Beyond Autosar: Challenges and directions

Martin Törngren, KTH
Royal Institute of Technology, Stockholm, Sweden
Embedded systems model based (integration) approaches

- All in one ~ multi-paradigm modeling
- E.g. UML2 and profiles
- Architectural design
- Model and tool integration approaches
- E.g. co-simulation, transformations
- Information/configuration management approaches
- E.g. PDM/SCM+new tools
- Software & hardware: Component based development
- E.g. AADL, Autosar, ...

Immature; Convergence?
Timing and safety/reliability

Timing issues
- Researched intensively - still open issues
- Key issue: adapt and transfer techniques to industry

Safety and reliability issues are more open
- Safety is system related
- Reliability is related to components
- Division of responsibilities: Architecture / components
  - Error detection, error diagnosis, error handling
- Design assumptions
- Hardware/software dependencies
- Test profiles
- Requirements& properties to state for components?

Has to consider functional level for design & reuse
- SW component level is insufficient
Concerns related to Autosar

Lack of systematic modeling and analysis
- Non-functional aspects: e.g. timing, fault-propagation, other design assumptions – required and actual behavior
- Functional reference architecture
  - To enable functional integration and to avoid feature interaction

Structured information management including software
- A fundamental enabler for analysis
- Development/production/maintenance, PDM/SCM
- Domain tool integration

Elaborated design methodologies
- Optimization, dependencies/trade-offs in the design-flow
- Systematic analysis

Dynamic configuration
- Modes, fault tolerance, upgrades, integration

Martin Törngren, Embedded Control Systems/Mechatronics, KTH
Directions towards solutions

Open up Autosar

This is the time to join forces between academia and industry to incorporate timing models into Autosar

Needs to consider solutions e.g. from
- MARTE, AADL, timing analysis communities

Different timing requirements for different automotive applications/domains have to be considered

Handling of timing:

Timing requirements established/derived from system (functional) level requirements

Implementation requirements/design can be established through synthesis or by implementation design followed by analysis, and subsequent iterations