SORS: Rigorous System Design

Objectives

Abstract: Today, the development costs of high confidence systems explode with their size. We are far away from the solution of the so called, software crisis. In fact, the latter hides another much bigger: the system crisis.

In my talk I will discuss rigorous system design as a formal and accountable process leading from requirements to correct-by-construction implementations. I will also discuss current limitations of the state of the art and advocate a coherent scientific foundation for system design based on four principles: 1) separation of concerns; 2) component-based construction; 3) semantic coherency; 4) correctness-by-construction. The combined application of these principles allows the definition of a methodology clearly identifying where human intervention and ingenuity are needed to resolve design choices, as well as activities that can be supported by tools to automate tedious and error-prone tasks.

The presented view for rigorous system design has been amply implemented in the BIP (Behavior, Interaction, Priority) component framework and substantiated by numerous experimental results showing both its relevance and feasibility. I will conclude with a discussion advocating a system-centric vision for computing, and a deeper interaction and cross-fertilization with other more mature scientific disciplines.

BIO: Joseph CIn my talk I will discuss rigorous system design as a formal and accountable process leading from requirements to correct-by-construction implementations. is Emeritus Senior CNRS Researcher at Verimag. His current research interests cover fundamental and applied aspects of embedded systems design. The main focus of his work is on the formalization of system design as a process leading from given requirements to trustworthy, optimized and correct-by-construction implementations.

Joseph Sifakis has been a full professor at Ecole Polytechnique Fédérale de Lausanne (EPFL) for the period 2011-2016. He is the founder of the Verimag laboratory in Grenoble, which he directed for 13 years. Verimag is a leading research laboratory in the area of embedded systems, internationally known for the development of the Lustre synchronous language used by the SCADE tool for the design of safety-critical avionics and space applications.

In 2007, Joseph Sifakis has received the Turing Award for his contribution to the theory and application of model checking, the most widely used system verification technique today. Joseph Sifakis has had numerous administrative and managerial responsibilities both at French and European level. He has actively worked to reinvigorate European research in embedded systems as the scientific coordinator of the « ARTIST » European Networks of Excellence, for ten years. He has participated in many major industrial projects led by companies such as Airbus, EADS, France Telecom, Astrium, and STMicroelectronics. Joseph Sifakis is a member of the French Academy of Sciences, a member of the French National Academy of Engineering, a member of Academia Europea, a member of the American Academy of Arts and Sciences, and a member of the National Academy of Engineering. He is a Grand Officer of the French National Order of Merit, a Commander of the French Legion of Honor. He has received the Leonardo da Vinci Medal in 2012. Joseph Sifakis has received in 2009 the Award of the Hellenic Parliament Foundation for Parliamentarism and Democracy. He is a commander of the Greek Order of the Phoenix. He has been the President of the Greek Council for Research and Technology for the period February 2014 – April 2016.

Barcelona Supercomputing Center - Centro Nacional de Supercomputación

---