SYMTA VISION

spid

Timing and Scheduling Analysis for Safe and Cost-Optimized ECU Development

Dr. Kai Richter, CTO, Symtavision GmbH

August, 2015

Leading timing analysis expertise

- Reliable, safe & cost-effective embedded real-time systems, on time
- Architecture optimization & timing verification for ECUs, networks, E/E

focus of today

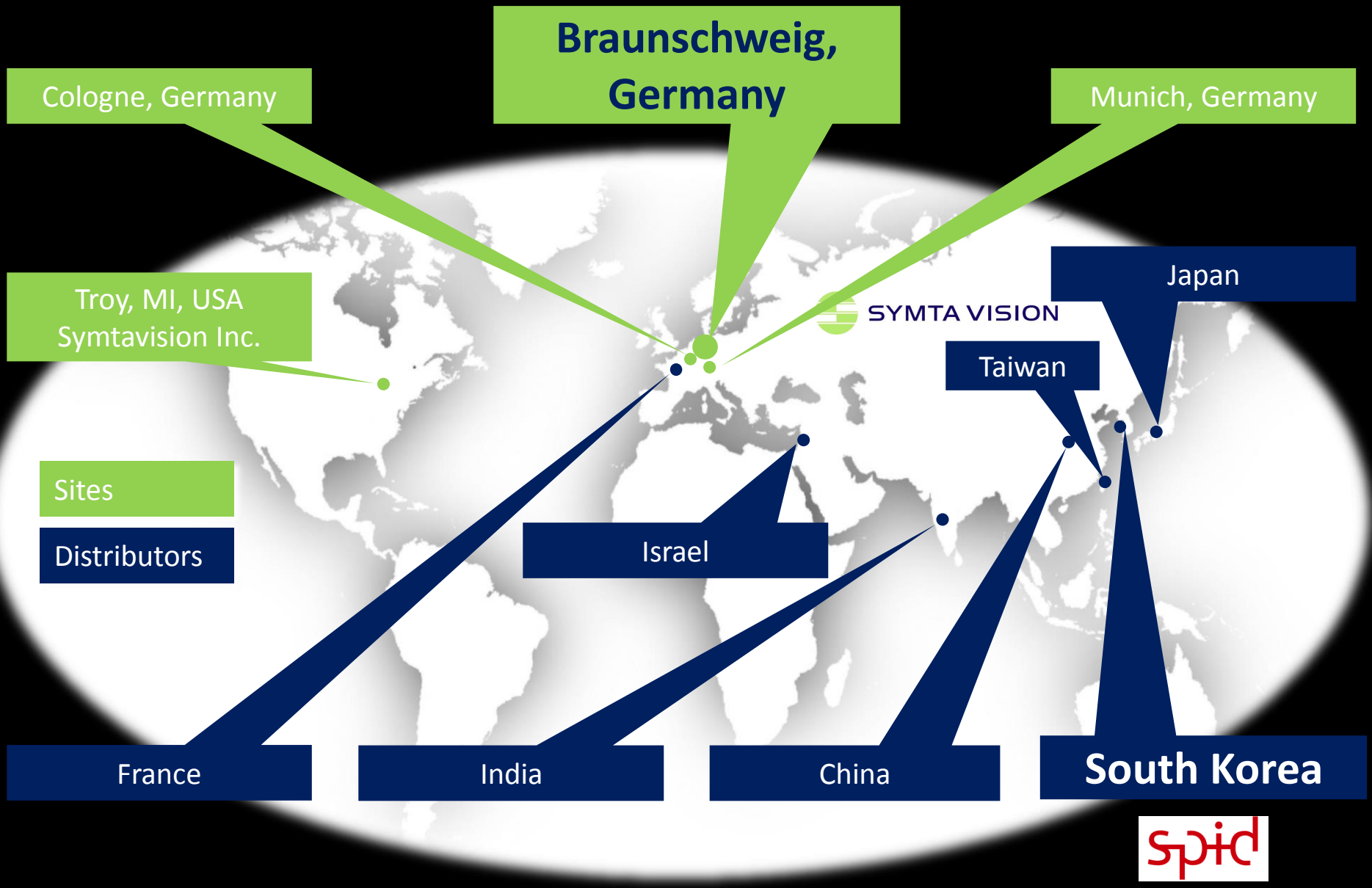
Custom-tailored timing analysis solutions

- Tools: SymTA/S & TraceAnalyzer
- Services: timing consulting, system optimization, timing audits, SW architecture audits, engineering, automation, training, support …

Selected Customers

BMW Group, GM, TOYOTA, VOLKSWAGEN, IVECO, EvoBus, DAIMLER, FCA FIAT CHRYSLER AUTOMOBILES, Audi Vorsprung durch Technik, HYUNDAI·KIA MOTORS, FAW, BAIC, CMC, THALES, Honeywell, BOSCH, DENSO, HYUNDAI MOBIS, HITACHI Inspire the Next, MOTION & CONTROL NSK, BWI GROUP DRIVING TECHNOLOGY, EADS, EMBRAER, SIEMENS

Global Presence



90% Innovation in Embedded Real-Time Systems

- Advanced Powertrain

Source: GM

- ADAS
- Chassis & Active Safety

Source: Daimler

Soft Real-Time → Cost, Quality

Hard Real-Time → Cost, Quality, **Safety**

- Body & Comfort
- Infotainment & Telematics

Why Timing Analysis?

From ideas, function models, prototypes …

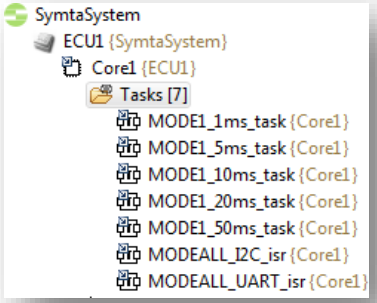
… to embedded control units ……

Mass production with limited resources

… to networked vehicle-level systems.

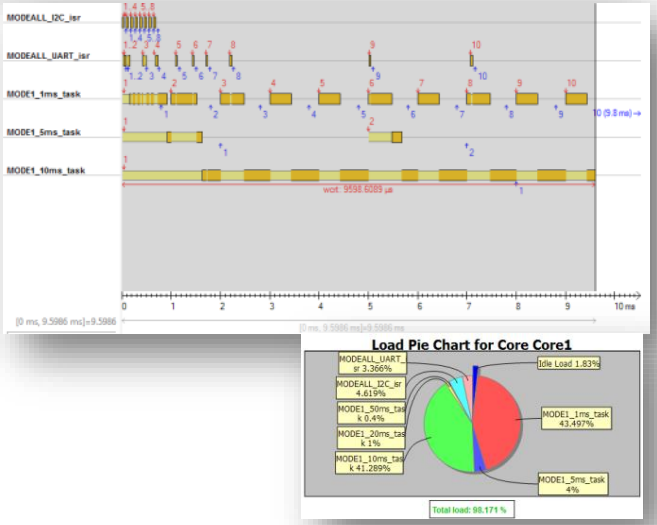
- ➔ Cost and resource performance go down.
- ➔ Timing requirements remain and quality must increase.
- ➔ Needs systematic planning of timing, performance and resources.

Symtavision Tools Help Understanding and Optimizing Timing, SW Architecture and Schedule



- Make the SW architecture explicit (= *model it!*)
  - Who are the time consumers?
- Model key timing characteristics incl. the schedule
  - How often do they run?
  - How long do they execute?
  - How are they scheduled?
- Simulate or analyze worst-case schedules
- Assess key acceptance criteria such as load, cycle time, response time, jitter
- Do this in architecture and concept development phase and compare with test results

Element	Execution Time	Internal	Osek Task Parameter	
Name	Core Execution Time	Activation	Priority	Task Type
MODE1_1ms_task	[0.36061542 ms;0.4349691 ms]	P(1 ms)	6	Preemptive
MODE1_5ms_task	[0.02 ms;0.2 ms]	P(5 ms)	5	Preemptive
MODE1_10ms_task	[0 ms;4.12891789 ms]	P(10 ms)	4	Preemptive
MODE1_20ms_task	[0.1 ms;0.2 ms]	P(20 ms)	3	Preemptive
MODE1_50ms_task	[0.1 ms;0.2 ms]	P(50 ms)	3	Preemptive
MODEALL_I2C_isr	[10 µs;40 µs]	I ([0...1 ms])	10	NonPreemptive
MODEALL_UART_isr	[10 µs;40 µs]	I ([0...5 ms])	8	NonPreemptive



SYMTA VISION

spid

ISO 26262 and Timing

ISO 26262 and Task Response Times

ISO 26262 – Part 6 – Clause 6: **”Specification of software safety requirements”**

6.4.1 The software safety requirements shall address each software-based function whose failure could lead to a violation of a technical safety requirement allocated to software.

NOTE 1 Functions whose failure could lead to a violation of a safety requirement include:

— functions related to performance or time-critical operations; and

6.4.2 The specification of the software safety requirements shall be derived from the technical safety requirements and the system design (see ISO 26262-4:—, 7.4.1 and ISO 26262-4:—, 7.4.5) and shall consider:

e) the timing constraints;

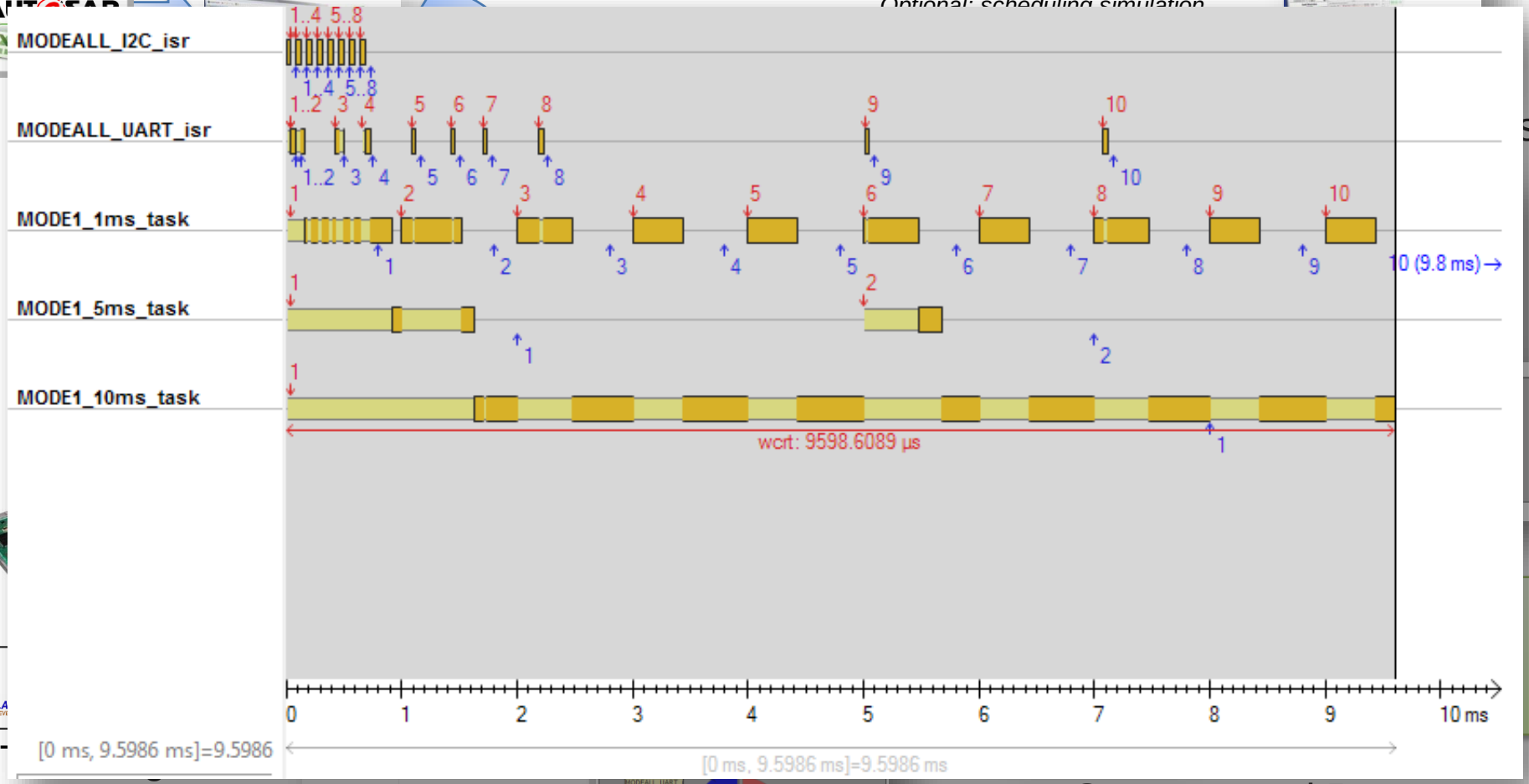
EXAMPLE 2 Execution or reaction time derived from required response time at the system level.

We must understand the timing of tasks including their response times (which result from the scheduling) in order to assess safety requirements.
→ Scheduling analysis is needed

Symtavision Tools in the Process

SW Architecture (incl. safety concept)

Optional: scheduling simulation



(from integration testing)

Measured Timing

Compare and Report

BMW Example: SymTA/S for SIL3 E-Power Steering

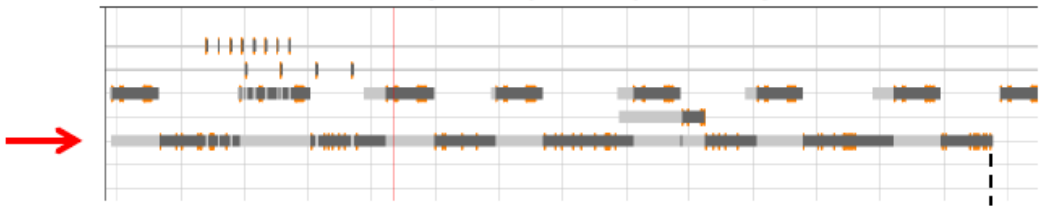
applied since first introduction of electric steering in BMW X5 in 2005

Time is Money – Real-Time is a lot of Money
BMW Group
Hans Sarnowski
22.-23.09.2008
Seite 11

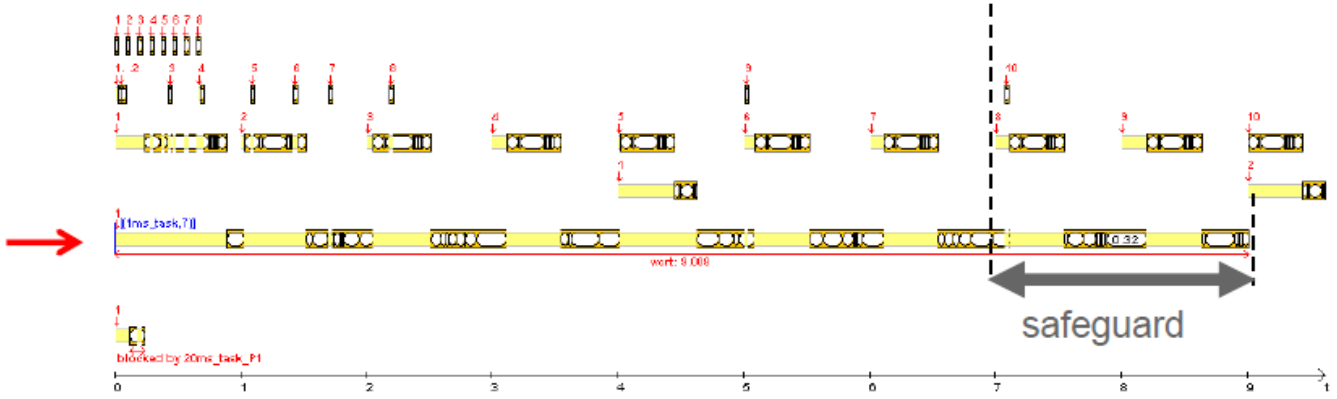
Use of Timing Tools

Safeguarding against worst-case timing

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

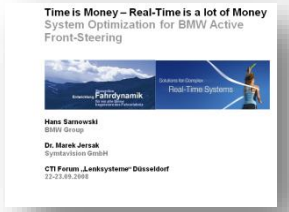


- **Worst-Case Analysis with SymTA/S:** Response time 9ms
  10 CAN, 8 SPI Interrupts, 9 preemptions by 1ms task, blocking



Selected Symtavision References – ECU & Safety

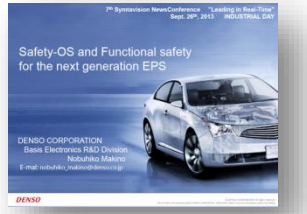
- **BMW** – Active Front Steering
  - Timing sign-off for safety architecture & software integration, ECU cost reduction



- **AUDI** – Electronic Chassis Platform (active damping & level control)
  - Design of SW architecture and safe schedule of mixed-criticality (ASIL-A/B/C) multi-core ECU, ensure freedom-from-interference

- **GM** – Lane Keeping
  - Capture relevant timing requirements, optimization of schedule to ensure safety concept

- **VW** – Central Body Control Multi-Core ECU
  - Virtual timing verification of SW architecture to avoid interference between body functions and gateway functions



- **VW Components** – Electronic Power Steering ECU
  - Integrated timing verification process including verification of three-layer ASIL-C safety architecture ECU cost reduction

- More: DENSO EPS, Hitachi chassis control, …

Customer references / success stories available on request

Summary: Key Timing Requirements for Safety

- Basic: CPU load < x% (for reserves and later updates)

- Quality: Task response time < 90% (or other value < 100%) of cycle time in nominal (error-free) case, every task executes within its cycle
  → SymTA/S worst-case scheduling analysis helps increasing the coverage of timing corner cases
  → this helps also to avoid false positives of error detection, which would lead to reduced availability / customer satisfaction.

- Safety: Make absolutely sure that the error detection (specific task) will always (in worst case) be schedulable. Otherwise, a problem in the monitored task (e.g. endless loop) could prevent the error detection from running, which results in a violation of safety requirements.
  → SymTA/S SW architecture checks detect such risk and help avoiding it through a suitable selection of the schedule
  → this is also known as *freedom-from-interference requirement* according to ISO 26262 in mixed-criticality systems

ISO 26262 and Freedom from Interference (FFI)

ISO 26262 – Part 6 – Clause 7: **"Software Architectural Design"**

7.4.9 The software safety requirements shall be allocated to the software components. As a result, each software component shall be developed in compliance with the highest ASIL of any of the requirements allocated to it.

7.4.11 If software partitioning (see Annex D) is used to implement freedom from interference between software components it shall be ensured that:

a) the shared resources are used in such a way that freedom from interference of software partitions is ensured;

NOTE 1 Tasks within a software partition are not free from interference among each other.

We must ensure this !

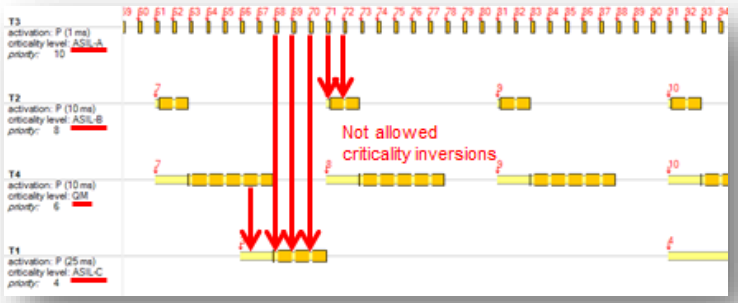
		This level must be …			
		A	B	C	D
… free from interference by this level	A	-	crit	crit	crit
	B	ok	-	crit	crit
	C	ok	ok	-	crit
	D	ok	ok	ok	-

How to read this matrix:
ASIL-C software must be
free from interference by ASIL-A and B
but can tolerate interference by ASIL-D

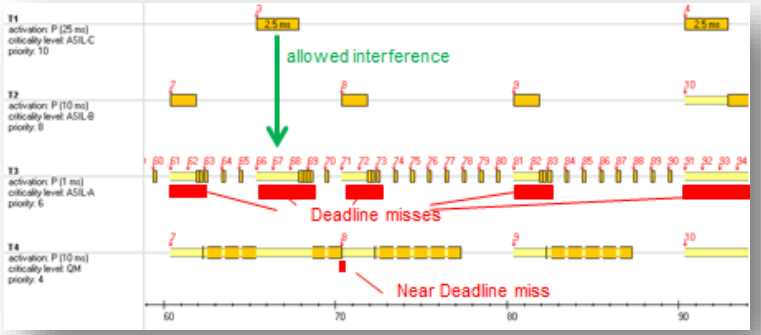
AUDI Example: Mixed-Criticality Schedule Development

from: K. Schmidt, M. Buhlmann, C. Ficek, K. Richter, Design patterns for highly integrated ECUs, ATZ elektronik 01/2012

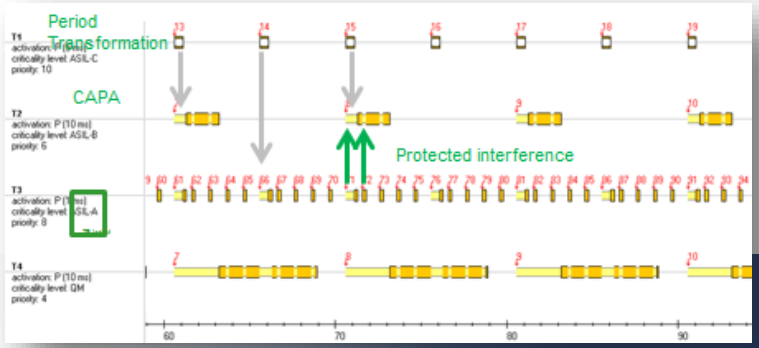
- Rate-Monotonic Schedule
  - very resource-efficient
  - but unsafe if priorities ≠ ASIL levels
  - ➔ execution time protection can help



- Criticality as Priority (CAPA)
  - very safe
  - but lousy if cycle time ≠ ASIL levels
  - ➔ cycle time changes can help



- CAPA + Period Transformation + Execution Time Protection



SYMTA VISION

spid

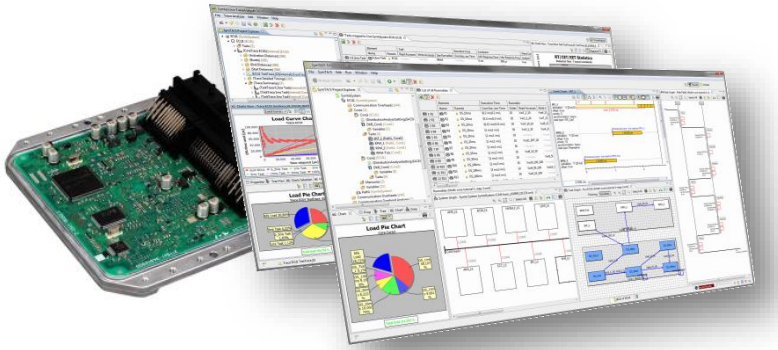
Summary

Development With and Without Timing Analysis

Without timing analysis

- Undetected timing errors
- Lower quality & reliability
- Additional debugging cycles
- Higher cost

With Symtavision Timing Analysis



SymTA/S & TraceAnalyzer

- Eliminate timing errors
- Higher quality, reliability, safety
- Quicker development
- Lower cost

Summary

- ISO 26262 formulates several requirements on the timing behavior of automotive systems
- Symtavision tools provide timing modeling, trace analysis and worst-case scheduling analysis for improved safety
  - Guarantee task deadlines in nominal case (error-free case)
  - Optimize SW architecture for error detection, task monitoring and mixed criticality
- Symtavision
  - Has 10 years of experience in key domains:
    chassis, driver assistance systems, powertrain, body, …
  - Is recognized expert for introduction of new technology:
    AUTOSAR, multi-core, ISO26262, FlexRay, CAN-FD, Ethernet, …
- Symtavision solutions are available through SPID in South Korea

Meet Timing Analysis Users at the 9th Symtavision NewsConference on Sept 30 + Oct 1

- Annual 2-day conference organized by Symtavision
- From 100 to 150 participants per year
- Attended by engineers, managers, and technology experts from industry and research to discuss and present the state-of-the-art and future developments in timing analysis

- Wednesday, Sep 30
  - 2 SymTA/S trainings
  - 5 Research presentations
  - 3 Interactive workshops

- Thursday, Oct 1
  - Industry presentations from Audi, BMW, Bosch, Fiat, Chrysler, Volkswagen …

- *On Friday there is an official AUTOSAR WP1 Timing User Group Meeting*