Development of Automotive Communication Based Real-Time Systems - A Steer-by-Wire Case Study

Kay Klobedanz, Christoph Kuznik, Ahmed Elfeky, and Wolfgang Müller

University of Paderborn/C-LAB
Faculty of Electrical Engineering,
Computer Science and Mathematics,
33102 Paderborn, Germany
{kay.klobedanz,christoph.kuznik,ahmed.elfeky,wolfgang.mueller}@c-lab.de

Abstract. Safety-critical automotive systems must fulfill hard real-time constraints to guarantee their reliability and safety requirements. In the context of network-based electronics systems, high-level timing requirements have to be carefully mastered and traced throughout the whole development process. In this paper, we outline the management of scheduling-specific timing information by the application of a steer-by-wire design example. We apply the principles of the AUTOSAR-compliant Timing Augmented Description Language (TADL) following the methodology introduced by the TIMMO project[2]. Focus of the example will be the identification of end-to-end timing constraints and their refinement by means of stimuli-response event chains.

1 Introduction

The development of embedded automotive electronic systems is at a turning point. Modern cars incorporate multiple embedded electronics systems and contain complex distributed heterogeneous bus networks like FlexRay^{TM}and CAN. For example, in the year 2004 the embedded electronic system of a Volkswagen Phaeton was composed of hundreds of electrical devices like sensors and actuators, 61 microprocessors, three controller area networks (CAN) and several subnetworks [1]. It is estimated that the average vehicle electronic and software part will rise continuously from its current level of 13 percent of the car's value up to 14.8 percent in 2012 [8]. Despite the first automotive electronics were mainly targeted in the power train domain, recent activities aim to replace traditional mechanical components by their electronic counterparts within the chassis domain. Developing electronics in these safety-critical domains like power train (i.e., control of engine and transmission) and chassis (i.e., control of suspension, steering, and braking) puts many constraints on reliability and predictability onto these components. Especially worst-case timing behavior is becoming more and more relevant to comply with European safety norms like IEC EN 61508 and the automotive focussed version ISO 26262 [10]. For example, a brake-by-wire

A. Rettberg et al. (Eds.): IESS 2009, IFIP AICT 310, pp. 218–225, 2009.

system should react as fast as possible. The designed technical solutions must ensure that the system is dependable (i.e., able to deliver a service that can be justifiably trusted) while being cost-effective at the same time [1].

An example is the Steer-by-Wire concept, whereas all driving commands are propagated electrically. Therefore, the steering wheel is no longer mechanically linked to the front wheels of the car but a system of sensors and actuators perform that way. As additional challenge a typical design process consists of one or more OEMs and several TIER-1 suppliers, which may again have sub contractors. Within in this complex product chain the responsibility for fulfilling end-to-end timing requirements is split between the involved partners [9]. This design trend demands methodologies augmented with timing and verification information in order to avoid costly iterations due to the fact that the actual integration of all distinct developed components takes place as recently as within the last design stages.

Within the TIMing MOdel (TIMMO) ITEA2 project[2] an EAST-ADL[6] based meta model was developed to capture timing requirements right from the most abstract levels of the design process to enable right by design timing behavior. We will show how the TIMMO concepts and the modeling of event chains can be used to gain extensive knowledge and coverage of the intended system timing behavior right from the first design decisions. Therefore, we will describe how the TIMMO concepts are efficiently used for the development of a steer-by-wire validator. Moreover, we will place comments on usability and effectiveness of the proposed workflow.

In Section 2 we will introduce the developed concepts and abilities of the TIMMO project. Thereby, we will focus on the Timing Augmented Description Language (TADL) event chain descriptions of TIMMO. Section 3 will describe how we made use of the TIMMO concepts for the steer-by-wire validator development. Finally, section 4 will draw conclusions with consideration of the designers and end-users' perspectives.

2 Methods and Concepts

Nowadays many different manufacturers and suppliers are involved in the development of modern automotive hardware and software components. Therefore, a standardization of the development process and the corresponding ex-change-formats among the manufacturers is desirable. This standardization is mainly accomplished by model-driven approaches like AUTOSAR and EAST-ADL2. AUTOSAR focuses on implementation relevant aspects, e.g. separation of software development and underlying hardware architecture. EAST-ADL2 addresses the description and refinement of vehicle features on higher abstraction levels [9]. Although a combination of both approaches enables a detailed modeling and implementation of automotive components, a comprehensive formalization of timing constraints throughout the whole development process is still missing. The TIMMO project introduces a methodology and workflow with the desired coupling of AUTOSAR and EAST-ADL2 (see figure 1). Moreover this

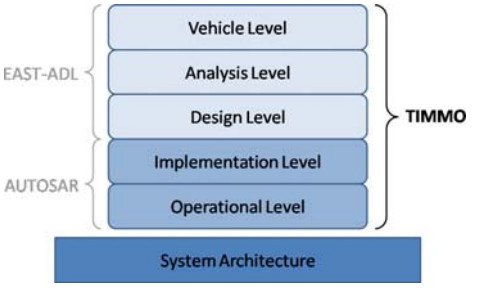

Fig. 1. Coupling of different design levels within the TIMMO project

approach allows the description of timing constrains using the stimuli-response event chains of the Timing Augmented Description Language (TADL). In general, timing information can be distinguished into timing requirements (what is demanded), timing properties (what is offered) and timing contracts (what is negotiated between stakeholders) [9]. In the following we will give a detailed overview of the syntactically and semantically properties of the TADL event chains.

The timing constraints of automotive systems, which are very often register-based multi-rate sampling systems, can be formalized well by the introduced event chains. The element of an event chain with an input register r is further specified by several attributes. These parameters are:

- **Period** T
  Specifies the period of the element, e.g. period of a task execution.

- **Sampling Period** T_r
  Describes the period at which the element reads data. T_r does not have to be equal to T.

- **Writing Period** T_w
  Describes the period at which the element writes data. T_w does not have to be equal to T_r or Tr.

- **Delay** d
  Specifies the time which is needed by the element internally between the stimulus and response, e.g. task execution time.

If there are no detailed information about the internal behavior of a component available, it can be modeled as so-called "black box"-element with the available timing properties (see figure 2). This allows complete verification on higher level of abstraction without having all implementation details on lower levels of abstraction present, for example if suppliers are not willing to share too much data among each other [9].

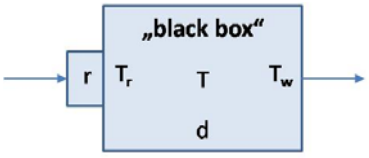

Fig. 2. Model of a "black-box"

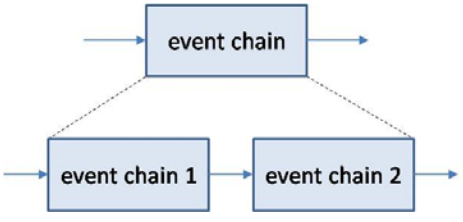

Fig. 3. Example for event chain refinement

TADL allows refinement and composability steps to represent timing on different abstraction levels with event chains. An event chain can be further refined until the actual existing architecture is defined, as shown conceptional in figure 3.

With the principles introduced by the TADL notation it is possible to describe and analyze the system for different end-to-end timing constraints. The most important variants of end-to-end timings in the context of typically automotive systems with sensors and actuators are:

- **Reaction**
  Represents the delay from a certain (sensor) input value until a corresponding (actuator) output value is available. This is essential for fast-response systems like x-by-wire.
- **Age**
  Represents the delay until a certain output (actuator) value is available from a corresponding (sensor) input value. The age of data has a great impact on the quality of control algorithms.

In the next chapter we will describe how we used the presented TADL event chains for the development process of a Steer-By-Wire system.

3 Design and Implementation

In the previous chapter we described concepts and methods proposed by the TIMMO project for the design of real-time automotive systems. Thereby we focused on the stimuli-response event chains as a valuable instrument for the definition and formalization of timing constraints throughout the whole development process. Here we will present how we applied the described approach for the design and implementation of a steer-by-wire-system validator from scratch to evaluate its capabilities.

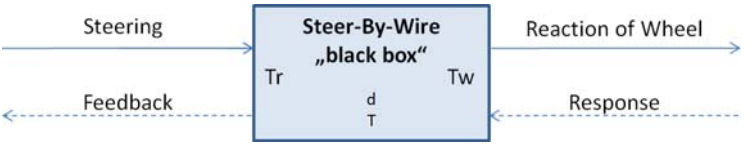

Fig. 4. "Black box"-element for steer-by-wire system

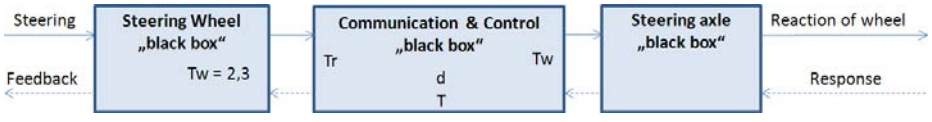

Fig. 5. First refinement step of the event chain with timing properties

At higher abstraction levels the requirements of a steer-by-wire system can be generally formulated for the whole system, e.g.: The reaction of the steering axle and wheel as well as the resulting feedback has to be "instantly". This means that the end-to-end reaction delay is constraint and must not be bigger than a few milliseconds. Based on the information of this abstraction level, we model the whole system as a single "black box"-element within a first abstract event chain (see figure 4).

Like common in the development of industrial automotive systems we use predetermined sensor/actuator components from third party manufacturers. As steering wheel we utilize an existing device from the manufacturer TRW Automotive [3]. This component is equipped with a CAN Interface over which messages with measured sensor values like torque, position and rotational velocity are send with a writing period of $T_W = 2,3ms$. Apart from that, little about the internal behavior is known. Therefore, we will model it as a "black box"-element in the upcoming event chains.

The second major component is a specially designed setup of a steering and damping test bed constructed by the department for control engineering and mechatronics from the University of Paderborn. It is composed of a steering axle with a standard tire and a wheel suspension equipped with active damping. The assembled electric actuating motors are connected to the system via CAN interfaces. The steering testbed is also modeled as a "black box"-element.

A first refinement step of the previous abstract event chain is shown in figure 5 and includes the combination of steering wheel, the steering and a communication & control "black box" element.

On this abstraction level the timing properties of the components of the event chain already allow to conclude properties for other elements of further refinement steps. For example, the given writing period T_w of the steering wheel imposes requirements for the sampling periods T_r of subsequent elements. Here, $T_r \leq T_w$ must hold for the avoidance of undersampling effects, e.g. message loss. The delay of the communication and control "black box" is composed of several subcomponent delays. Hence, an additional refinement step to the functional component level is necessary, to realize a detailed description of the timing

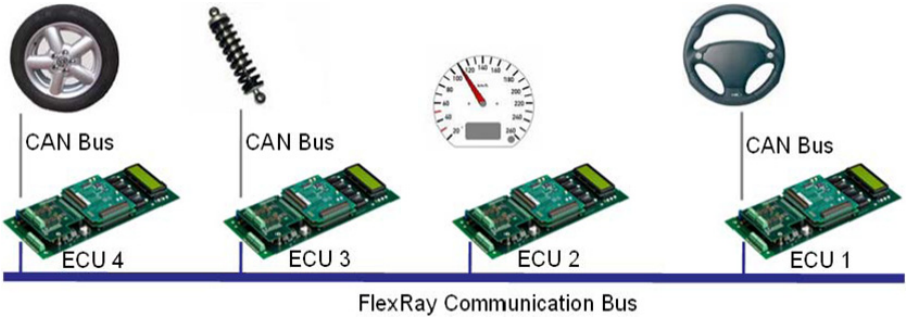

Fig. 6. System Architecture of the Steer-By-Wire Validator

constraints of the system. To allow a detailed definition and analysis of the timing requirements on this abstraction level an identification of the used components and their temporal properties is essential. In the following we give an overview of the functional architecture and components of the communication & control part of our steer-by-wire system.

Architecture. The functionality of our validator is implemented by a distributed communication based system. It consists of the already mentioned actuator and sensor units as well as several electronic control units (ECUs) communicating over a heterogeneous network infrastructure with CAN and FlexRay interfaces (see architecture in figure 6).

Hardware (ECUs). As ECUs we use Universal FlexRay Control Units from TTTech Computertechnik AG[4] with a TriCore TC1796 CPU and integrated CAN interface. The connection between the ECUs and the sensors/actuators is realized via CAN. The Units are also equipped with a FlexRay controller for the communication between the ECUs. Due to the CAN and FlexRay interfaces the ECUs can also act as gateway between these two communication protocols. Like common in distributed automotive systems every ECU is dedicated to a specific sensor/actuator and running a single control task. The implementation of control and communication tasks is based on a cluster design and node configuration realized with a toolchain from TTTech which generates COM-Stacks confirm to AUTOSAR [5].

The previous described complex system and communication architecture in combination with the given hard real-time constraints result in a big challenge for the design and the definition of appropriate schedules for tasks and messages. Based on the information from our defined event chains (writing period of the steering wheel $T_w = 2,3ms$) we set the period T of the FlexRay cycle to $2ms$, which results in an according sampling period T_r and writing period T_w. Additionally the control and communication tasks as well as the other necessary CAN Bus are synchronized to the FlexRay cycle to minimize the end-to-end delays throughout the whole system. The timing constraints of the elements on the functional component level can now be described by the event chain in figure 7 with its significant properties.

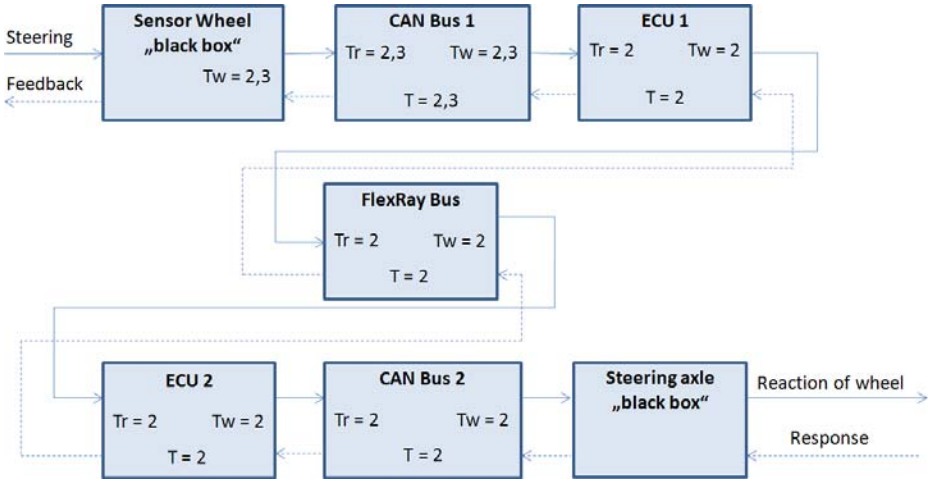

Fig. 7. Event chain of steer-by-wire system on functional component level

The event chain in figure 7 represents the system architecture in a sufficient level of detail for our scope. Therefore, we perform the implementation on this level of abstraction. The implemented communication tasks including the protocol translations for the gated-network components do work correctly regarding the specified reaction end-to-end timing constraints. Experiments with the validator prove that the desired timing requirement of sensed instant reaction between steering wheel and the steering axle, as defined on feature level, is fulfilled. Additionally we made use of worst-case execution time analysis tools, as proposed by the TIMMO methodology. Based on assumptions for the WCETs of the control and communication tasks we get results for the steering path worst-case end-to-end delays which show that our system will react in a few milliseconds, as intended. The worst case-reaction delay for the implementation is estimated to be $\sim 8ms$.

4 Evaluation and Outlook

With help of the TIMMO TADL language and the usage of formal scheduling analysis as proposed by the TIMMO workflow, an issue for the response path (feedback) could be identified. In the worst case the scheduling delays the actuator response to the steering wheel so much that the data age is getting to big. In general, this affects the quality of control. Within the Steer-by-Wire validator the controlling algorithm could show abnormal behavior.

In order to avoid this case, an ideal combination of task schedule and offsets was calculated with help of SymTA/S from Symtavision GmbH [7]. Moreover, we decided to further separate SWC functions into smaller modules, resulting in the chance of a tighter schedule. In general, the application of the principles of the Timing Augmented Description Language (TADL) gives great benefit to network-based electronic systems design. Timing properties (and later scheduling properties) can be annotated to features within early design phases and can be verified

prior the actual implementation. The measured timings coincides with the estimated timing behavior, assumed an accurate architecture event chain model is specified. The event chain based evaluation of system behavior reveals possible design flaws and is a good starting point for design partitioning and revision.

On applying the TIMMO methodology the challenge for the user will be to perform accurate and consistent functional decomposition and refinement of top-level functions from Analysis Level down to SWC component level. Moreover, the segmentation for end-to-end delays into single timing chain segments has to be considered at the same time [9].

With help of this "timing is right-by-design" approach the implementation caused no trouble. The avoidance of costly iterations can save high amounts of money within large industry projects. Moreover, the possibility of WCET and scheduling analysis can avoid over-provisioning within electronic systems design, resulting in lower overall costs.

It is planned to validate additional timing related concepts within the steer-by-wire validator in the near future. Ideas range from the estimation of hardware execution time based on a SystemC library as well as usage of static program analysis tools to estimate the necessary ECU cycles of the software. Combining all these concepts the TIMMO workflow will further advance the accuracy of right-by-design timing behavior modeling of complex HW/SW systems.

Acknowledgements

This work described herein was partly supported by the DFG Sonderforschungsbereich 614 and by the German Ministry for Education and Research (BMBF) through the ITEA2 project TIMMO (01IS07002).

References

1. Navet, N., Simonot-Lion, F.: Automotive Embedded Systems Handbook. CRC Press, Boca Raton (2008)
2. TIMing MOdel (TIMMO) project: (2009), http://www.timmo.org/
3. TRW Automotive Inc. (2009), http://www.trwauto.com/
4. TTTech Computertechnik AG: (2009), http://www.tttech.com/
5. Janouch, S.: FlexRay and AUTOSAR get it right, Elektronik automotive (2009), http://www.elektroniknet.de/
6. Advanced Traffic Efficiency and Safety through Software Technology (ATESST2) project (2008), http://www.atesst.org/
7. Symtavision GmbH: (2009), http://www.symtavision.com/
8. Hammerschmidt, C.: Automotive electronics to recover slowly after deep dip, EE-Times (2009)
9. Cuenot, P., Frey, P., Johansson, R., et al.: Developing Automotive Products Using the EAST-ADL2, an AUTOSAR Compliant Architecture Description Language, Mentor Graphics Techpub (2009)
10. Reif, K.: Automobilelektronik, Eine Einführung für Ingenieure. Vieweg-Verlag, Wiesbaden, 3. Auflage (2008)