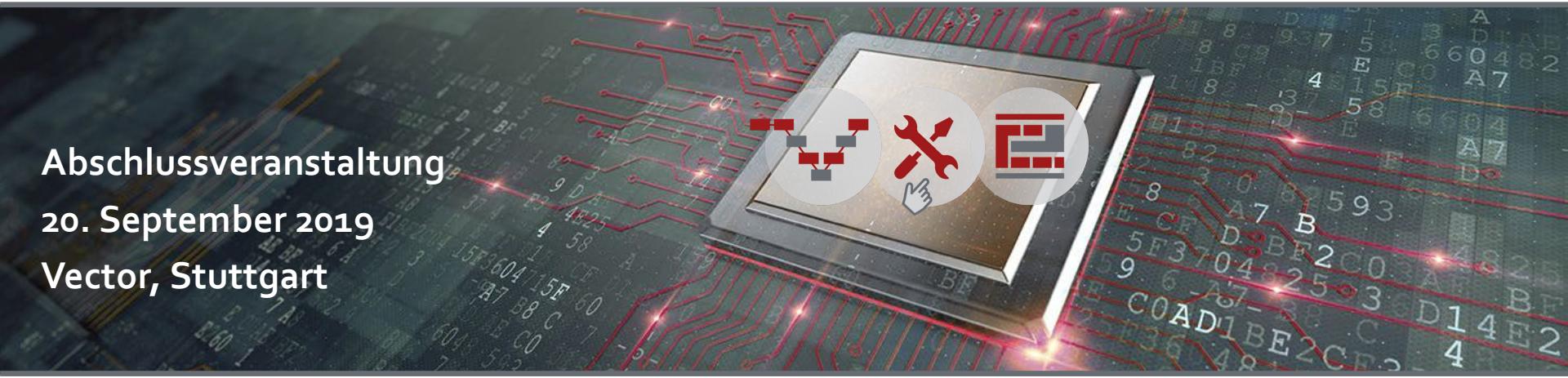
Fazit

- Deutliche Schritte vorwärts
  - Bei Prozessen
  - Werkzeugen
  - Verifikationsmethoden



aramis II

ENTWICKLUNGSPROZESSE I WERKZEUGE I PLATTFORMEN
FÜR SICHERHEITSKRITISCHE MULTICORESYSTEME



Abschlussveranstaltung
20. September 2019
Vector, Stuttgart

Industrieautomatisierung

WIKA, KSB, Siemens

Dr. Tobias Schüle (Siemens)

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Partner Industrieautomatisierung

WIKA MOBILE CONTROL

Echtzeitanwendungen und Datenkommunikation im Industriebereich mobile Maschinen

KSB

Hydromechatronische Systeme für Gebäude- und Industrietechnik, Wassertransport/-reinigung sowie kraftwerkstechnische Prozesse

SIEMENS

Produkte, Anlagen sowie maßgeschneiderte Lösungen in den Bereichen Automatisierung, Digitalisierung und Elektrifizierung

aramis2-automatisierung@lists.kit.edu

Themen Industrieautomatisierung

aramis II
ENTWICKLUNGSPROZESSE I WERKZEUGE I PLATTFORMEN
FÜR SICHERHEITSKRITISCHE MULTICORESYSTEME

	Herausforderungen	Aktivitäten & Ergebnisse
Entwicklungs-prozesse	• Sicherheitskritische Anwendungen nach IEC61508 / IEC60730 • Zertifizierbare Partitionierung mittels Hardware-Virtualisierung • Methoden für den Entwurf deterministischer Multicore-Systeme	• Untersuchung bestehender Entwicklungsprozesse und Abgleich mit ARAMiS-II-Prozess • Definition von für die Industrieautomatisierung geeigneten Prozessen und Frameworks gemäß IEC61508 / IEC60730
Methoden und Werkzeuge	• Deployment und Schedule-Synthese • Parallelisierung und funktionale Zerlegung von Bestandssoftware • Sicherstellung der Korrektheit (Nebenläufigkeitsfehler) • Plattformunabhängige Werkzeugketten	• Tool für die Analyse von Softwarearchitekturen mit Fokus auf Parallelisierung • Effizienter dynamischer Data Race Detector • Prototypische Umsetzung einer plattformunabhängigen Werkzeugkette
Plattformen	• Effiziente Nutzung heterogener Hardwarearchitekturen • Ausfallsichere Systeme • Hardwarebasiertes Scheduling • Optimierung bestehender Plattformen	• Bibliothek und Laufzeitsystem für die parallele Programmierung heterogener SoCs • Methoden für ausfallsichere Systeme sowie Demonstrator zu Software Upgrades • „Proof of Concept" der Optimierungsschritte

Zusammenarbeit der Domäne mit ARAMiS-Partnern

aramis II
ENTWICKLUNGSPROZESSE | WERKZEUGE | PLATTFORMEN
FÜR SICHERHEITSKRITISCHE MULTICORESYSTEME

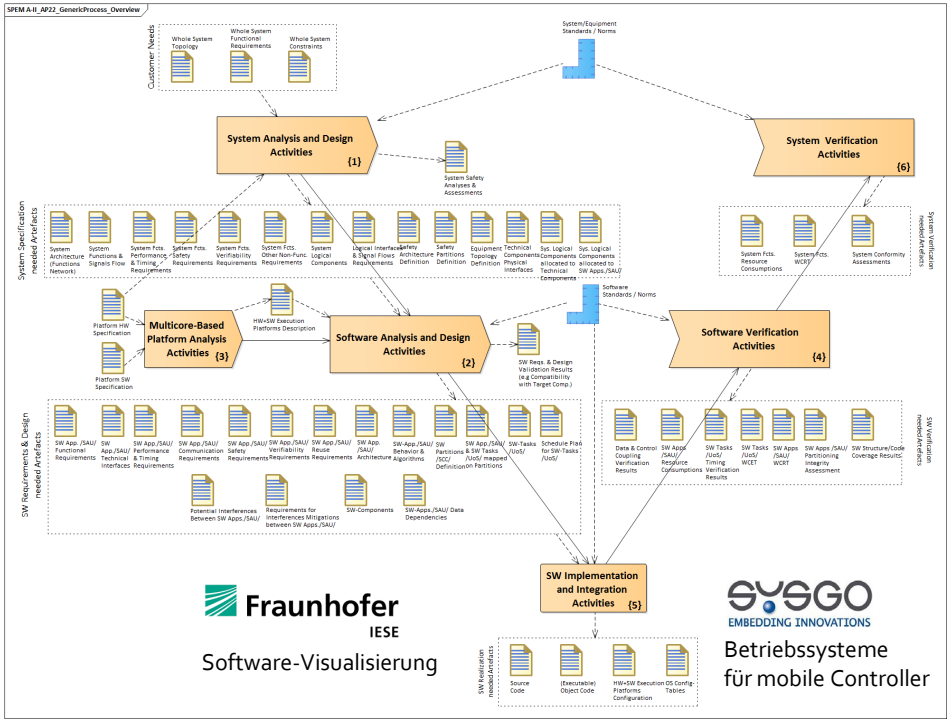
fortiss
Modellierung und Design Space Expl.

Universität Augsburg University
Funktionale Partitionierung

DLR
Deployment / Scheduling für Echtzeitsysteme

KIT
Plattformunabhängige Werkzeugketten

SILEXICA
Code-Parallelisierung



Fraunhofer IESE
Software-Visualisierung

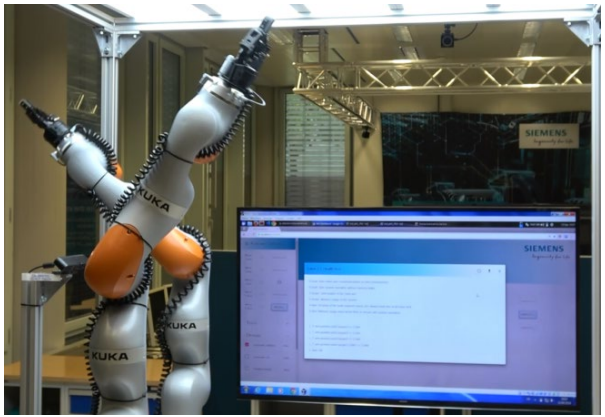
SYSGO EMBEDDING INNOVATIONS
Betriebssysteme für mobile Controller

Statische Analyse von Data Races

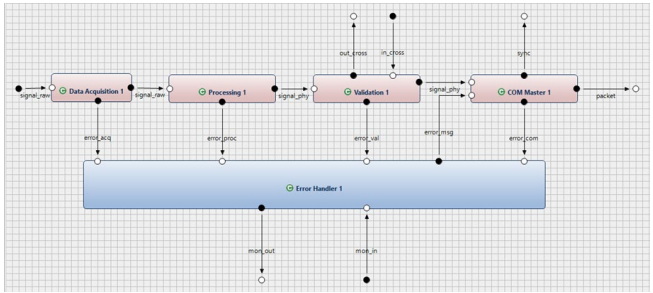
CAU
Christian-Albrechts-Universität zu Kiel

Ergebnisse (Auswahl)

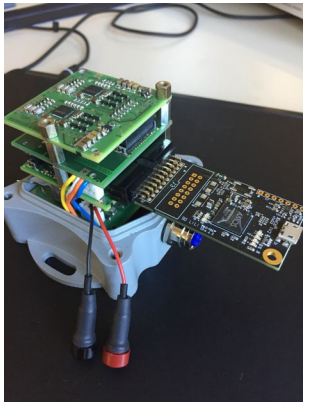
Hardware für Pumpenregelung



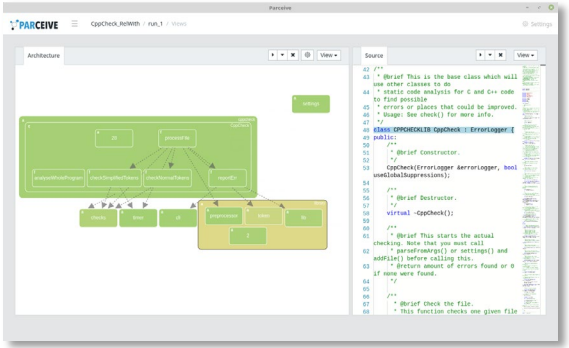
Roboter-Demonstrator zu Software Upgrades



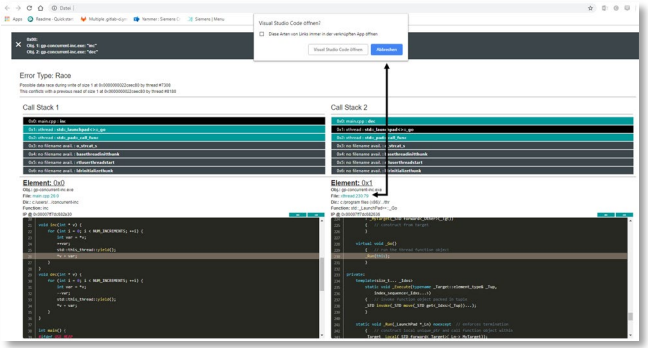
AutoFOCUS3-modellierter, hardwarebasierter Schedulingansatz für Low-Power-Sensorik



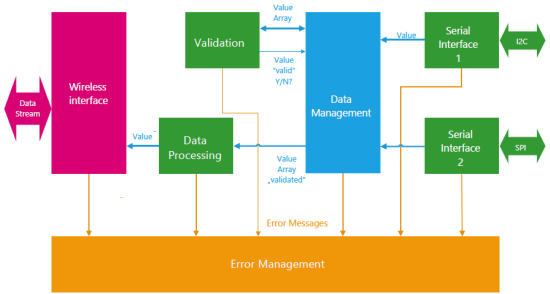
Ergebnisse (Auswahl)



Tool für Software-Architekturanalyse



Dynamischer Data Race Detector



SW-Realisierung redundanter Multicore-Sensor

Open Source Software:

- Data Race Detector (DRace): https://github.com/siemens/drace
- Embedded Multicore Building Blocks: https://github.com/siemens/embb
- Jailhouse Hypervisor: https://github.com/siemens/jailhouse