Federal Ministry
Republic of Austria
Digital and
Economic Affairs

Christian Doppler
Forschungsgesellschaft

Safety in every case

The control of modern facilities relies on complex hardware and software systems that process data locally or centrally, according to demands. Efficient and reliable test methods contribute to the safety of these systems, accelerate the development processes and simplify licensing procedures.

JR Centre for Verification of Embedded Computing Systems

Head
Prof.(FH) DI Dr Martin Horauer; Technikum Wien University of Applied Sciences

Operation
01.05.2013 – 30.04.2018

Commercial partners
Infineon Technologies Austria AG, Kapsch TrafficCom AG, LOYTEC electronics GmbH, Oregano Systems – Design & Consulting GmbH, Siemens AG Österreich; Bluetechnix R&D GmbH

The topic

Whether we are dealing with underground transport, with power plants, with train safety systems or with intelligent power grids, embedded systems are controlling these systems, driving power-plant turbines and processing data for forwarding to a central process control. The distribution of tasks results in a highly complex hardware and software landscape that enables the facility to function efficiently, requires, however, a custom development for each individual application. Safety plays a very important part, as a small mistake may have large and often life-threatening consequences. No matter what happens, which part of the system fails, the overall system must switch quickly to the next safe state: the high-speed train stops before the tunnel, the power plant reacts correctly to an earthquake and the power grid remains stable despite the outage.

Three questions to ...

DI Harald Loos
Head of the Central Research Unit at Siemens Austria

Why is (basic) research so important for innovation?
Without (basic) research there would be no new technologies and no new business possibilities or models, which form the basis for value creation and education.

What are the biggest challenges in collaborating with universities and universities of applied sciences?
I personally do not see any particularly difficult challenge in the collaboration if the financing of the projects is clear and guaranteed.

What do you like most about the CD Laboratory funding scheme?
The special feature of the CDG model is that it enables the three-way relationship between basic research, applied research and industry. The stability of the relationship is based on the expert evaluation AND support of the individual laboratories by experts from science and the private sector. I think the model is a perfect showcase for research support.

The research question

Embedded systems can be thought of as small computers paired with sensors (components that measure values in the surroundings) and actuators (e. g. motors or turbines). The necessary electronics (hardware) is tailor-made and directly coupled to the equipment. So-called FPGAs (field-programmable gate arrays) are often used for these computers. They contain a large number of basic digital components (processors, memories, gates etc.) that are interconnected in a variety of ways and are thus able to carry out new functions, i. e. they can be reconfigured to respond to changing demands. Doing so generally requires a language to describe the hardware from which the new hardware should be made. It is not possible to check every connection and interface in these complex hardware and software systems and thus it is not feasible to test every possible combination of errors. However, many of the applications must be safe and error-tolerant under all conditions. Validated testing and verification solutions should be able to identify problems early in the design flow – and the check that systems have passed validated test procedures.

Collaboration in the JR Centre

Developing efficient tests and verification solutions for embedded systems requires expertise at the interface between hardware and software, where special methods and languages are used. Siemens found this expertise in Prof. Horauer and his team at the Technikum Wien University of Applied Sciences. Test systems for the safety of embedded systems represent a clearly defined workpackage and are highly suited to the collaborative study in a Josef Ressel Centre.

Results

The collaboration in the JR Centre has enabled the development of a number of benchmarks to define the safety of a system. FIJI, the Fault Injection Tool, represents an important result. This open-source tool was developed in the JR Centre and enables a range of errors to be introduced into a variety of FPGA-based solutions, thereby enabling developers to test whether the safety measures built into the system can cope with these errors. The tool has been published by the University of Applied Sciences and is being maintained and updated by the research community. Siemens is benefiting from the progress in the entire sector and from advance knowledge through the collaboration in the JR Centre.

Scientific challenge

When developing safety-critical systems, how is it possible to simulate all conceivable errors quickly and inexpensively and to test whether the systems react appropriately in all cases? How should adaptive hardware and software be conceived and implemented to maintain systems that are as robust as possible? These questions in the fields of electronics and technical informatics are particularly relevant to embedded systems. Understanding and controlling systems of this kind, and satisfying the numerous regulations and certification processes, requires detailed knowledge and an extremely high level of diligence. The test system developed in the JR Centre, FIJI, is making an important contribution to the development of the field and can be applied to all safety-critical FPGA-based electronic systems, independent of the system.

Added value for the company

Siemens is using FIJI, the open-source tool developed in the JR Centre, in its development process to identify possible safety gaps at an early stage (correct by construction). The development of a demonstrator for training and teaching purposes has helped transfer the technology into education. Siemens is benefiting from the progress in the sector and from advance knowledge through the collaboration.

Christian Doppler Forschungsgesellschaft (CDG)
Boltzmanngasse 20/1/3, 1090 Vienna, Austria, tel.: +43 1 5042205, e-mail: office@cdg.ac.at
CD Laboratories and JR Centres are funding programmes of the Austrian Federal Ministry for Digital and Economic Affairs.

www.cdg.ac.at

04/2019