Certification of Trusted MpSoC Platforms

Rolf Ernst
Institut für Datentechnik und Kommunikationsnetze
MpSoC 2010, Gifu City, Gifu, Japan

Motivation

- MpSoCs are an efficient platform for systems integration
- due to physical resource sharing, safety critical systems integration becomes more challenging
Mixed Critical MpSoC Certification/Qualification

- resulting multi-core ECU subject to **highest safety standard involved**

- high certification (or qualification, resp.) cost
  - must cover ALL applications and hardware
  - often qualified data of non-critical application not available
  - re-certification for any non-critical application update required

- alternative: isolation of different criticalities
  - approach 1: strict *physical separation* of all HW resources → multiplication of resources → **high hardware cost**
  - approach 2: strict *separation* of HW resource usage → functional and timing isolation
  - approach 3: “controlled” separation - controlling application dependencies
Separation - Basics

• partitioning into certified/qualified core components that control the resources used for any of the critical applications
  – basic software
  – communication
  – shared resources used for critical applications

Approach 2: Strict Separation of HW Resource Usage

• challenges
  – isolation must not be limited to functionality, but must include resource usage, performance guarantees and possibly energy constraints
  – redundancy and physical separation requirements of safety standards must be preserved
• solution: Conservative partitioning in time and/or space
• most popular: Time triggered architecture – TDMA
  principle:
  – periodic assignment of fixed time slots for resource access
  – unused time slots remain empty - efficiency
  – main advantage is predictability in integration
    • non-critical application can run in a timing “sand box”
Why not just use Virtualization?

- virtualization is an appropriate way to control effects of (uncertified) applications
- control covers functionality only
  - timing is still affected
  - critical for real-time systems
→ „weak“ separation, not sufficient in general

Application Timing Dependencies in MpSoC

competing accesses to shared resources challenge worst-case execution time assumptions!

Increased worst-case response time!!
**Approach 3: Controlled Separation**

- combine virtualization (or other functional isolation) with tool based analysis and systematic mitigation of side effects
  - example: tool based timing analysis/optimization with (e.g. SymTA/S)
- support by HW architecture
  - example: NoC scheduling for isolation (today often cross bar)
  - memory partitioning to avoid access collisions
- consider required error models and fault redundancies (incl. transient faults)
- optimize efficiency combining different techniques
- rather unexplored area
(Re-)Certification Cost ↔ Systems Cost

- the different approaches generally enable a tradeoff on (re-)certification costs ↔ product costs
- goal is a design process that supports modular certification reuse backed by HW/SW architecture and tools
- optimum depends on application, volume, criticality, and product lifetime

<table>
<thead>
<tr>
<th>strict physical separation</th>
<th>strict separation of HW resource usage</th>
<th>controlled separation of HW resource usage</th>
<th>unconstrained integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>lowest (re-) certification cost</td>
<td>highest (re-) certification cost</td>
<td></td>
<td></td>
</tr>
<tr>
<td>highest HW cost</td>
<td>lowest HW cost</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The RECOMP Project 2010 - 2013

- estimated between 30-95% (segment dependent) of all industrial embedded MpSoC in Europe will be affected by mixed criticality in 2015
- RECOMP (Reduced Certification Costs for Trusted Multi-core Platforms)
  - European project, 41 partners, 25 Mio € budget
  - develop HW and SW architectures, design methods, and tools to efficiently design and (re-)certify MpSoCs for mixed critical systems
- RECOMP covers the whole supply chain
  - semiconductor vendors (Infineon, Intel)
  - OS (e.g. Elektrobit, Sysgo, Wittenstein)
  - suppliers and integrators (Kone (coord.), Danfoss, Delphi, PSA, EADS, Honeywell, Thales, …)
  - certification service providers (e.g. TÜV Süd, Sysgo)
  - several SMEs as software, service, tool suppliers
  - several research institutions and universities
- RECOMP covers several industries
  - avionics, space, automotive, industrial, medical
  - to define common technologies for joint VLSI, OS, and tool developments
RECOMP Project Challenges

• flexible tradeoff between development, certification, and hardware cost
  – requires configurable core-to-core communication and separation/virtualization technologies
  – compatibility to existing certification standards
• software update capability for non-critical functions
  – requires modular certification process
• modular certification process
  – requires re-use of component certification
  – supported by HW and SW separation features
• tool support
  – for verification (safety, timing, function)
  – for integration
  – for synthesis of OS and HW configurations
  – for functional safety certification/qualification

Conclusion

• merging safety critical ECU functions on MpSoCs typically leads to mixed criticality devices
• mixed criticality is a serious certification cost driver and limits update capabilities of non-critical functions
• no silver bullets for integration available
• potential integration technologies span broad design space but still lack coherence and completeness
• RECOMP project consortium solely dedicated to the MpSoC mixed criticality challenge
• further research needed

Thank you!
Literature

- RECOMP website to come
  - as a starter see
    www.ida.ing.tu-bs.de/en/research/projects/recomp

- for the challenge of MpSoC performance dependencies see