Establishing Formal Scheduling Analysis in Automotive Design Processes

Lecturer : Kai Richter
CTO
Symtavision GmbH, Germany

http://www.artist-embedded.org/
Outline

- SYMTA VISION – Who we are & what we do
- Examples of industrial application of scheduling analysis
- Challenge: Establishing formal analysis in industry
  - Technology customization
  - Integration into existing design processes & tool chains
  - Cooperation with strong partners
- Conclusion
Scheduling Analysis for ECU, Networks and Systems saves time, money and headaches

Solutions Overview
July 2008
SYMTA VISION

- Founded May 2005
- Spin-Off from Braunschweig University, Germany (Prof. Ernst)
- Focusing on real-time systems for over 10 years
- 12+ staff and growing

Expertise
- Real-time system design and integration
- Timing verification and performance optimization for
  - ECU
  - Buses
  - Networked systems
- Technology: scheduling analysis, symbolic simulation, optimization
- Tool: SymTA/S (Symbolic Timing Analysis for Systems)
What is Scheduling Analysis?

Scheduling Analysis is a reliable, model-based approach to verify the real-time properties of embedded systems.

- Necessary for real-time systems, where the correct function depends on correct timing.

- Examples:
  - Automotive: E-steering, engine control, ESP …
  - Aerospace: steering, navigation …
  - Infotainment: communication, video, HMI …

Quelle: BMW
Why Scheduling Analysis

Scheduling Analysis avoids integration problems and failures, and helps to cost-optimize real-time systems.

- **Goals of our customers**
  - Avoid expensive integration problems
  - Optimize total cost
  - Speed-up design
  - Easy extensibility
Why SYMTA VISION

- Full focus on timing / performance
- Reliable and fast timing-analysis tools
- Unique, complete system view
- From 1\textsuperscript{st} design to final verification

- Best integration
- Highest expertise in the market
  - confirmed by our customers and partners
Customer Benefit

- **Time / Cost**
  - Avoid timing-problems early instead of fixing them late
  - Speed-up system dimensioning by factor 2x – 10x
  - Save up to 50% on the cost of components

- **Quality**
  - Reliability can be verified
  - Needed for safety-critical systems, e.g. IEC 61508

- **Savings potential**
  - 1 – 10 M€ savings during development
  - 10 – 100 M€ savings after delivery
  - 1 – 10 M€ savings in purchasing
SymTA/S: Symbolic Timing Analysis for Systems

Input: System model

Output:
- Verified timing
- Optimized system
Customers, Partners, Networks

- OEMs and suppliers
- For ECUs and Networking
- From early design to final verification

- Product-, engineering- and sales-partners
- Networks
ALL-TIMES Timing Analysis Partnership

Timing analysis

Code analysis
- Measurement
- Measurement based analysis
- Static code analysis

System analysis
- Tracing and displaying
- Static scheduling analysis

Work in Progress:
- CLIWA
- AbsInt
- SYMTA VISION
SYMTA VISION Goals

- **Market leader** for timing analysis and optimization
- **Standard solution** for the complete design-flow
  - Consistent Solution (1-Stop Shop)
  - Seamless Integration in development processes
  - Tight cooperation with strong partners
- **Outstanding Services and Support**
- **Global operation**
- **Multiple markets** (Automotive, Aerospace, Infotainment, …)
Established Design Process

- Requirements
- System Design
- Network Design
- ECU Design

- Requirements Verification
- System Verification
- Network Verification
- ECU Verification

OEM

Supplier

Symtavision Overview, July 2008
© Symtavision GmbH, Germany
SYMTA VISION adds Performance Design and Verification
SymTA/S Tool Suite
Symbolic Timing Analysis for Systems

Plug-Ins
- Exploration
- Sensitivity
- ...

Open interfaces
- Analysis Engine

Component libraries
- OSEK variants
- ERCOS®, RTA, ...
- AUTOSAR OS
- CAN
- FlexRay®
- Gateway®

Import / export interfaces
- FIBEX®
- XML
- K-Matrix
- Trace tools
- WCET tools
- AUTOSAR®
- Excel
- OIL®
- TraceGURU, WinRTM, ...
- aiT, ...

3rd party

* = work in progress
Design Space Exploration / Automatic Optimization

1. Define search space
2. Define objectives
3. Explore effects of parameter changes on objectives
Sensitivity Analysis

- Determines
  - Robustness
  - Flexibility
  - Criticality of current implementation
SYMTA VISION Services

- SYMTA VISION Engineering
  - Timing analysis and optimization services
  - Customization and extension of SymTA/S
  - Integration of SymTA/S into customer design flow

- SymTA/S Training
  - 2 - 3 day in-depth training
  - In Braunschweig or at customer site
Technology Excursion
Coverage of Simulation / Test / Measurement

- Simulation does not reliably cover all corner cases.
- Coverage decreases with increasing complexity (integration).
- Certain applications require more reliable analysis.

⇒ Scheduling analysis ⇒ SYMTA

Skip theory
RMS Theory – The response time formula

\[ R_i = C_i + \sum_{j \in hp(i)} C_j \left\lceil \frac{R_i}{T_j} \right\rceil \leq D_i = T_i \]

- **fix-point problem**
- **response time**
- **core execution time**
- **# of preemptions**
- **interference term** \( I_i \)
Non-Preemptive Blocking

lower priority T2 blocks, because it has started just before T1

higher priority T0 does not preempt here, because T1 has already started

\[ B_i = \sum_{j \in hp(i)} C_j \left( \frac{I_i}{T_j} \right) \]
SymTA/S structures the influences on scheduling

**task timing behavior:**
- varying execution times
- task modes

**activation timing:**
- jitter
- burst
- time table offsets
- dynamic profiles
- **system-level interactions**

\[
R_i = C_i + \sum_{j \in hp(i)} C_j + \left\lfloor \frac{R_i}{T_j} \right\rfloor
\]

# of preemptions

**scheduling strategy:**
- non-preemption
- deferred preemption
- other strategies

**SYMTA**
- modular combination of features
- configurable accuracy / efficiency
- flexible input data
Focus: Tracing vs. SymTA/S Analysis

- Measured 10ms task: Response time 6.9ms
  - 4 CAN, 8 SPI interrupts, 7 preemptions by 1ms task

- SymTA/S Analysis of 10ms task: Worst-case response time 9ms
  - 10 CAN, 8 SPI interrupts, 9 preemptions by 1ms task, **blocking**
Confidence-accuracy trade-offs

- accuracy
- analysis efficiency
- available data
- usefulness
  - worst case often overly pessimistic
  - depends on application area (consider also multimedia or avionics)
Why SYMTA VISION?

SYMTA VISION has

- selected most relevant concepts from scheduling analysis research
- tailored them towards industry requirements (automotive), and
- integrated them into a unique, comprehensible tool suite

SymTA/S provides:

- formal analysis → systematic timing coverage
- efficient abstraction → convenient modeling & early application
- sophisticated algorithms → quick analysis results
- comprehensive visualization → easy understanding and debugging

→ Systematic control on key timing influences
ECU-level and network-level
SymTA/S Use Cases
Example 1: Safety-Critical ECU

Chassis domain: Active Front Steering
- Verifying Performance and Timing for all critical cases
- Safeguarding against liability claims (IEC 61508 SIL 3)
- Optimizing ECU performance and cost (use of cheaper CPU)

Hans Sarnowski, responsible BMW Engineer: „You really get to know your system and can detect real-time errors in a fraction of time“
Integration: Tracing + SymTA/S

- Single function execution times

<table>
<thead>
<tr>
<th>Process</th>
<th>Task</th>
<th>BCET</th>
<th>WCET</th>
<th>Freq.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proc_001</td>
<td>200ms_Task (5)</td>
<td>1.62</td>
<td>2.16</td>
<td>200</td>
</tr>
<tr>
<td>Proc_002</td>
<td>1000ms_Task (2)</td>
<td>3.08</td>
<td>3.18</td>
<td>1000</td>
</tr>
<tr>
<td>Proc_003</td>
<td>1000ms_Task (2)</td>
<td>2.36</td>
<td>2.36</td>
<td>1000</td>
</tr>
<tr>
<td>Proc_004</td>
<td>TSK_Dynamic (12)</td>
<td>2.76</td>
<td>2.76</td>
<td>5</td>
</tr>
<tr>
<td>Proc_005</td>
<td>TSK_Dir+</td>
<td>3.44</td>
<td>4.26</td>
<td>5+</td>
</tr>
</tbody>
</table>

- Interrupt Frequency
Focus: Tracing vs. SymTA/S Analysis

- Measured 10ms task: Response time 6.9ms
  - 4 CAN, 8 SPI interrupts, 7 preemptions by 1ms task

- SymTA/S Analysis of 10ms task: Worst-case response time 9ms
  - 10 CAN, 8 SPI interrupts, 9 preemptions by 1ms task, blocking

Risk avoided
Example 2: High-Performance ECU

Powertrain domain: Engine Control

- Verifying Performance and Timing for all engine speeds (RPM)
- Avoiding Deadline Overruns (would lead to ECU reset)
- Optimizing ECU performance and cost for different markets

![Graph showing ECU load percentage against engine speed (RPM)]
Detecting "Anomalies"

Additional preemption by RPM-synchronous tasks (increases task interference)

Task cut-off (reduces core execution time)
Example 3: High-Integration ECU (e.g. central body unit)

Typically Dual-Processor / Dual-Core ECUs
- Exploring alternative Hardware/Software architectures
- Integration of functions and communication from multiple sources
- Migration from Prototype to series ECU
Example 4: End-to-End Timing Analysis

Chassis domain: Active Suspension
- Analyzing End-to-end Function Timing
- Detecting Inefficiencies in Implementation
- Integrating 3rd Party Black-Box ECUs and SW Components

chained tasks
under-sampling: signals get lost (last is best)
over-sampling: lastest read is critical (max age)
Focus: End-to-end Timing

- Chained tasks
- Under-sampling: signals get lost (last is best)
- Over-sampling: lastest read is critical (max age)
Example 5: Adding an ECU

New traffic → Need to verify and optimize bus load and timing
Scheduling analysis makes this easy
Two aspects are key
- Message offsets
- Sporadic messages
Static (e.g. Excel®-based) analysis is NOT ENOUGH

- Varying loads must be considered (see below) – in the body domain, most of the load is sporadic!
- Complex and dynamic interdependencies affect end-to-end timing
Message offsets

- Assigning good offset values between messages sent by the same ECU can dramatically lower worst-case message transmission times.
- (It is not possible to assign offsets between messages sent by different ECUs.)
Comparing two Configuration Variants (optional ECUx)

Absolut Response Times for periodic messages only without dynamic load (AR000)

Potential data loss
Sporadic messages

- Since their number / frequency is often not known, it helps tremendously to analyze various what-if scenarios.
System-Level SymTA/S
Use Cases
Automotive Electronics Evolution

- Adding new components to existing architecture
  - Software functions
  - ECUs
  - Subsystems
Automotive Electronics Revolution?

- Novel topology
- Restructuring, higher integration of functions (e.g. small number of powerful domain control units - DCUs)
- Becomes feasible with AUTOSAR and FlexRay
Example 6: Network Extension

**Bus / Network : Gated Network**
- Verifying end-to-end Timing
- Gateway dimensioning
- Optimizing synchronization to reduce end-to-end latency
Focus: End-to-end Timing Analysis

e.g.: Source → ECU1 → CAN → Gateway → FlexRay → ECU2 → Sink
Example 7: from CAN to FlexRay

- **Original System:**
  - CAN, several sync/async ECUs
  - Path Delay: **143ms**

- **First Adaptation:**
  - FlexRay, same sync/async ECU situation as original system
  - Path Delay: **120ms**

- **Second Adaptation:**
  - FlexRay, all ECUs are in sync with FlexRay and to each other
  - Path Delay: **29ms !!!**

⇒ FlexRay alone does not reduce latencies
⇒ good synchronization is a design challenge!
CAN Communication, asynchronous ECUs

- Signal written to RTE
- Frame generated in COM
- Frame available for reading at receiver
- Receiver-side delay
- Bus congestion

Overall delay: 143 ms
Asynchronous ECUs on FlexRay

Faster bus communication (20 instead of 43ms) but still large receiver-side delay (100ms)!
Synchronized ECUs on FlexRay

Significantly reduced **receiver-side** delay possible
but requires good synchronization

29 ms
Scheduling Analysis for ECU, Networks and Systems saves time, money and headaches

Solutions Overview
July 2008
Challenge:
Establishing formal analysis in industry
SYMTA VISION Goals

- **Market leader** for timing analysis and optimization
- **Standard solution** for the complete design-flow
  - Seamless integration in development processes and tool chains
  - Offer best-in-class solutions
- **Achieved by**
  - Selection and customization of work from research community
  - Tight cooperation with strong partners (industry and academia)
- Outstanding services and support
- Global operation & markets (Aerospace, Infotainment, …)
Strategic Activities

- Own industry-relevant research → customization
  - combine most relevant concepts (accuracy, usability)
  - support for layered software architectures (AUTOSAR)
  - end-to-end analysis
- Partnering with tool vendors → best-in-class solutions
  - WCET analysis, tracing, design tools, operating systems, ...
- Partnering with academia → future technologies
  - multi-core, power, dynamic reconfiguration, multi-media, ...
- University program → research, teaching, labs
- Standardization activities → expertise & networking
  - AUTOSAR, FlexRay, ...
Technology Customization
Technical Challenges – Scheduling Analysis

- Right level of accuracy → selection of right analysis technology
  - response time approach with offsets for tasks and frames
  - arbitrary bursts and dynamic load models
  - otherwise: no usable results

- Flexibility of technology
  - OSEK, CAN, FlexRay → customization
  - combinations in networked systems → composition
  - otherwise: limited applicability

- Support for layered automotive software architectures → own research
  - end-to-end & RTE/COM register communication
  - multiplexing
  - otherwise: no broad market
End-to-End Timing Chain in AUTOSAR

- Function View
  - SW-Cs and Signals
- Platform View
  - Tasks and Frames
- Hardware

ECU 1
- SWC 1
- SWC 2
- RTE
- VFB
- BSW
  - I/O
  - OS
  - COM

ECU 2
- SWC 3
- RTE
- BSW
  - OS
- COM

Bus with Frames
Software-Components vs. Tasks - Structure

[Diagram showing the relationship between software components (SWCs) and tasks (Tasks 1, 2, and 3) within an ECU (ECU 1). Diagram includes SWCs 1 and 2, each with runnables A and B, and runnables C, D, and E. Tasks 1, 2, and 3 are connected to SWCs and runnables, illustrating the flow of signals and tasks within the platform view and function view.]
Software-Components vs. Tasks Scheduling

- software components cannot be scheduled
- only tasks can
- needs transformations
Different “Semantics” of End-to-End Timing

- term “end-to-end delay” requires definition
- analyses must distinguish these

- first-through is important for body electronics
- max-age is important for control engineering
Asynchronous ECUs on FlexRay bus

- bad synchronization → bad responsiveness

2 FlexRay cycles (more when using mux)

- clock skew effects → large send & receive signal jitters

„ok window“, given by FlexRay schedule
Partnerships and Interfaces
Industry-driven Research Projects

- **INTEREST** (FP6 STREP)
  - INTEgretion EuROpean Embedded System Tools
  - goal: interoperability of design tools
  - AbsInt, EB, Esterel, ETAS, Evidence, UNIS, TTTech, ...

- **INTERESTED** (FP7 IP) also with
  - Airbus, Artisan, CEA, Magneti Marelli, Siemens, SysGO, Thales,

- **TIMMO** (ITEA 2)
  - TIMing MOdel
  - goal: define TADL (timing language) and methodology for AUTOSAR
  - AUDI, Bosch, CEA List, Conti, Denso, ETAS, Mentor, Siemens, TTTech, Volkswagen, Volvo, ZF + Univ. Chalmers & Paderborn

- **ALL-TIMES** (FP7 STREP)
  - goal: Integrating European Timing Analysis Technology
  - AbsInt, Gliwa, Rapita + Universities of Vienna and Märladalen
INTEREST Automotive network validator
(with ETAS, EB, AbsInt and Esterel)
INTEREST Automotive network validator
(with ETAS, EB, AbsInt and Esterel)
Tool Partnership in ALL-TIMES Project

- **aiT (AbsInt)**: Establishing Formal Scheduling Analysis in Automotive Design Processes

- **debugGURU (Gliwa)**: Tool Partnership

- **SWEET (MDH)**: Instrumentation

- **RapiTime (Rapita)**: Evidence from measurement

- **SATiRE (TU Vienna)**: Sharing of analysis results

- **SymTA/S (Symtavision)**: Automated annotation generation

- **Flowfacts & flowhypotheses**

- **Executable reader**

- **Combination of analysis and measurement**

- **Mutually exclusive execution paths**

- **Comparison of static and measurement-based analysis**

- **Measurement**

- **Flowfacts & flowhypotheses**

- **Automated annotation generation**

- **Activation events**

- **Code execution time**

- **Combination of analysis and measurement**

- **Comparison of static and measurement-based analysis**

- **Measurement**

- **Flowfacts & flowhypotheses**

- **Automated annotation generation**

- **Activation events**

- **Code execution time**

- **Combination of analysis and measurement**

- **Comparison of static and measurement-based analysis**

- **Measurement**

- **Flowfacts & flowhypotheses**

- **Automated annotation generation**

- **Activation events**

- **Code execution time**
SymTA/S and Tracing (traceGURU from Gliwa)

- Single function execution times

<table>
<thead>
<tr>
<th>Process</th>
<th>Task</th>
<th>BCET</th>
<th>WCET</th>
<th>Freq</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proc_001</td>
<td>200ms_Task (2)</td>
<td>1.62</td>
<td>2.16</td>
<td>200</td>
</tr>
<tr>
<td>Proc_002</td>
<td>1000ms_Task (2)</td>
<td>3.08</td>
<td>3.18</td>
<td>1000</td>
</tr>
<tr>
<td>Proc_003</td>
<td>1000ms_Task (2)</td>
<td>3.35</td>
<td>3.36</td>
<td>1000</td>
</tr>
<tr>
<td>Proc_004</td>
<td>TSK_Dynamic (12)</td>
<td>2.78</td>
<td>2.78</td>
<td>9</td>
</tr>
<tr>
<td>Proc_005</td>
<td>TSK_Dyn (16)</td>
<td>4.44</td>
<td>4.20</td>
<td>5</td>
</tr>
</tbody>
</table>

- Interrupt Frequency
Support for the Entire Design Process
SYMTA VISION adds
Performance Design and Verification

- no single technology can cover the entire design process
  → needs selection of best-in-class solutions
- applicability of technology depends on
  - input data availability
  - result relevance for decision making process
  - user confidence in results
Conclusion
Conclusion

- 35 years real-time systems research
  → extensive set of formal approaches, waiting to be applied in industry
- In automotive, timing analysis is becoming a “hot topic”
- Industry demands integrated solutions, no islands

SYMTA VISION

- Goal: Standard solution for the complete design-flow
  - Seamless integration in development processes & tool chains
  - Offer best-in-class solutions
- Strategic orientation
  - Customization and flexibility enabled by compositional approach
  - Tight cooperation with strong partners (industry and academia)
## Program on 09.10.2008

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:30 - 9:00</td>
<td>Registration</td>
</tr>
</tbody>
</table>
| 9:00 - 9:15 | **Welcome**  
Dr. Marek Jensaik, CEO of Symta vision                                  |
| 9:15 - 9:45 | **Einsatz von SymTA/S in der Lenkungsentwicklung bei VW**  
Dieter Brinkema, Volkswagen                                                   |
| 9:45 - 10:15 | **Integrating Timing-Analysis into ECU Software-Development**  
Patrick Frey, ETAS                                                              |
| 10:15 - 10:45 | Coffee break                                                          |
| 10:45 - 11:15 | **Symta vision Engineering - Lessons Learned from various Timing Analysis Projects**  
Ralf Klein, Symta vision                                                            |
| 11:15 - 11:45 | **ALL-TIMES: Combining best Techniques for Different Timing Problems**  
Peter Gliwia, Gliwa GmbH                                                      |
| 11:45 - 12:15 | **The TIMMO Project and Perspectives for Timing in AUTOSAR R4.0**  
Stefan Kunzis, Continental                                                    |
| 12:15 - 14:00 | Lunch break                                                           |
| 14:00 - 14:30 | **SymTA/S Release 1.4 and beyond**  
Dr. Kai Richter, CTO of Symta vision                                          |
| 14:30 - 15:00 | **Using Timing Analysis for Evaluating Networks in an Early Design Phase of Automotive E/E-Architectures**  
Matthias Treib, Daimler                                                        |
| 15:00 - 15:30 | **Reliability and Cost-Optimization: Analysis of Networks and Multicore-Communication**  
Prof. Dr. Rolf Emerl, TU-Braunschweig                                         |
| 15:30 - 15:45 | Closing address  
Dr. Marek Jensaik                                                            |

## Exhibits on 8./9.10.2008

- AbsInt
- aquitos
- ETAS
- GIWA
- RAPITA

**2nd SymTA/S NewsConference**

8./9.10.2008

Braunschweig-Riddagshausen