SACRES: A Step Ahead in the Development of Critical Avionics Applications

Philippe Baufreton

Snecma systèmes, Centre de Villaroche, BP 42
77552 Moissy–Crayamel Cedex, France
philippe.baufreton@snecma.fr

Abstract. Basically, aircraft engines can be divided into a control embedded system and a controlled system with its environment. The behaviour of the controlled system is given a priori, while the control system still needs to be designed in a way guaranteeing the correct overall behaviour under all operational conditions depending on the flight domain. A large quantity of functions in control systems can be described by a formal system expressed in block diagrams and state-based representations. These representations can be translated to formal based tools relying on the synchronous languages Signal and Statecharts.
SACRES is a tool set supporting the design of safety-critical embedded control systems. It integrates the tools and specification techniques Statemate, Sildex, and Timing Diagrams with tool components for automatic code generation, formal verification based on model checking techniques, and an innovative approach for automatic code validation for target code generated from DC+. Technical achievements are

- Integration of dataflow and state-based specification styles
- Formal specification of safety-critical properties
- Integration of efficient symbolic model checking techniques with Statemate and Sildex
- Automatic generation of efficient distributed code
- Automated correctness proofs for the generated code

The main benefits of the SACRES approach are reduced risks for design errors and decreased design times and costs for the development of dependable (safety critical) embedded systems. SACRES is an attempt to avoid unpredictability (particularly that arising from late feedback from testing) associated with development of safety critical systems, through the use of the maximum degree of automation, especially in respect of code generation and verification.
An outstanding property of SACRES is the combination of specification styles and specification tools being applied in practice with automatic tools to establish provable correctness with respect to required properties. Both dependability and productivity are increased by automatic code generation from high-level specifications such that the generated code can be validated against higher levels by rigorous proofs.
These techniques allow traditional tests by sampling to be replaced by rigorous checking techniques which correspond to 100% coverage of test cases. In order to address a global innovative approach in the near future which match the whole software configuration, the SACRES tool set should be interfaced with asynchronous techniques matching the operating system development. This raises an open question in the software development future new process.

F.W. Vaandrager and J.H. van Schuppen (Eds.): HSCC'99, LNCS 1569, pp. 1–1, 1999.