Institute of Computer and
Communication Network Engineering
TU Braunschweig, Germany

SYMTA VISION

Scheduling Analysis in the Automotive Design Flow

Kai Richter, Marek Jersak - Symtavision GmbH

Arne Hamann, Rolf Ernst - TU Braunschweig

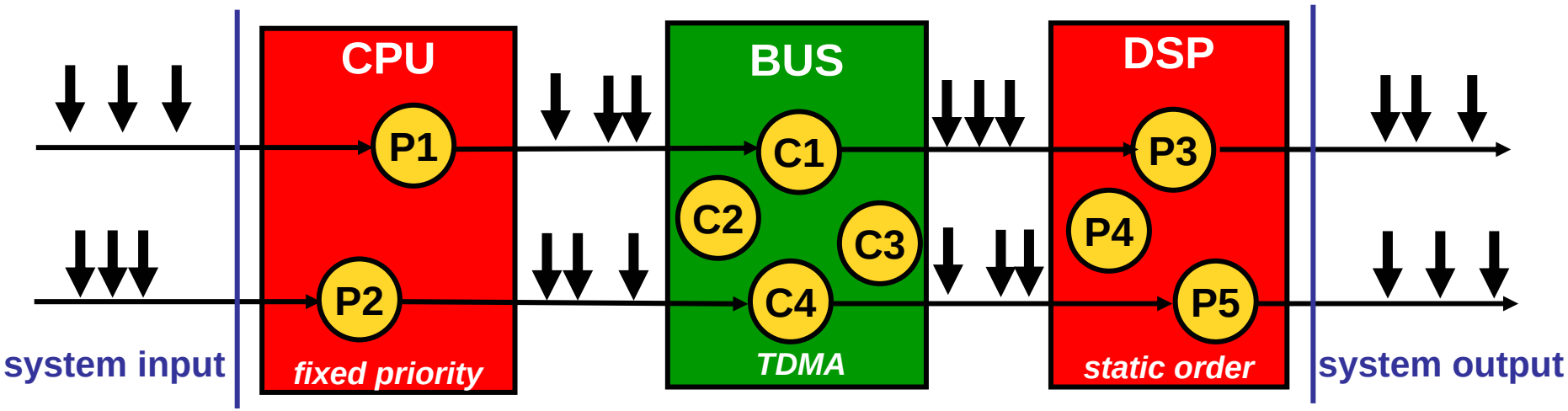
Outline

- Compositional system level analysis with SymTA/S (short overview)
  - Basic formal model
  - Iterative system level analysis approach
- Two case studies …
  - Supplier view: engine ECU analysis (ERCOS^{EK})
  - OEM view: Bus Bottleneck Detection (CAN)
- … with discussions about
  - requirements for formal analysis in the automotive industry
  - supply chain issues (IP protection, data availability)
  - relation to AUTOSAR
- Conclusion

Basic formal model

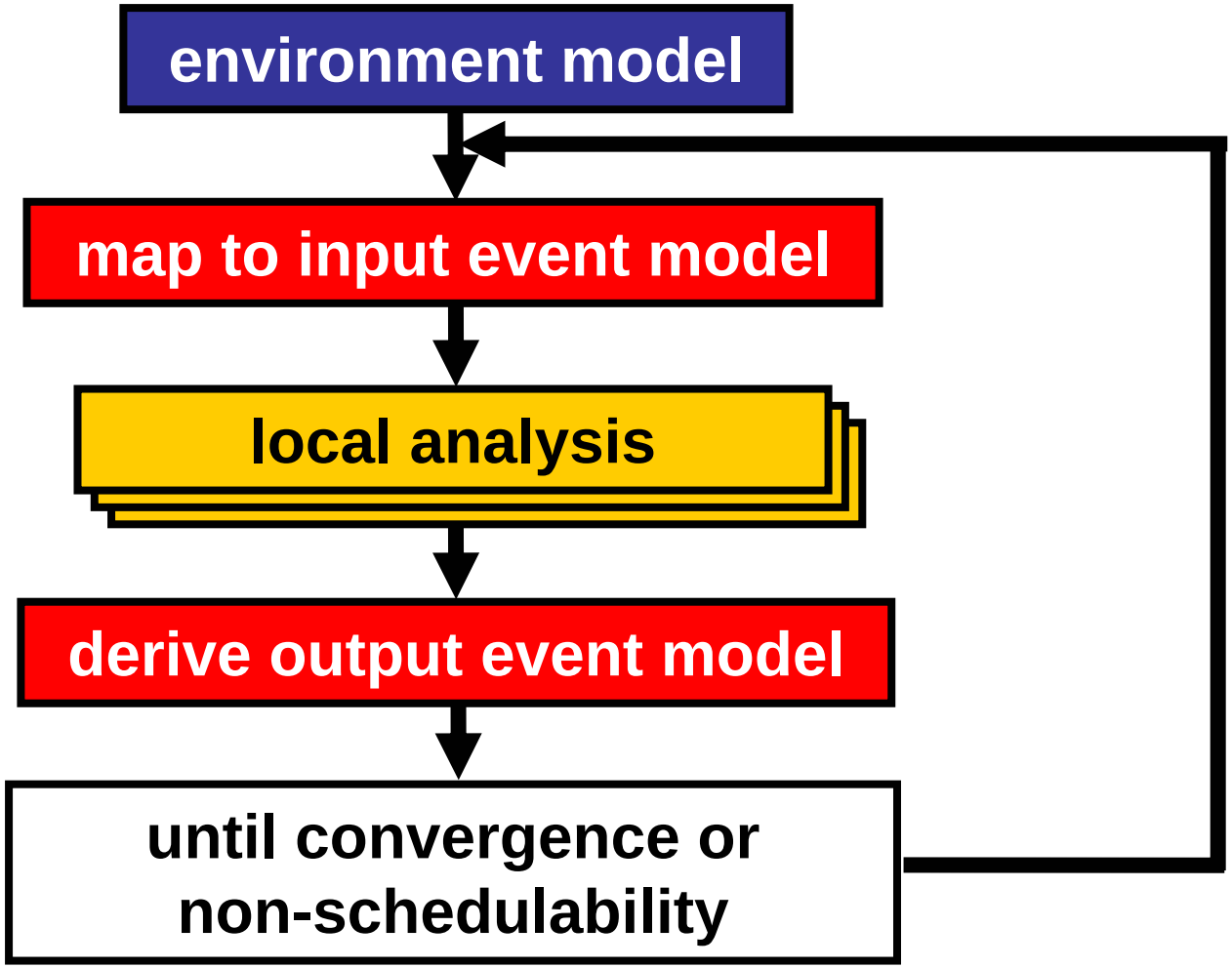
- Application model
  - Task graph: functional and timing task dependencies
  - Activation triggered by events
  - Cyclic dependencies, AND/OR activations
- Heterogeneous architecture
  - Text book schedulers: SPP, RMA, TDMA, EDF, etc.
  - Automotive components: CAN, ERCOS^{EK}, Flexray, etc.
- Timing task characteristics
  - Interval model: [BCET,WCET]
  - Task modes
  - Task offsets
  - Activating event models: periodic, sporadic, jitter, burst
  - Hard real-time constraints

SymTA/S: Compositional analysis



- Performance analysis of heterogeneous architectures
- Tasks are coupled by event streams
- Composition by means of event stream propagation
  - Apply scheduling analysis at resource level
  - Determine the behavior of the output stream
  - Propagate to the next component

SymTA/S: System Analysis Loop



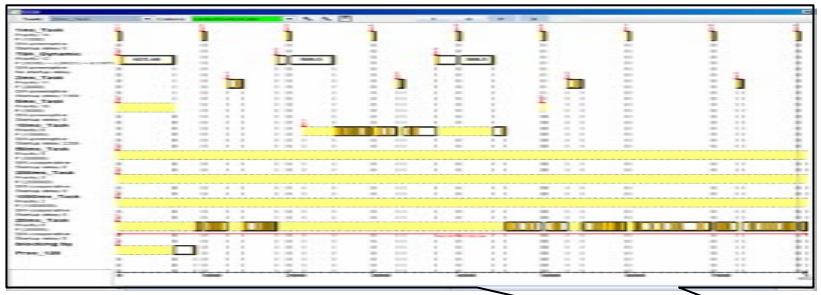
Components and Analysis in the Automotive Industry

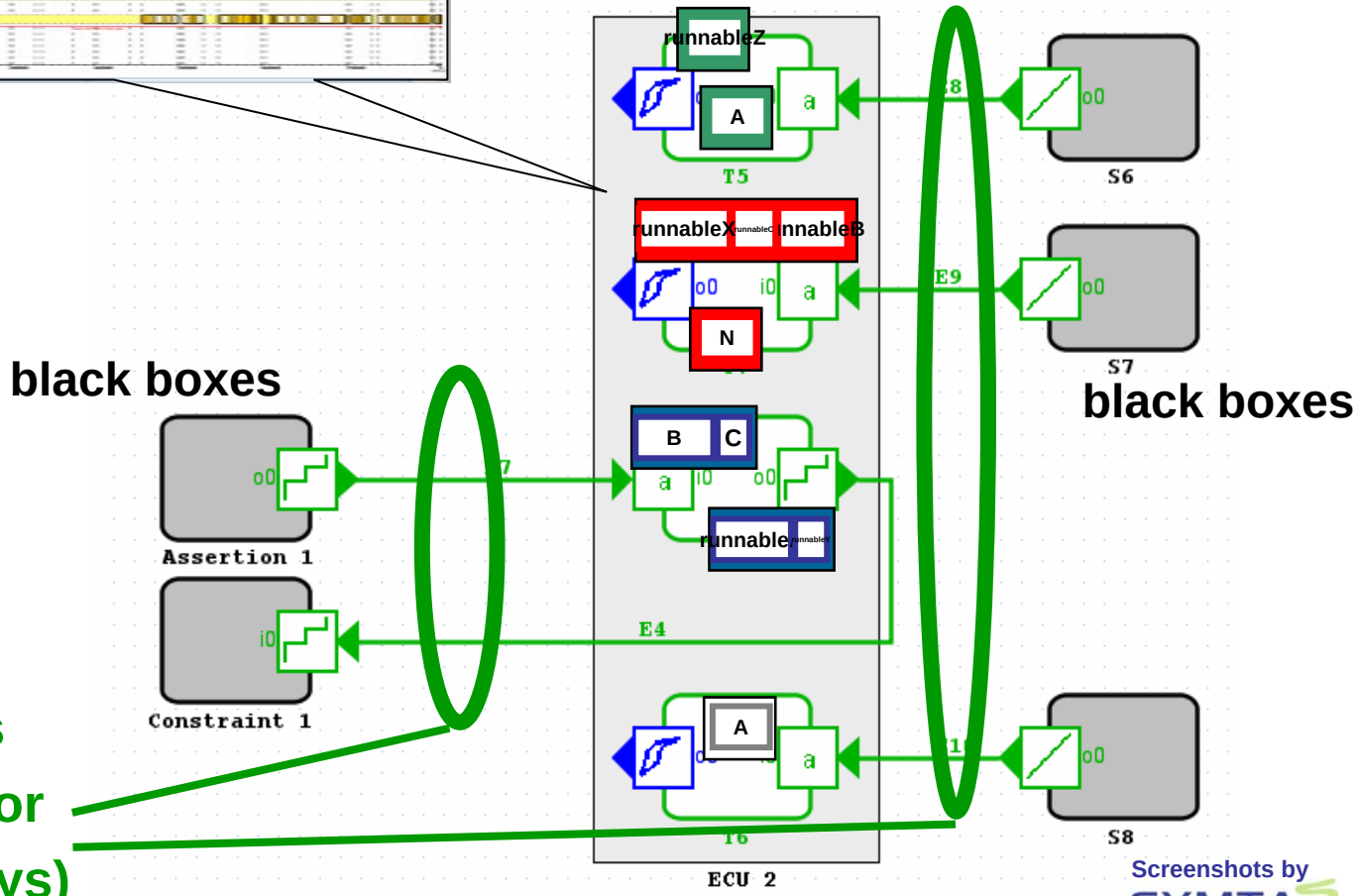
- Scheduling analysis in industry
  - complex and „dirty“ mechanisms challenge analysis accuracy
  - → basic model and scheduling analyses need to be extended
- Supply-Chain Issues
  - IP protection challenges „holistic“ approaches
  - analysis & models must consider data (un) availability
- Relation to AUTOSAR
  - SW component model different from platform execution model
  - no „timing model“ defined yet

Outline

- Compositional system level analysis with SymTA/S (short overview)
  - Basic formal model
  - Iterative system level analysis
- Components and formal analysis in the automotive industry
  - Requirements
  - Supply chain issues
  - Relation to AUTOSAR
- Two case studies
  - Supplier view: engine ECU analysis (ERCOSEK)
  - OEM view : CAN Bus Bottleneck Detection
- Conclusion

ECU Suppliers View: Timing Analysis on ECUs





interface captures dynamic I/O behavior (jitter, min/max delays)

Screenshots by SYMTA

Case Study 1 - Engine ECU

Engine ECU

- Engine ECU with cyclic and engine-synchronous tasks
- Specialties:
  - load of engine-synch. tasks increases with engine speed
  - compensation by „task expansion“ mechanisms

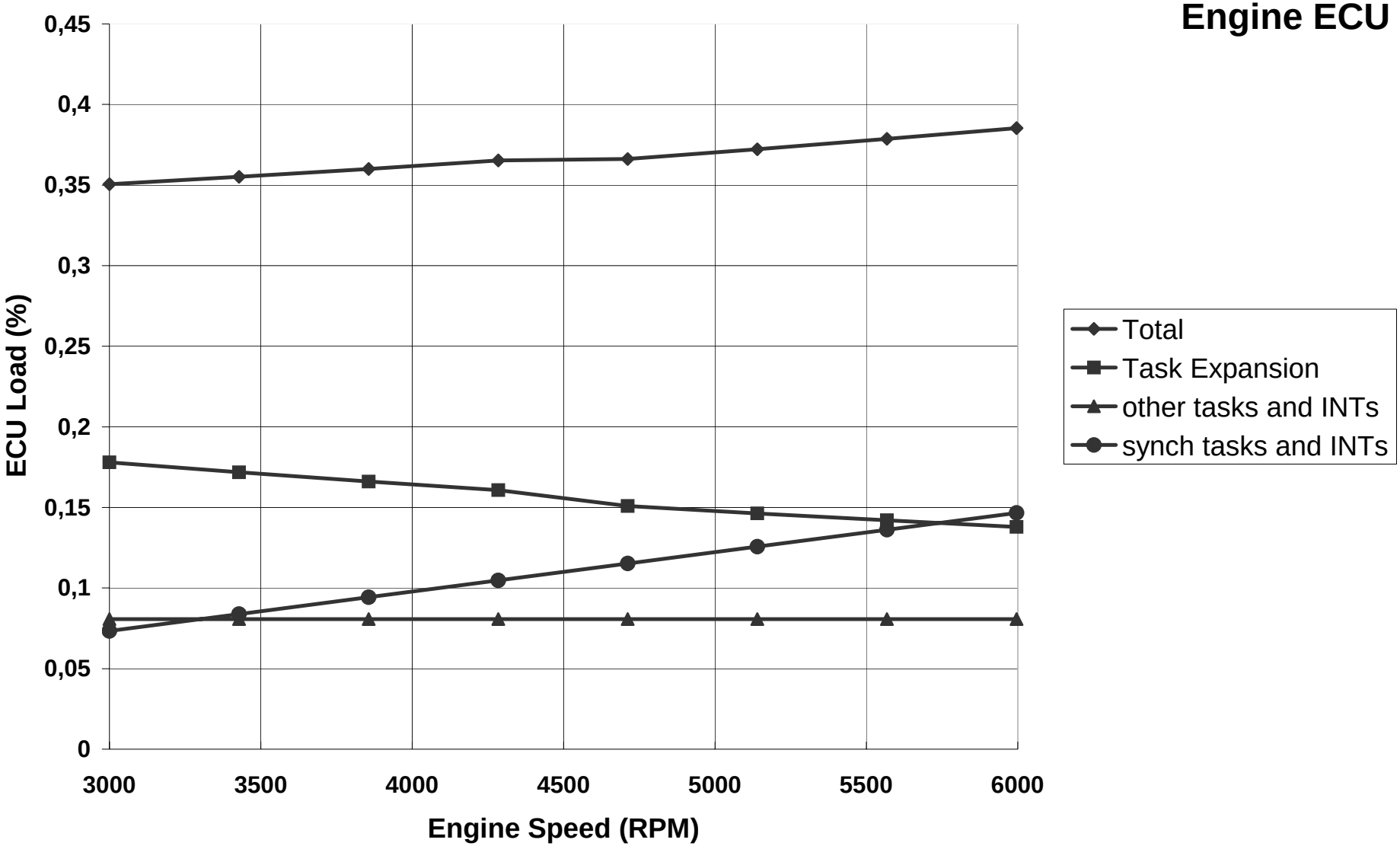
- Accuracy issues:
  - chained task activations w/ preemptive & cooperative tasks
  - alternating task executions (mutex)

Goals:

- automatic analysis of multiple „points of interest“ (RPM curve)
- increasing test coverage, reducing test time/cost
- consideration of platforms (4-, 6-, 8- cylinder engine)

Results I – Characteristic Load Curve

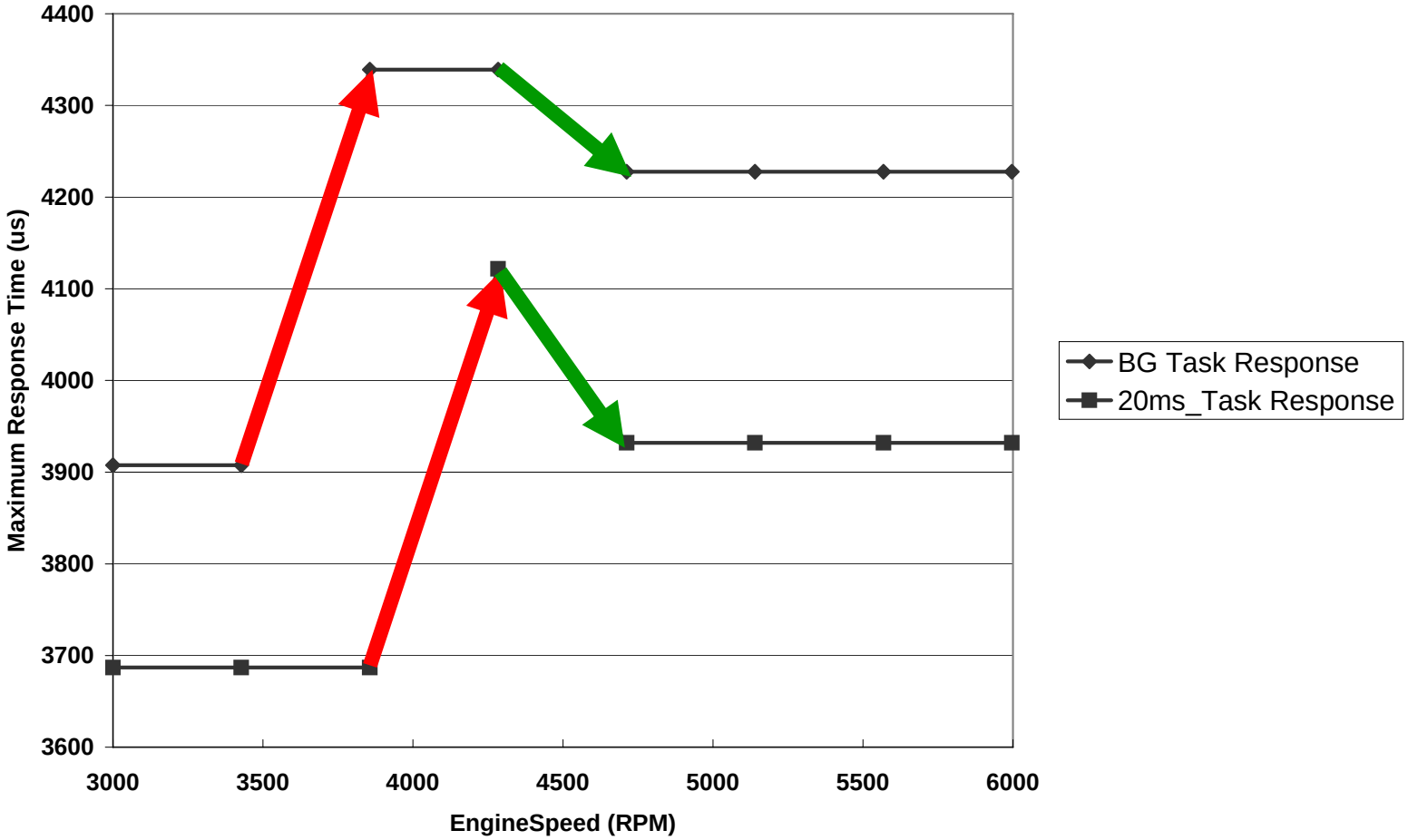
Engine ECU



Results II – Detecting "Anomalies"

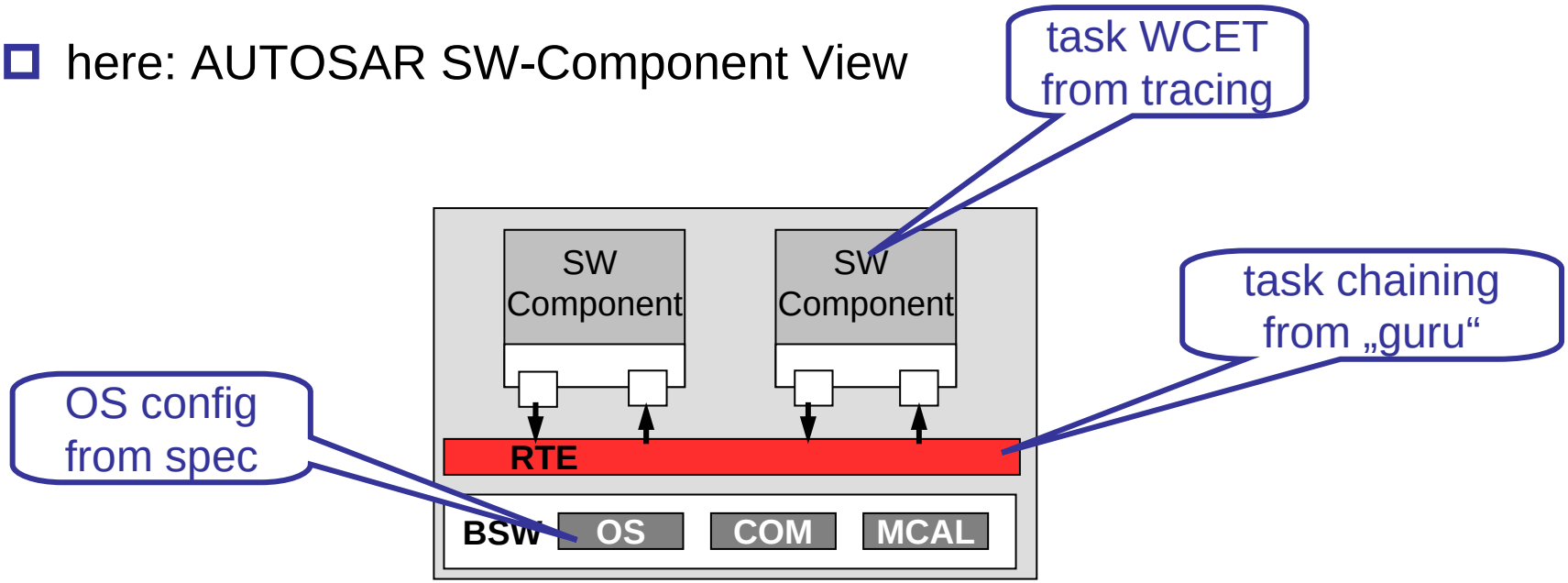
Additional preemption by RPM-synchronous tasks (increases task interference)

Task cut-off (reduces core execution time)



Where are the Components? Where is the Data?

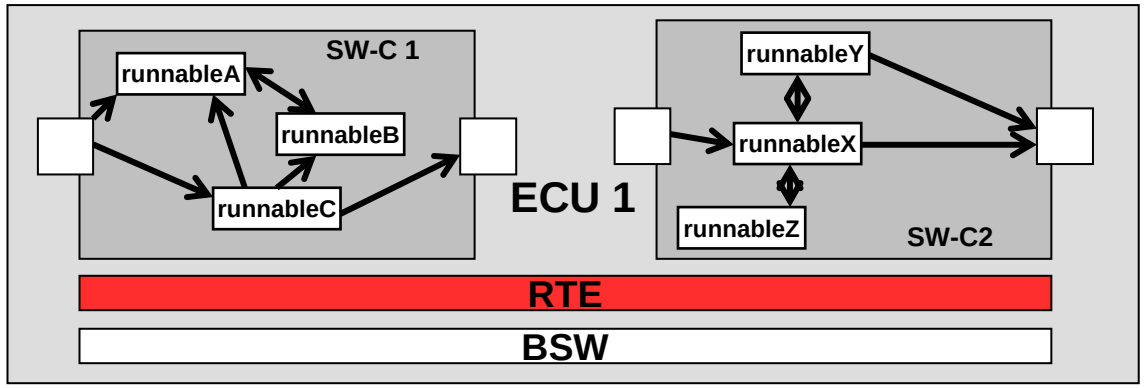
- here: AUTOSAR SW-Component View



- not covered, very specialized:
  - sophisticated „task expansion“ mechanisms
    → we personally talked to „the architecture guru“
  - engine interrupt events
    → customer could NOT deliver that info (although in-house)

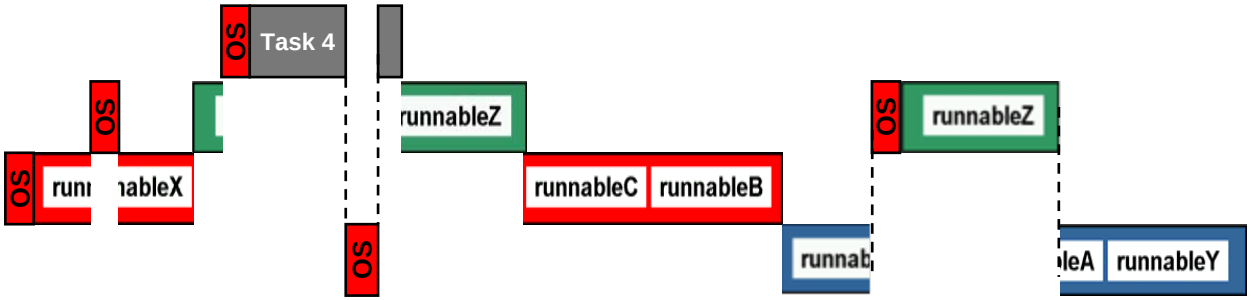
SW-Components vs. "Runnables" and Tasks

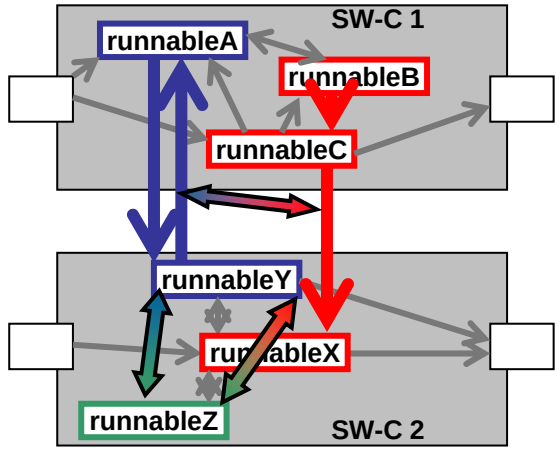
- SW architecture:
  2 SW components,
  6 runnables



- Implementation: 3 Tasks

- Schedule and timing dependencies



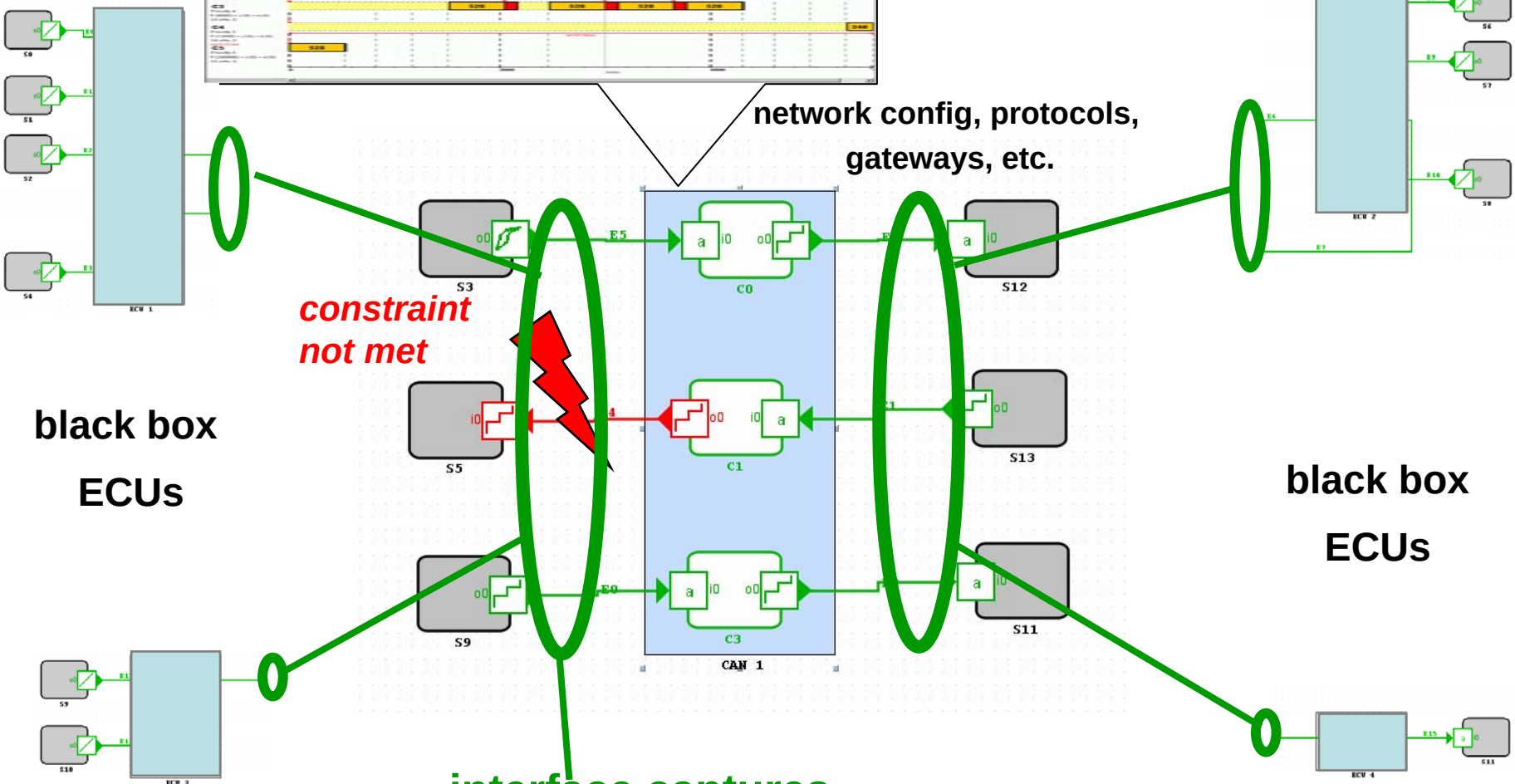


Outline

- Compositional system level analysis with SymTA/S (short overview)
  - Basic formal model
  - Iterative system level analysis
- Components and formal analysis in the automotive industry
  - Requirements
  - Supply chain issues
  - Relation to AUTOSAR
- Two case studies
  - Supplier view: engine ECU analysis (ERCOSEK)
  - OEM view : CAN Bus Bottleneck Detection
- Conclusion

OEM View: Control Timing on Bus/Network

network config, protocols, gateways, etc.

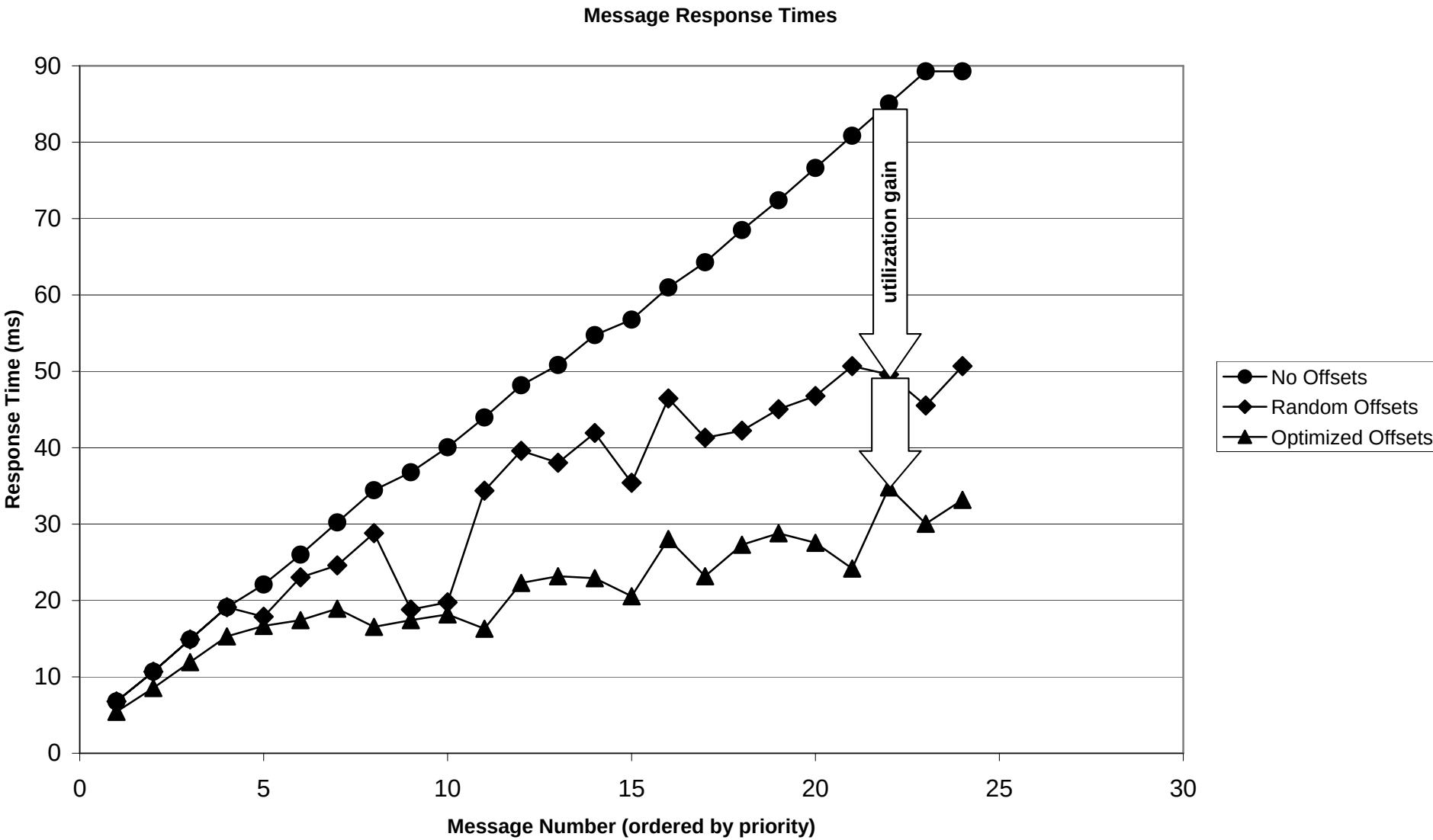


Screenshots by SYMTA

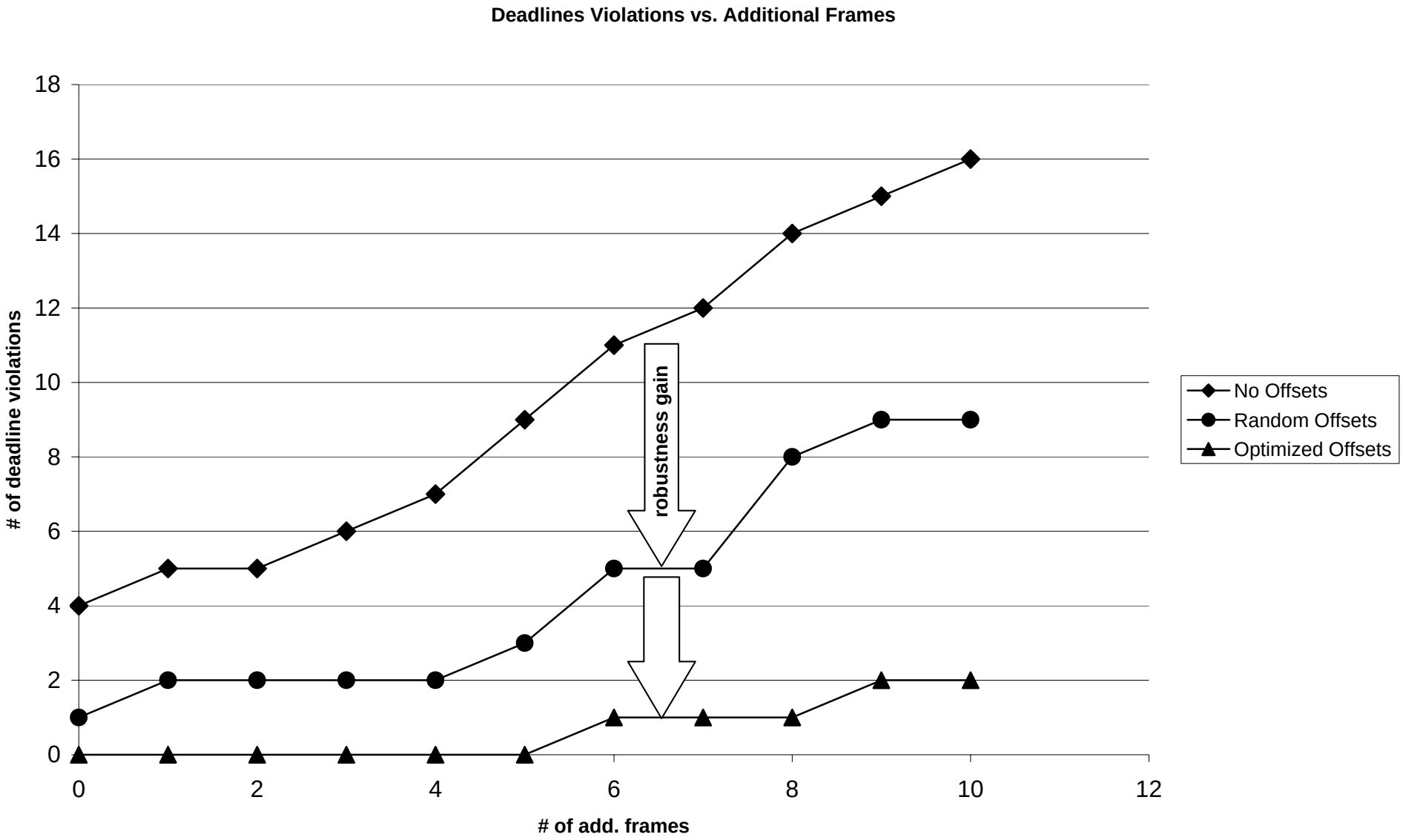
Case Study 2: CAN Bus Analysis

- CAN bus with 10+ ECUs, 70+ frames, 200+ signals
- specialties
  - periodic, direct, and mixed *frame transmission modes*
  - pending and triggered *signal transfer properties*
- accuracy & complexity issues
  - frame „offsets“ (time-driven)
  - dynamic mixed frames (data-driven)
- Goals
  - determine „quality“ of bus utilization
  - determine flexibility / extensibility
  - control robustness against additional frames

Results I – Offset-Dependent Frame Response Times

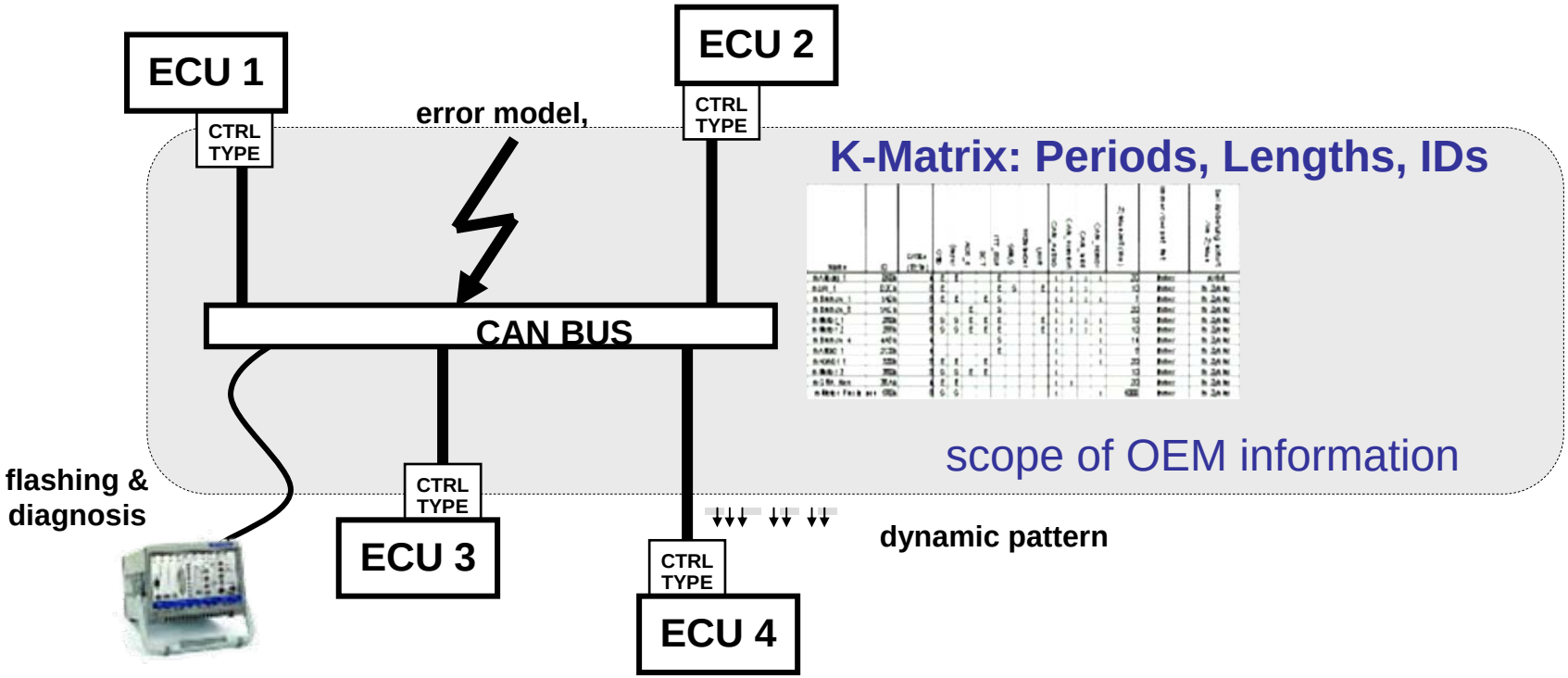


Results II – Robustness Against Additional Frames



Where are the Components? Where is the Data?

- no AUTOSAR Bus-View available →„own“ model



- not covered, even though generally important:
- frame offsets & dynamic behavior of „triggered“ signals
  → is ECU-specific, mostly unknown to OEMs
  → good news: „what-if“ analysis is possible

Conclusion

- Formal performance verification in industry design
  - Existing techniques from real-time research are a good starting point …
  - …but need to be extended to be “industry-ready”
- Compositional performance analysis methodologies adequate for industrial supply chain
  - Enables performance verification…
  - …while protecting IP
- Problem of data unavailability can be partially circumvented by “what-if” analyses
  - Speed as an advantage of formal analysis techniques
- Standardization helps but is slow!

Institute of Computer and
Communication Network Engineering
TU Braunschweig, Germany

SYMTA VISION

Scheduling Analysis in the Automotive Design Flow

Kai Richter, Marek Jersak - Symtavision GmbH

Arne Hamann, Rolf Ernst - TU Braunschweig