IF Validation Environment Tutorial

Marius Bozga, Susanne Graf, Laurent Mounier, and Iulian Ober

VERIMAG, Centre Equation, 2 avenue de Vignate, F-38610 Gières
http://www-verimag.imag.fr/~async/IF

Introduction

IF[3, 7] is an open validation platform for asynchronous timed systems developed at Verimag during the last 5 years.

The toolbox is built upon a specification language based on communicating extended timed automata supporting various communication primitives and dynamic process creation and destruction. This language is expressive enough to represent most useful concepts of modeling and programming languages for distributed systems (like SDL, UML, Java, ...)

The core of the toolbox consists of a set of model-based validation components including exhaustive/interactive simulation, on-the-fly temporal logic model-checking, test case generation and optimal path extraction. In order to control state explosion, the toolbox provides several static analysis tools operating at the source level such as live variable analysis, dead-code elimination and slicing. Finally, the toolbox is connected to commercial environments (such as Rational Rose, Rhapsody, Objecteering, Object Geode) and may be used for validating SDL and UML specifications [1, 6].

The toolbox has been successfully applied on several case studies including telecommunication protocols, distributed algorithms, real-time controllers, manufacturing, asynchronous circuits [2, 5, 4].

Objectives

The objectives of this tutorial are first, to give a complete presentation of the main functionalities of the IF validation environment, and second, to show how this environment can be used to experiment on new model-checking techniques.

Expected attendees are people interested in model-checking techniques, either from an (experienced) user or from a tool designer or researcher point of view.

Summary of Material

In this tutorial, we will guide participants trough the concepts and the use of the IF language and the associated tools. More precisely, we will focus on the following items:

Language: In the first part we will provide a survey of the main concepts of the IF language. We will focus on both functional features (structure, communication, dynamic creation, external code integration) and non-functional ones (real-time primitives, resource management, priorities). Moreover, we will show how to express properties on IF specifications by means of dedicated observers.

Core tools: In this second part we will introduce the toolbox architecture and its main components. We will describe the two main APIs: the syntax level API (abstract syntax tree) and the semantic level API (state graph). Among the tools, we will focus on the static analyser and some of the model based tools (e.g, model checker, test generator, optimal path extractor).

Front-ends and applications: Finally, the third part will be dedicated to existing front-ends to SDL and UML. It will also give an overview of the most relevant case studies handled with the IF toolbox.

The tutorial will be illustrated with examples, on-line demos and comparisons with other related tool environments (Spin, CADP, Kronos, Uppaal, etc). Participants will receive CDs with the latest version of the IF toolbox and an example repository including the examples used in the tutorial.

References

1. M. Bozga, J.Cl. Fernandez, L. Ghirvu, S. Graf, J.P. Krimm, L. Mounier, and J. Sifakis. IF: An Intermediate Representation for SDL and its Applications. In R. Dssouli, G. Bochmann, and Y. Lahav, editors, *Proceedings of SDL FORUM'99 (Montreal, Canada)*, pages 423–440. Elsevier, June 1999.
2. M. Bozga, S. Graf, and L. Mounier. Automated Validation of Distributed Software using the IF Environment. In *Workshop on Software Model-Checking*, volume 55. TCS, July 2001.
3. M. Bozga, S. Graf, and L. Mounier. If-2.0: A validation environment for component-based real-time systems. In K.G. Larsen Ed Brinksma, editor, *Proceedings of CAV'02 (Copenhagen, Denmark)*, volume 2404 of *LNCS*, pages 343–348. Springer, July 2002.
4. M. Bozga, D. Lesens, and L. Mounier. Model-Checking Ariane-5 Flight Program. In *Proceedings of FMICS'01 (Paris, France)*, pages 211–227. INRIA, 2001.
5. S. Graf and G. Jia. Verification Experiments on the Mascara Protocol. In *Proceedings of the SPIN'01 Workshop (Toronto, Canada)*, volume 2057 of *LNCS*. Springer, 2001. ISBN 3-540-42124-6.
6. Iulian Ober, Susanne Graf, and Ileana Ober. Validating timed uml models by simulation and verification. In *Proceedings of the SVERTS'03 Workshop (satellite of UML'03 Conference), San Francisco, California*, 2003.
7. VERIMAG/DCS. If web page. http://www.verimag.imag.fr/~async/IF.