Research area:
Software and Knowledge Engineering Methods

Holger Hermanns

Time is on your side?

Last year, Holger Hermanns received the Innovation Impulse (Vernieuwings-impuls) award, a Dutch innovation award for excellent and somewhat unusual research. He focuses on the reliability of complex embedded systems, using solid mathematics. It is his conviction that this is the only way to make accurate predictions. Now, the only problem seems to be finding people to do the job.

"If you insert your cash card into a cash dispenser, you expect a simple response. Either 'Enter your PIN code please' or something like 'System Error'. You don't accept a blank screen. You would think that checking that the system works is simple. As long as one of both messages is displayed to every customer, the system can be said to work correctly. But that implies that the system is considered correct even if the message is displayed after five minutes or two days. The customer wouldn't accept that, of course! This indicates that system requirements often need to be fulfilled within a limited period of time, or at least with a pretty high degree of probability. To guarantee such requirements, you have to find ways of considering probabilities, time and correctness within a single framework."

"Model checking is a very reliable way to check a new system before it is implemented, or even before programming is commenced. At an early stage, you define very precisely what a system has to do. We have developed powerful tools for checking complex systems. Nowadays, we frequently deal with embedded systems, and this means that you can't simply push the 'reset button' if something does not work properly. Introducing 'time' as a parameter is essential for checking many types of systems, as in the cash dispenser case. But that is not an easy 'extension' to model checking. Take for instance a system with twenty 'almost' perfectly working components, you have no guarantee that the entire system does almost perfectly what the user wants it to do. The stochastics of the components, the complete system and the user demands all have to be taken into account."

"In cars, for example, there will be a strong increase in the number of embedded systems and even complete in-vehicle communication networks. There appears to be a common agreement in European automotive industries that an 'event-driven' system may not respond well enough. If an infotainment system on the dashboard wants to inform you about something, and at the same time you have to brake immediately, absolute priority must be given to the brake. An event-driven system does not provide you with enough guarantees in such a case. Introducing a time-driven system, with a kind of global synchronous clock, is the current preferred solution. The brake then gets a fixed time slot, say every nanosecond, and you can be absolutely

Examples of current projects:

- Easy Composition in Future Generation Component Systems (EasyComp; EU Fifth Framework Program)
- Advanced Methods for Timed Systems (Ametist; EU Fifth Framework Program)
- Verfication of Performance and Dependability (Netherlands Science Foundation / Vernieuwingsimpuls)

certain of it. However, checking a system like this is very complex and requires new techniques for solid stochastic analysis."

"I am also interested in the 'pain' aspect for the IT user. This is not always linearly related to time. We will see more and more systems communicating with one another, without user intervention. For instance, imagine you enter a room with your personal organiser that logs on automatically to the wireless network in the room. For this to happen it must first guess a unique name, so it cannot simply say: "Hi, I'm Frits and here's my data." It has to make sure that there's not another Frits in the room and so it asks "Is there someone called Frits?" a few times, to make sure his name is unique. This may take a few seconds, and there is still a slight risk of ending up with two Frits in the room, as wireless messages may get corrupted. Now what is more annoying to the user: waiting for his system to log on or running the risk of having a 'double' who may sense private data. For this reason we are examining communication protocols in co-operation with Philips."

Having detected the ringing, the theater's automatic cell phone suppression system kicked in.

"Nowadays, systems are being introduced whose operation no one can really assess. I am not at all sure that the approaches we are developing will offer a solution, but I am convinced that these approaches are the only chance we have to get to grips with the problem. The strong mathematical basis is the key, and I am convinced that industry is becoming more and more aware of this. The Innovation Impulse award has given a real boost to our work, but it is difficult to allocate resources; to find people for this research with excellent qualifications. Last week my first PhD student arrived. He's from Kazakhstan and I think he is a very good candidate, so we can move on!"