ARTIST2 Summer School 2008 in Europe
Autrans (near Grenoble), France
September 8-12, 2008

Establishing Formal Scheduling Analysis in Automotive Design Processes

Lecturer : Kai Richter
CTO
Symtavision GmbH, Germany

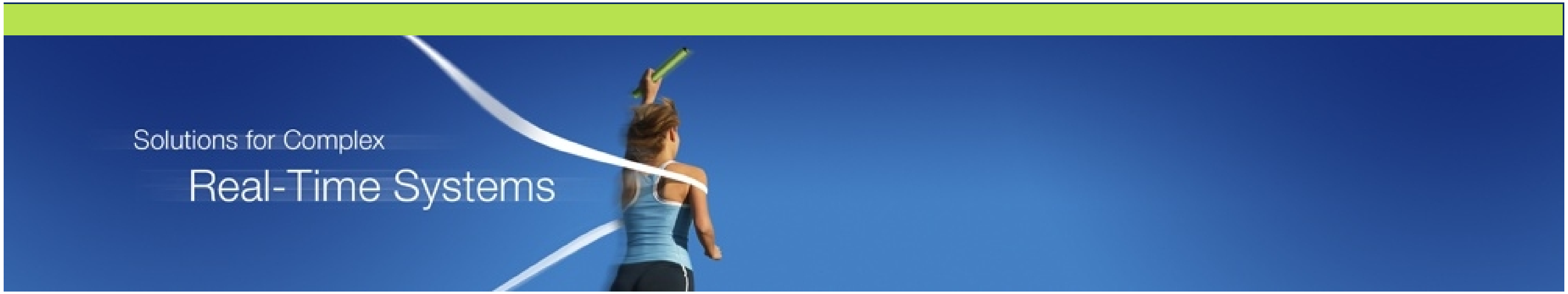
Outline

- 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

SYMTA VISION

Scheduling Analysis for ECUs, 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

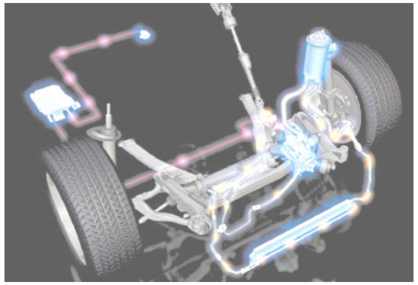
Expertise

- Real-time system design and integration
- Timing verification and performance optimization for
  - ECUs
  - 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 …

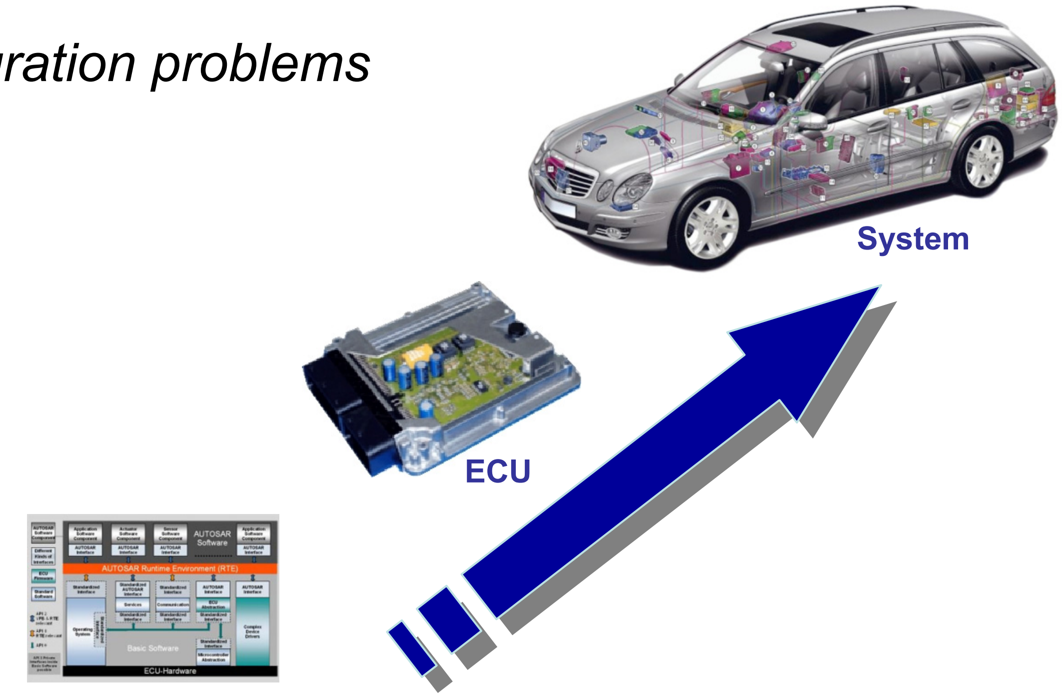


Quelle: BMW

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

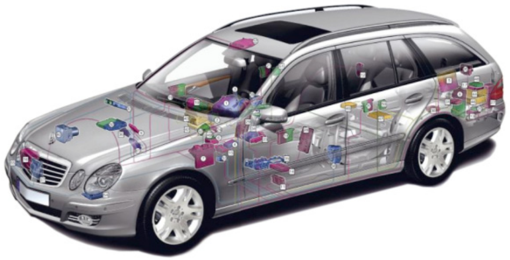
- **Full focus on timing / performance**
- **Reliable and fast timing-analysis tools**
- **Unique, complete system view**
- **From 1st design to final verification**

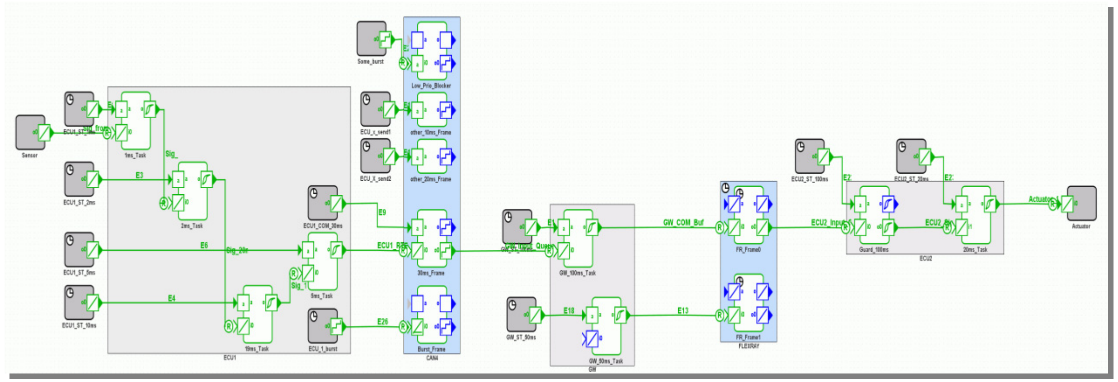
- **Best integration**
- **Highest expertise in the market**
  - confirmed by our customers and partners

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

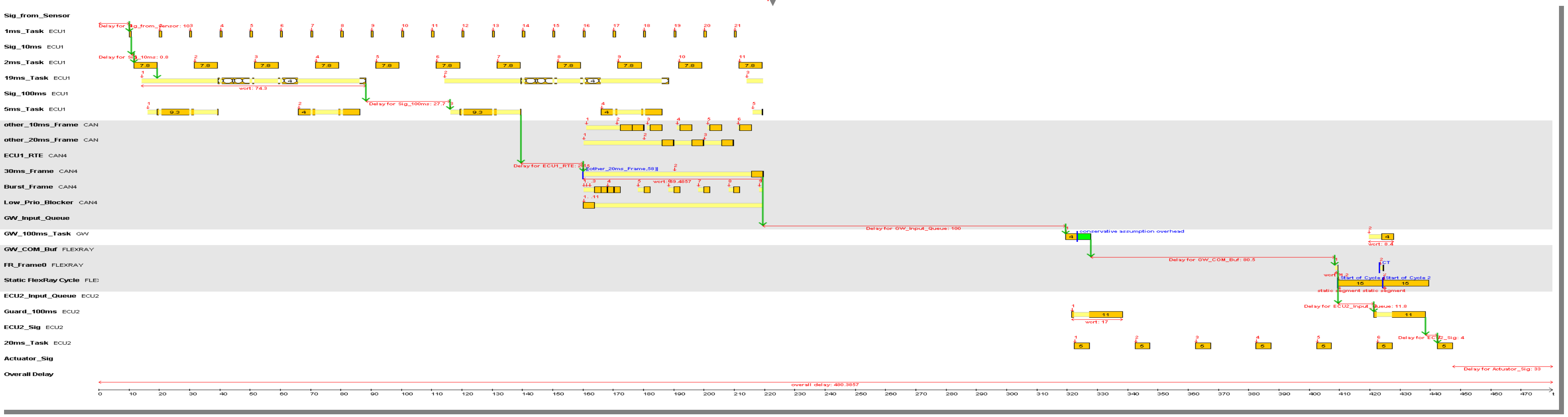
SymTA/S: Symbolic Timing Analysis for Systems





Input: System model

Output: - Verified timing
- Optimized system

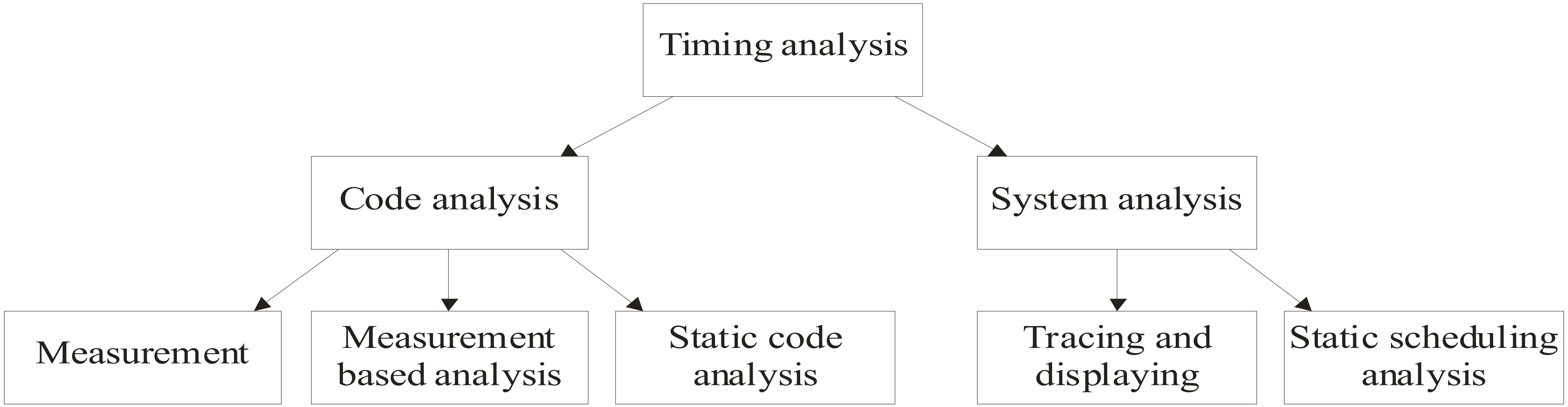


Customers, Partners, Networks

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

- Product-, engineering- and sales-partners
- Networks

ALL-TIMES Timing Analysis Partnership



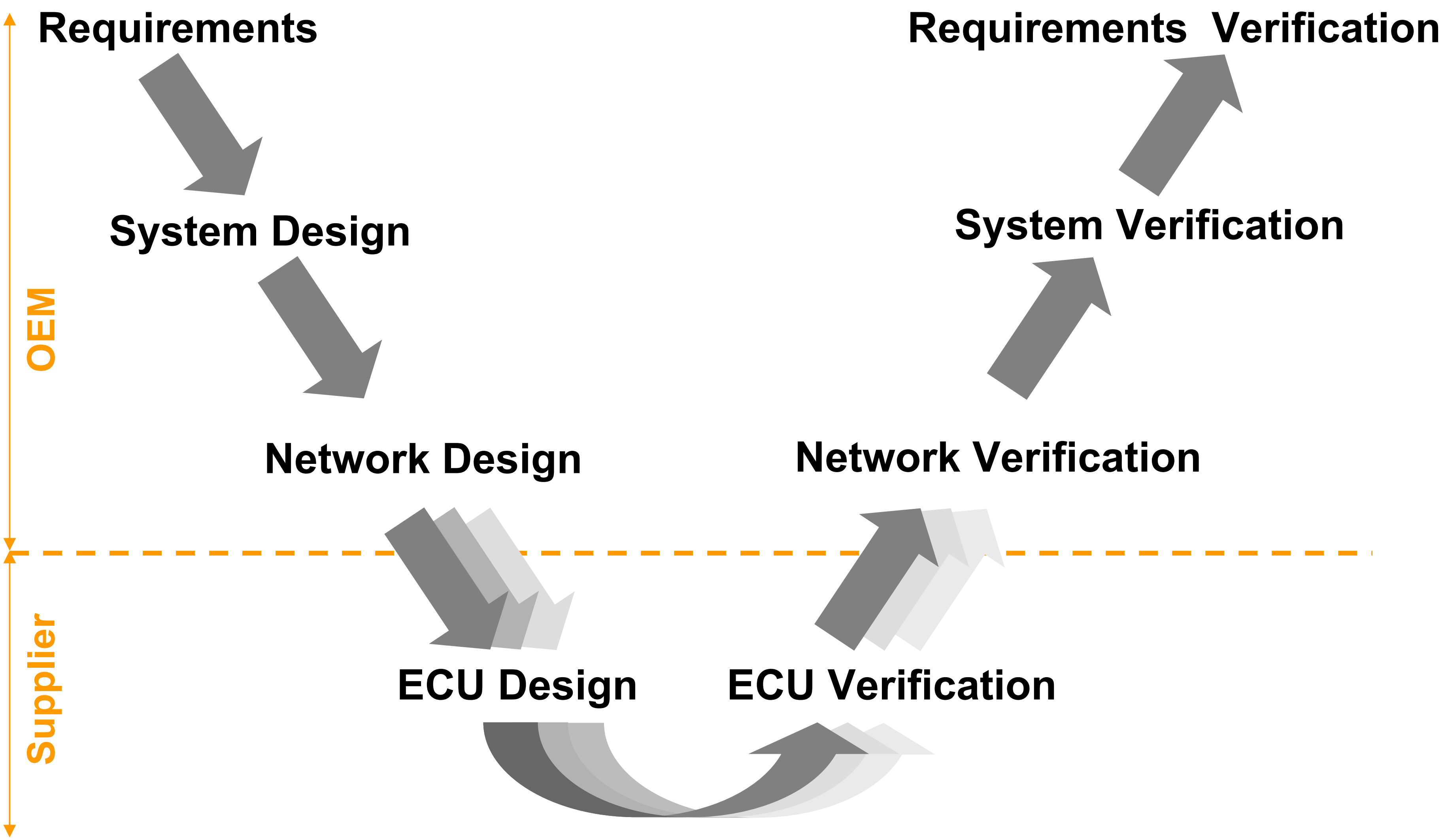
Work in Progress:

Work in Progress:

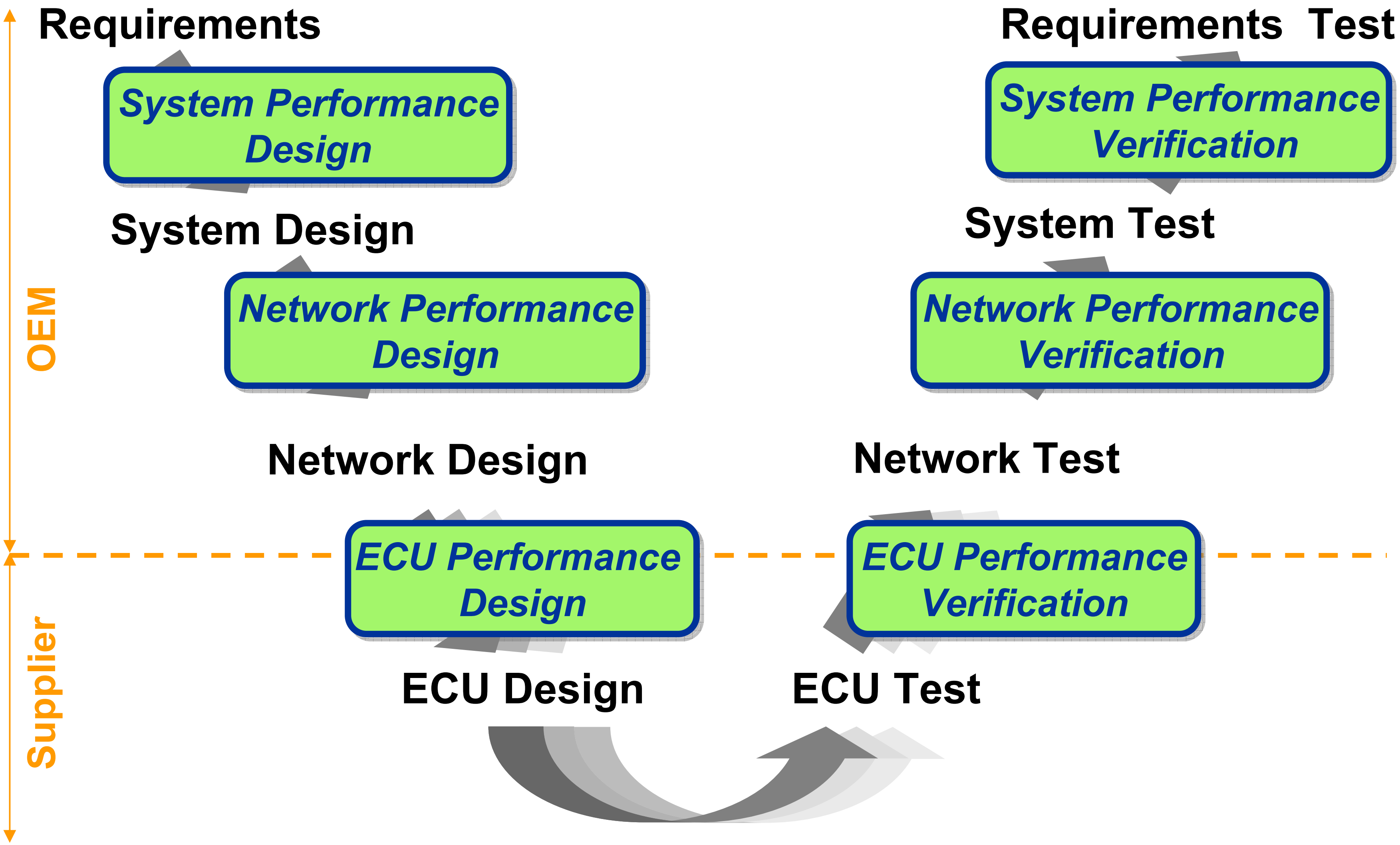
SYMTA VISION Goals

- **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

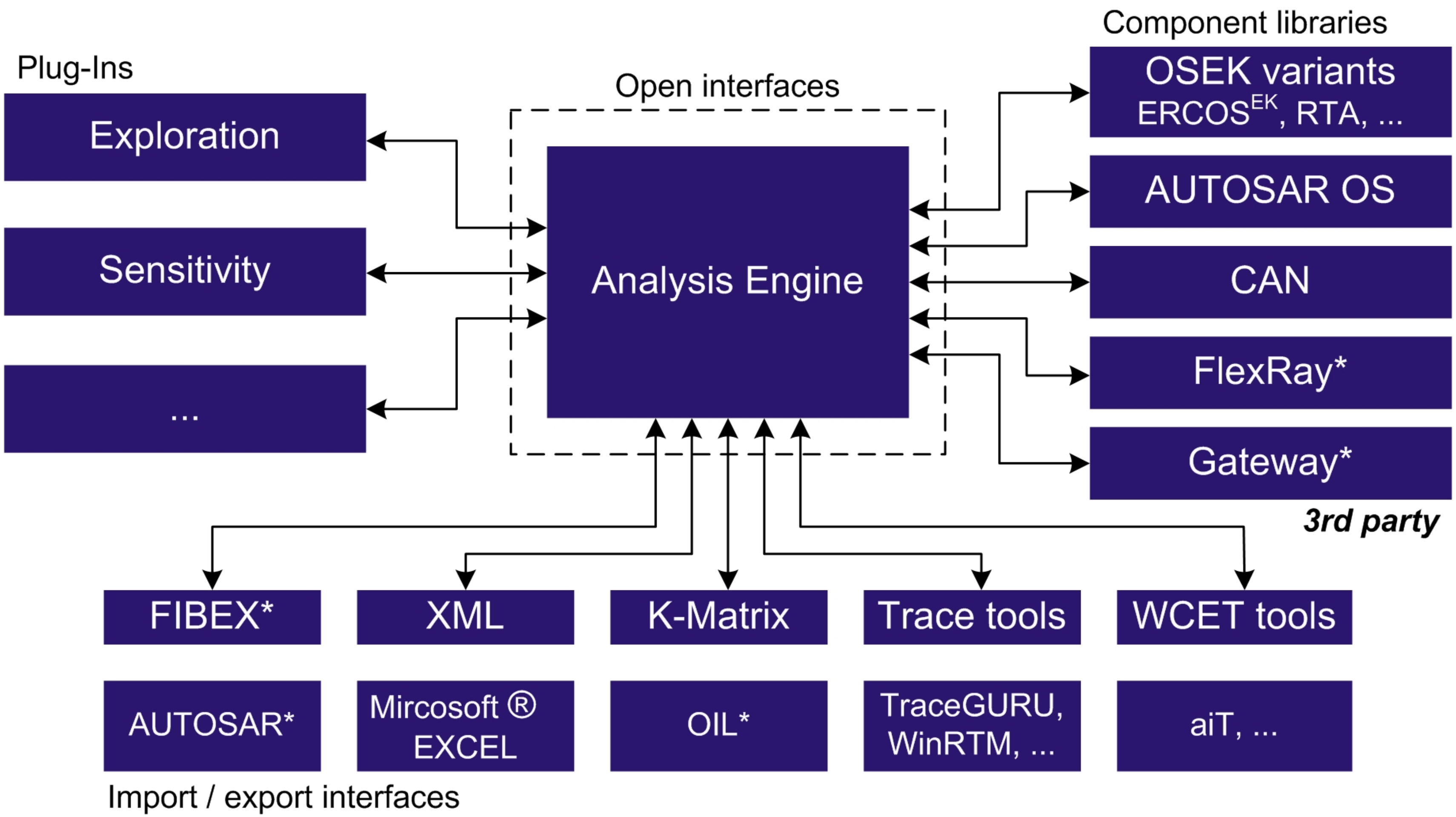


SYMTA VISION adds Performance Design and Verification



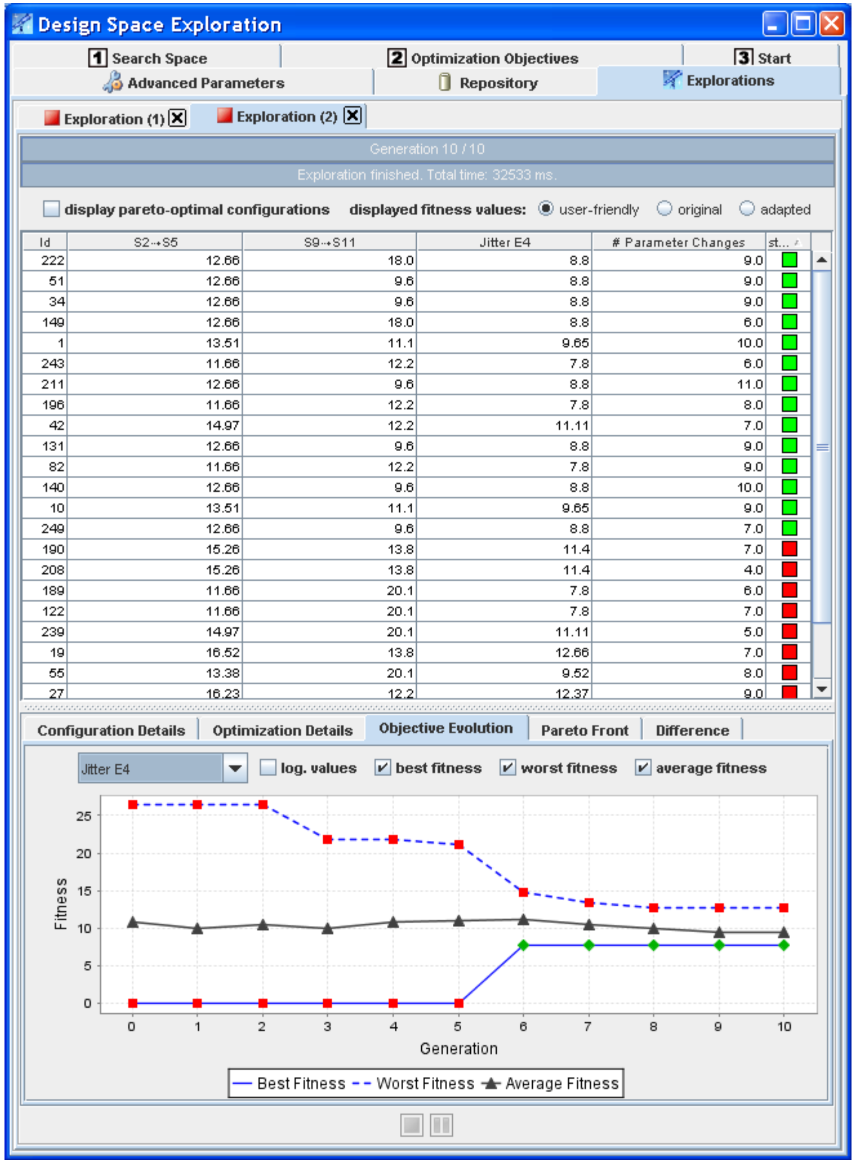
SymTA/S Tool Suite

Symbolic Timing Analysis for Systems



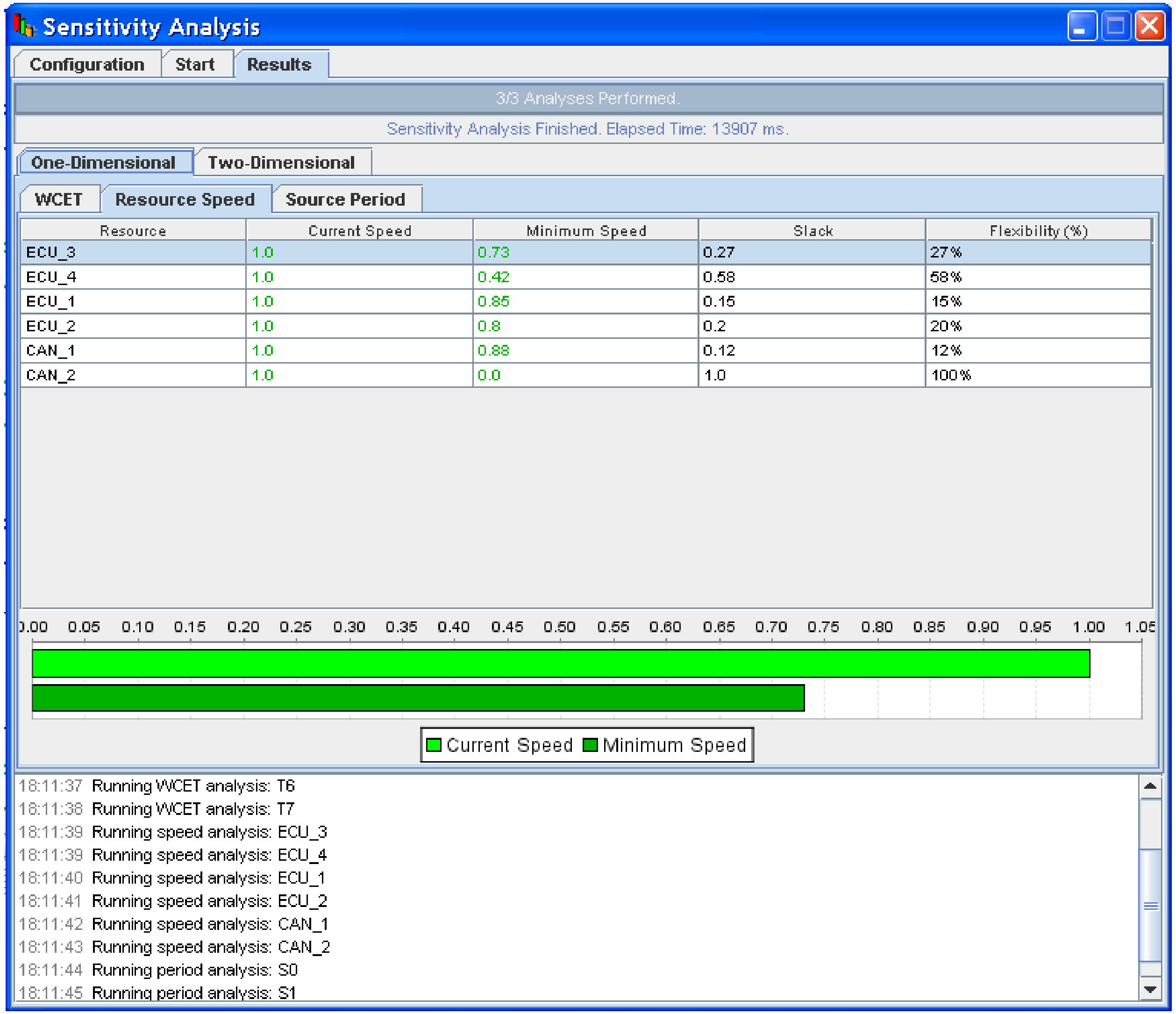
* = work in progress

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

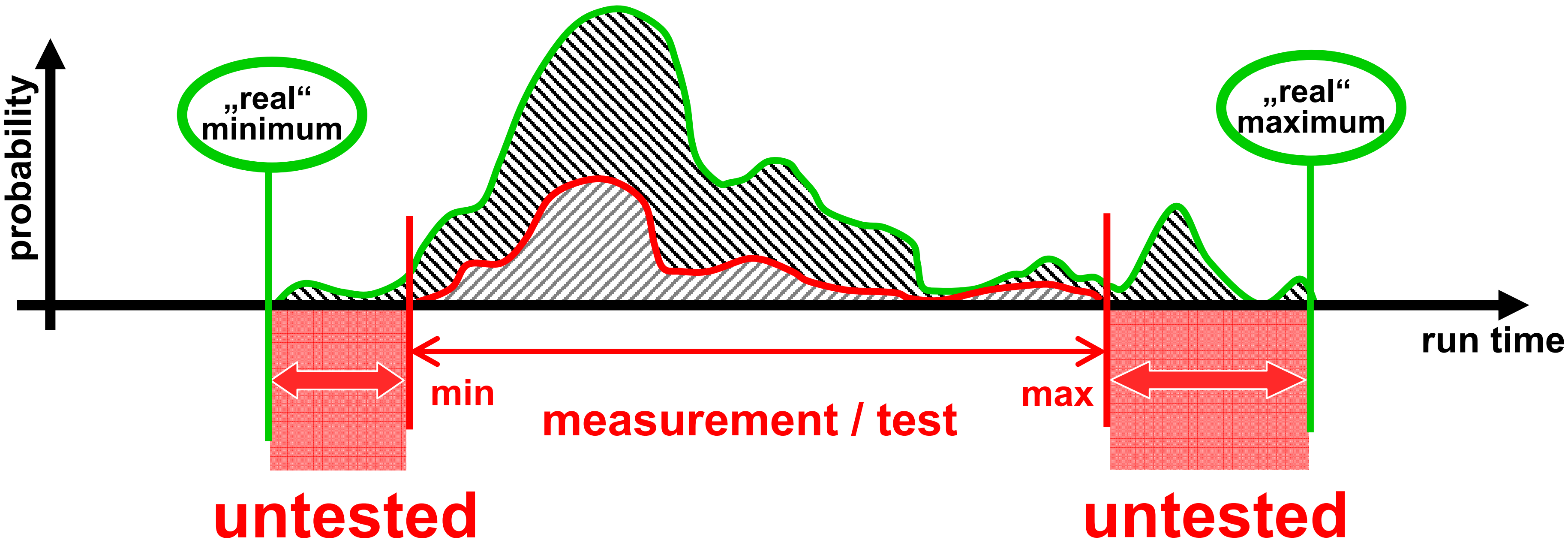
  of current implementation

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 reliabily cover all corner cases
- coverage decreases with increasing complexity (integration)
- **certain applications require more reliable analysis**

➔ **scheduling analysis ➔** SYMTA/S

Skip theory

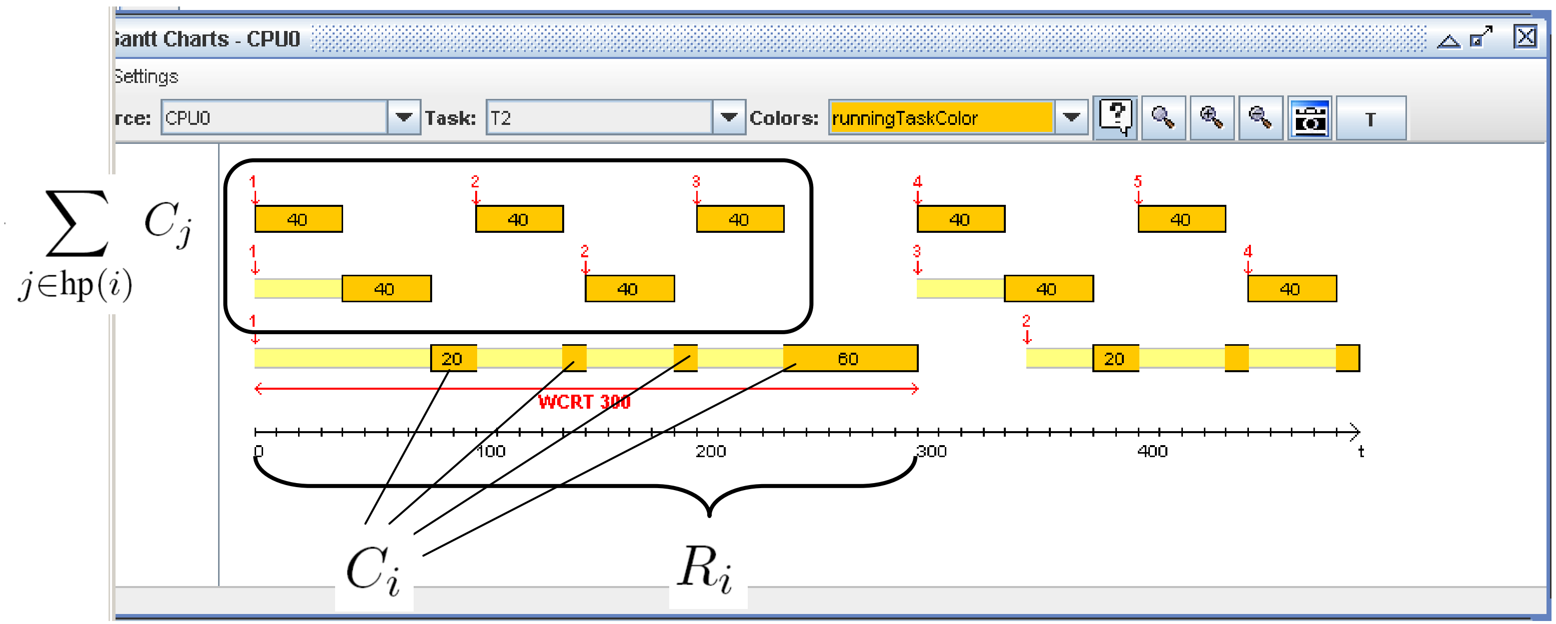
RMS Theory – The response time formula

fix-point problem

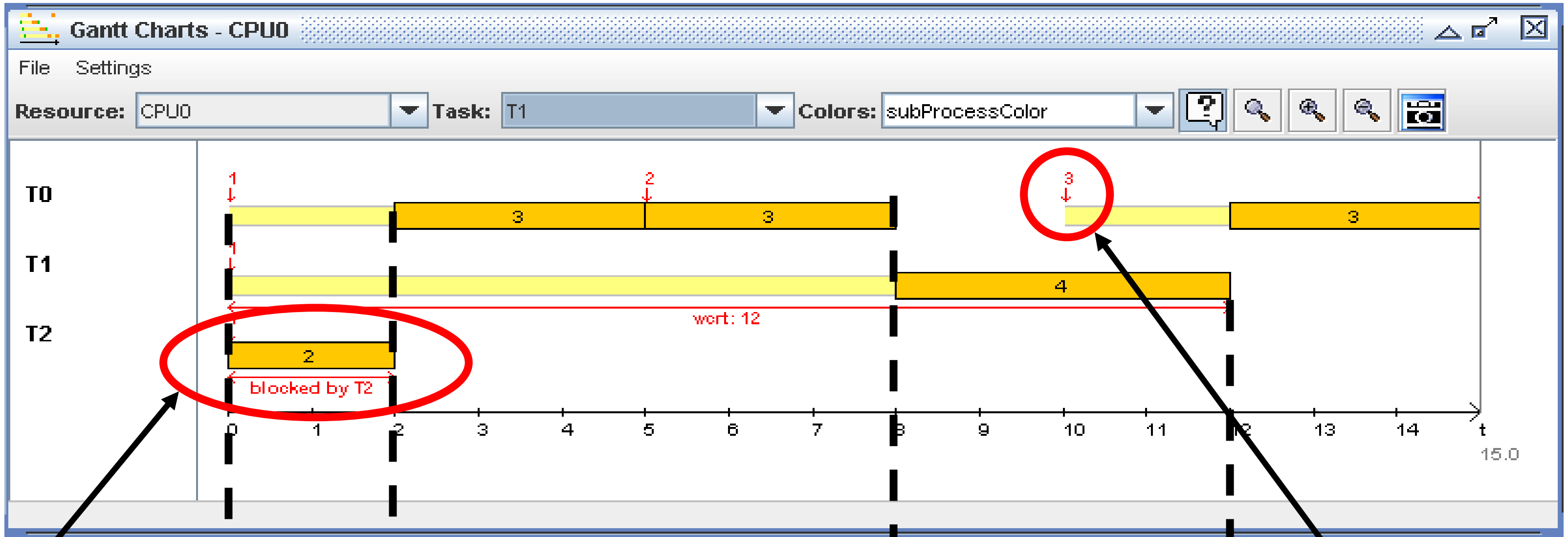
$$R_i = C_i + \underbrace{\sum_{j \in \mathrm{hp}(i)} C_j \underbrace{\left\lceil \frac{R_i}{T_j} \right\rceil}_{\#\text{ of preemptions}}}_{\text{interference term } I_i} \leq D_i = T_i$$

response time

core execution time



Non-Preemptive Blocking



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

$$\underbrace{\underbrace{B_i \sum_{j \in hp(i)} C_j \left\lceil \frac{I_i}{T_j} \right\rceil}_{I_i} \quad C_i}_{R_i}$$

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

SYMTA VISION

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*

$$R_i = C_i + \sum_{j \in \mathrm{hp}(i)} C_j \underbrace{\left\lceil \frac{R_i}{T_j} \right\rceil}_{\#\ \text{of preemptions}}$$

scheduling strategy:

- non-preemption
- deferred preemption
- other strategies

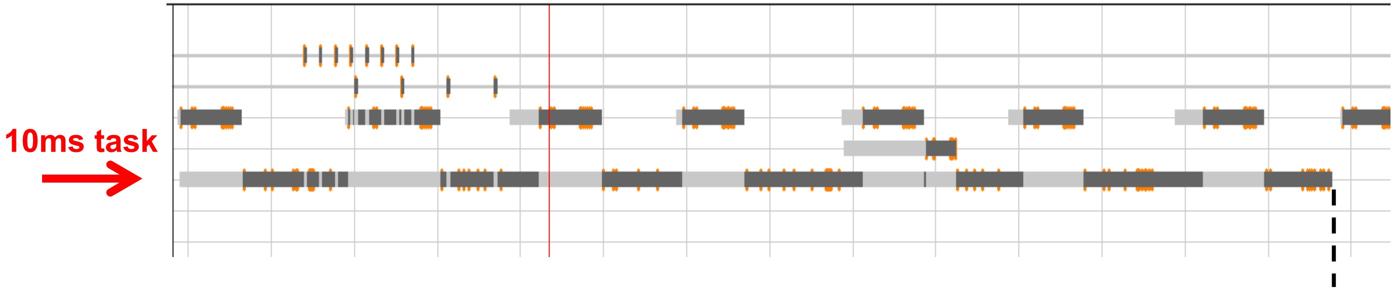
➔ modular combination of features

➔ configurable accuracy / efficiency

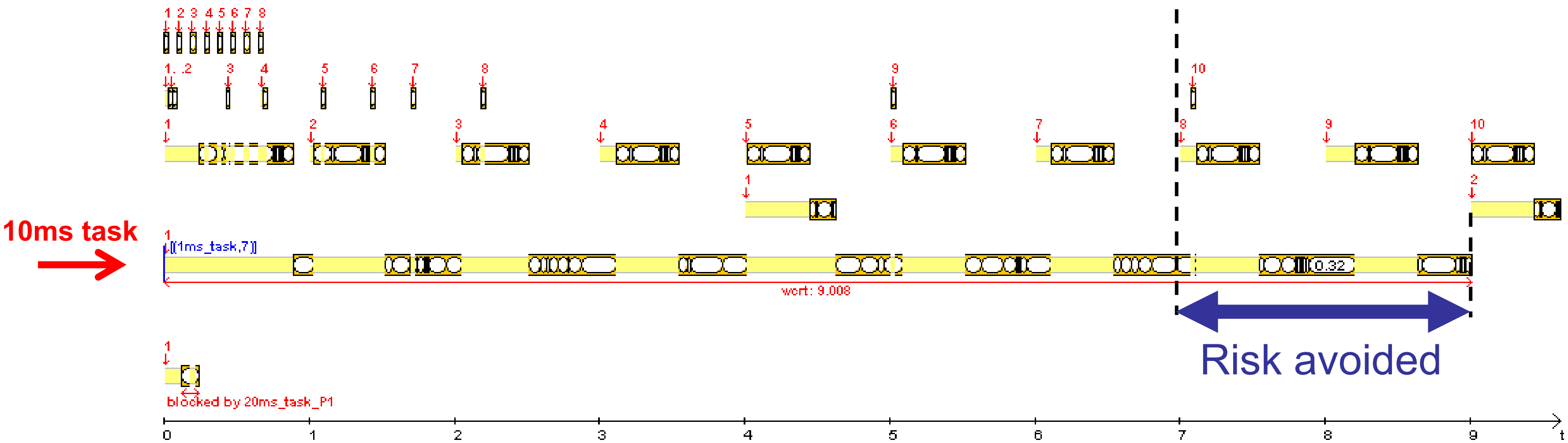
➔ flexible input data

Focus: Tracing vs. SymTA/S Analysis

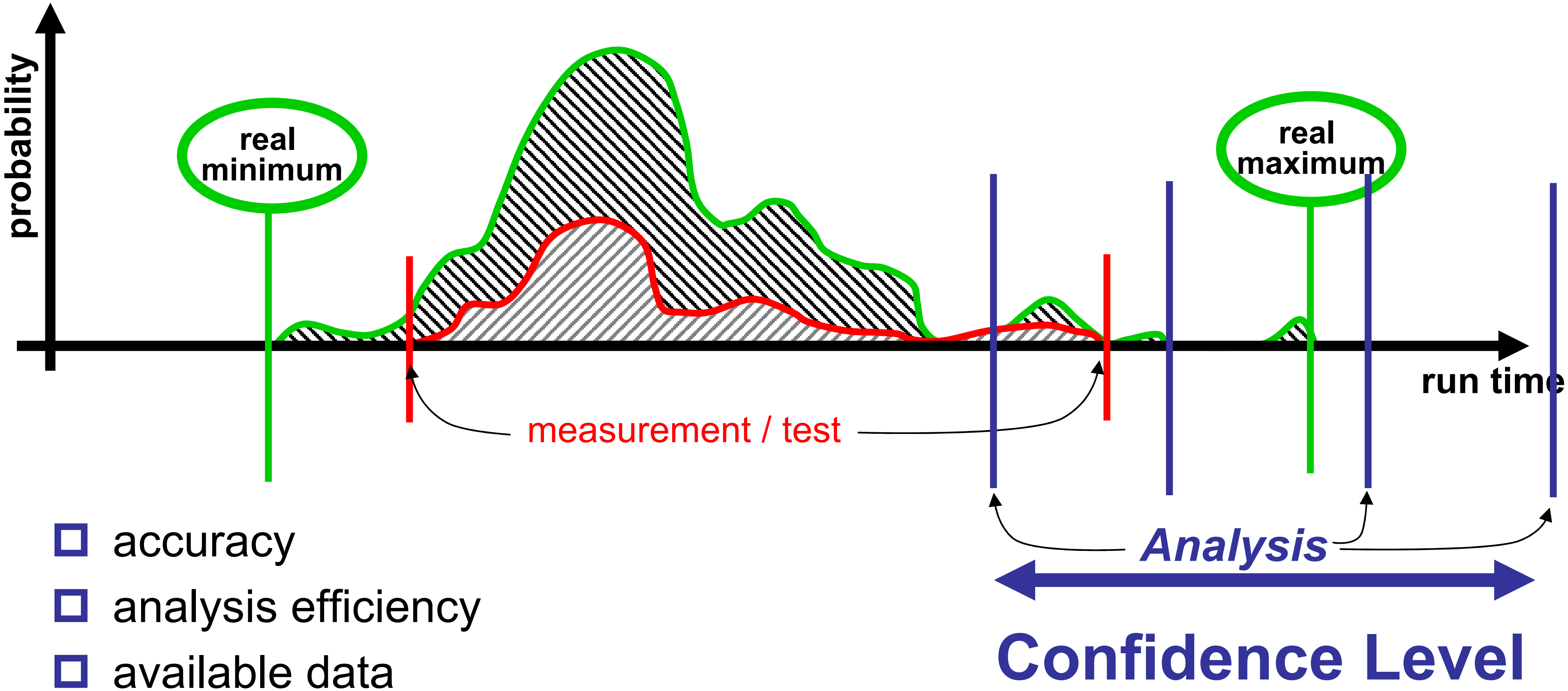
- Measured 10ms task: Response time 6,9ms
  - 4 CAN, 8 SPI interrupts, 7 preemptions by 1ms task



- 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

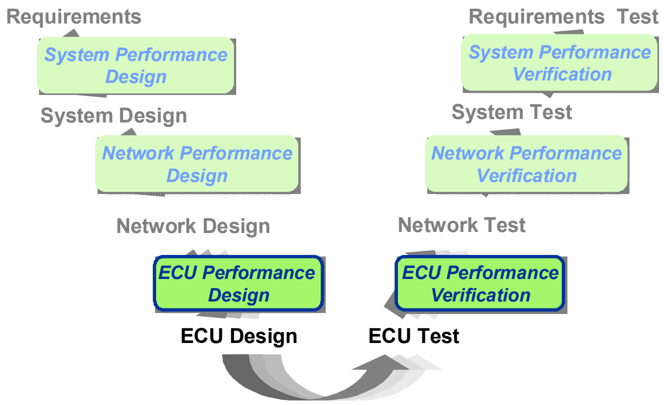
ECU-level and network-level

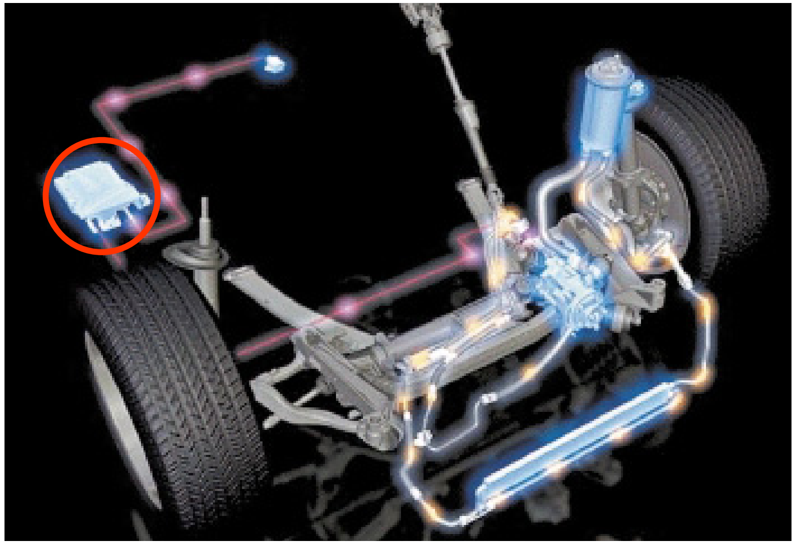
SymTA/S Use Cases

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)





Source: BMW

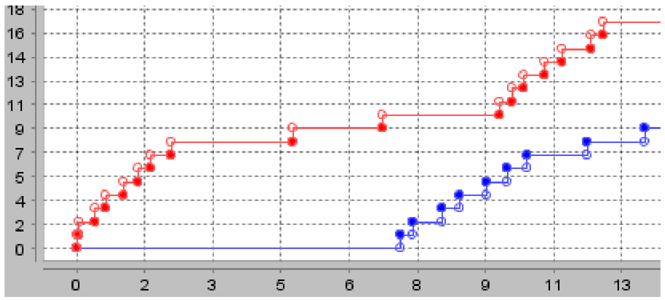
Hans Sarnowski, responsible BMW Engineer: „You really get to know your system and can detect real-time errors in a fraction of time“

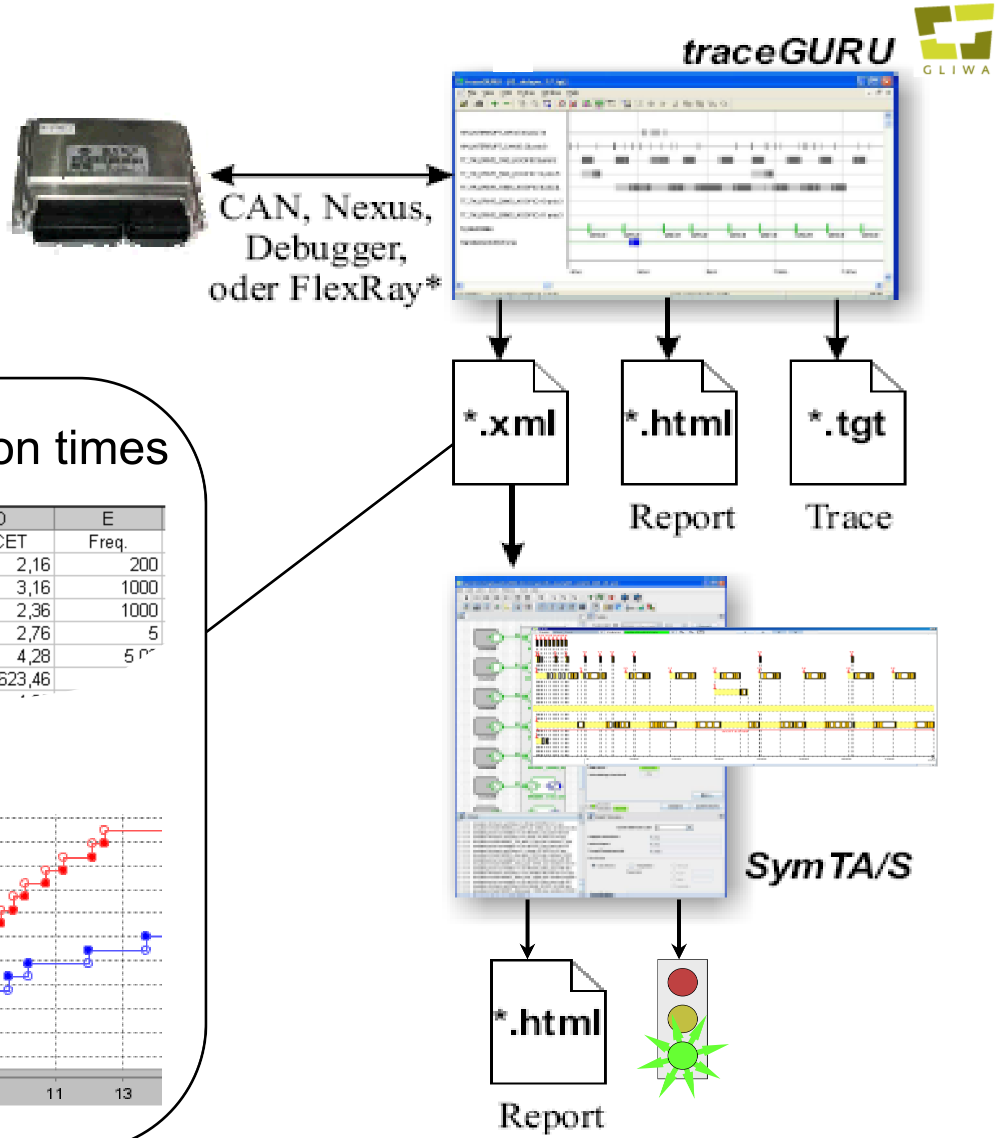
Integration: Tracing + SymTA/S

– Single function execution times

	A	B	C	D	E
1	Process	Task	BCET	WCET	Freq.
2	Proc_001	200ms_Task (3)	1,62	2,16	200
3	Proc_002	1000ms_Task (2)	3,08	3,16	1000
4	Proc_003	1000ms_Task (2)	2,36	2,36	1000
5	Proc_004	TSK_Dynamic (12)	2,76	2,76	5
[illegible]	[illegible] 005	TSK_Dy[illegible]	3,44	4,28	5[illegible]
[illegible]	[illegible]	TS[illegible]	[illegible]43,7	623,46	[illegible]

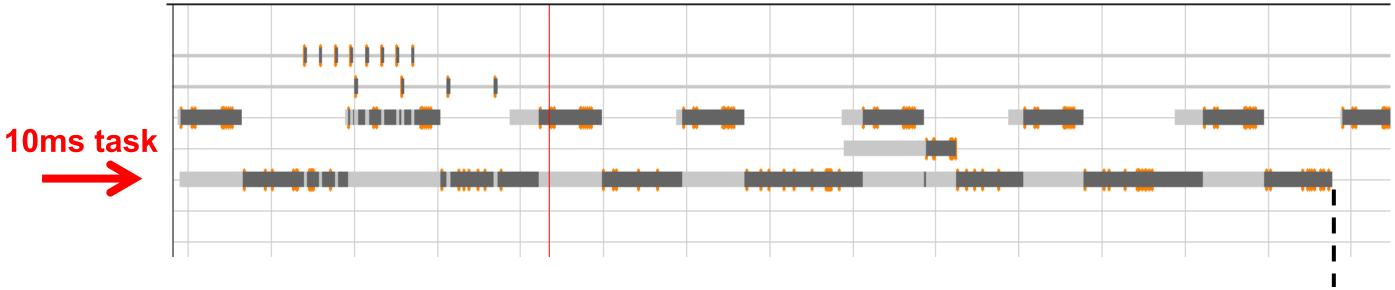
– Interrupt Frequency



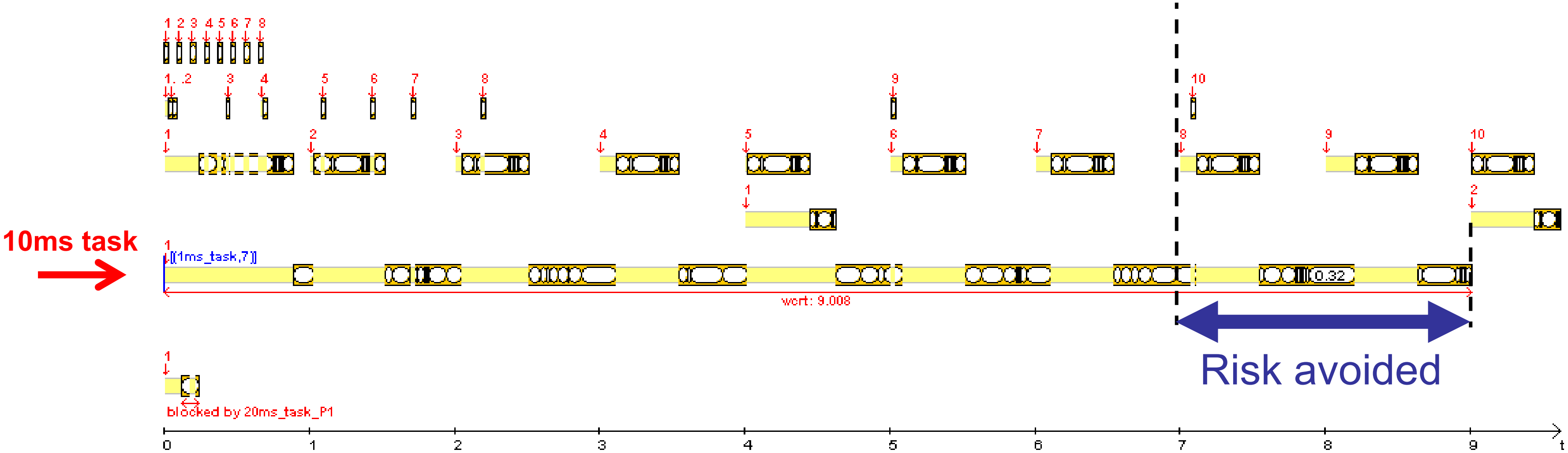


Focus: Tracing vs. SymTA/S Analysis

- Measured 10ms task: Response time 6,9ms
  - 4 CAN, 8 SPI interrupts, 7 preemptions by 1ms task



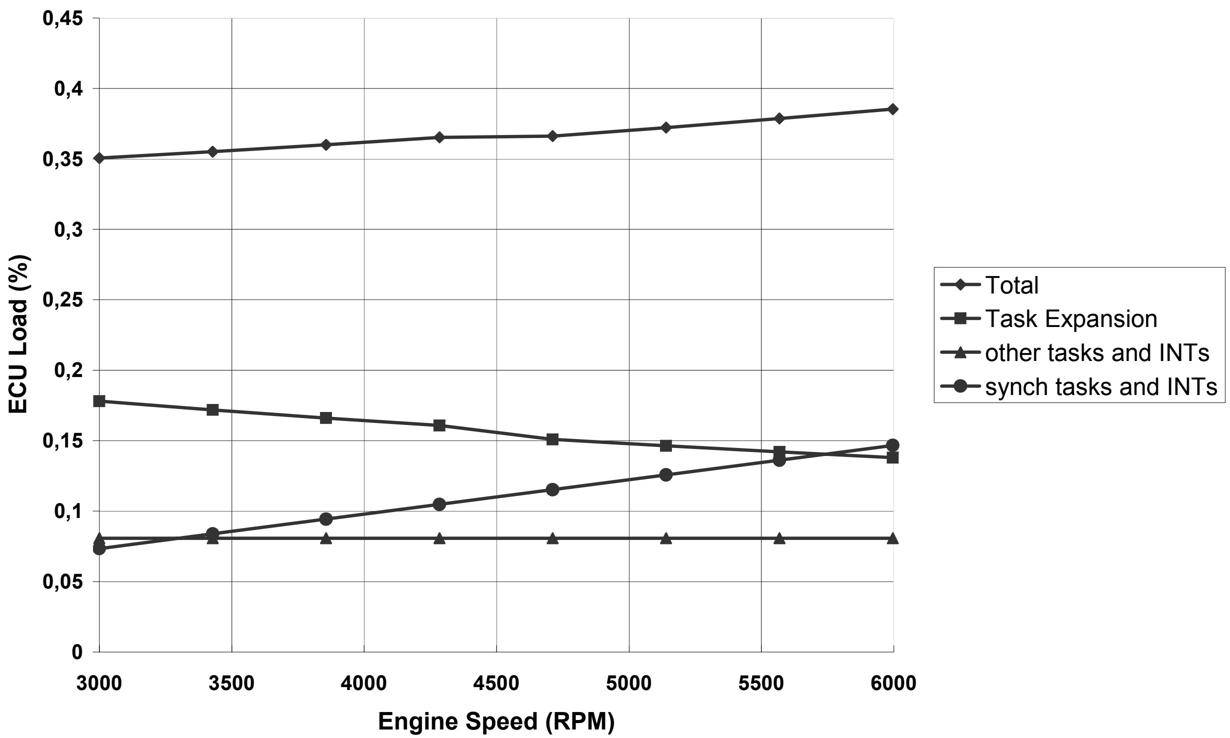
- SymTA/S Analysis of 10ms task: Worst-case response time 9ms
  - 10 CAN, 8 SPI interrupts, 9 preemptions by 1ms task, blocking



Example 2: High-Performance ECU

Powertrain domain: Engine Control

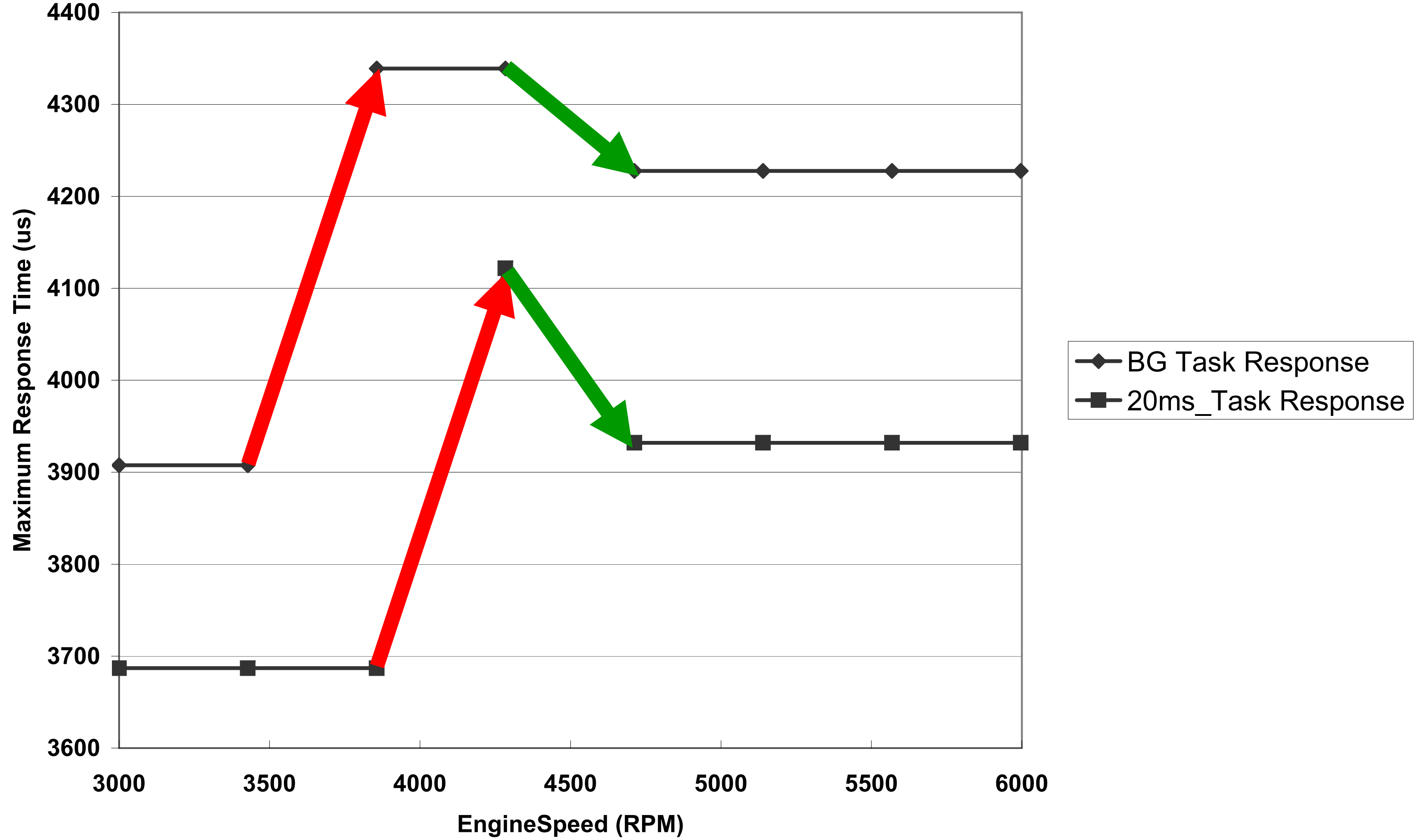
- Verifying Performance and Timing for all engine speeds (RPM)
- Avoiding Deadline Overruns (would lead to ECU reset)
- Optimizing ECU performance and cost for different markets



Detecting "Anomalies"

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

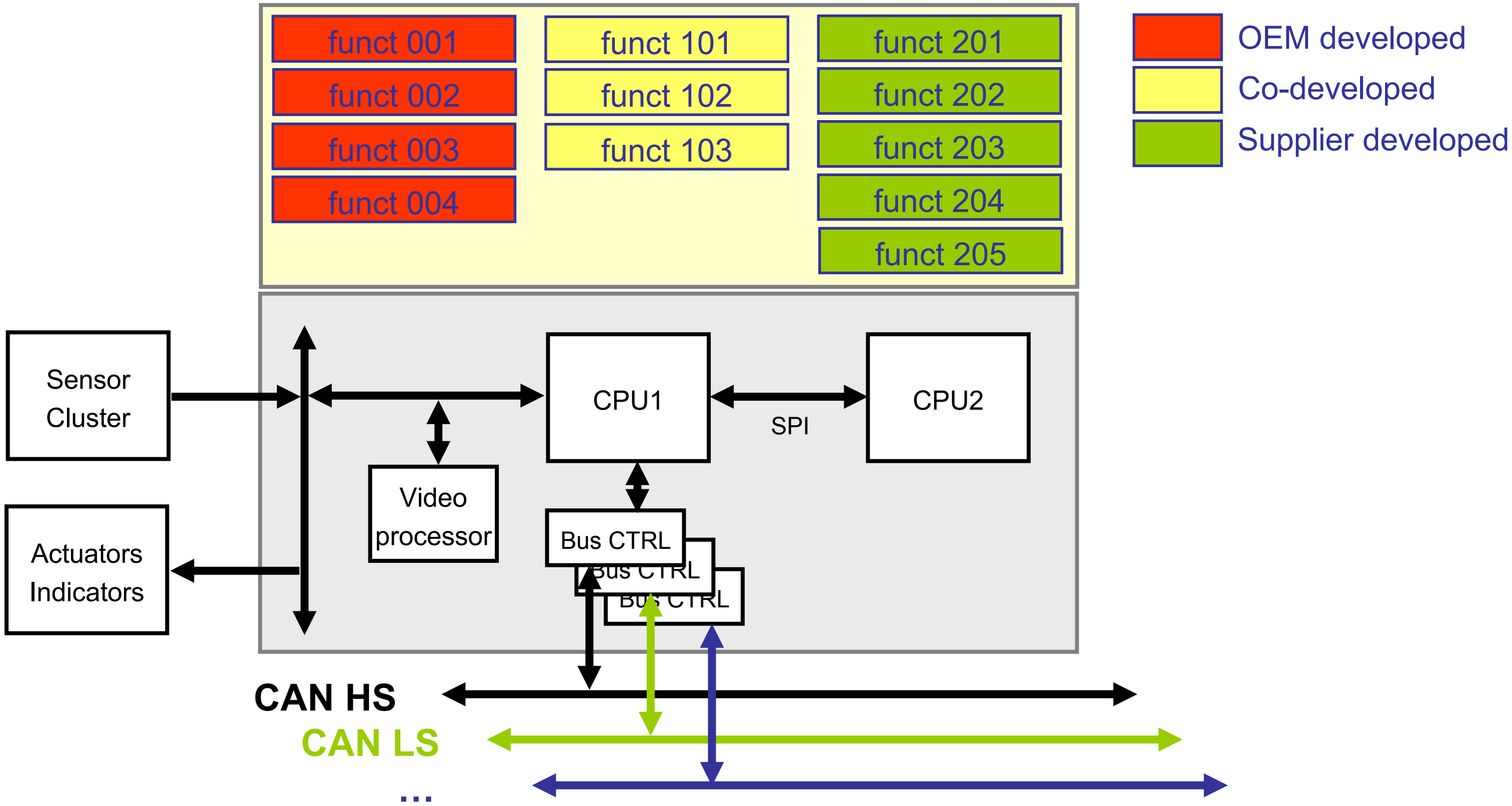
Task cut-off (reduces core execution time)



Example 3: High-Integration ECU (e.g. central body unit)

Typically Dual-Processor / Dual-Core ECUs

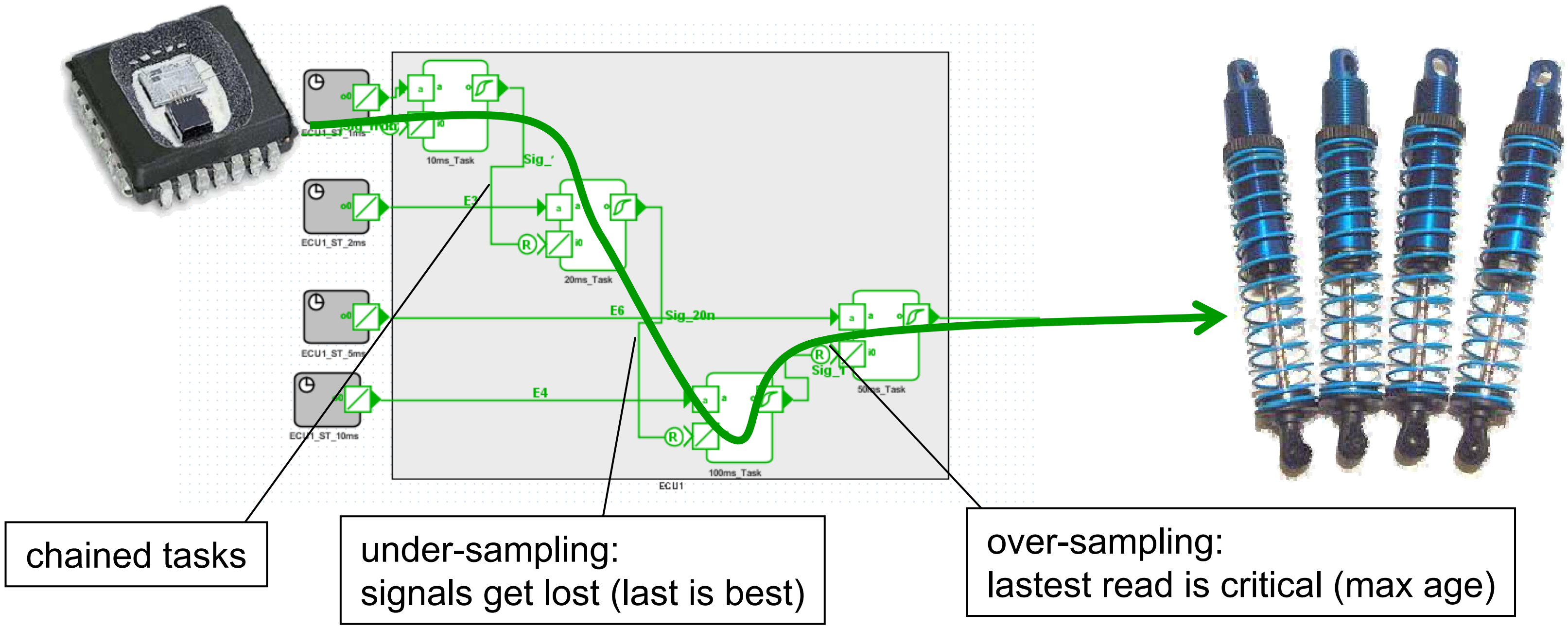
- Exploring alternative Hardware/Software architectures
- Integration of functions and communication from multiple sources
- Migration from Prototype to series ECU



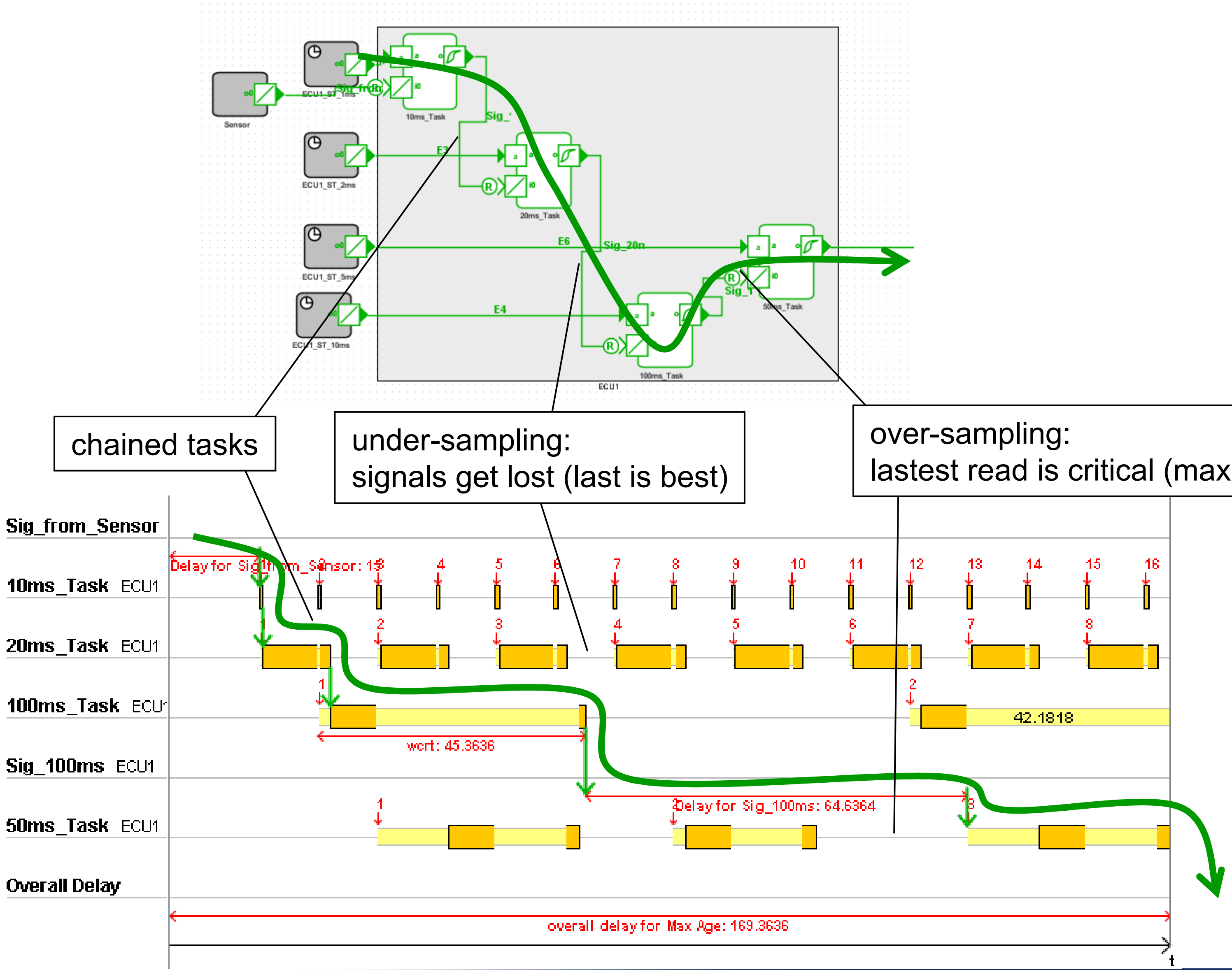
Example 4: End-to-End Timing Analysis

Chassis domain: Active Suspension

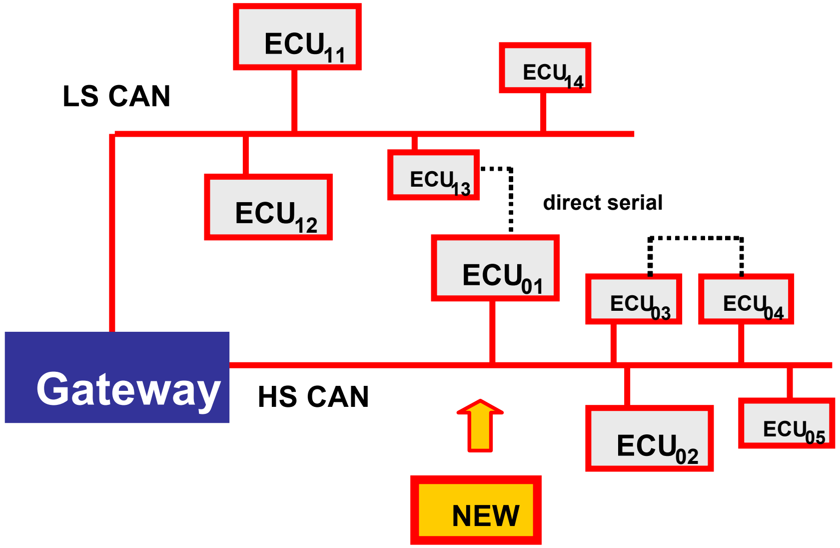
- Analyzing End-to-end Function Timing
- Detecting Inefficiencies in Implementation
- Integrating 3rd Party Black-Box ECUs and SW Components



Focus: End-to-end Timing



Example 5: Adding an ECU



New traffic → Need to verify and optimize bus load and timing

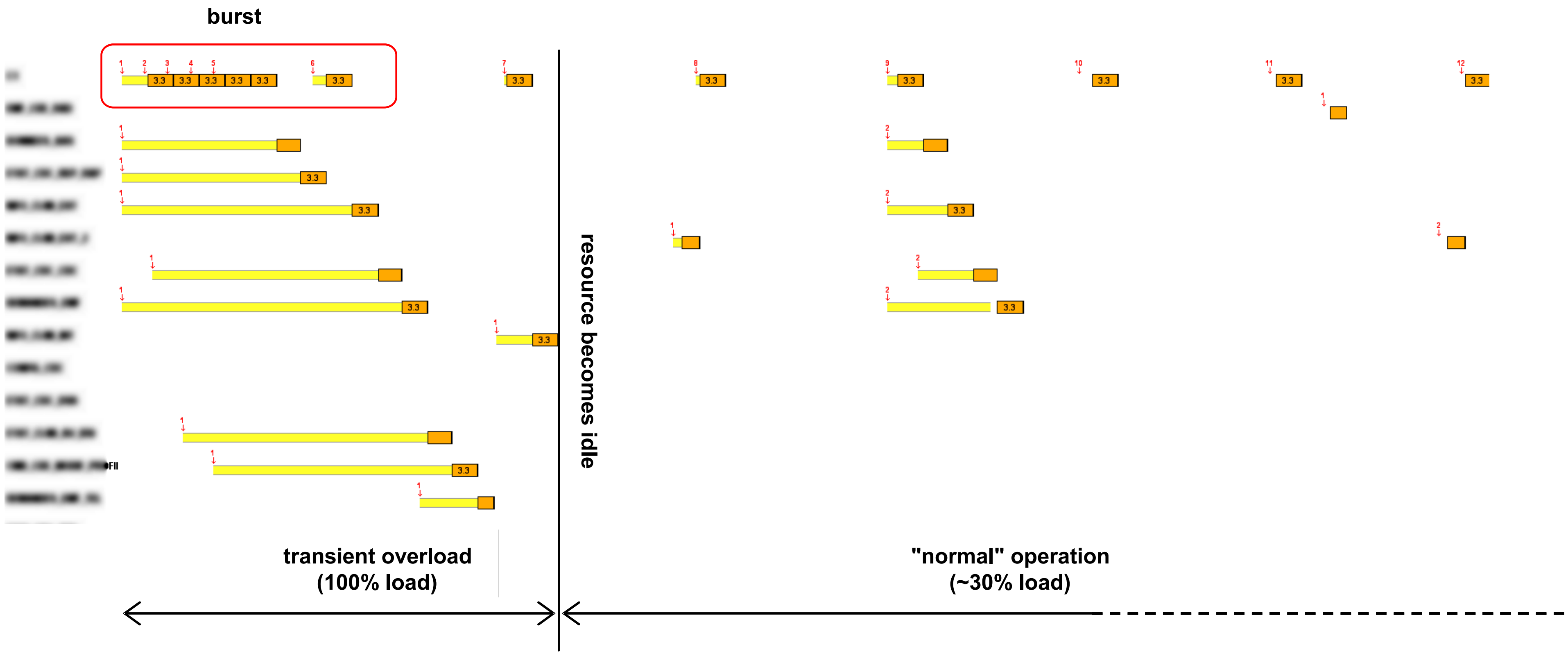
Scheduling analysis makes this easy

Two aspects are key

- Message offsets
- Sporadic messages

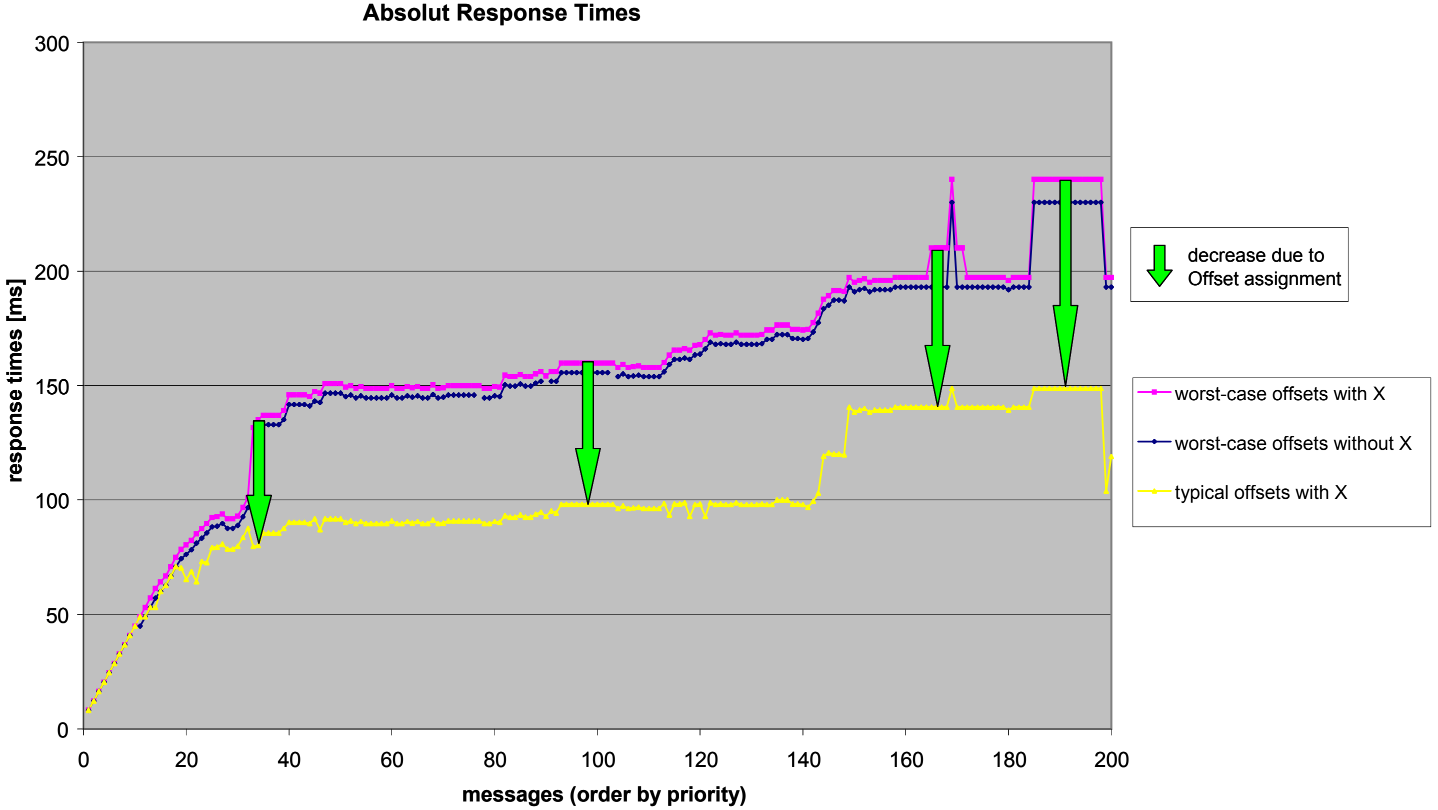
Static (e.g. Excel®-based) analysis is NOT ENOUGH

- 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

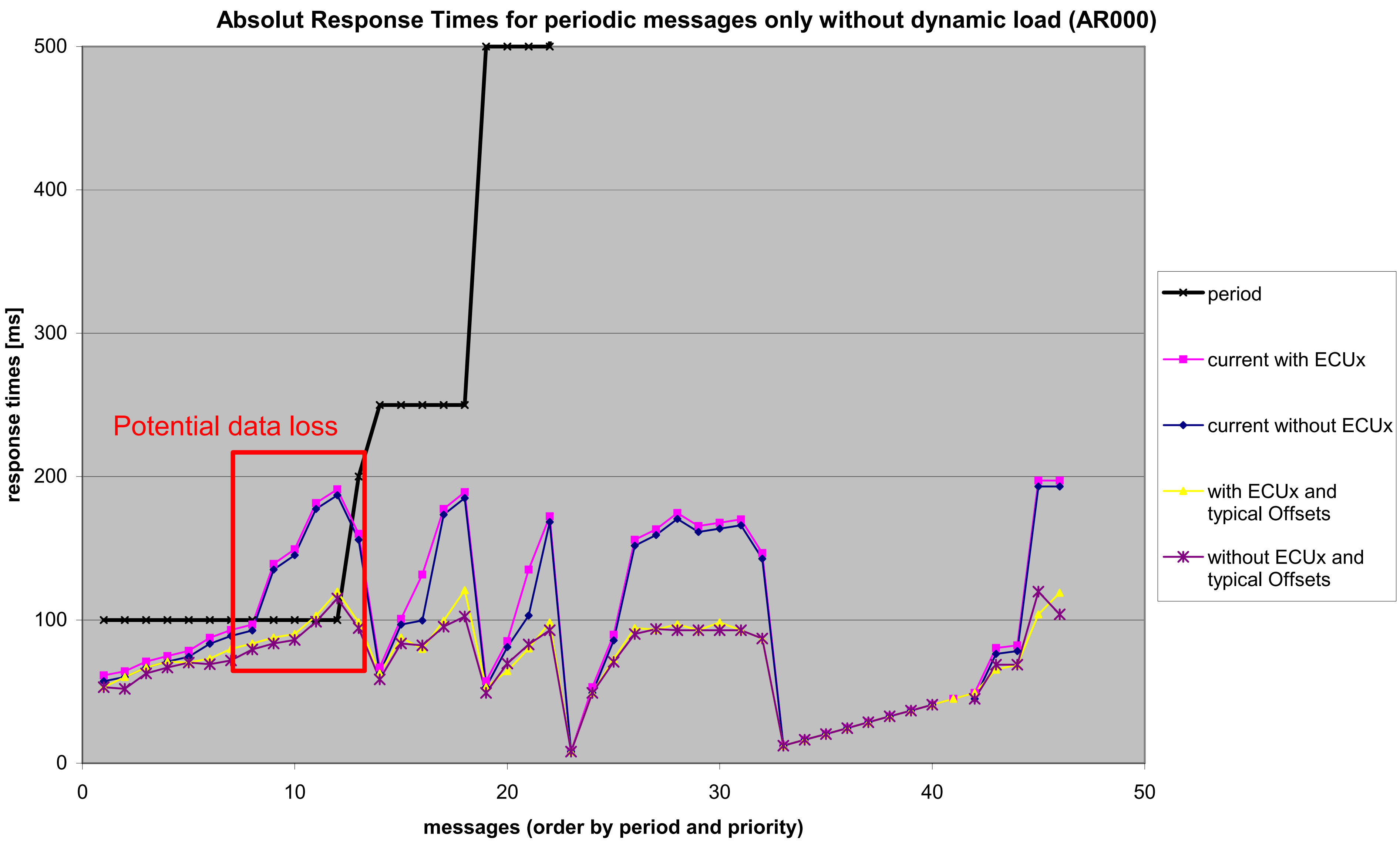


Message offsets

- 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 message sent by *different* ECUs)

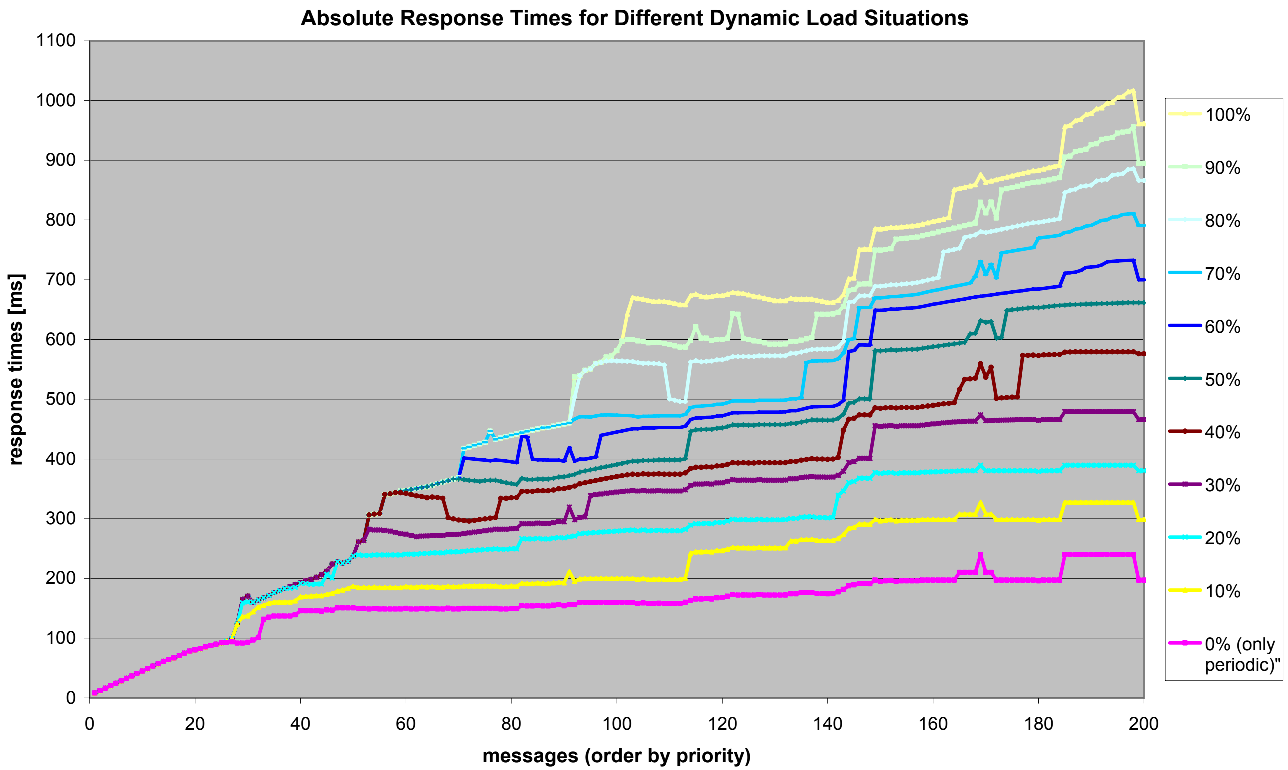


Comparing two Configuration Variants (optional ECUx)



Sporadic messages

- Since their number / frequency is often not known, it helps tremendously to analyze various what-if scenarios

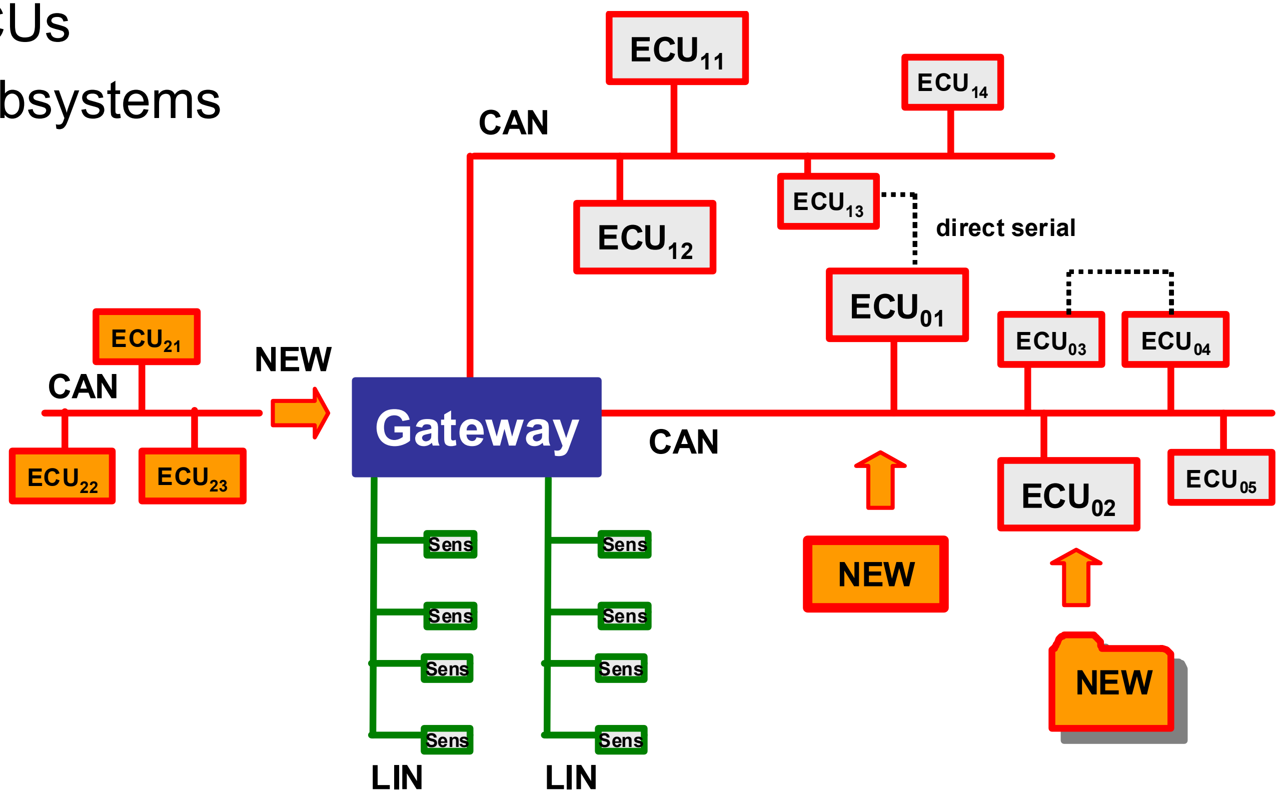


System-Level SymTA/S

Use Cases

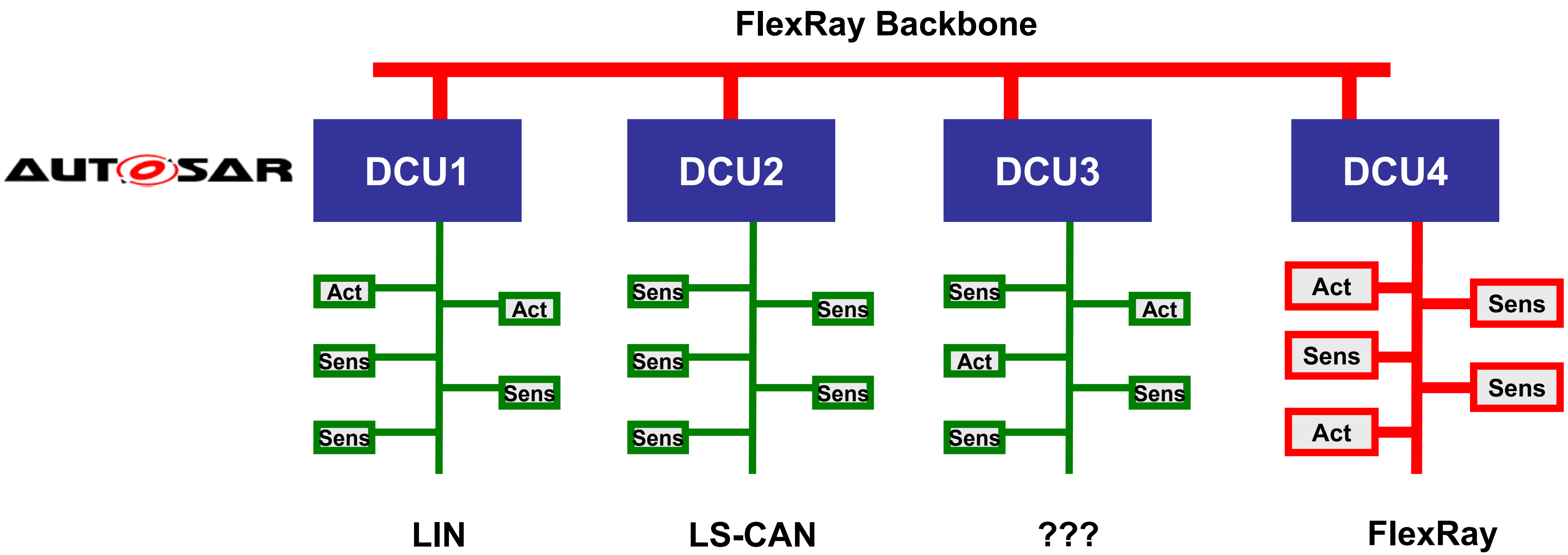
Automotive Electronics Evolution

- Adding new components to existing architecture
  - Software functions
  - ECUs
  - Subsystems



Automotive Electronics Revolution?

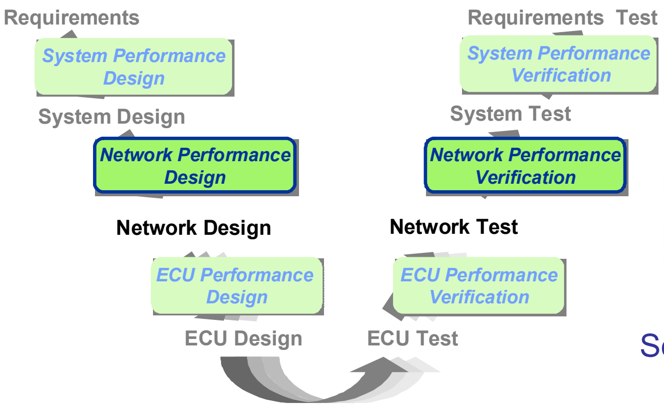
- Novel topology
- Restructuring, higher integration of functions
  (e.g. small number of powerful *domain control units - DCUs)*
- Becomes feasible with AUTOSAR and FlexRay

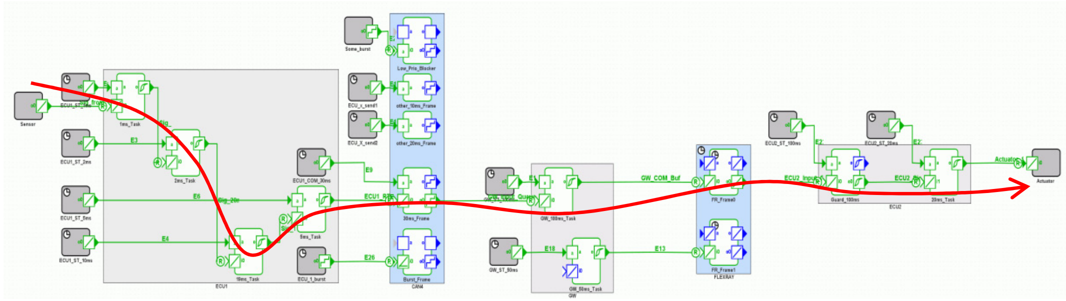


Example 6: Network Extension

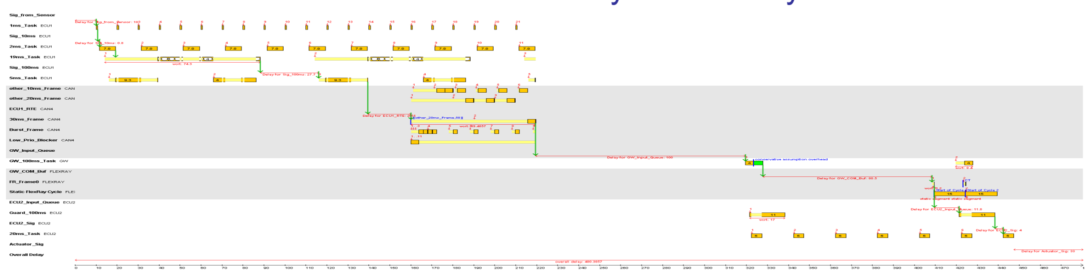
Bus / Network : Gated Network

- Verifying end-to-end Timing
- Gateway dimensioning
- Optimizing synchronization to reduce end-to-end latency



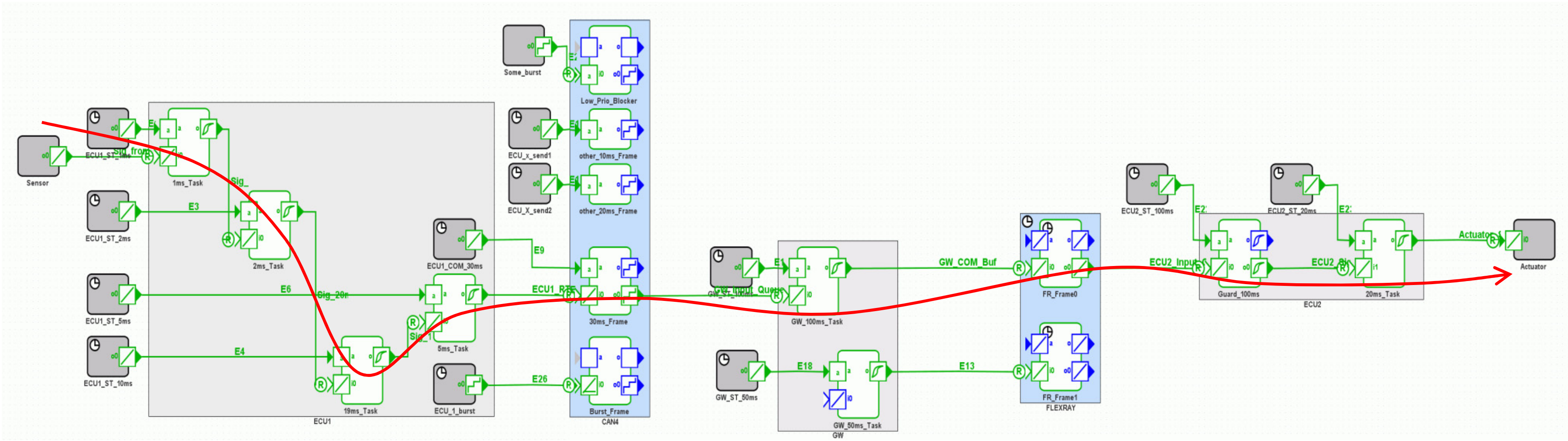


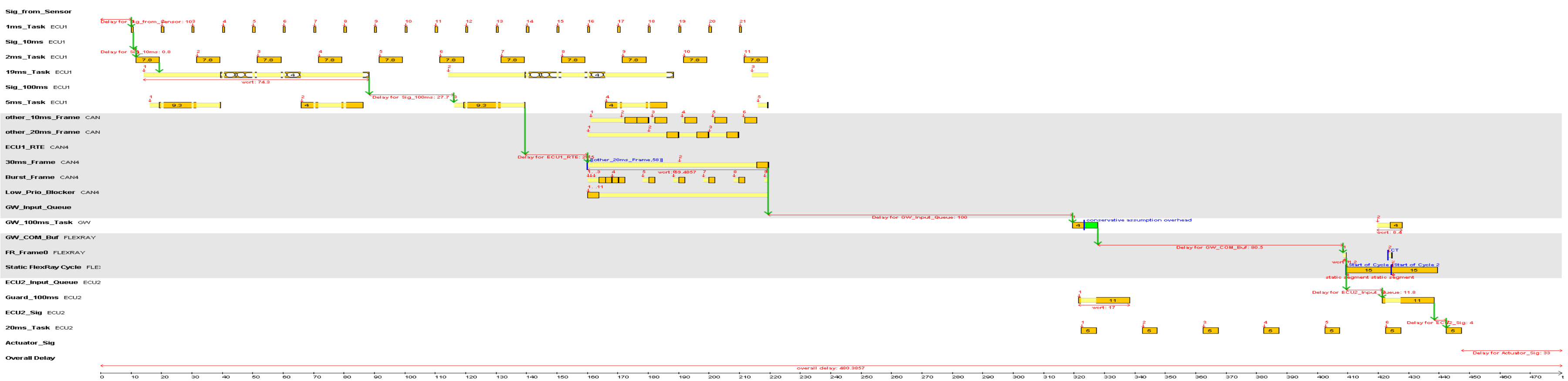
Source → ECU1 → CAN → Gateway → FlexRay → ECU2 → Sink



Focus: End-to-end Timing Analysis

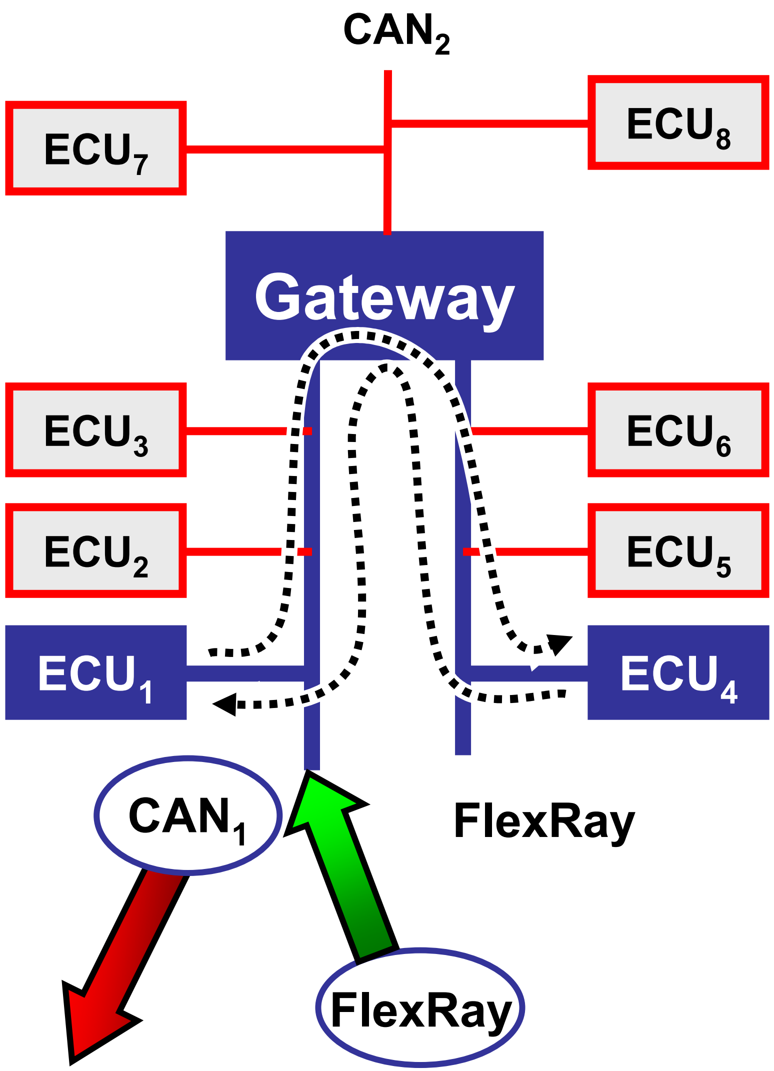
e.g.: Source → ECU1 → CAN → Gateway → FlexRay → ECU2 → Sink





Example 7: from CAN to FlexRay

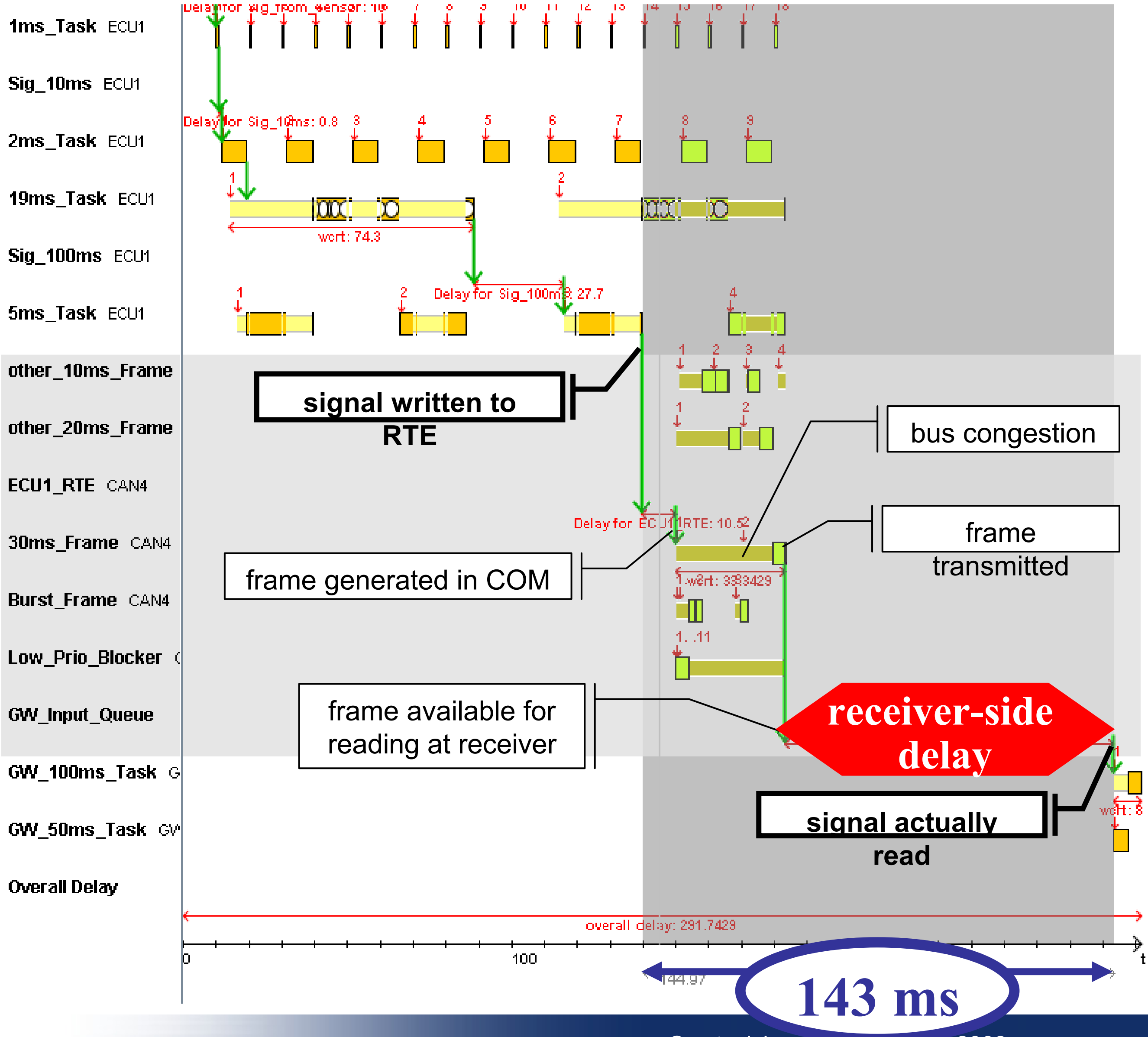
- Original System:
  - CAN, several sync/async ECUs
  - Path Delay: **143ms**
- First Adaptation:
  - FlexRay, same sync/async ECU situation as original system
  - Path Delay: **120ms**
- Second Adaptation:
  - FlexRay, all ECUs are in sync with FlexRay and to each other
  - Path Delay: **29ms !!!**



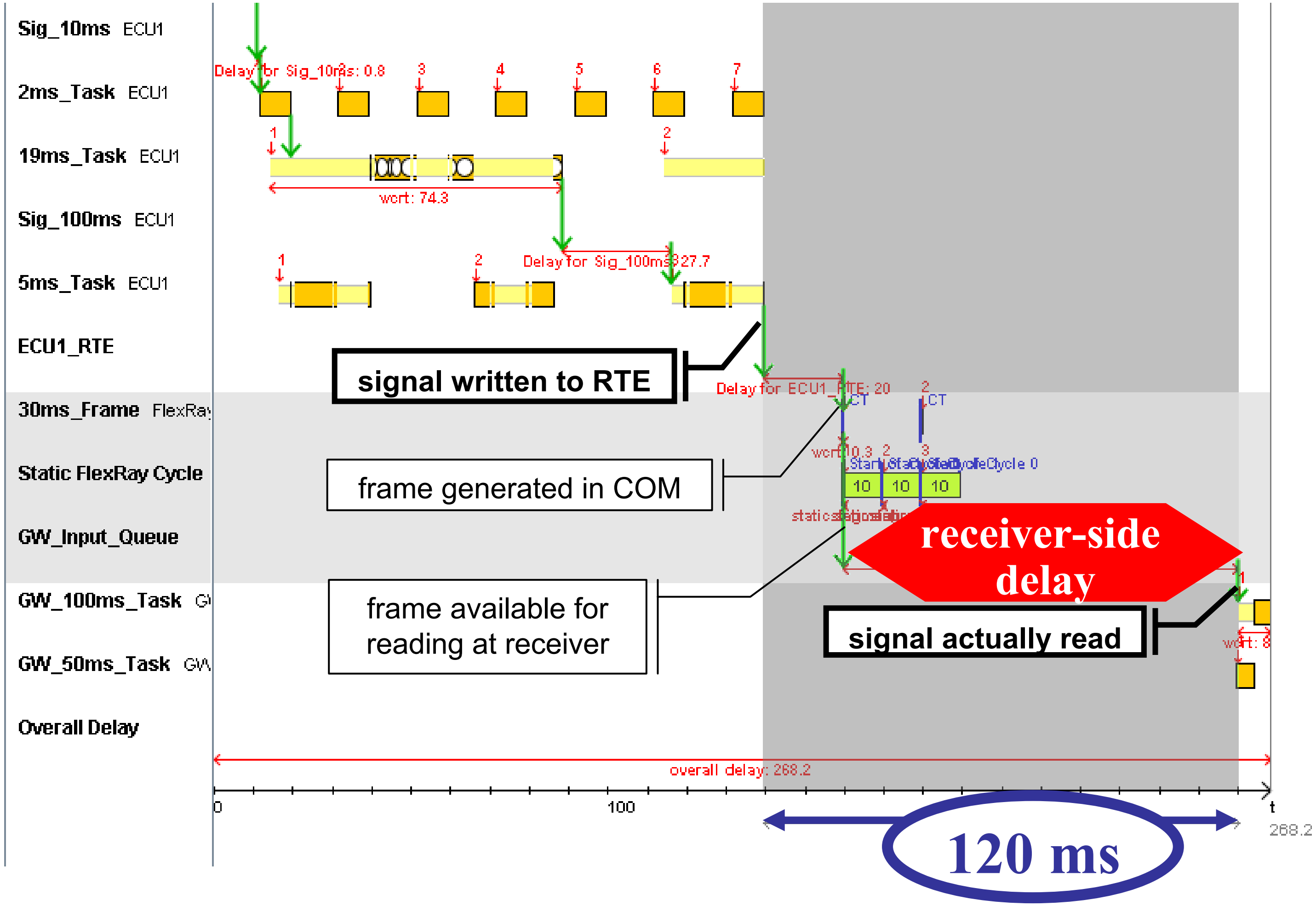
⇒ **FlexRay alone does not reduce latencies**

⇒ **good synchronization is a design challenge!**

CAN Communication, asynchronous ECUs



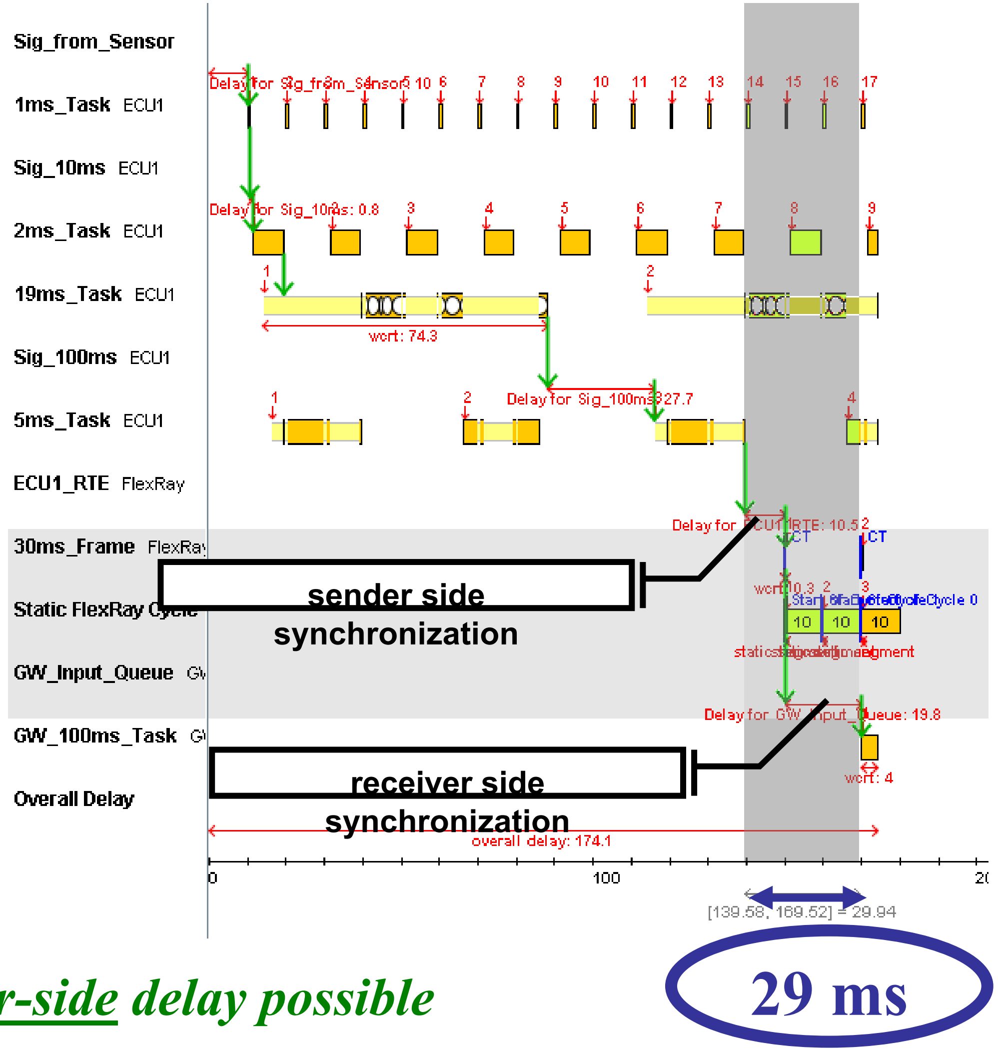
Asynchronous ECUs on FlexRay



Faster bus communication (20 instead of 43ms)

but still large receiver-side delay (100ms)!

Synchronized ECUs on FlexRay



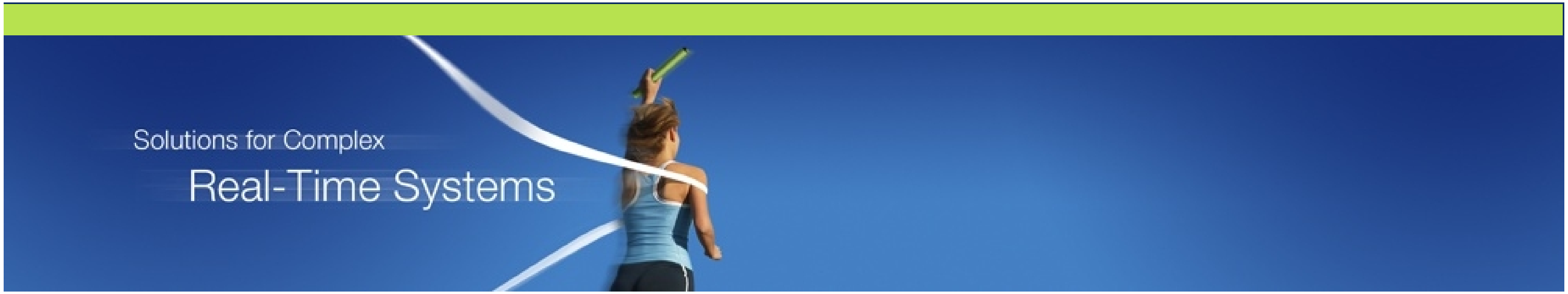
Significantly reduced <u>receiver-side</u> delay possible

but requires good synchronization

SYMTA VISION

Scheduling Analysis for ECUs, 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, ...

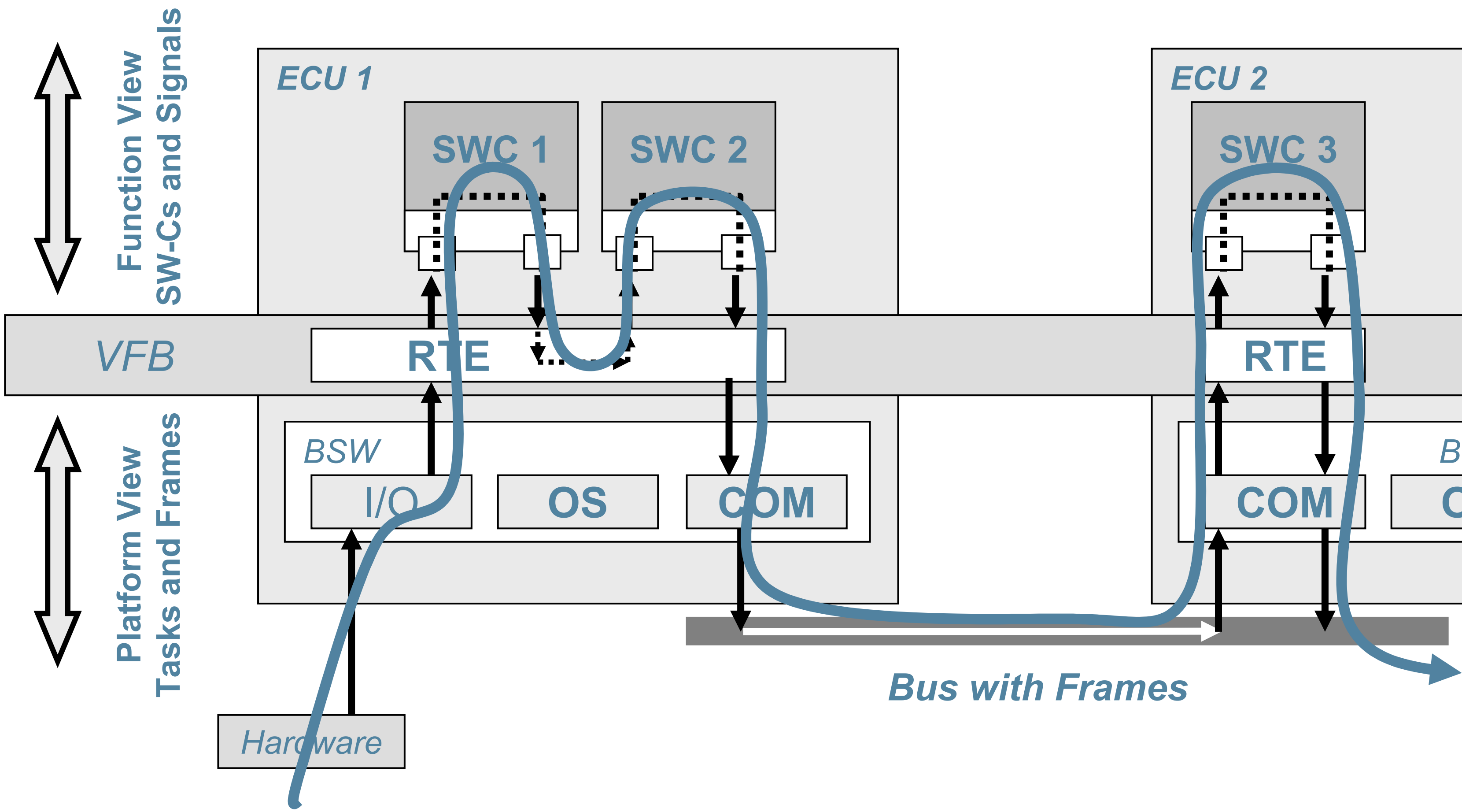
Technology Customization

Technical Challenges – Scheduling Analysis

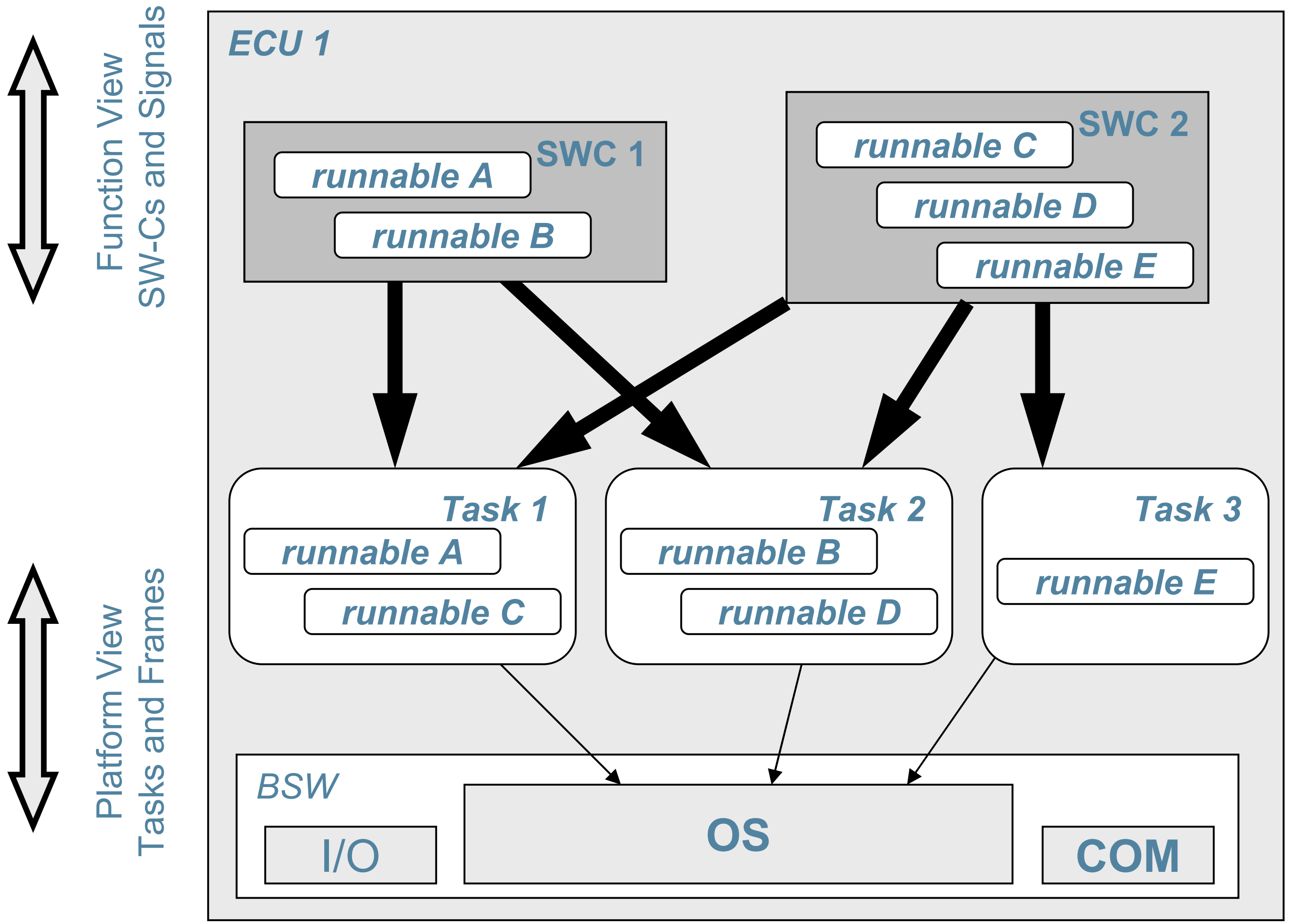
- Right level of accuracy → selection of right analysis technology
  - response time approach with offsets for tasks and frames
  - arbitrary bursts and dynamic load models
  - *otherwise: no usable results*
- Flexibility of technology
  - OSEK, CAN, FlexRay → customization
  - combinations in networked 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*

artist

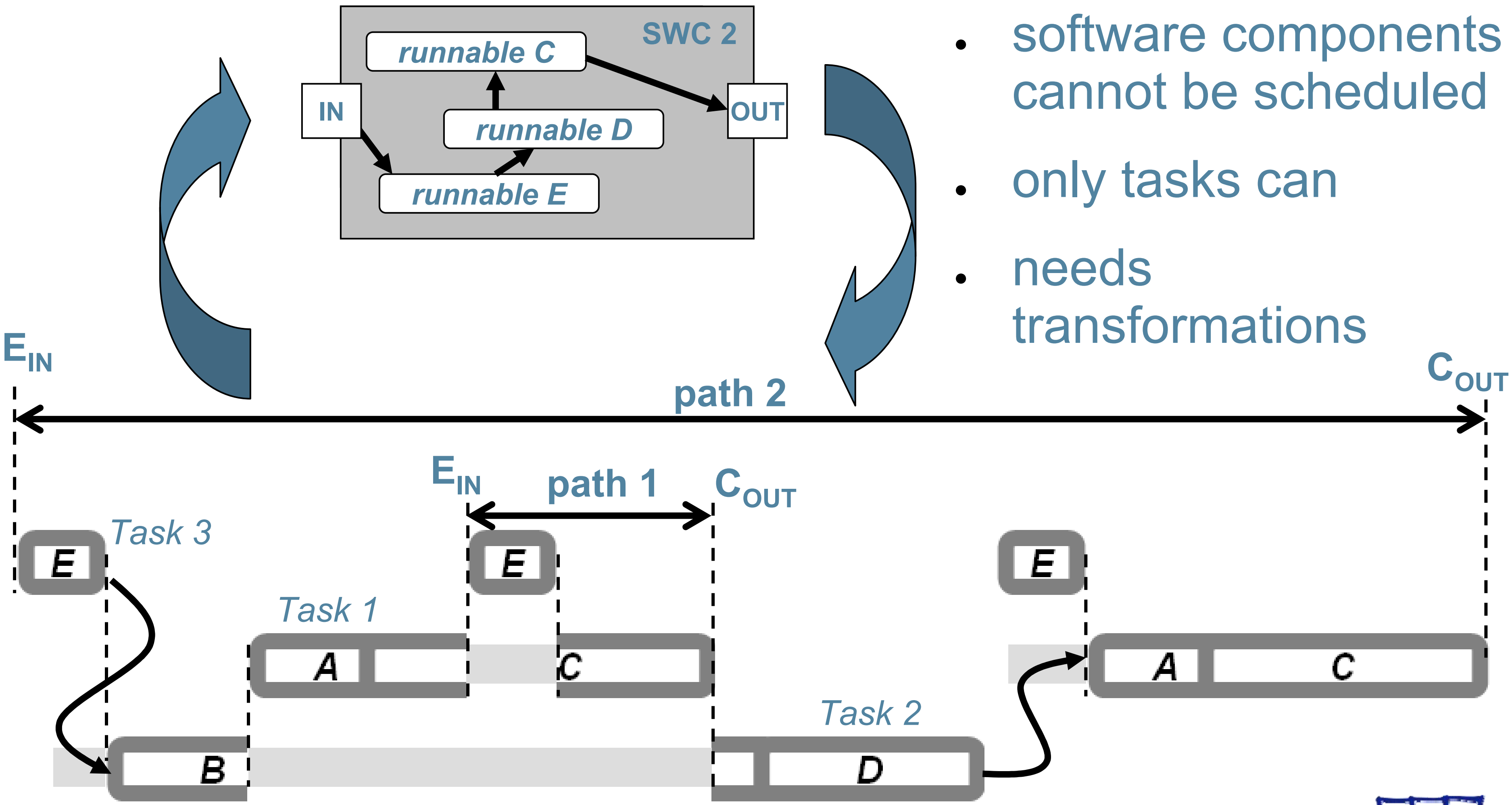
End-to-End Timing Chain in AUTOSAR



Software-Components vs. Tasks - Structure



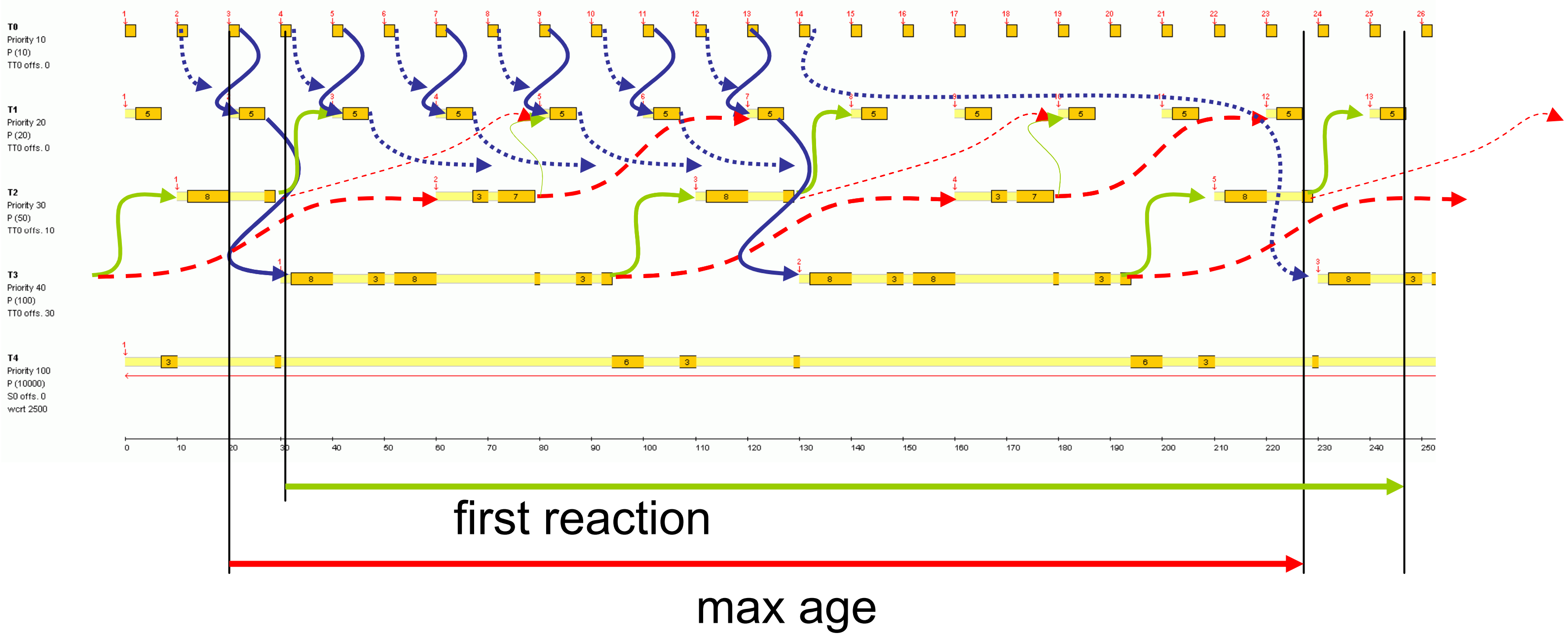
Software-Components vs. Tasks Scheduling



- 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

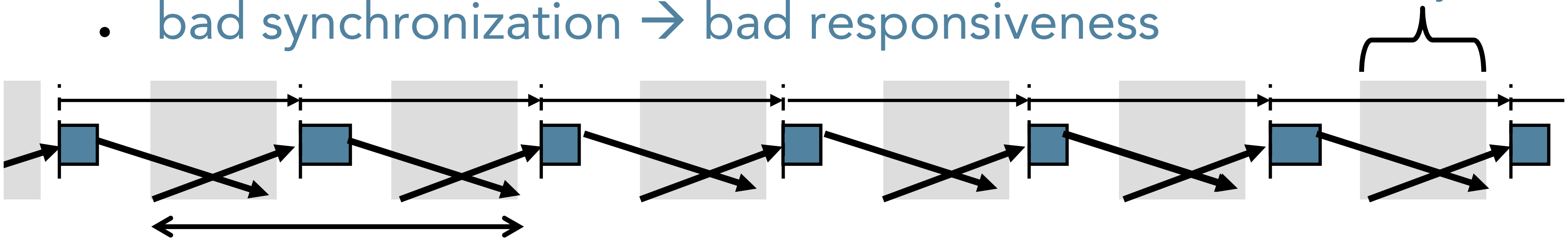


- first-through is important for body electronics
- max-age is important for control engineering

Asynchronous ECUs on FlexRay bus

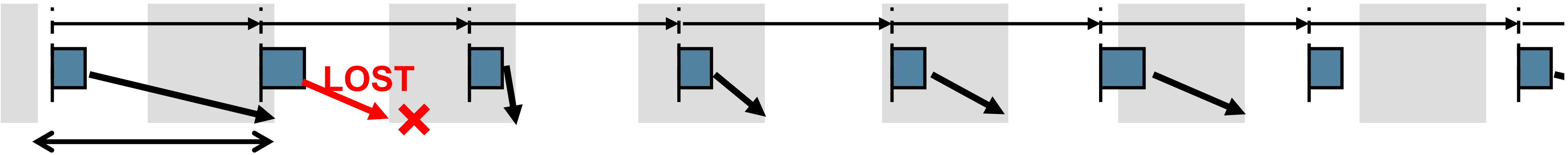
„ok window“, given by FlexRay schedu

- bad synchronization → bad responsiveness

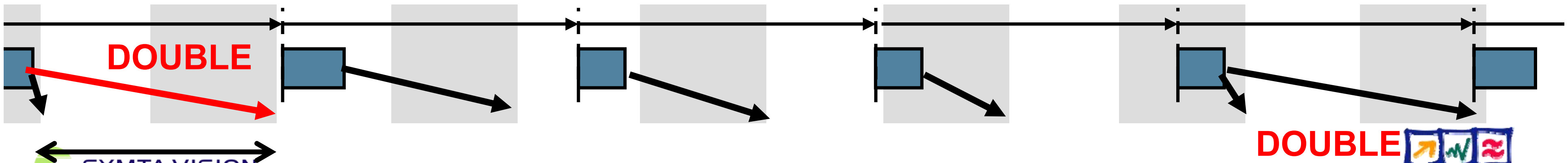


2 FlexRay cycles (more when using mux)

- clock skew effects → large send & receive signal jitters



full FlexRay cycle (more when using mux)



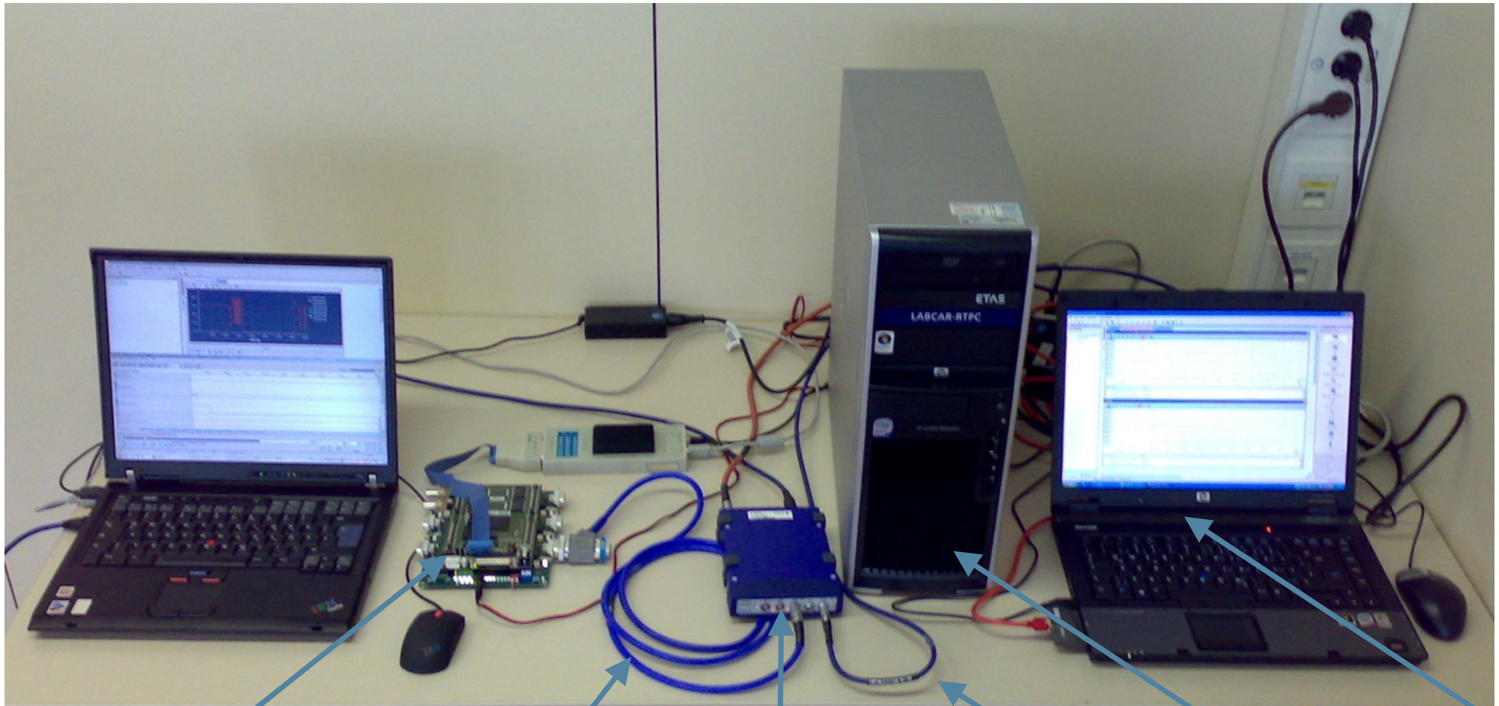
Partnerships and Interfaces

Industry-driven Research Projects

- **INTEREST** (FP6 STREP)
  - INTegration 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)



1. TriCore1796 Eval. Board With Engine Management System

2. CAN Bus

3. CAN ←→ Flexray Gateway (ES910)

4. Flexray Bus

5. Real-Time PC

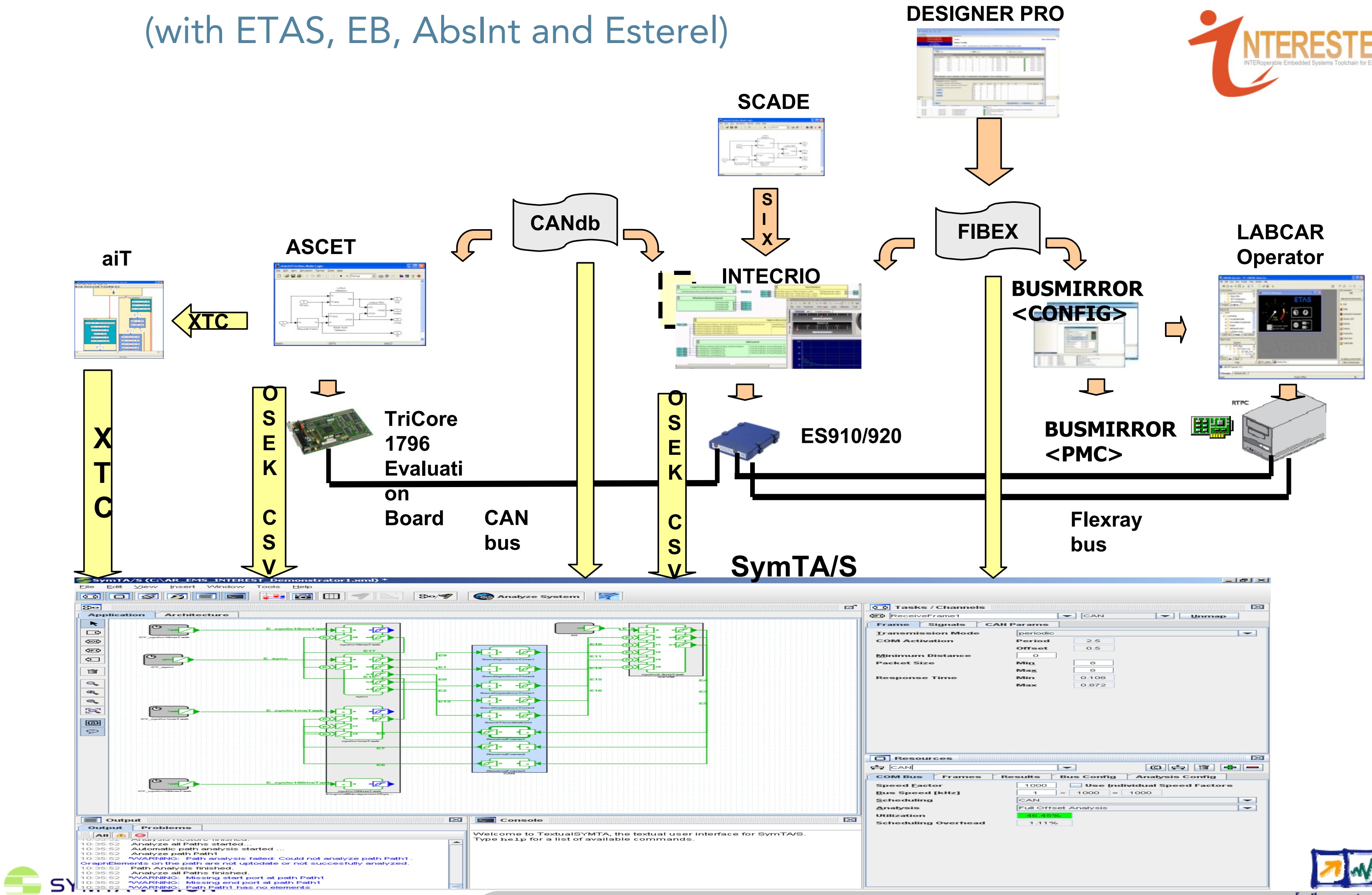
6. Labcar IP /w Flexray

SYMTA VISION

artist

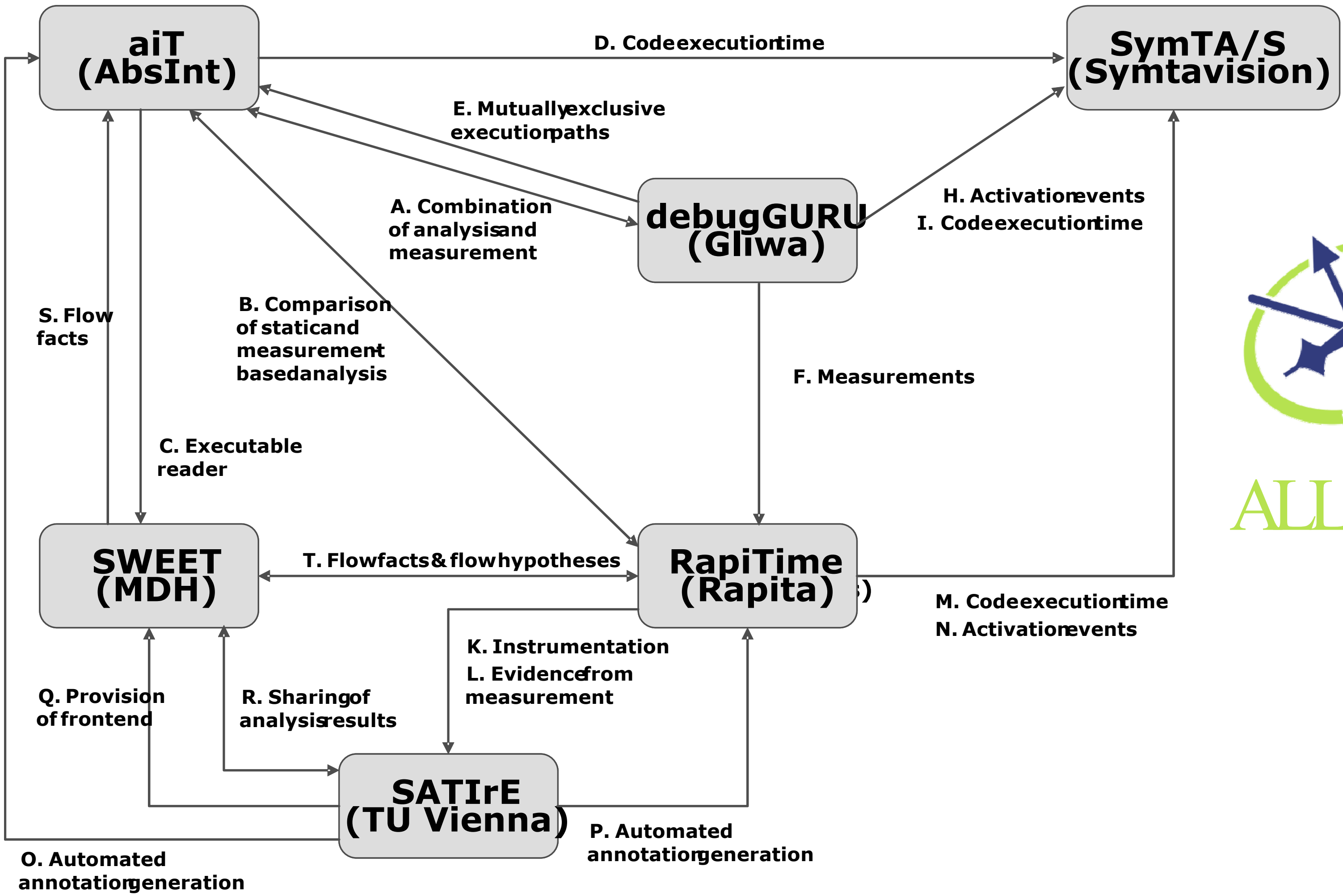
INTEREST Automotive network validator

(with ETAS, EB, AbsInt and Esterel)



Information Society Technologies

Tool Partnership in ALL-TIMES Project



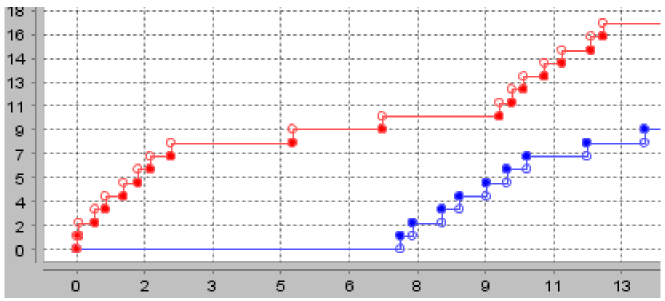
artist

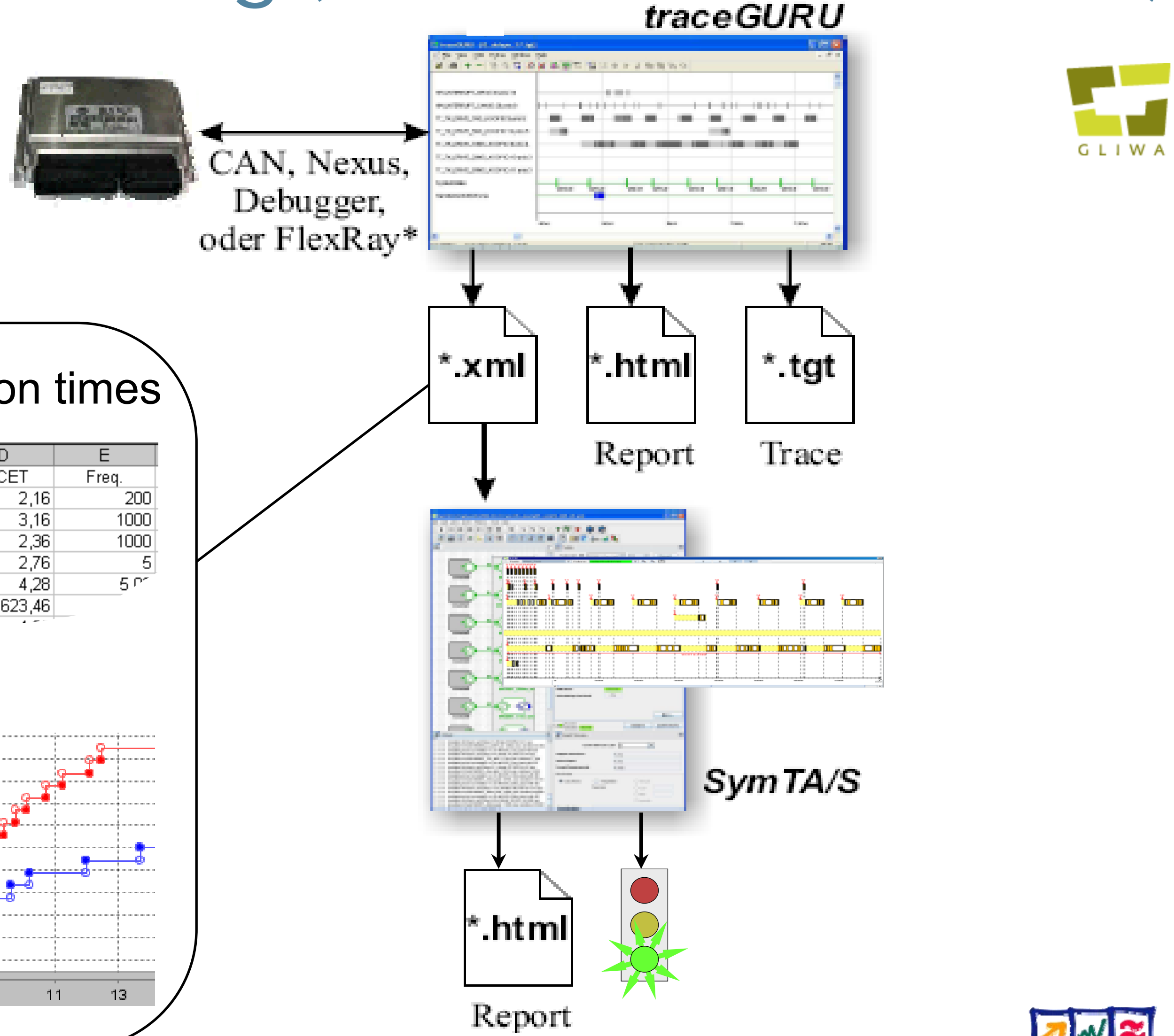
SymTA/S and Tracing (traceGURU from Gliwa)

– Single function execution times

	A	B	C	D	E
1	Process	Task	BCET	WCET	Freq.
2	Proc_001	200ms_Task (3)	1,62	2,16	200
3	Proc_002	1000ms_Task (2)	3,08	3,16	1000
4	Proc_003	1000ms_Task (2)	2,36	2,36	1000
5	Proc_004	TSK_Dynamic (12)	2,76	2,76	5
	005	TSK_Dyr	3,44	4,28	5
		TSK	43,7	623,46	

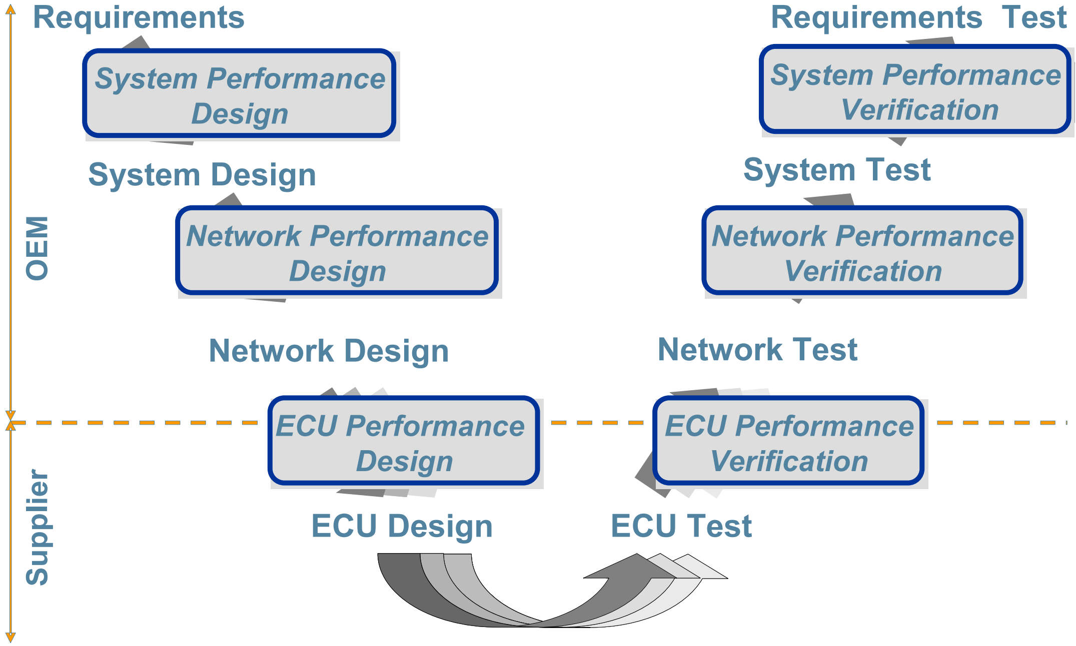
– Interrupt Frequency





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)

Announcement: 2nd SymTA/S News Conference

2nd

SymTA/S NewsConference

8./9.10.2008

Braunschweig-Riddagshausen

Program on 09.10.2008

8:30 – 9:00	Registration
9:00 – 9:15	**Welcome** Dr. Marek Jersak, CEO of Symtavision
9:15 – 9:45	**Einsatz von SymTA/S in der Lenkungs-entwicklung bei VW** Dieter Brinkema, Volkswagen
9:45 – 10:15	**Integrating Timing-Analyses into ECU Software-Development** Patrick Frey, ETAS
10:15 – 10:45	*Coffee break*
10:45 – 11:15	**Symtavision Engineering - Lessons Learned from various Timing Analysis Projects** Ralf Klein, Symtavision
11:15 – 11:45	**ALL-TIMES: Combining best Techniques for Different Timing Problems** Peter Gliwa, Gliwa GmbH
11:45 – 12:15	**The TIMMO Project and Perspectives for Timing in AUTOSAR R4.0** Stefan Kuntz, Continental
12:15 – 14:00	*Lunch break*
14:00 – 14:30	**SymTA/S Release 1.4 and beyond** Dr. Kai Richter, CTO of Symtavision
14:30 – 15:00	**Using Timing Analysis for Evaluating Networks in an Early Design Phase of Automotive E/E-Architectures** Matthias Traub, Daimler
15:00 – 15:30	**Reliability and Cost-Optimization: Analysis of Networks and Multicore-Communication** Prof. Dr. Rolf Ernst, TU-Braunschweig
15:30 – 15:45	**Closing address** Dr. Marek Jersak

Exhibits on 8./9.10.2008

AbsInt Angewandte Informatik

aquintos integration experts

ETAS

GLIWA embedded systems

RAPITA SYSTEMS LTD

SYMTA VISION