Timing model and methodology for AUTOSAR

It was soon realized that AUTOSAR required new methodologies and models to properly address performance and timing requirements in system design. The TIMMO consortium is currently developing solutions that will allow virtual architectures to be mapped on physical hardware reliably and cost-effectively.

An increasing number of functions are implemented in modern automobiles as distributed systems. Adaptive cruise control, for instance, needs a minimum of five ECUs (engine, gearbox, braking, MMI, radar). Mastering the overall timing behavior of a distributed system is a fundamental requirement in highly sophisticated control solutions, especially in the power train and chassis domains. The modern automobile has to be seen as a complex network of distributed embedded control systems with hard realtime constraints.

Take sensors for example, connected to one network node and communicating with an actuator connected to another node (**Fig.**). The different software components (SW-Cs) mapped onto different ECUs form a distributed control system. End-to-end timing from sensor to actuator must meet a specific deadline derived from application requirements. Bus timing, ECU timing and the timing of the communication controllers all have to be taken into account to fulfill requirements.

Possibly timing may have to be optimized across multiple suppliers, a challenging task in a complex distributed system. A key result of TIMMO will consequently be a systematic approach to timing constraints in the design of complex automotive embedded systems. The project objectives are:

- Improved, predictable development cycle
- Capturing and verifying end-to-end timing constraints from requirements to implementation
- Formal and standardized specification, analysis and verification of timing behavior at all abstraction levels

A potential scenario in the chassis domain, derived from a basic example (Fig.):

- ECU 1 is a sensor cluster that contains many sensors and performs sensor fusion. It generates virtual sensor signals from separate real sensor values by aggregation. This avoids redundant sensors in an automobile.
- ECU 2 is a standard ECU as commonly used in the automobile industry.
- ECU 3 can be an intelligent actuator, connected to the control actuator via a bus.

Another common scenario is the integration of new, still untypical functions in a specific ECU. The goal is to properly dimension the network and the ECU, and to use available resources as effectively as possible. Therefore the timing requirements and constraints of different functions and OS tasks and the communication effort have to be taken into account. Effectively supporting cooperation between OEMs and suppliers is another key issue to be addressed.

A time-triggered bus system like FlexRay is one solution to designing high-performance, distributed open-loop or closed-loop control systems. The absence of communication jitter and uncertainty simplifies the design of new, distributed control algorithms. With FlexRay, determinism comes at the cost of flexibility. As today's E/E ar-

The TIMMO consortium

Members of the TIMMO consortium: Symtavision, Audi, Bosch, Carmeq, Chalmers University (Sweden), Continental, ETAS, Paderborn University (Germany), Siemens VDO, TTTech, Volvo, ZF.

chitectures evolve, one of the challenges will be to achieve predictability, flexibility and efficiency in mixed time- and event-triggered systems.
Yet another approach is to concentrate functions in domain control units, thus localizing the integration issues and reducing the need for further high-speed buses. Regardless of the type of architecture, timing analysis and performance optimization will play a key role in software and system integration.
The goal of TIMMO is to support developers with new methods, models and tools. A predictable development process that systematically addresses timing and performance issues in all phases, from early exploration through final verification, is the key to handling the complexity of new innovative features. Otherwise a considerable number of functions cannot be implemented cost-efficiently, and so may not be implemented at all.
TIMMO intends to develop a practical, common approach to the question of timing throughout the development process. It will define a solid, theoretical basis for addressing the timing aspects of distributed embedded automotive systems, and develop an accompanying methodology founded on systematic analysis that explicitly includes cross-company tool interoperability and appropriate exchange formats.

The TIMMO language

A major objective of TIMMO is to define a timing-augmented description language (TADL) that can bridge the specified application requirements and development methodology. To that end TADL should be able to model system aspects such as:

- Properties of hardware resources and time-consuming elements
- Relationships between time-consuming elements
- End-to-end timing constraints and their breakdown structure over several resources
- Relationships of time-consuming elements and resources

TADL syntax is formalized as a meta model written in the unified modeling language (UML). To guarantee homogeneity of the TADL meta model and simplify understanding, a guide will be provided. This will list rules and common patterns to be used in definition of the TADL meta model, and also constitute the basis for TADL semantics. The meta model of TADL defining its domain view will be translated in terms of a UML profile, thus making it possible to use TADL concepts in the context of UML models.
An exchange format is to be defined for the transfer of design data between future TADL-compliant design, development and analysis tools. The TADL model exchange format will be XML-based and thus an XML scheme is to be defined. To provide an efficient exchange format, the TADL model exchange format will be defined by transformation rules between the TADL meta model and the XML scheme.
TADL semantics are defined on the basis of the provided meta modeling guide and described in the form of UML classes. To identify valuable input, the outcome from similar initiatives will be taken into account, such as the AUTOSAR timing team or OMG MARTE (object management group, modeling and analyzing realtime and embedded systems). To ensure the correctness of a TADL model, care is to be taken that each concept introduced in the language can be analyzed and verified.
To validate the functions of TADL, a model editor will be developed in parallel with the meta model of the language. The editor is based on a model-driven architecture approach that makes it possible to generate large parts of a software tool from a UML model and to minimize the amount of hand-written model-specific code. The technology used to specify and develop the TADL model editor is based on the Eclipse modeling framework (EMF). Using EMF it is possible to describe a meta model and then automatically generate the model. The TADL model editor will be delivered as an Eclipse plug-in by building TADL as an extension of an existing language.

Validating results

The TIMMO project will perform several proof-of-concept studies to consolidate the developed means and demonstrate their real-world applicability for the exchange of timing information and constraints. One focus is on managing, refining and transferring timing information and constraints between suppliers and OEMs during the different phases of the development process. In that context it is of special interest to detect and react on potential timing problems as soon as they become visible. During early phases the focus is on architecture optimization for costs, scalability and maintainability, whereas in later phases the focus lies on timing verification for robustness, reliability and performance.
In general, the validation of project results covers two main aspects:

- Tool and process interoperability
- Complete validation of the handling of timing properties and requirements during all development phases

The project will demonstrate compatibility of the developed process and language with the AUTOSAR standard, also addressing upgrades for upcoming releases. To validate the complete coverage of timing-related issues, including interrupts, blocking, preemptions, offsets or startup delays, TIMMO will perform different case studies, which are currently being defined. The studies will focus on power train systems, for which the TIMMO results are of considerable interest. Implementation will be on evaluation boards or close-to-series control units in a laboratory environment.
One planned case study will focus on a single ECU, which could be an engine management system (EMS) implemented using the AUTOSAR specification. The goal then is to investigate timing characteristics of AUTOSAR basic software and timing-related annotations in the meta model, as well as the extension and integration of software functions on the ECU.
Another case study will investigate timing aspects for a FlexRay-based system with applications allocated to different ECUs that are relevant for the power train. FlexRay is scalable via multiple parameters, including speed, number of slots, bytes per slot, idle time between static and dynamic segments. This makes it highly sensitive to changes that may significantly affect time-related system properties like clock synchronization, end-to-end latency, and efficient bandwidth use. Here the relocatability of tasks between ECUs and trade-off analysis between fixed and variable schedules are of major interest.
Tools from different vendors involved in TIMMO are used as a starting point for an AUTOSAR-compliant tool chain based on the TIMMO approach. Existing tool couplings between ASCET (www.etas.com), SymTA/S (www.symtavision.com) as well as third-party tools already allow management of execution time bounds through static code analysis, scheduling analysis and measurements. TTTech Automotive (www.ttautomotive.com) and Symtavision will include FlexRay tools for system-level case studies. Other tools will be added as needed. *Jersak et.al./sj*

Figure see page 10
Typical end-to-end timing situation of a sensor/actuator system.