Esterel v7: From Verified Formal Specification to Efficient Industrial Designs

Gérard Berry

Chief Scientist, Esterel Technologies Member, Academie des Sciences

Synchronous languages were developed in the mid-80's specifically to deal with embedded systems. They are based on mathematical semantics and support formal compilation to classical software or hardware languages as well as formal verification. Esterel v7 is a major industrial evolution of the original Esterel synchronous language, mostly directed to complex hardware applications. The language is supported by the Esterel Studio integrated development environment, which provides a smooth path from verifiable executable specification to efficient circuit synthesis. The graphical Safe States Machines derived from Esterel are also used in the SCADE tool which is widely used for safety-critical software applications in avionics.

Through the examples of Esterel v7 and SCADE, we discuss the impact and evolution of formal methods for actual industrial design. In particular, we discuss some issues that are central for actual applications but are usually either not considered as such or viewed as too difficult to handle in research or R&D projects. We demonstrate that the difference between industrial success and failure often lies in precisely these aspects.