Model-based design and schedulability analysis for avionic applications on multicore platforms

Wenceslas GODARD, Airbus Group Innovations
Geoffrey NELISSEN, ISEP
Ada-Europe 2016 - Industrial Workshop

Reliable Software

June 16th, 2016
Agenda

• CONCERTO (ARTEMIS project)
• Avionic concepts modeling support
• Multicore modeling support
• Partition schedule generation and response time analysis
• Experimentations
• Conclusions
Agenda

• CONCERTO (ARTEMIS project)

• Avionic concepts modeling support

• Multicore modeling support

• Partition schedule generation and response time analysis

• Experimentations

• Conclusions
A Word on CONCERTO

“Guaranteed Component Assembly with Round Trip Analysis for Energy Efficient High-integrity Multi-core Systems”

• An ARTEMIS project, built on top of CHESS, a component-based modelling framework
• Several application domains: telecare, space, avionics, automotive, petroleum
• For the avionics use case:
  – Use of UML/MARTE profile (timing annotations)
  – Behavior description (activity)
  – Assignment to hardware
  – Response time analysis with MAST
• Ended in April 2016
• Results transferred to Polarsys (“CHESS”)
Agenda

• CONCERTO (ARTEMIS project)

• Avionic concepts modeling support

• Multicore modeling support

• Partition schedule generation and response time analysis

• Experimentations

• Conclusions
Avionic concepts

Integrated Modular Avionics (IMA) architecture

Based on robust partitioning (time, memory, IO)
With focus on timing aspects: Major and Minor Frames (MAF and MIF) for each processing unit.

P1: period = 1; P2 = period = 3; P3: period = 4

MIF = GCD(1,3,4) = 1
MAF = LCM (1,3,4)= 12
Avionic concepts

Definitions:
• A partition is a group of tasks (ARINC-653 processes)
• A process is composed of several functions, with optional information for exclusion relation
• An operation is related to piece of code, a function. It can have a rate and precedence constraints

Scheduling is two-level:
• Periodic and fixed at partition level (activation windows)
• Priority based at process level
Avionic concepts

Operations precedence and exclusions:

**partition P1**

**process T1**: Group of operations: (Operation_B); (Operation_C)
- Operation_A: period = 1 * MIF; followed by B
- Operation_B: period = 2 * MIF
- Operation_C: period = 2 * MIF; followed by A
Agenda

- CONCERTO (ARTEMIS project)
- Avionic concepts modeling support
- Multicore modeling support
- Partition schedule generation and response time analysis
- Experimentations
- Conclusions
Multicore

Pros:
Power, weight and size reduction

Cons:
• Each core has its own partitions and schedule
• Each core interfere with each other: partitioning is broken
• Explosion of the complexity to find an optimal allocation

Solution in CONCERTO:
• Do not take into account the penalty from sharing resource (no support for interference awareness)
• Based on basic representation: number of cores. A graphical interface for static allocation of partitions to cores
• Generate partition schedules and compute response times

June 16th 2016
Multicore

Allocation of partitions to cores can be done manually...or automatically
Agenda

• CONCERTO (ARTEMIS project)

• Avionic concepts modeling support

• Multicore modeling support

• **Partition schedule generation and response time analysis**

• Experimentations

• Conclusions
## Schedule generation

### What is generated?

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partition</td>
<td>Tasks allocated; [assigned core][^1]</td>
</tr>
<tr>
<td></td>
<td>Assigned core; MIF, MAF per core; Time-table for partition schedule (activation windows);</td>
</tr>
<tr>
<td>Process</td>
<td>Period; WCET; Priority; Deadline; Group of operations</td>
</tr>
<tr>
<td>Operation</td>
<td>Deadline; WCET; [following operation] Rate</td>
</tr>
<tr>
<td></td>
<td>Priority; Phase</td>
</tr>
</tbody>
</table>
Response time analysis

System is schedulable if all operations respect their deadline

Extension of MAST (http://mast.unican.es/):
  • Taking into account multicore
  • Model partition, processes and operations
  • Transformation (to) and backpropagation (from)

Exact worst-case response time of each operation is computed
Agenda

• CONCERTO (ARTEMIS project)
• Avionic concepts modeling support
• Multicore modeling support
• Partition schedule generation and response time analysis
• Experimentations
• Conclusions
Experimentations

- Currently at research level (ARTEMIS project)

- Most input data from a real application specification – manually “extracted”

- Assumptions made on the WCET for operations and processes (no code)

- Subset implemented (tutorial is in preparation)

- Dissemination made and planned in and outside Airbus Group and its divisions
Experimentations – demo (1/6)

Definition of:

- **Interfaces**

- **Component Types**

- **Component Implementations**
Experimentations – demo (2/6)

Composition of:

- Component instances
- Timing properties
- Partitions
Experimentations – demo (3/6)

Assignment of Processes to **Partitions**
Experimentations – demo (4/6)

Allocation of Partitions to **Cores**
Experimentations – demo (5/6)
Experimentations – demo (6/6)

The system is schedulable

<table>
<thead>
<tr>
<th>HW Instance</th>
<th>Utilization</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>HW.processor_core0</td>
<td>64.00%</td>
<td>OK</td>
</tr>
<tr>
<td>HW.processor_core1</td>
<td>25.00%</td>
<td>OK</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SW Instance</th>
<th>Operation</th>
<th>Response Time</th>
<th>Deadline</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>SW_System.c1_1</td>
<td>op_1_1_a</td>
<td>0.079819s</td>
<td>0.1s</td>
<td>OK</td>
</tr>
<tr>
<td>SW_System.c1_1</td>
<td>op_1_1_b</td>
<td>0.039273s</td>
<td>0.05s</td>
<td>OK</td>
</tr>
<tr>
<td>SW_System.c1_2</td>
<td>op_1_2_c</td>
<td>0.001000s</td>
<td>0.05s</td>
<td>OK</td>
</tr>
<tr>
<td>SW_System.c1_2</td>
<td>op_2_2_a</td>
<td>0.003300s</td>
<td>0.05s</td>
<td>OK</td>
</tr>
<tr>
<td>SW_System.c1_2</td>
<td>x</td>
<td>0.004000s</td>
<td>0.05s</td>
<td>OK</td>
</tr>
<tr>
<td>SW_System.c1_2</td>
<td>op_1_2_b</td>
<td>0.002200s</td>
<td>0.05s</td>
<td>OK</td>
</tr>
<tr>
<td>SW_System.c2_1</td>
<td>op_2_2_a</td>
<td>0.006000s</td>
<td>0.05s</td>
<td>OK</td>
</tr>
<tr>
<td>SW_System.c2_2</td>
<td>op_2_2_a</td>
<td>0.008000s</td>
<td>0.05s</td>
<td>OK</td>
</tr>
<tr>
<td>SW_System.c1_1</td>
<td>op_2_2_a</td>
<td>0.010000s</td>
<td>0.05s</td>
<td>OK</td>
</tr>
<tr>
<td>SW_System.c1_1</td>
<td>op_2_1_b</td>
<td>0.008000s</td>
<td>0.05s</td>
<td>OK</td>
</tr>
<tr>
<td>SW_System.c3</td>
<td>op_3_a</td>
<td>0.015079s</td>
<td>0.1s</td>
<td>OK</td>
</tr>
<tr>
<td>SW_System.c3</td>
<td>op_3_b</td>
<td>0.011079s</td>
<td>0.1s</td>
<td>OK</td>
</tr>
</tbody>
</table>
Agenda

• CONCERTO (ARTEMIS project)
• Avionic concepts modeling support
• Multicore modeling support
• Partition schedule generation and response time analysis
• Experimentations
• Conclusions
Conclusions

Summary
Extension of CHESS environment with an extension of modelling and verification supporting IMA partitioning (SW + HW)
Includes response time analysis with backpropagation from MAST++
Formal approach, as recommended by certification authorities

Future:
Complete the modelling objects to be able to represent: ARINC-653 OS services as operations so that it can be linked with real software by code generation
Bind interference for multicore memory accesses (and caches)
Test real HW platform (ARINC-653 OS configuration according with this methodology)

Check out other use cases: http://www.concerto-project.org/

June 16th 2016