Early power and performance optimization of algorithm implementation on ARM processors

Francesco Regazzoni
ALaRI Institute, University of Lugano (CH)
Outline

- Motivation of the work.
- Overview of used tool: Mirabilis VisualSim.
- Case study: AES algorithm.
- First system.
- Second system.
- Conclusions.
Motivations

- Achieving the required throughput at the lowest power consumption is a primary concern in the architecture of mobile handheld devices.
- The selection of the processor and the architecture of the full system must be determined before committing to hardware and software.
- A preliminary investigation of the performance vs. power trade-off can be performed leveraging on macro-architecture exploration.
- Using Mirabilis VisualSim a model of the system that provide such accuracy can be constructed in a few hours.
VisualSim is a graphical and platform-independent architectural analysis and exploration software tool.

VisualSim can be used in any application that requires the design of hardware and software elements.

All of the system design aspects are addressed by VisualSim using the building blocks.

All of the building blocks, simulation platforms, analysis and debugging required to construct a system are provided within a single framework.

Thus models in all these analyses can be constructed quickly and easily.
Key features:

- Design with multiple abstraction levels.
- Integrated multi-simulation engines and JIT data types.
- Extensive libraries of parameterized models.
- Publish to the Web for communication and remote execution.
- Graphical entry and hierarchical modeling.
- Robust visualization and analysis capabilities.
- Import Java/C/C++ and link to Excel & MatLab.
- Automatic error checking between SmartBlocks models.
- Enable assertions for system-coverage.
Applications

- Design new and custom hardware and software architectures.
- Design sub-systems such as CPU, memory controllers and DMA.
- Sizing CPU speed, Bus width, Cache, Memory & Pipeline stages.
- Architect embedded software.
- RTOS consideration.
- Design of new wireless and communication protocols.
VisualSim Overview 4/4

- Analysis
  - Architecture utilization.
  - Application response time.
  - Functional correctness of algorithms.
  - Buffer requirements.
  - Implementation and design constraints generation.
  - Power
Case Study 1/3

AES (Advanced Encryption Algorithm, FIPS 197):

- Block cipher: block size 128.
- Key size: 128; 192; 256.
- Round operations:
  - Shift row.
  - Mix Column.
  - Non linear transformation (SBOX).
  - Add Round key.
- The Number of rounds depends on the key length.
The algorithm runs on ARM processors in different systems. Different key length are tested. Measurements of:
- Latency.
- Power consumed by the processor
The trade off is analyzed.
Case Study 3/3

- The AES code is an open source version taken from the web.
- The code was annotate and compiled with the gcc compiler to obtain the execution trace.
- The trace was used as input for the model of the CPU inside Mirabilis VisualSim.
System one (Full system details)

- Dual processor ARM7TDMI.
- AES tasks are loaded on the two CPU.
- Parameters checked:
  - System utilization.
  - Processor latency.
  - Processor instant power.
  - Battery power.
System one (Full system in VisualSim)

AES Dual ARM7 Platform Model.

**Scenarios**

**Scenario (1): AES Annotated Software**

**Performance Model Parameters**
- Sim.Time: 6.0E-04
- Key_Size: Index: 4
- Bytes_Sent: 10
- Processor_Speed_MHz: 133.0

**HW Architecture**

**SW Architecture**

Read C Code Annotation Data Structures from annotate.txt file and send to Processor.

Source: www.arm.com
System one (ARM7TDMI in VisualSim)

Dual ARM7 + L2 Cache + SDRAM

Detailed processor portion of model.

Parameters:
- Processor_Speed_Mhz: Processor_Speed_Mhz
- L_Cache_KB: "16"
- D_Cache_KB: "8"
- Bus_Speed_Mhz: Processor_Speed_Mhz
- Cache_Speed_Mhz: Processor_Speed_Mhz
- Cache_Size_KB: 32
- RAM_Speed_Mhz: Processor_Speed_Mhz / 2.0
- RAM_Size_MB: 8
- RAM_Access_Time: "Read 8.0, Prefetch 8.0, Refresh 8.0, Write 7.5"

source: www.arm.com
System one (Processors Utilization)
System one (battery and instant power)
System two (Full system details)

- Single processor ARM-8 Cortex.
- All AES tasks are loaded on the same CPU.
- Parameters checked:
  - System utilization.
  - Processor latency.
  - Processor instant power.
  - Battery power.
System two (Full system in VisualSim)

AES ARM8 Platform Model.

Scenarios
--------------------------------------------------------------
Scenario (1): AES Annotated Software

Performance Model Parameters
---------------------------------------------
- Sim_Time: 3.0E-04
- Key_Size_Index: 4
- Bytes_Sent: 10
- Processor_Speed_Mhz: 600.0

Simulator Engine
------------------------
DE Simulator

HW Architecture

State Plot Block

SW Architecture

Read C Code Annotation Data Structures from annotate.txt file and send to Processor.

www.alari.ch

source: www.arm.com
System two (ARM8-Cortex in VisualSim)

**ARM8 + L2 Cache + SDRAM**

**Detailed processor portion of model.**

**Parameters.**
- Processor_Speed_MHz: Processor_Speed_MHz
- L_Cache_KB: "16"
- D_Cache_KB: "8"
- Bus_Speed_MHz: Processor_Speed_MHz
- Cache_Speed_MHz: Processor_Speed_MHz
- Cache_Size_KB: 32
- RAM_Speed_MHz: Processor_Speed_MHz / 2.0
- RAM_Size_MB: 8
- RAM_Access_Time: "Read 3.0, Prefetch 3.0, Refresh 3.0, Write 2.5"

**Source:** www.arm.com
System two (Processor Utilization)
System two (battery and instant power)
System Comparison

- ARM8-Cortex/ARM7TDMI power consumption:
  - 9.5

- ARM8-Cortex/ARM7TDMI speed:
  - 2

- ARM8-Cortex is faster

- Two ARM7TDMI consume less power
Conclusions

- Performance/Power Trade off is of crucial importance in embedded systems design.
- The presented case study demonstrates that using Mirabilis VisualSim was possible to:
  - Model the full system in few hours (the full experiment was realized in less then 10 hours).
  - Analyze the latency and the power consumed by the full system ad its main components.
  - Explore very quickly different implementation and platform.
Questions?
Thank you for attention.
(regazzoni@alari.ch)

Please feel free to come to Mirabilis Design (booth F-51) for a demo