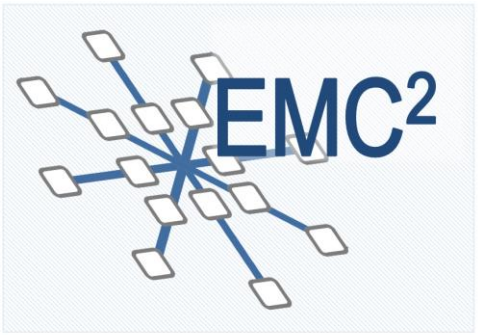


EMC2/WP2

APPLICATION MODELS AND DESIGN TOOLS FOR MIXED-CRITICAL, MULTI-CORE EMBEDDED SYSTEMS

Albert Cohen, Zhen ZHANG
INRIA-Parkas

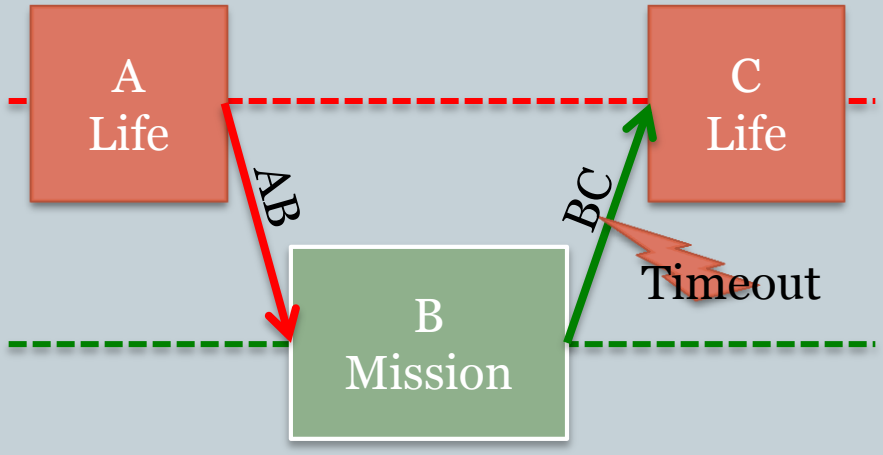
Objectives

- Functional and non-functional criteria
- Safety level independent unique modeling (correct by construction)
- OS independent executable model with interference analysis
- Formal, Graphical (block diagram) entry for
  - Application and architecture modeling and configuration
  - Timing instrumentation/annotation configuration
- Code generation efficiency
- Simulation performance constraints
- Design, analysis, verification tools

INRIA - Activities

- Mixed time-criticality systems
  - Life (hard), Mission (soft), Non-critical (non)
- Synchronous Language : Heptagon
  - Semantic extension
  - Asynchronous communication modeling
  - Non-functional properties
- Case-study: Passenger-Exchange (Alstom Transport)
  - Railway signal control
  - IRT/SystemX, FSF project
- Experimental Implementation
  - Zynq SoC/Fpga platform

Design Model

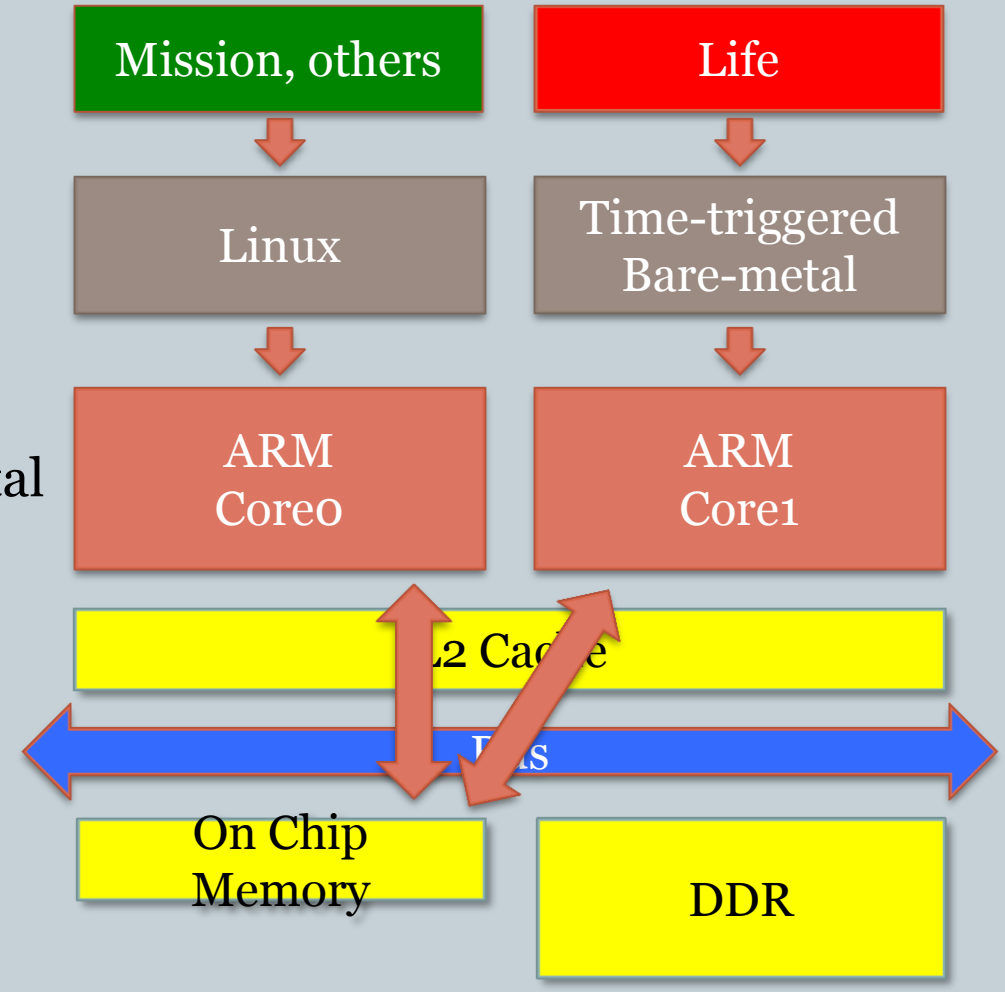



```
Node C (unpunctual BC)
let
        If ontime BC then
                Deal with BC;
        Else /* Data Absence */
                Deal with Timeout;
        End
tel
```

- Allow mission-critical tasks to miss deadlines to reduce certification cost (the timing dimension at least) !!! Late != fault !!!
- Mission-critical tasks must not delay Life-critical ones
- Handle data absence programmatically
- Isolate the components in need of true or high-assurance WCET
- Isolate time from other dimensions of criticality -> deploy safety-critical system on off-the-shelf hardware with high efficiency
- Safety vs Availability (mission)

Experimental Implementation

- Zynq 7k SoC/Fpga
  - Dual ARM + FPGA
- Implementation
  - AMP configuration
  - Life
    - Time-triggered/Bare-metal
    - OCM
  - Mission and others
    - Linux
    - DDR
  - Communication
    - OCM



Thanks