Synchronous Design and Verification of Critical Embedded Systems Using SCADE and Esterel

Gérard Berry

Esterel Technologies, France
Gerard.Berry@esterel-technologies.com
http://www.esterel-technologies.com

SCADE (Safety Critical Application Design Environment) is a design environment dedicated to safety-critical embedded software applications. It is widely used for avionics, railways, heavy industry, and automotive applications. For instance, most critical systems of the Airbus A380 have been developed with SCADE. The core element is the Scade synchronous formalism, which can be viewed as a graphical version of Lustre coupled with synchronous hierarchical state machines. The Scade to C compiler is certifiable at level A of DO-178B avionics norm, which removes the need for unit-testing the embedded C code and brings big savings in the certification process. The SCADE tools encompasses a simulator, a model coverage analyzer, a formal verifier, a display generator, and gateways to numerous other prototyping or software engineering tools. Esterel Studio is a similar hardware modeling, design, and verification environment based on the Esterel v7 formal synchronous language. Esterel Studio is used by major semiconductor companies to specify, verify, and synthesize complex hardware designs. It can generate both an optimized circuit and a behaviorally equivalent software model from a single formal specification. It also supports simulation and formal verification, which is widely used in production applications. We discuss the advantages and limitations of the underlying synchronous concurrency model. We explain why the same core science and technology can be applied to such different domains, however with quite different integration in global system-level design flows according used in the different industries.

S. Leue and P. Merino (Eds.): FMICS 2007, LNCS 4916, p. 2, 2008.