Chapter 8

Generation and Verification of a Safety–Aware Virtual Prototype in the Automotive Domain

Ralph Weissnegger
CISC Semiconductor GmbH, Austria

Martin Schachner
Graz University of Technology, Austria

Markus Pistauer
CISC Semiconductor GmbH, Austria

Christian Kreiner
Graz University of Technology, Austria

Kay Römer
Graz University of Technology, Austria

Christian Steger
Graz University of Technology, Austria

ABSTRACT

The electrification of today’s vehicles and the high number of new assistance features imply more and more complex systems. New challenges are arising through heterogeneous and distributed systems which interact with each other and have an impact on the physical world, so-called cyber-physical systems. The sensing and controlling of these systems is the work of the highly distributed electronic control units and it is no surprise that more than 100 of these microcontrollers are currently integrated in a modern (electric) car. Technological, organizational and design gaps in today’s development flows are not covered by current methods and tools. Therefore, new approaches are essential to support the development process and to reduce costs and time-to-market, especially when systems are safety-critical and demand reliability. Through applying reliability analysis and simulation-based verification methods on the proposed model-based design flow, we are able to reduce the number of tools involved and achieve correctness, completeness and consistency of the entire system.

DOI: 10.4018/978-1-5225-2845-6.ch008
INTRODUCTION

In the world of today, the number of embedded electrical/electronic (E/E) systems used in many different domains is increasing greatly. When we review the complexity issue over the past years, it is plain that new applications have now emerged in which systems not only interact with each other but also have impact on the physical world. These systems are known as cyber-physical systems. Depending on their application, they must fulfill different requirements such as timing constraints, performance behavior, low power consumption and cope with thermal or even different environmental conditions. The point at issue here is, we live in a world where cyber physical systems are ubiquitous, they have a direct impact on our daily life and it is imperative that we must assure the dependability of these systems.

This is nowhere more clearly apparent than in the automotive domain. We are witnessing a shift to towards fully E/E systems resulting from the trend to electric vehicles. In fact, a car has now become more or less a smartphone on wheels. The sensing and controlling is the work of the highly distributed electronic control units (ECU) and it is no surprise that all these new features mean more than 100 microcontrollers (Charette, 2009) are currently integrated in a modern car and can require up to 150 million lines of code (FORD GT - Lines of code, 2016). The communication between these systems has now extended far across the internal borders of a car. When complex assistance features are in use, cars now need to communicate with each other (Car2Car) and the infrastructure must also be involved in the computation (Car2X). The goal in the development of a car has remained the same as ever: to develop better, more reliable and safer products to reduce the number of deadly accidents. But the industry is facing new problems through the emergence of many new (assistance) features that are also influencing each other. This in turn raises the complexity level in the design, development and verification of complex systems and imposes a task of enormous dimensions on the engineers who develop the applications.

In terms of safety, these systems must fulfill standards such as the ISO26262 (functional safety for road vehicles), (ISO, Road vehicles - Functional safety, 2011). Since this standard is now treated as state of the art in court, OEMs and their suppliers are required to develop and test their systems directed specifically to the recommended measures and methods. Moreover, it is no longer sufficient to test single hardware or software components, the functionality of the entire system must be given.

Whenever the design of a system is in discussion, one modeling language always comes to mind, the Unified Modeling Language (UML), (Group, 2015). Having the routes in the software domain, UML paved the way and established model-based thinking in various engineering domains and far across the borders of conventional software design. Engineers from different domains can use the full potential of an object-oriented approach here, since UML comes with several extensions such as MARTE (The UML Profile for MARTE: Modeling and Analysis of Real-Time and Embedded Systems, 2015), SysML (Omg, 2015) or EAST-ADL (EAST-ADL Association, 2014). MARTE was introduced to overcome the enormous complexity issues in the design of real-time and embedded systems. It provides capabilities to model hardware, software and also system design and provides the representation of timing, resource and performance behavior. Furthermore, UML/MARTE is already in use for several reliability analysis techniques. In addition, many semiconductor companies and suppliers are relying on this modeling language and it is used by several European projects such as the OpenES (Catene, 2016). OpenES is a European initiative to fill the gaps in today’s design flows and to develop common solutions to stay competitive on the global market.

Since a modern car today no longer exists in one single version, but rather in several hundreds of variants all with different features, each of them must be exhaustively tested to fulfill the standards. Millions