Electronic Communications of the EASST
Volume X (2011)

Proceedings of the
11th International Workshop on
Automated Verification of Critical Systems
(AVoCS 2011)

Is my Formal Method Tool Ready for the Industry?

Christophe Ponsard, Jean-Christophe Deprez, Renaud De Landtsheer

2 pages

Guest Editors: Jens Bendisposto, Cliff Jones, Michael Leuschel, Alexander Romanovsky
Managing Editors: Tiziana Margaria, Julia Padberg, Gabriele Taentzer
ECEASST Home Page: http://www.easst.org/eceasst/ ISSN 1863-2122

Is my Formal Method Tool Ready for the Industry?

Christophe Ponsard, Jean-Christophe Deprez, Renaud De Landtsheer

{cp,jcd,rdl}@cetic.be, CETIC Research Centre, Belgium

Abstract: Using formal methods requires adequate tool support. Many formal tools emerge from academic prototypes and evolve towards Industry. This short paper summaries our on-going work under the auspices of DEPLOY project on providing answers to many practical questions frequently raised by Industry users regarding formal method tools notably performance, scalability, integration, user-friendliness, qualification/certification with respect to Industry standards.

Keywords: Formal Methods, Industry, Tooling, Certification

1 Introduction

The use of formal methods (FM) in the 21th century, especially in an industrial setting, cannot be considered without adequate tool support [BFLW09]. Quality aspects of FM tools are therefore a major factor influencing adoption. Potential industrial adopters frequently raise questions on this topic and it is not easy for them to find an answer given FM tools are a niche market requiring highly specialized skills.

This short paper presents some evidence taking the form of Frequently Asked Questions (FAQ) about tooling gathered during FM deployment experiments. Real experiments were carried out in the industry by the DEPLOY project (www.deploy-project.eu) and were compared with experience reported by others. In many cases, a comparative discussion is made between Open vs. Closed Source tools. A concise set of answers is presented here. More elaborated answers on this topic and other formal related themes can be found at: www.fm4industry.cetic.be.

2 Some FAQ about Formal Tools

Is there guarantee of long term Tool availability and support ? Industry projects may last tens of years from the development to the decommissioning of a system. It is therefore crucial for Industry to ensure proper support throughout the complete project lifetime including its retirement. Tools can be distributed under Open Source or Proprietary Licenses. Each model comes with its own risk to disappear (bankruptcy for proprietary code vs. community disappearance for Open Source). Given the niche market, securing the support is nontrivial task (e.g. escrow for proprietary code, direct community involvement or support for Open Source).

Is the Tool reliable? Closed source reliability is a mater of trust that can be provided by a certification scheme for example. Concerns have been raised about Open Source tools capability to achieve higher reliability [Cra99]. However the large number of industrial strength tools available nowadays tends to prove the contrary: e.g. PVS, nuSMV, and several others. Some reasons are related to the potential of massive peer review and at the design level, better defined interfaces and careful designs required for a distributed development. Furthermore, extensive test suites are often available for such Open Source tools.

Is the Tool scalable? The ability to scale up depends on different factors. Tool-induced limitations may be due to the underlying formal technology, implementation problems (e.g. some bottleneck in a processing chain) or simply usability (e.g. limitation to manage large pieces of models). To assess scalability, references, feedback and reviews provide initial information that is useful to directly rule out inadequate tools for Industry. A second step is to challenge the tool on realistic case study in various Industry sectors as the way models are built can also impact the ability to scale up. Open Source tools might have higher risk of not scaling up, especially if they are still at the R&D stage. However, there are also highly scalable Open Source tools in the area of FM (e.g. SPIN and nuSMV model-checkers, ACL2 and Isabelle theorem provers).

Is the Tool usable? It is important that tools facilitate various tasks when building or modifying a model, carrying out validation and verification activities, working in team, etc. Commercial tools generally have better usability because special attention is devoted to this aspect whereas Open Source tools tend to focus more on the core functionality and efficiency, with sometimes only a command line interface.

Does the Tool integrate well in Industry tool chains? The ability to integrate into existing industrial tool chains is fundamental. This requires the existence of well-documented data format, availability of APIs/binaries on specific OS's/integration with popular tool platforms. This is an area where Open Source usually outperforms proprietary tools. Furthermore, Open Source often adopt open standard data format. On the other hand, heightened competition frequently pushes proprietary tools to keep internal data format hidden.

What is the impact of my Tool w.r.t. Certification? Using a formal tool in the design flow (i.e. at design time) might have an impact on the certification process, especially if the tool is generating production artifacts such as source code for systems requiring higher integrity levels. Evidence of correctness of the output produced by these tools has to be provided by various means: redundant implementation, extensive test coverage, and specific verification activities. As a supporting success story, the ProB tool used by Siemens and developed by the University of Düsseldorf is undergoing a qualification for the railways EN-50128 standard.

Acknowledgements: This work is funded by the European Commission under the EU project DEPLOY (project reference number 214158).

Bibliography

[BFLW09] J. C. Bicarregui, J. S. Fitzgerald, P. G. Larsen, J. C. Woodcock. Industrial Practice in Formal Methods: A Review. In *Proceedings of the 2nd World Congress on Formal Methods*. FM '09, pp. 810–813. Springer-Verlag, Berlin, Heidelberg, 2009.

[Cra99] D. Craigen. Formal Methods Adoption: What's Working, What's Not! In *Proceedings of the 5th and 6th International SPIN Workshops on Theoretical and Practical Aspects of SPIN Model Checking*. Pp. 77–91. Springer-Verlag, London, UK, 1999.