Part IV

TOOLS

SIGNAL: A Formal Design Environment for Real-Time Systems

EP-ATR Project

IRISA / INRIA, F-35042 RENNES, France, e-mail: Paul.Leguernic@irisa.fr

The purpose of the EP-ATR Project at IRISA / INRIA-Rennes, is to provide methods and tools for software development, formally founded on a mathematical semantics and model of dynamic systems, integrated within an interactive environment, for the design and implementation of real-time systems. Real time and reactive systems are characterized by their permanent interaction with the external world, the reliability required for their safe execution, their response time and their execution on multi-processor architectures. Targeted application domains feature: aerospace, telecommunications, robotics, signal processing.

Our approach supports a variety of techniques, such as specification, simulation, validation, verification and code generation, all around the synchronous data-flow language SIGNAL, developed at IRISA / INRIA-Rennes. They are integrated into a global software development environment. SIGNAL allows for:

- programming with a user-friendly, interactive graphical interface,
- high-level description of the algorithms, independently of the target hardware, or any implementation consideration,
- reusability of sub-processes through modularity,
- automated analysis of properties, statical as well as dynamical, required to be satisfied for full reliability of the systems,
- automated analysis of the dependencies between sub-processes, for their distribution on multi-processor architectures,
- simulation of the behavior of architectures, of which the components as well as their interactions have been described in SIGNAL,
- automatic code generation and optimization, in portable languages like C and FORTRAN 77,
- hardware / software codesign and generation of VHDL

The SIGNAL environment exists in the INRIA H2 version, developed at IRISA / INRIA-Rennes, and in the CNET / TNI V3 version, which is commercially available from TNI Inc. (Brest, France). The SYNDEX environment developed at INRIA-Rocquencourt can perform automatic distribution of SIGNAL programs on multiprocessor architectures.

The SIGNAL environment has been experimented in a variety of small and large applications concerning signal processing and the control of complex systems. The SIGNAL environment is demonstrated by the following examples:

- a speech recognition system: this automatic speech-to-phoneme system illustrates the power of the constructs of the language when specifying complex timing behaviours and properties;

- a digital watch: this example of complex automaton, where numerous different modes must be controlled, focuses on the development method, emphasizing modularity and reusability. It is composed of modules (the stopwatch, the alarm, and the watch setup) that could be developed and verified separately.
- a control system for a rail/road crossing: it follows a specification of a real crossing between a road and two railway tracks. It illustrates a general methodology of decomposition into three separate parts: the controller itself, a simulation environment, and a graphical interface, all specified in SIGNAL.
- a robotic vision application (see figure below), where data flow tasks implementing the control laws are sequenced in reaction to event occurrences. This application uses a recent extension to SIGNAL facilitating the specification of the sequencing and hierarchical preemption of data flow tasks.

- the specification and verification of a production cell: this is our contribution to a case study proposed by the FZI in Karlsruhe, comparing the application of a variety of formal methods for reactive systems.

The SIGNAL environment and the demonstrations presented run on SUN 4 under SunOS 4.1, and are also available for HP 9000 under HP-UX A.B8.

Reference: P. Le Guernic, T. Gautier, M. Le Borgne, C. Le Maire. Programming Real-Time Applications with SIGNAL. *Another look at real-time programming*, special section of *Proceedings of the IEEE*, 79(9), September 1991.