

IF Validation Environment

Marius Bozga, Laurent Mounier, Iulian Ober

VERIMAG - Distributed and Complex Systems Group
Centre Equation, 2 Avenue de Vignate, 38610 Gières, France
<http://www-verimag.imag.fr/~async/IF>

1 Introduction

IF[5, 6, 10, 15] is an open validation platform for asynchronous timed systems such as telecommunication protocols or distributed applications developed at Verimag during the last 5 years.

The toolbox is built upon an specification language based on timed automata extended with discrete data variables, various communication primitives, 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 [3, 4]. Finally, the toolbox is connected to commercial environments (such as Rational Rose, Rhapsody, Objectteering, Object Geode) and may be used for validating SDL and UML specifications [7, 8, 11, 14].

The toolbox has been successfully applied on several case studies including telecommunication protocols, distributed algorithms, real-time controllers, manufacturing, asynchronous circuits [9, 13, 12, 2, 1].

2 Objectives

The objectives of this tutorial are the following:

- first, it will give a complete presentation of the main functionalities of the IF validation environment, and

- second, it will 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 tool designer or researcher point of view.

3 Summary of Material

In this tutorial, we will guide participants through 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] Dominique Borrione, Menouer Boubekour, Laurent Mounier, Marc Renaudin, and Antoine Sirianni. Validation of asynchronous circuit specifications using if/cadp. In *IFIP Intl. Conference on VLSI, Darmstadt, Germany*, December 2003.

- [2] M. Boubekeur, D. Borriane, L. Mounier, M. Renaudin, and A. Sirianni. Modelling chp descriptions in labelled transition systems for an efficient formal validations of asynchronous circuit specifications. In *Forum on Specification and Design Language (FDL'03)*, Frankfurt, Germany, September 2003.
- [3] M. Bozga, J.Cl. Fernandez, and L. Ghirvu. State Space Reduction based on Live Variables Analysis. In A. Cortesi and G. Filé, editors, *Proceedings of SAS'99 (Venice, Italy)*, volume 1694 of *LNCS*, pages 164–178. Springer, September 1999.
- [4] M. Bozga, J.Cl. Fernandez, and L. Ghirvu. Using Static Analysis to Improve Automatic Test Generation. In S. Graf and M. Schwartzbach, editors, *Proceedings of TACAS'00 (Berlin, Germany)*, LNCS, pages 235–250. Springer, March 2000.
- [5] M. Bozga, J.Cl. Fernandez, L. Ghirvu, S. Graf, J.P. Krimm, and L. Mounier. IF: An Intermediate Representation and Validation Environment for Timed Asynchronous Systems. In J.M. Wing, J. Woodcock, and J. Davies, editors, *Proceedings of FM'99 (Toulouse, France)*, volume 1708 of *LNCS*, pages 307–327. Springer, September 1999.
- [6] M. Bozga, J.Cl. Fernandez, L. Ghirvu, S. Graf, J.P. Krimm, and L. Mounier. IF: A Validation Environment for Timed Asynchronous Systems. In E.A. Emerson and A.P. Sistla, editors, *Proceedings of CAV'00 (Chicago, USA)*, volume 1855 of *LNCS*. Springer, July 2000.
- [7] 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.
- [8] M. Bozga, S. Graf, A. Kerbrat, L. Mounier, I. Ober, and D. Vincent. SDL for Real-Time: What is Missing ? In *Proceedings of SAM'00: 2nd Workshop on SDL and MSC (Grenoble, France)*, pages 108–122. IMAG, June 2000.
- [9] 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.
- [10] 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.
- [11] M. Bozga, S. Graf, L. Mounier, I. Ober, J.L. Roux, and D. Vincent. Timed Extensions for SDL. In *Proceedings of SDL FORUM'01 (Copenhagen, Denmark)*, volume 2078 of *LNCS*, pages 223–240. Springer, June 2001.
- [12] 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.
- [13] 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.
- [14] 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*.
- [15] VERIMAG/DCS. If web page. <http://www.verimag.imag.fr/~async/IF>.