Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 83 (2016) 245 – 252

Procedia Computer Science

The 7th International Conference on Ambient Systems, Networks and Technologies (ANT 2016)

Simulation-based Verification of Automotive Safety-Critical Systems based on EAST-ADL

Ralph Weissnegger[a,b,*], Markus Schuss[a], Christian Kreiner[a], Markus Pistauer[b], Kay Römer[a], Christian Steger[a]

[a] *Institute for Technical Informatics, Graz University of Technology (TU Graz), Austria*
[b] *CISC Semiconductor GmbH, Klagenfurt, Austria*

Abstract

The increasing amount of assistance features in today's vehicles to ensure safe and reliable operation, imply increasingly complex systems. New challenges are arising due to highly heterogeneous and distributed systems which interact with and have an impact on the physical world, so called cyber-physical systems. Since millions of test kilometers must be driven to ensure a reliable system, simulation-based verification is becoming more important to reduce costs and time-to-market. This situation prompts the urgent demand for new techniques to simulate the behavior in early development phases by reusing verified system components. Best combined within a model-based approach that both unites different stakeholders and helps non-specialists to understand problems in the design. In this paper, we present a novel method for simulation-based verification of automotive UML/EAST-ADL design models. To demonstrate its benefits, our methodology is applied in an industrial use case of a battery management system.

Peer-review under responsibility of the Conference Program Chairs
Keywords: UML; EAST-ADL; automotive; ISO26262; simulation; verification; SystemC;

1. Introduction

Today's cars consist of highly complex electric/electronic (E/E) systems with sensors and actuators networking with each other. In fact a car is now more or less a smartphone on wheels. It can be observed that there is a shift towards fully E/E cars, since electric cars are getting more popular. The sensing and controlling of these systems is the work of the highly distributed electrical control units (ECU) and it is no surprise that more than 200 of these micro-controllers are currently integrated in a modern electric vehicle[1]. Since the electrification in the automotive domain continuous, new challenges in the development process are arising. This is especially the case where multiple stakeholders including specialists for hardware, software and system design have to work together with safety engineers to ensure a reliable and safe system. A model-based approach helps non safety-specialist to also understand problems in the design and development of safety-critical systems. One modeling languages which has established

* Corresponding author: Ralph Weissnegger
E-mail address: ralph.weissnegger@tugraz.at

Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2016.04.122

itself in the automotive domain is EAST-ADL[2]. It allows the detailed design of automotive E/E systems on different levels of abstraction. The last two layers conform with the AUTOSAR standard. Furthermore, they are in line with the development process of safety-critical systems according to ISO26262[3] and allow the evaluation and formal verification of design models. Since millions of test kilometer must be driven to ensure a reliable system, simulation is becoming more and more important[4], because it is no longer possible to cover the costs of physical tests. A drawback in today's development process is that simulation tools are often detached from the design tools and require cumbersome imports and exports of files between the environments. It is important that simulation tools are tightly and seamlessly integrated into the design and development process[5], meeting the requirements of ISO26262. Furthermore, approaches are needed that allow a high traceability to requirements and make it possible to derive requirements from simulation-results. This must be done as early as possible and on different abstraction levels.

In this work, we present a model-based simulation framework for the verification of E/E systems in the automotive domain. We link quickly executable simulation models, implemented in SystemC (-TLM) and SystemC-AMS, with EAST-ADL design models. The level of granularity of the models can be easily switched depending on the complexity. Using these reusable components, we achieve an early behavior simulation of the whole system. The result is a tool-aided methodology built as an Eclipse plugin in Papyrus[6], which makes it easy to verify the behavior of automotive safety-critical systems.

2. Related Work

An approach for generating simulation models from EAST-ADL architecture models was presented in[7]. In this work, several architecture levels of EAST-ADL have been mapped to abstraction levels of SystemC-TLM. The architecture of an automotive use case was presented on analysis and design level. For the expression of the behavior, the authors used SystemC code and state machines. This approach works very well for the digital domain, but lacks proper definition needed for analog and mixed-signal components. Through the use of code generators, it is possible to achieve synthesis of very detailed EAST-ADL models. It would also benefit of analyze and verification mechanisms for their simulations.

The authors of[8] presented three different analysis techniques for architectural models described in EAST-ADL, to guarantee the quality in the context of ISO26262. One of the proposed techniques is the simulation of EAST-ADL functions in Simulink. The behavior of each function was linked to FMU or Simulink models to facilitate the simulation. The authors also described mapping rules for the EAST-ADL to Simulink transformation (one-to-one mapping). The results of the simulation have been traced back to the requirements. This approach was applied to an industrial use case of a brake-by-wire system on Design Level. However, in contrast to our approach, they use proprietary simulation engines with high license costs and external tools which are not integrated into the design and development flow.

The authors of[9] demonstrated how to use MARTE for hardware design and simulation. They introduced a step-by-step methodology for hardware modeling with Hardware Resource Models (HRM) stereotypes. The platform models are refined until the final platform class is reached. In a later step, these models are used to generate code with the help of a Java plugin. A tool called Simics was used to facilitate the simulation. Instead of using the whole MARTE spectrum for simulation, this approach only uses HRM models for code generation of very detailed platforms instead of system level design.

3. Model-based System Design

Model-based design plays an ever increasing role in today's development to deal with complex systems. Organization of specialized people in projects of a certain size requires a lot of effort. Therefore, it is becoming increasingly important that stakeholders from different domains, e.g. hardware, software, safety or even security can efficiently work together. Particularly in the evaluation of safety-critical systems, safety specialists need a entire view of the system, that includes all domains of the system. Best combined in a tool where even entire processes like the ISO26262 can be addressed.

One modeling-language which has established itself in the automotive domain is EAST-ADL. It allows the capturing of detailed automotive electric and electronic systems on five layers of abstraction, each with a clear separation