aramis II

ENTWICKLUNGSPROZESSE I WERKZEUGE I PLATTFORMEN
FÜR SICHERHEITSKRITISCHE MULTICORESYSTEME

ARAMiS II Abschlussveranstaltung
20.09.2019 Stuttgart

Zusammenfassung und Ausblick

Jürgen Becker, KIT und Stefan Kuntz, Continental

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Von ARAMiS zu ARAMiS II

aramis II
ENTWICKLUNGSPROZESSE I WERKZEUGE I PLATTFORMEN
FÜR SICHERHEITSKRITISCHE MULTICORESYSTEME

ARAMiS
Prinzipieller Nachweis der Anwendbarkeit von Multicore in sicherheitskritischen Anwendungen

ARAMiS II
zielt auf einen effizienten Einsatz von Multicore in sicherheitskritischen Anwendungen in der Praxis durch eine Bereitstellung von:

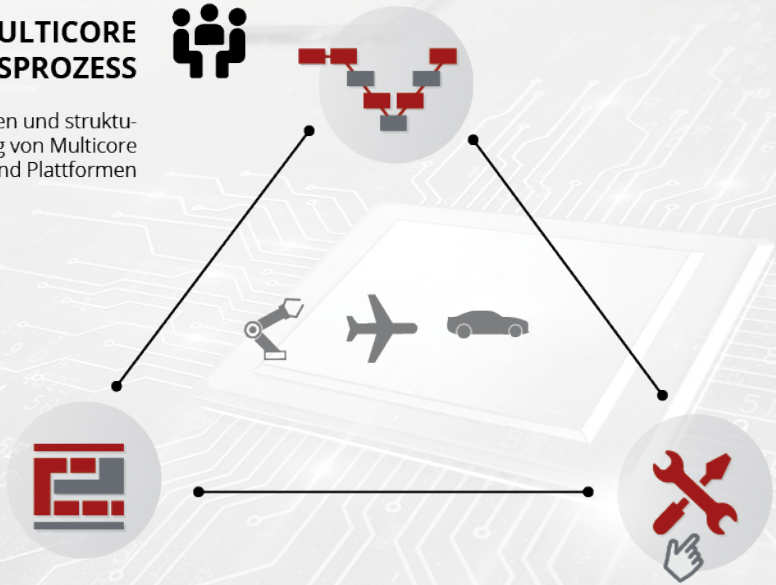
- STRUKTURIERTER MULTICORE ENTWICKLUNGSPROZESS
- MULTICORE METHODEN UND WERKZEUGE
- INDUSTRIELLE PLATTFORMEN FÜR MULTICORE SYSTEME

Projektstruktur und übergeordnete Ziele

aramis II
ENTWICKLUNGSPROZESSE I WERKZEUGE I PLATTFORMEN
FÜR SICHERHEITSKRITISCHE MULTICORESYSTEME

STRUKTURIERTER MULTICORE ENTWICKLUNGSPROZESS

Bereitstellung eines systematischen und strukturierten Ansatzes zur Entwicklung von Multicore Software und Plattformen



NEUE INDUSTRIELLE PLATTFORMEN

Entwicklung und Erweiterung von etablierten industriellen Plattformen unter Berücksichtigung Multicore spezifischer Anforderungen.

NEUE METHODEN UND WERKZEUGE FÜR DEN ENTWICKLUNGSPROZESS

Entwicklung von Methoden und Werkzeugen, welche den strukturierten Multicore Entwicklungsprozess unterstützen

Herausforderungen bei der Entwicklung von Multicore-Systemen

1. **Getrennte Schritte in der Multicore-Entwicklung sind für eine strukturierte Entwicklung von Multicore-basierten Systemen nicht ausreichend:**
   - **Prozess:** Wie muss ein übergeordneter (generischer) Multicore-Entwicklungsprozess aussehen?
   - **Durchgängigkeit:** Wie kann Durchgängigkeit erreicht werden und welche Artefakte werden benötigt?

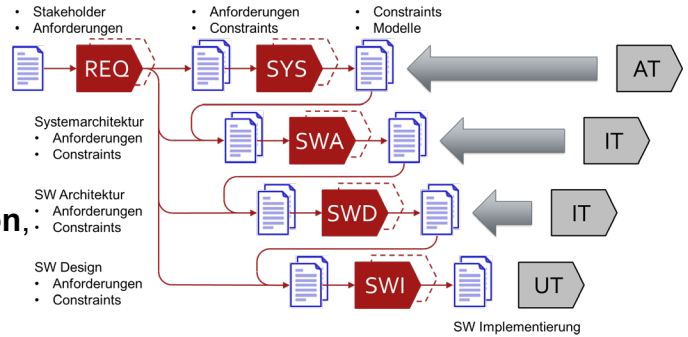
2. **Verfügbare Methoden und Werkzeuge reichen nicht aus, um die Komplexität bei der Entwicklung von Multicore-basierten Systemen zu beherrschen:**
   - **Partitionierung:** Wann und wo soll die Funktionalität aufgeteilt und verteilt werden?
   - **Allokation:** Welche Plattform ist für ein bestimmtes Anwendungsszenario die richtige?
   - **Binding:** Welches Deployment von (Basis-)Softwarekomponenten bietet die optimale Lösung?
   - **Scheduling:** Welches Scheduling von Software-Komponenten führt zur effizientesten Ausführung?
   - **Garantien:** Wie können Plattformaspekte (z.B. WCET, Safety, Korrektheit) sichergestellt werden?
   - **Entwurfsraum:** Wie kann eine Entwurfsraum-Exploration in solchen Systemen durchgeführt werden?

3. **Etablierte Plattformstandards & Softwarearchitekturen unterstützen nicht die Anforderungen von Multicore-basierten Systemen (z.B. Isolation, Synchronisation, Kommunikation)**

ARAMiS II-Lösungen für die Entwicklung von Multicore-Systemen

ENTWICKLUNGSPROZESSE I WERKZEUGE I PLATTFORMEN
FÜR SICHERHEITSKRITISCHE MULTICORESYSTEME

1. **Getrennte Schritte in der Multicore-Entwicklung sind für eine strukturierte Entwicklung von Multicore-basierten Systemen nicht ausreichend:**
   - Der entwickelte generische Multicore-Entwicklungsprozess orientiert sich an den Vorgaben aktueller Standards und wurde erweitert für die Multicore-spezifischen Tätigkeiten, um eine **strukturierte, durchgängige Entwicklung** zu ermöglichen
     - Fokus auf Neuentwicklung von Systemen bzw. Systeme, für die bereits Modelle existieren
   - Formale Spezifikation der erforderlichen **Artefakte** für Zertifizierung oder Qualifizierung in Hinblick auf Multicore-Systeme
   - Definition einer einheitlichen, **domänenübergreifenden Terminologie**
   - Durchgängige Verwendung des **gemeinsamen Metamodells** AMALTHEA
     - Toolchain-Beschreibungen und **Interoperabilitätsspezifikation**, Schnittstellendefinitionen
     - Möglichkeiten zur **Automatisierung** durch zusammenhängende Toolchains



ARAMiS II-Lösungen für die Entwicklung von Multicore-Systemen

2. Verfügbare Methoden und Werkzeuge reichen nicht aus, um die Komplexität bei der Entwicklung von Multicore-basierten Systemen zu beherrschen:

- Entwicklung spezifischer **Methoden und Werkzeuge** zur Unterstützung der Multicore-Entwicklung
- Erweiterung der Methoden für alle **Schritte im Entwicklungsprozess** (z.B. Partitionierung, Deployment, Scheduling)
- **Höherer Automatisierungsgrad** in der Entwicklung durch Werkzeugunterstützung
- Entwicklung von **domänenübergreifenden Methodiken und Tools** für Multicore Architekturen
- Einsatz eines **durchgängigen, gemeinsamen Metamodells** – AMALTHEA
- ARAMiS II Ergebnisdokumente stellen für Entwickler einen „**Tool Baukasten**“ zur Verfügung

Die in TP3 entwickelten Methoden und Tools gewährleisten die Entwicklung von Software für Multicore Architekturen im sicherheitskritischen Umfeld

ARAMiS II-Lösungen für die Entwicklung von Multicore-Systemen

3. **Etablierte Plattformstandards & Softwarearchitekturen unterstützen nicht die Anforderungen von Multicore-basierten Systemen (z.B. Isolation, Synchronisation, Kommunikation):**
   - **Erweiterungen der Plattformen und Standards für sicherheitskritische Multicore-Systeme**
     - Logical Execution Time im Rahmen von AUTOSAR standardisiert
     - Parametrisierbare Laufzeitumgebung für ECUs
   - **Konzepte und Implementierungen für Synchronisation und Kommunikation in Multicore-Architekturen**
     - Kommunikationsschicht für On-Chip Netzwerke
   - **Virtualisierung heterogener Systeme**
     - Online-Überwachung des Hypervisor-Betriebs
   - **Konzepte und Implementierungen für Multicore-basierte fail-operational-fähige Systeme**
     - Dynamische Migration von kritischen Funktionen für heterogene SoCs
     - Ausfallsichere “switch-over“ Mechanismen

ARAMiS II Ergebnisse

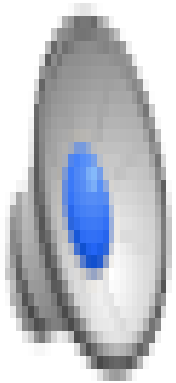
- **400 Anforderungen** erfasst und systematisch **ausgewertet/evaluiert**
- **4 Meilensteine** erreicht (inkl. ***Requirements-Abgleich*** – Analyse + Bewertung)
- 22 Ergebnisdokumente fertiggestellt
- **9 Use Cases** zur Evaluation der Ergebnisse bzgl. Prozess, Methoden und Tools sowie Plattformen und Standards – ***Proof-of-Multicore-Concept***
- **Domänenübergreifende** Verwendung - gemeinsames Metamodell ***AMALTHEA***
- **Methoden- und Tool-Baukasten aus TP3**
- >80 Publikationen veröffentlicht
- Beiträge zur **Standardisierung**, z.B. **LET im AUTOSAR-Kontext**
- Umfangreiche **Toolschnittstellendokumentationen**
  - Datenformate & Interoperabilitäten

Anschlussthemen – Ausblick

- Standardisierung & *Eco-Systeme*
- Weiter-/Ausbildung & Technologietransfer
- Umsetzung der Erkenntnisse in Produkten bei den Partnern
- Verwendung der Methoden und Tools bei der Entwicklung
- Basis für weiterführende Arbeiten und neue Herausforderungen
  - Heterogene Multicore-Systeme, Manycore -> Eingebettete zuverlässige Performanz
  - Fehlertoleranzmaßnahmen in heterogenen MC-Systemen
  - Dynamische & Verteilte MC-Systeme, *Adaptive AUTOSAR*
  - Skalierbarkeit, Vernetzung, Verifikation/Garantien
  - Komplexe MC-Systeme inkl. verifizierbare AI-Komponenten (*Explainability)*
  - ….

Projektbeginn + *weitere Optionen* ....

„ARAMiS-Initiative": Kick-off @ Cassidian ...



„Globale Mobilitätslösungen ...

Danke für die Aufmerksamkeit, Zeit und Kooperation!