9

TripleS - A Formal Validation Environment for Functional Specifications

J-P. Soininen, J. Saarikettu, V. Veijalainen and T. Huttunen
VTT Electronics
Kaitoväylä 1, FIN-90571 Oulu, Finland, tel. +358 8 551 2111, fax +358 8 551 2320 and e-mail: Juha-Pekka.Soininen@vtt.fi

Abstract

A TripleS formal validation environment for the analysis of functional specification is presented. The approach is based on the state space generation, model abstraction, data hiding and advanced analysis techniques.

Keywords

Validation, State space generation, System level specification, VHDL

1 INTRODUCTION

Validation and verification are required to avoid costly design errors. The idea of validation is to check that the system fulfils the requirements. Typically it is done by simulation, animation or prototyping. Model checking and state space generation are formal approaches. In the state space exploration the idea is to generate a FSM presentation of the system. The verification checks that the result of design refinement is equivalent with the input description. Typical approaches rely on testing, simulation and equivalence checking.

2 TRIPLES ENVIRONMENT

The TripleS environment consist of modelling, model abstraction, state space generation and analysis tools. The idea is to support the validation of system

model properties and the analysis of implementation requirements. Prosa SA editor supports the data flow and the state transition modelling. SAARA, VHDLSAX and Ids2Win tools link the SA/VHDL modelling with ARA tools (Valmari, 1995). SAARA and VHDLSAX are responsible for the abstraction of SA/VHDL model into ARA Lotos. ARA State Space Generator and Normalizer are used for state space generation (Savola, 1995). The analysis of LTS graph is done using ARA state space illustrator and ARA Editor. Focusing to specific parts of the model is done by LIM filtering tool.

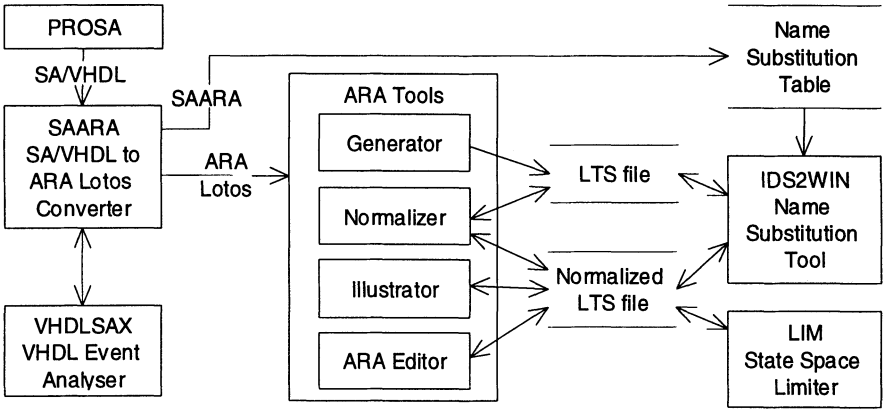

Figure 1 TripleS Tools.

State Space Generation from SA/VHDL

SA/VHDL is a graphical specification method to be used in specifying the functionality and the behaviour of the system. SA/VHDL description consists of parallel processes described with sequential algorithms. The communication between parallel processes is atomic and occurs only at the start and finish of the process. Therefore it is possible to replace processes with simple FSM models for the analysis. TripleS extracts process events from individual processes and then constructs respective system event tree for the complete model. After that each process event is replaced with system events containing respective process event. This synchronizes parallel processes. Finally the complete state space is generated by exhaustive simulation (Soininen, 1995).

3 VALIDATION OF FUNCTIONAL SPECIFICATION

TripleS was experimented with a Viterbi-based DSP algorithm, which represented a typical data flow application, and with an Ethernet Bridge, which represented a control oriented design. Both examples were modelled with SA/VHDL and simulated with VHDL simulator. Simulation descriptions of Viterbi and EB were about 2700 and 2200 lines respectively. However the EB

example consisted of parallel processes while Viterbi was more sequential. The generated state space of Viterbi had 10 states and 12 transitions. In case of EB the respective figures were and 481 states and 6115 transitions.

Several errors were found from the specification during the analyses. In order to focus on interesting behaviours filtering, test bench and model modification techniques were used. Typical situation was that the resulting state space differed from expected. In the EB the errors were related to the ageing of messages and to the manipulation of forwarding queue. The detection of such errors by functional simulation would have required dedicated test benches.

4 CONCLUSIONS

A method and a set of tools called TripleS for the state reachability analysis of functional specifications are presented. The tool is used for the validation of model behaviour and analysis of implementation requirements. Several errors were identified during the analyses of CASE-examples. The state space generation can and should be used together with simulation and analysis during model checking.

5 REFERENCES

Savola, R. (1995). A State Space Generation tool for LOTOS specifications. Technical Research Centre of Finland, VTT Publications 241. 99 pages.

Soininen, J-P., Saarikettu, J. & Huttunen, T. (1995). Specification of State Reachability Analysis Method. Cobra EP-8135 Project Report. VTT Electronics. 44 pages.

Valmari, A. & Savola, R. (1995). Verification of the behaviour of Reactive Software with CFFD-Semantics and ARA Tools. *Proceedings of an International Symposium on On-board Real-time Software*, ESTEC, Noordwijk, The Netherlands, 13-15 November 1995, ESA SP-375, pp. 173-180.

6 BIOGRAPHIES

Juha-Pekka Soininen is a Senior Research Scientist at VTT Electronics and earned his MSc in 1987 at University of Oulu.

Janne Saarikettu is a Research Assistant at VTT Electronics.

Ville Veijalainen is an ASIC Design Engineer and earned his MSc in 1996 at University of Oulu. He currently works at Martis Oy.

Tuomo Huttunen is Research Scientist at VTT Electronics and earned his MSc in 1994 at University of Oulu.