TELECOM
PARIS

Tool demonstrations Proceedings

SPIN'98 workshop
(2 November 1998)

Session on Educational Case Studies in Protocols
(3 November 1998)

FORTE/PSTV'98 Conference
(4-6 November 1998)

FORTE PSTV'98

IFIP WG 6.1

CNRS

Formal Verification of Fault Tolerant Mechanisms by Model-Checking

Demonstrator: Alessandro Fantechi
Presented at: FORTE/PSTV'98 Conference
Schedule: From Tuesday 3rd to Friday 6th November (Room B206)

Software used: JACK-2
Authors:

- C. Bernardeschi - Dipartimento di Ingegneria dell'Informazione - Università di Pisa - Italy
- A. Fantechi - Dipartimento di Sistemi e Informatica - Università di Firenze - Italy
- S. Gnesi - IEI - CNR - Pisa - Italy
- F. Mazzanti - IEI - CNR - Pisa - Italy
- A. Santone - Dipartimento di Ingegneria dell'Informazione - Università di Pisa - Italy

Abstract: The JACK environment combines different specification and verification tools, independently developed at different academic sites (IEI-CNR in Pisa, Italy, University of Rome, Italy and INRIA Sophia-Antipolis, France). The environment is mainly based on the use of a common format for the representation of finite state labelled transition systems, FC2. JACK has been successfully tested on several case studies, including some industrial ones.

JACK-2 upgrades the functionalities of JACK by means of a new BDD-based model checker, and other new verification tools, accessible through a new common user interface, developed in Java.

The demo will show the use of the verfication tools on a case study derived from the fault-tolerance mechanisms analysed inside the ESPRIT GUARDS project.

Through this case study the different features of the JACK-2 environment are explored, exploiting the new user-interface.

Required Software: JDK 1.1

Distribution: public license for academic purposes, Solaris 2.5.1+

For further information:
`http://repl.iei.pi.cnr.it/projects/JACK/JACK2/Jack2.html`

Bibliography:

- A. Bouali, S. Gnesi, S. Larosa: "The integration Project for the JACK Environment", Bulletin of the EATCS, n.54, pp.207-223, 1994.
- A.Anselmi, C. Bernardeschi, A. Fantechi, S. Gnesi, S. Larosa, G. Mongardi, F. Torielli: "An Experience in Formal Verification of Safety Properties of a Railway Signalling Control System", Proc. SAFECOMP '95 , Springer-Verlag, 1995.
- C. Bernardeschi, A. Fantechi, S. Gnesi, G. Mongardi: "Proving safety properties for embedded control systems", Proc. EDCC-2, LNCS 1150, Springer-Verlag, 1996.

- G. Ferrari, G. Ferro, S. Gnesi, U. Montanari, M. Pistore, G.Ristori: "An automata based verification environment for mobile processes", Third International Workshop on Tools and Algorithms for the Construction and Analysis of Systems, TACAS'97, LNCS 1217, Springer - Verlag, 1997.
- C. Bernardeschi, A. Fantechi, S. Gnesi: "An Industrial Application for the JACK Environment", Journal of Systems and Software, vol 39, n. 2,Elsevier Science Inc., 1997.
- C. Bernardeschi, A. Fantechi, S. Gnesi, S. Larosa, G. Mongardi, D. Romano: "A Formal Verification Environment for Railway Signaling System Design", in Formal Methods in System Design 12, 139-161, 1998.
- A. Fantechi, S. Gnesi, F. Mazzanti, R. Pugliese, E. Tronci: "A Symbolic Model Checker for ACTL", International Workshop on Current Trends in Applied Formal Methods , LNCS, Springer - Verlag, 1998.