SANITAS: Enabling Design of Highly Reliable Next Generation Products

Part 1: Formalizing Product Data and Auto-Generating Verification Infrastructure Top-Down the Value Chain

Authors:
W. Ecker, M. Velten, V. Esen, P. Janssen, H. Brazdrum, H. Le, D. Große, W. Müller, O. Bringmann, A. Viehl, A. Burg

Within the project "Enabling Safer Systems by a new Collaborative Verification Methodology across the Value Chain" (SANITAS), the partners developed an approach to break the barrier between product developer and subsystem supplier by formalizing the communication between product developer and subsystem supplier in two ways: Requirements are passed to the subsystem supplier in a structured and formalized way and the subsystem supplier provides a fast simulation model to the product developer allowing the product developer to early build a virtual prototype of his system. In addition, the subsystem provider derives verification items from the requirements in order to verify the various views of the delivered subsystem.

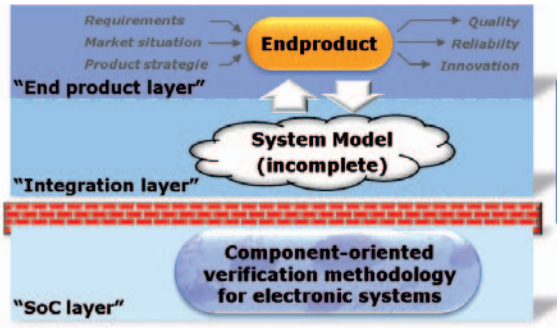
This article (as one part of the SANITAS reporting) focuses on the first part of the SANITAS solution, the formalization of the requirements and the generation of verification items.

Motivation

The mastering of highly automated and complex manufacturing makes Germany a unique industrial site being still competitive even in comparison to low-wage countries. Prerequisite to stay in this leading position are powerful electronic automation systems driven by enhanced virtual planning tools such as the so-called Digital Factory. The success strongly depends on a seamless verification methodology in place to ensure that such systems fulfill safety-critical properties.

The research project SANITAS targets the development and exploration of a new system verification methodology for the design of highly reliable next generation applications and products. SANITAS integrates several layers of the product development chain from the layer of micro- and nanoelectronic components up to the layer of final products into a holistic verification strategy. This, for the first time, provides a seamless verification process along the whole development chain which is capable of capturing the effects of micro-/nanoelectronic components and embedded software – the key drivers for building safe, reliable, and highly energy efficient products – at an early stage of the overall development process.

As shown in Figure 1.02, the SANITAS approach is to break the wall between product development, integrator (e. g. a plant, car) and supplier (e. g. board, chip) by two main innovations:



1. The requirements are passed to the supplier in an electronic form, so that the supplier derives correct by construction test cases for the product.

2. A highly efficient simulation model is passed from the supplier to the product integrator in order to allow early simulation of the complete product long before the final chip is shipped. An overall virtual product is built by using the highly efficient simulation model: Product use cases are simulated and thus bugs can be detected early and feedback can be given early as well.

Goals

To make this happen, SANITAS had to develop several new methodologies and technologies.

- A methodology to handle and manage requirements such that verification items can be generated hereof.
- A methodology to structure the test cases and to generate test environments (testbenches) and test scenarios.
- A modeling style to build highly efficient simulation

Project partners:
Forschungszentrum Informatik,
Fraunhofer-Institut für Integrierte Schaltungen,
Infineon Technologies AG,
Micronas GmbH,
Robert Bosch GmbH,
Siemens AG,
Tieto Deutschland GmbH,
Universität Bremen
Universität Paderborn.

Subcontractors:
Technische Universität München,
University of Tübingen,
Offis

Runtime:
1.10.2009–31.12.2012

Funding Label:
16 M 3088

Webpage:
http://sanitas.fzi.de/
Das Verbundprojekt SANITAS wurde unter dem Förderkennzeichen 16 M 3088 durch das Bundesministerium für Bildung