Findings of the Artist2 Workshop "Beyond Autosar"

Werner Damm

OFFIS

Acknowledgements

- This presentation reports on Results of the NoE Artist2, Workshop "Beyond Autosar" (co-organized with Albert Benveniste, INRIA)

- All rights rest with the contributors – see individual acknowledgements in sections of presentation

Structure of Presentation

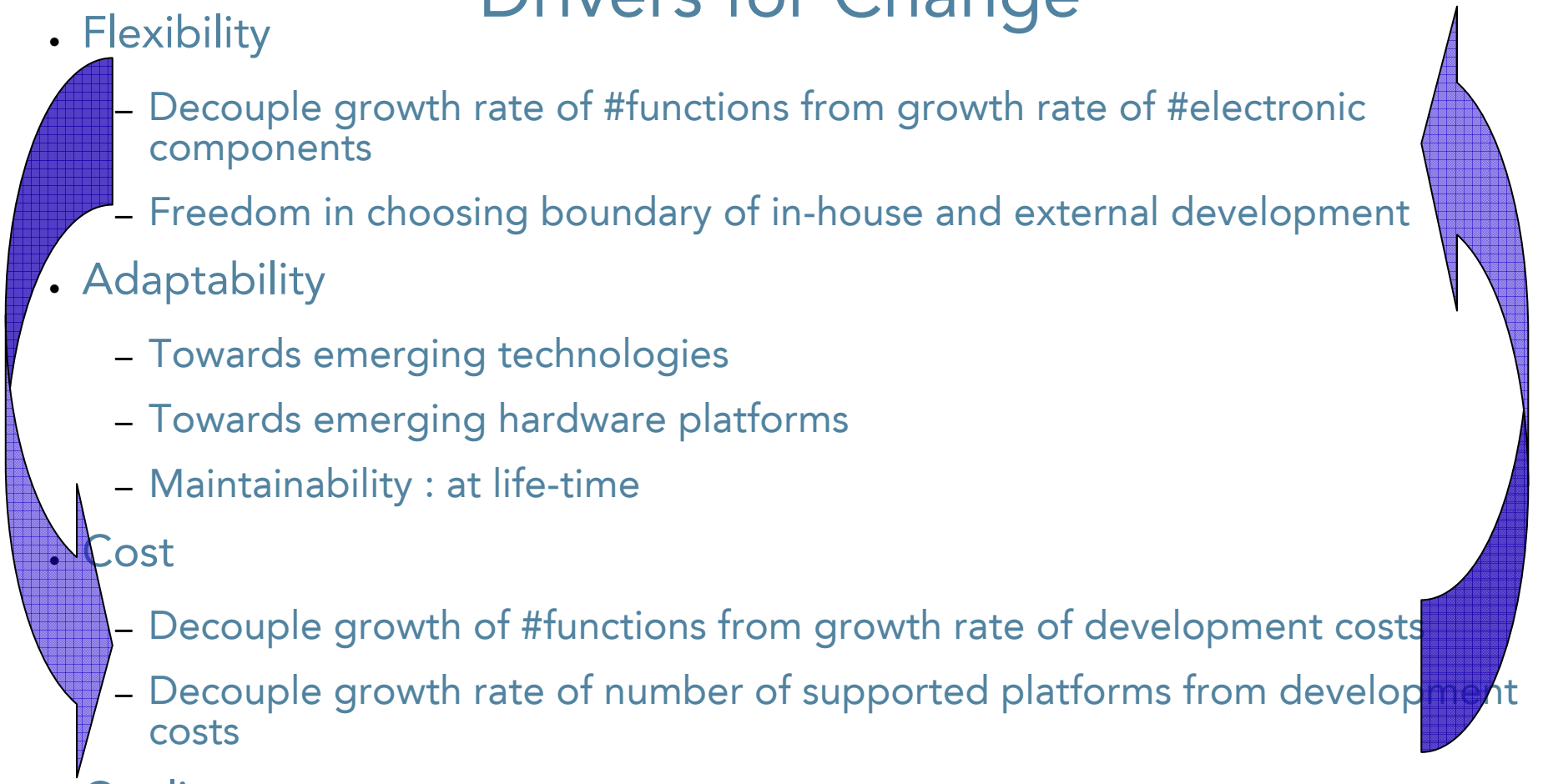
- (The Automotive Market)
- The Autosar Approach
- Impact and Challenges on Real-Time Analyis
- Impact and Challenges on Control
- Impact and Challenges on Safety Analysis
- Impact of the Beyond Autosar Meeting

The Autosar Approach

Based in part on presentation by Christian Salzmann, BMW CarIT at workshop *Beyond Autosar*

Drivers for Change

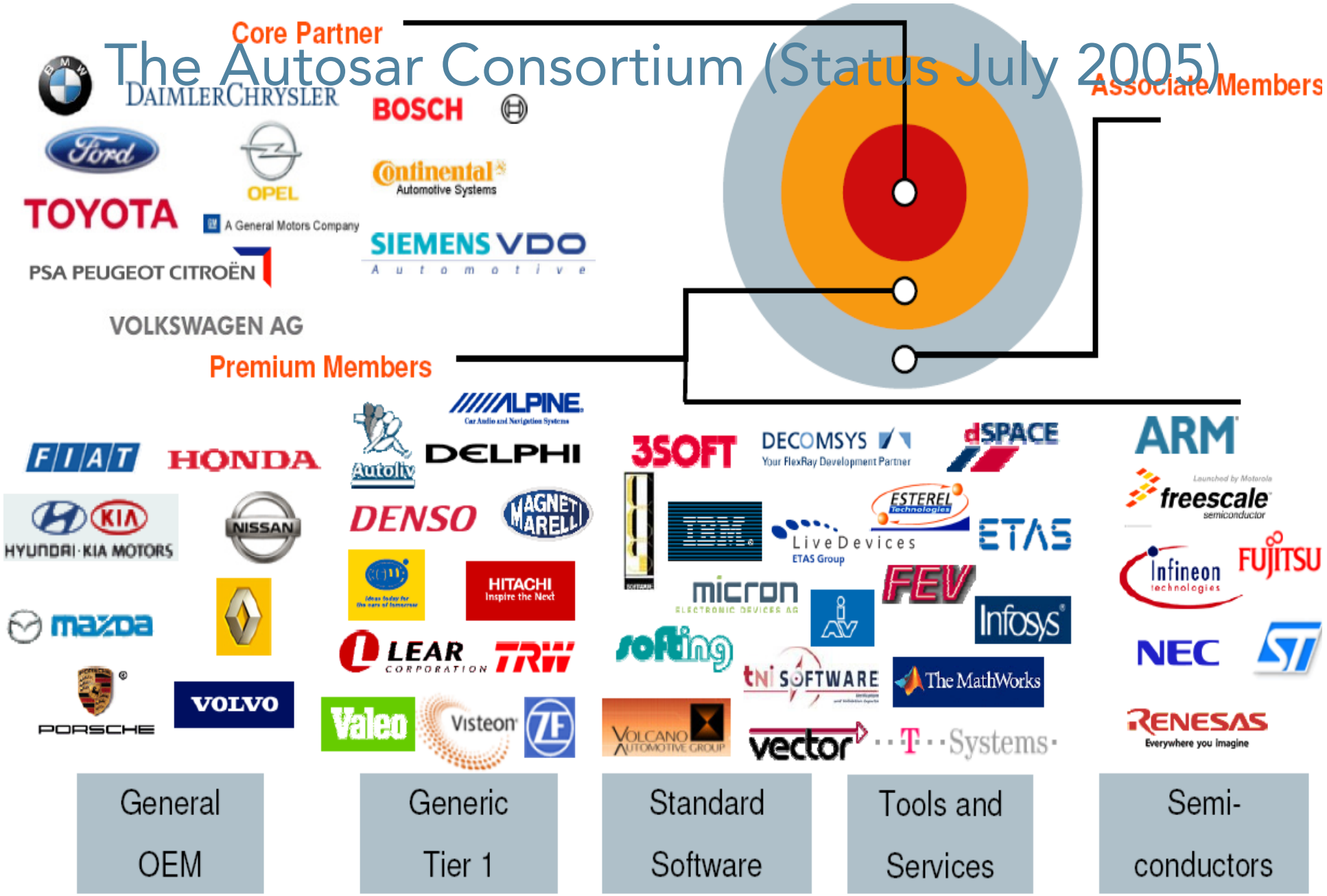
- Flexibility
  - Decouple growth rate of #functions from growth rate of #electronic components
  - Freedom in choosing boundary of in-house and external development
- Adaptability
  - Towards emerging technologies
  - Towards emerging hardware platforms
  - Maintainability : at life-time
- Cost
  - Decouple growth of #functions from growth rate of development costs
  - Decouple growth rate of number of supported platforms from development costs
- Quality
  - Maintain/Improve Quality while allowing growth of #functions



Anticipated Changes in Processes

- Strong push to virtual subsystem models (function-level) for time reduction
  - Target independent
  - Topic in Autosar
- Strong push towards component based development
  - Topic in Autosar
  - Requires component characterizations dealing with non-functional aspects (e.g. real-time, safety, ...)
- Need to boost quality
  - to support IEC 61508 customized to automotive domain – safety cases
  - Reduce number of re-calls
  - Topic in Autosar
- Deployment analysis capabilities will be key competence
  - for price-competetive offerings of tier 1 supliers
  - For realizability analysis of new functions for innovator OEMs

The Autosar Consortium (Status July 2005)

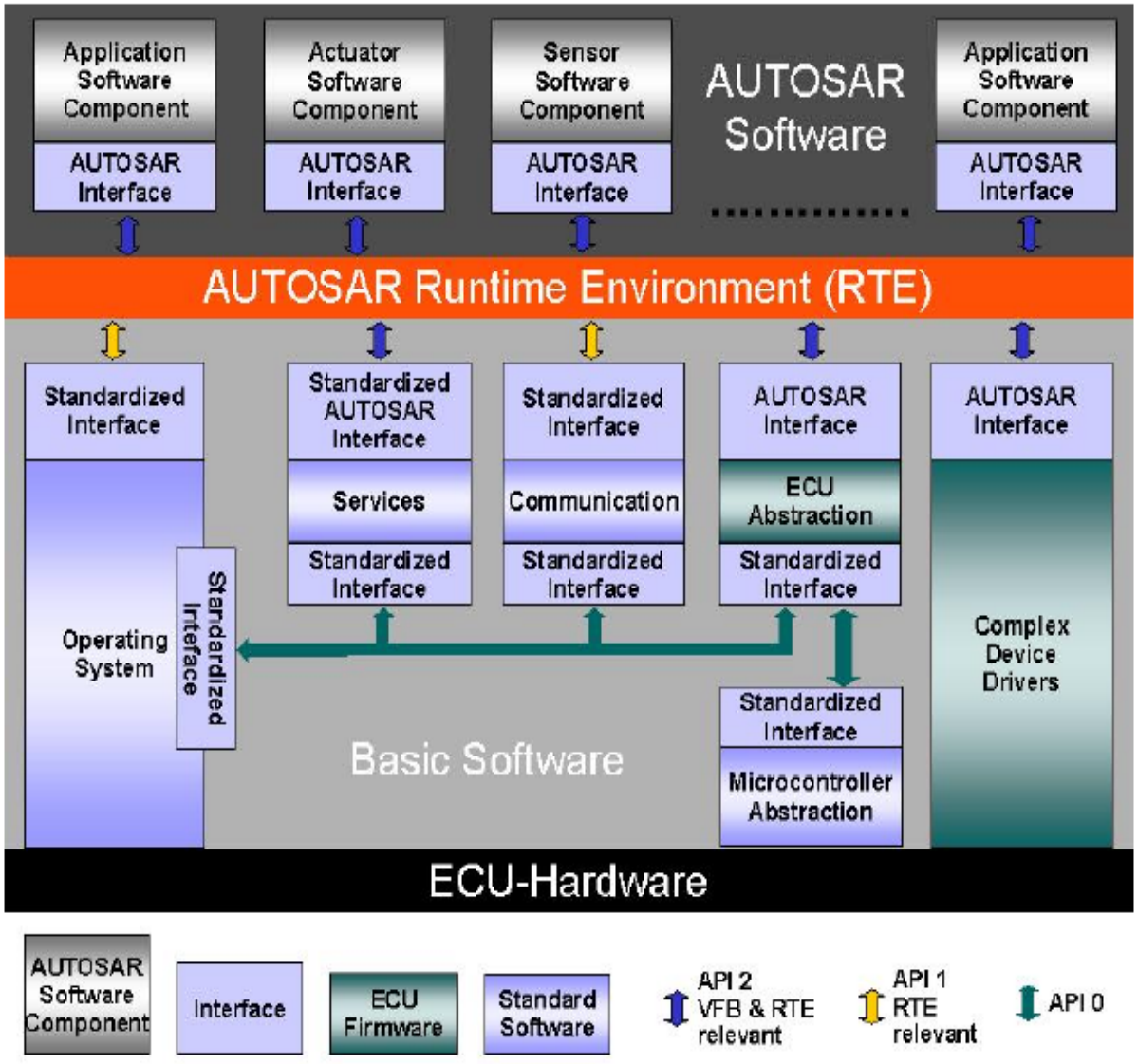


Standardization

© BMW CarIT

AUTOSAR

AUTOSAR – ECU Software Architecture



Automotive Open System Architecture (AUTOSAR):

- Standardized, openly disclosed interfaces
- HW independent SW layer
- Transferability of functions
- Redundancy activation

AUTOSAR RTE:
by specifying interfaces and their communication mechanisms, the applications are decoupled from the underlying HW and Basic SW, enabling the realization of Standard Library Functions.

Highlights

- Strong industrial take up
  - Large privat investment: equivalent to 175 full time staff
  - Accepted on international scale
  - Strong vendor involvement
- Autosar Metamodel defined in UML/OCL
  - description of SW-Cs, their interfaces and resource needs
  - description of HW resources, network topologies and communication matrices (covering CAN, LIN and FlexRay).
- Pilot Powertrain demonstration 2005 demonstrated complete flow with minimal overhead against conventional implementation
  - Key to success is to be able to compile away RTE for given configuration (similar to OSEK approach)
- Phase 2 will push towards strong deployment

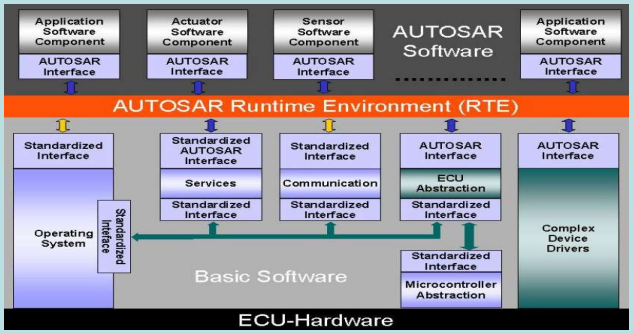
Impact and Challenges on Real-Time Analysis

based in part on presentation of

Kai Richter, Symtavision GmbH

Workshop Beyond Autosar

Integrating Real-Time Analysis Techniques into Autosar Based Design Processes



Hierarchical Task Graphs
End-to-End Latencies

Real-Time Systems Community

Tasks

Messages

Schedulability Analysis

??

The Basic Dilemma

- Autosar is all about decoupling functional design from architecture
- However, response-time analysis is inherently impacted by architectural choices
- Depending on allocation decisions taken late in designs, end-to-end latencies vary drastically from local single ECU implementations to hierarchical distributed designs

Research Challenges I: Bridging the timing gap

- How can we assess early the impact of architectural choices on key system timing characteristics, such as end-to-latencies, so as to assess the feasibility to realize new automotive functions?
- What architectural abstractions are required to perform such assessments with sufficient precision, thus allowing to narrow down the design space?

Research Challenges II: Bridging the timing gap

- How can we decompose overall timing analysis both horizontally and vertically taking into account responsibilities and roles of OEMs and suppliers?
- Can we develop compositional timing analysis methods allowing to decouple global timing analysis into local analysis within the scope of OEMs/suppliers?
- Which expressiveness for timing interface specifications of components is required to support compositional timing analysis?

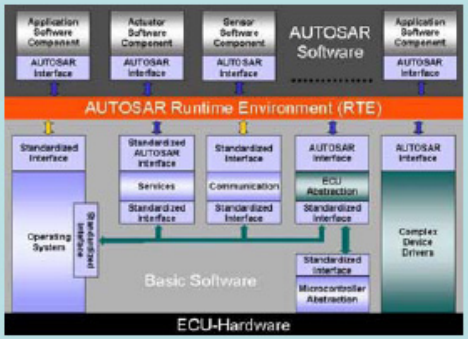
Impact and Challenges on Control

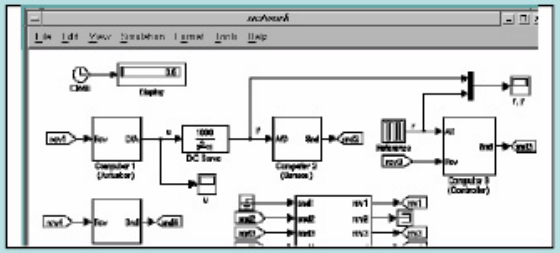
based in part on presentation of

K.-E. Arzen, Lund University

Workshop Beyond Autosar

Integrating Control Design in Autosar Based Development Processes





Simulink components

Control Community

Stateflow

Real-Time Workshop

Model-based design

Robustness

Stability

??

"Autosar"

"Matlab/Simulink"

The Basic Dilemma

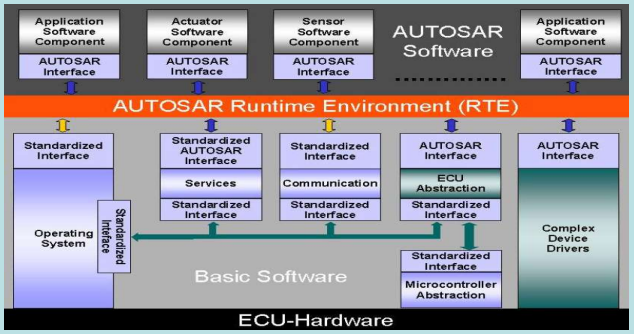
- Autosar is all about decoupling functional design from architecture
- However, control design is inherently impacted by architectural choices
- Depending on allocation decisions taken late in designs, control-loop implementation varies drastically from tight closed loop control to hierarchical distributed control

Research Challenges

- How can we assess early the impact of architectural choices on stability and controllability? What architectural abstractions are required to perform such assessments with sufficient precision?
- How can we design control strategies sufficiently robust so as to "smoothly degenerate" when implemented in a distributed fashion? Can we learn from the analogy to QoS requirements in soft real-time vs hard real-time?
- What degree of determinism must be provided by interconnects? E.g. trade off between latency and determinism between time-triggered and event triggered solutions.
- How can we re-use control-components in spite of possible drastically varying architectural choices in given implementations (tied to Q1)?
- How can we assure key control properties such as stability (or stronger variants) in a compositional way? C.f. also work on distributed implementation of self-stabilizing algorithms.

Impact and Challenges on Safety

Integrating Safety Analysis Techniques into Autosar Based Design Processes



ISO WD 26262
ASIL Levels

Safety Plan
Safety Cases

FMEA, Fault Trees
Common Cause Analysis

Failure Hypotehesis

Functional Safety

??

ISO WD 26262 – a forthcoming safety standard for the automotive industry

- IEC 61508 Metanorm for Safety Critical Systems
- Many application domains have derived domain specific versions of this metanorm
  - E.g. CENELEC EN 50126, 50128, 50129 for Railway Systems
- Ongoing initiative to establish harmonized derivation of IEC 61508 for automotive applications
  - No public draft available
- Calls for establishment of safety cases
- Consideration of availability and safety top priority in Autosar

Research Challenges I:

- How can we assess early the impact of architectural choices on key system safety aspects, so as to assess the feasibility to realize new automotive functions?
- What architectural abstractions are required to perform such assessments with sufficient precision, thus allowing to narrow down the design space?

Research Challenges II:

- How can we decompose overall safety analysis both horizontally and vertically taking into account responsibilities and roles of OEMs and suppliers?
- Which expressiveness for safety interface specifications of components is required to support compositional safety analysis?

Expected Impact of the Artist2 Workshop Beyond Autosar

Public Dissimination

- Presentation as Keynote Lecture at EMSOFT 2006
  - Available from the Artist2 Website
- Detailed Minutes
  - Available from the Artist2 Website
- Written Report under Preparation, to be published in applied journal addressing application domain

Research Impact

- Challenges are partly addressed in recently launched research projects involving Artist2 participants
  - Integrated Project Speeds
    - INRIA, OFFIS, Parades, Verimag
    - Airbus, Bosch, DaimlerChrysler, Israeli Aircraft Industries, Magna Powertrain, Knorr Bremse, Saab
    - Esterel Technologies, Extesy, Telelogic, TNI
  - IST Project ATEST
    - Develops a UML Profile EAST-ADL2 for automotive architecture and component modeling compatible with the Autosar metamodel
    - Involves KTH and CEA from Artist2

Technical Highlights of the IP Speeds

- Speeds provides
  - The capability of Modeling and Integration of Architectural Abstractions at all System Design Levels for multiple viewpoints including real-time and safety
  - A Rich Component Model allowing to completely encapsulate functional and non-functional aspects of a design in an assume-guarantee style with cross viewpoint dependencies, including the capability of expressing assumptions on lower design levels captured as architectural abstractions
  - A harmonized meta-model allowing a semantic integration of industry standard system- and software design tools supporting rich components based on an open tool integration standard, compatible with the Autosar Metamodel
  - A suite of compositional analysis and design space exploration methods supporting real-time and safety analysis

Impact on Roadmapping Activities

- The findings will be integrated in the Artemis Roadmapping Activities through direct participation of Artist2 Members in the Artemis Working Groups
- The findings will be integrated in the Roadmapping Activities of SafeTRANS through direct participation of Artist2 Members in the SafeTRANS Steering Board
- The findings of the meeting will be presented to the Current and Past Chair of the Autosar Consortium
  - Dr. Helmut Fennel, Continental Automotive Systems
  - Dr. Thomas Scharnhorst, Carmeq GmbH