Towards Precise Timing Modeling for Industrial System Engineering

FMTV 2014
Singapore, May 12th 2014

Rafik HENIA, Laurent RIOUX
Thales Research & Technology France
• THALES profile

• Forecasting the real-time behavior: why? when?

• Industrial design process practices

• Connecting timing analysis to design: experience feedback

• Conclusions
OUTLINE

- THALES profile
- Forecasting the real-time behavior: why? when?
- Industrial design process practices
- Connecting timing analysis to design: experience feedback
- Conclusions
THALES Profile

DUAL markets: Defence & Civil

A balanced revenue structure

<table>
<thead>
<tr>
<th>Defence</th>
<th>Civil</th>
</tr>
</thead>
<tbody>
<tr>
<td>55%</td>
<td>45%</td>
</tr>
</tbody>
</table>
The information contained in this document and any attachments thereto is the property of THALES. You are hereby notified that any review, dissemination, distribution, copying or otherwise use of this document is strictly prohibited without Thales prior written approval. ©THALES 2011. Template trtp version 7.0.8.

Global leadership

N 1 worldwide
- Payloads for telecom satellites
- Air Traffic Management
- Sonars
- Security for interbank transactions

N 2 worldwide
- Rail signalling systems
- In-flight entertainment and connectivity
- Military tactical radiocommunications

N 3 worldwide
- Avionics
- Civil satellites
- Surface radars

€14 billion in revenues

FMTV 2014, Singapore, May 12th 2014
GLOBAL REACH, LOCAL EXPERTISE

Employees

65,000
(workforce under management at 31 Dec. 2012)

Global presence

56 countries

Research and development

2.5 billion euros
(approx. 20% of revenues)

FMTV 2014, Singapore, May 12th 2014
OUTLINE

- THALES profile
- Forecasting the real-time behavior: why? when?
- Industrial design process practices
- Connecting timing analysis to design: experience feedback
- Conclusions
THALES Systems are mostly safety or mission critical real-time systems:

- Timing is relevant to the correctness of the systems execution
  - In the civil aerospace domain, the requirement of DAL A functions corresponds to a failure rate requirement of $1 \times 10^{-9}$ per flying hour

- Mastering the timing behavior is crucial
  - Overestimation may lead to over-dimensioning
    - Impact on competitiveness
  - Underestimation may lead to failures
    - Impact on reliability, credibility, image, etc…

FMTV 2014, Singapore, May 12th 2014
Forecasting the Real-Time Behavior is difficult, why?

The timing behavior is **hard** to predict due to the...

- **Increasing system complexity**
  - Delivered products implement more and more complex features making the verification space covering the system timing behavior very large

- **Increasing heterogeneity of software and hardware**
  - Involving more and more providers makes the control and efficiency of the integration at a global level difficult
  - E.g. more than 2000 suppliers for AIRBUS, 1260 for FORD

- **Various changes across the development process phases**
  - The timing behavior is a moving target which is very sensitive to changes (butterfly effect)

FMTV 2014, Singapore, May 12th 2014
Forecasting the Real-Time Behavior, when to start?

Traditional V-cycle: timing verification starts **after** implementation and integration
Starting performing timing verification after implementation and integration is hazardous!

- Timing issues are more difficult to detect
  - High risk of deficiency due to undetected timing errors
- Timing issues are more difficult and expensive to fix
  - High risk of penalties due to delivery postpone
- No support for potential evolutions and upgrades of systems with a long life cycle
  - Negative impact on competitiveness and customer confidence
There is a need for **reliable** and **efficient** timing engineering practices starting at **early** design stages and continuing throughout the **whole** development cycle.

FMTV 2014, Singapore, May 12th 2014
OUTLINE

- THALES profile
- Forecasting the real-time behavior: why? when?
- Industrial design process practices
- Connecting timing analysis to design: experience feedback
- Conclusions
Current trend is model-based design to...

- Master the software and hardware complexity
- Support incremental population of the design
- Track the impact of the various changes across the different phases of the design process
  - Easy traceability management
  - Consistent and coherent design
- Increase the design productivity
  - Automated tooled process
  - Reuse of Models (components, platforms, …)
  - Models are used to produce design process artefacts
Models essentially used for generation of design documentation

- E.g. specification of the system, the software, the interfaces,…
- No interpretation of models (models seen as pictures)

Evolution of models use to automated generation of code

- Mainly structural code
- Models evolution toward their interpretation
  - There is a need for function and non-functional unambiguous modeling

Fork call

Duplicate

Split
Models evolution toward their interpretation

- There is a need for function and non-functional unambiguous modeling.

Task response time = 100ms

- milliseconds or microseconds?
- From task activation to termination?
- From task execution start to termination?
- From task chain input activation to task termination?
- From task effective activation?
- From task earliest possible activation?
Generic Design Engineering Languages:

- UML
- F-UML
- ALF
- PS UML composite-structure

SAE AADL: AADL $\rightarrow$ formal behavioural annex
Forecasting the timing behavior in industry is already performed at early design stages, but is usually...

- **Almost limited to ad hoc timing verification**
  - Use of excel sheets
  - Manual timing verification

- **Loosely connected to the design model**
  - Duplication of work
  - No synchronization with design

- **Performed occasionally, not systematically**
  - No continuous and rigorous process
Evolution of Performance Engineering Activities Over Time

Not supported or loosely connected to the design model

Point to point interaction with the design model

Integrated in the design flow
OUTLINE

- THALES profile
- Forecasting the real-time behavior: why? when?
- Industrial design process practices
- Connecting timing analysis to design: experience feedback
- Conclusions
Component-based model of satellite on-board software
Connecting Timing Analysis to Design Model

Required by analysis tool

- Application model
- Platform and mapping model
- Timing characteristics
- Scheduling characteristics
Available in modelling tool

- Application model

Required by analysis tool

- Application model
- Platform and mapping model
- Timing characteristics
- Scheduling characteristics
Design Model Extension with Performance Model

Component based model
(lwCCM)

Definitions of call sequences and modes

Tasks declaration

Budget

Estimated

Measured

PRODUCER_Impl.EXECUTE_PROD_FUNCTIONS :
  scenario NOMINAL {
    call PRODUCER_Impl.DF.NOM, EXEC_NOM_DATA_FILTERING
    call PRODUCER_Impl.DP.NOM, EXEC_NOM_DP
  }
  scenario COARSE_PRECISION {
    call PRODUCER_Impl.COARSE, EXEC_COARSE_DP
  }
  scenario ERROR {
    call PRODUCER_Impl.DF.NOM, EXEC_NOM_DATA_FILTERING
    call PRODUCER_Impl.DP.NOM
    raise EVENT.PRODUCER
  }

FMTV 2014, Singapore, May 12th 2014
Connecting Timing Analysis to Design Model

Available in modelling tool
- Application model
- Platform and mapping model
- Timing characteristics
- Scheduling characteristics

Required by analysis tool
- Application model
- Platform and mapping model
- Timing characteristics
- Scheduling characteristics
Connecting Timing Analysis to Design Model

Available in modelling tool
- Application model
- Platform and mapping model
- Timing characteristics
- Scheduling characteristics

Required by analysis tool
- Application model
- Mapping
- Timing characteristics
- Scheduling characteristics

A task produces output data at the end of its execution

FMTV 2014, Singapore, May 12th 2014
Design Model Semantic

Task 1

Task 2

asynchronous call

Task 3

synchronous call
Design Model Transformation

Task 1

Timing behavior

Task 1,a

Timing behavior

Task 1,b

Task 2

[1-4 ms]

Task 2

[1-4 ms]

Modeling tool

Analysis tool
Design Model Transformation

Task 1
Timing behavior

Task 2

Task 1,a

Task 1,b

Modeling tool

Analysis tool

FMTV 2014, Singapore, May 12th 2014
Model transformation allows filling the semantic gap between design and analysis models.
However...

- Requires expertise in the design model and the analysis model
- Has limitations and there is no generic transformation solution

Model transformation allows filling the semantic gap
Connecting Timing Analysis to Design Model

Different tools, different analysis model semantics, different model transformations

Modeling tool

MAST

CHEDDAR

SymTA/S

FMTV 2014, Singapore, May 12th 2014
However...

- Requires expertise in the design model and the analysis model
- Has limitations and there is no generic transformation solution
- Requires result adaptation to design model

Model transformation allows filling the semantic gap
From Timing Analysis Back to Design Model

Task 1,a

Task 1,b

Task 2

Task 1,c

Task 3

FromTiming Analysis Back to Design Model
Fill the Semantic Gap Between Design and Analysis Models

Model transformation allows filling the semantic gap

However...

- Requires expertise in the design model and the analysis model
- Has limitations and there is no generic transformation solution
- Requires result adaptation to design model
- Would require additional certification effort in case of safety critical applications

FMTV 2014, Singapore, May 12th 2014
OUTLINE

- THALES profile
- Forecasting the real-time behavior: why? when?
- Industrial design process practices
- Connecting timing analysis to design: experience feedback
- Conclusions
• **Timing Verification at early design phases is essential to…**
  - decrease design time and increase productivity
  - reduce risks of costly timing errors detected after implementation and integration

• **Trends toward precise interpretable models opens the door to the use of formal timing verification techniques**

• **Adoption and acceptance of formal timing verification techniques in the industrial design process requires**
  - a seamless automated integration in the model-based design process
  - Filling the semantic gap between industrial design models and the various existing timing models from academic research
Thank you for your attention!