Project DEPLOY
Grant Agreement 214158
“Industrial deployment of advanced system engineering methods for high productivity and dependability”

DEPLOY Deliverable D2

D14.05 Electronic Newsletter

Thierry Lecomte (ClearSy)

Public Document

31th July 2010

http://www.deploy-project.eu

DEPLOY PROJECT

Newsletter N° 5

Contents

Partners

Introduction

The DEPLOY project aims at making major advances in engineering methods for developing dependable systems through the use of formal methods and tools. The project approach is totally driven by industry needs and is based on large deployment experiments in four major industrial sectors, namely Automotive, Transportation, Space, and Business Information. The project's success will therefore be largely determined by the degree of industrial take-up of the proposed formal methods and tools by the DEPLOY industrial partners.

The DEPLOY controlled deployments offer a unique opportunity to understand the decisive factors favouring or hindering the adoption of formal methods. During the project, the DEPLOY industrial partners are experimenting with the whole process of introducing formal engineering methods in their organisation. They are facing issues like having to decide the scope of what to formalise, how to adapt the development process to ease the formalisation and to make it valuable, how to train people on the formal methods, tools and techniques. These deployments are thus closely monitored to identify and collect evidence related to the impact of deploying formal methods in an industrial context. A consolidation with experiences reported by others is also part of this work.

While the primary audience of this activity is currently the DEPLOY industrial partners who need to convince their own organisations, **the end goal is to produce public material that will help companies to make an informed decision about the opportunity to adopt formal engineering methods and how best to address the major issues that often arise when taking up formal methods**.

In order to make the evidence publicly available to a wider audience, it is necessary to think carefully about the way to structure and format the collected material. At some point, it will also be important to open the process to external contributors.

Learning from Experience: DEPLOY develops Role-based FAQ

To best grab the attention of an industrial audience, a FAQ (Frequently Asked Question) structure listing important questions is used to present DEPLOY's key results. Furthermore, it is also observed that different roles in an organisation are interested by different types of questions. Thus, FAQ questions are organised by Themes and Roles. Beside a few general questions, specific key themes of interest are:

- The impact on an organisation with regards to training scope and resourcing
- The impact on the quality of a product developed using formal methods
- The capability to exploit formal models at various stages of the development process
- The capability to perform reuse across development projects when formal methods are used, including reuse of formal and proven artifacts
- The capability to phase the learning of a formal method in an organisation and eventually to restrict the scope of who must understand and become an expert in a formal method
- The capability to phase the migration to using a formal method (given the existing context)
- The known strengths and weaknesses of tools associated with a formal method as well as the support quality of the tool providers
- The external factors (from competition, standards bodies, laws) pushing the take-up of formal methods

To make sure that the essential points of these themes are covered, questions are raised from four different viewpoints roughly corresponding to the following organisational roles:

- **High-Level Managers:** managers of production or R&D departments have to take strategic decisions and assess the financial impact of using new methods and techniques. Furthermore, this role includes product and product line managers who are concerned with the commercial aspects of products.
- **Project and Quality Assurance Managers** directly manage engineers, analysts, and QA practitioners. They have to determine project feasibility and they directly manage staff working on system development projects. They do not perform technical tasks but often need to have a good understanding of the methods and tools used by their teams so they can determine the feasibility of a project, decide the profile to allocate tothe project and possibly identify the associated training, and adapt quality assurance procedures.
- **Engineers and Analysts** represent people who work directly on system development projects. They are among those who apply the engineering methods selected and who use the associated tools.
- **QA Practitioners** perform the QA tasks such as document review, traceability checks, integration and system testing. In general, QA practitioners do not need to apply formal methods but they need to understand them because work products that they review and use are expressed in the selected formalisms.

The four roles presented above cover a large range with diverse needs. Thus, identifying questions that interest each of these roles on all the themes listed earlier will undeniably cover all the important aspects related to the impact of deploying formal methods in a company.

The natural way to structure this information is a web-based FAQ. It provides the appropriate mechanism to structure information along different dimensions: themes, roles, and industry sectors. A partial example of a question/answer is presented below. In addition to the question/answer, the theme and the role associated to the question are also listed.

Theme	Exploiting formal models at various stages of the development process
Roles	• Engineer and Analyst • QA practitioner
Question	Is it possible to take advantage of formal models beyond using them to guarantee certain properties of a system, for example, to automate certain development and QA tasks?
Answer	Siemens Transport is showing how Engineers can generate FMEA and system documentation from Event-B models and to connect those to their existing B development chain. SAP showed how Engineers could help QA practitioners by generating integration test cases for testing business processes. Formal models were developed to prove certain properties of the business processes and then these formal models generated interesting test cases not yet imagined by QA practitioners.

Success (and Failure) Stories

In addition to a question oriented approach, it is also interesting to provide stories reporting more comprehensively on key topics, explaining in detail how a real world industrial situation benefited or not from formal methods. Not only success shall be reported as one should also learn from mistakes. Examples of success stories elaborated within the project include:

- the use of requirements models to prepare the formalisation (Bosch)
- the improved capacity to model and prove complex systems in the space sector (SSF)
- the use of model-checking techniques to perform time-consuming data validation (Siemens)
- the use of domain specific notations to hide formal methods and foster adoption (SAP)
- the benefits of formal models for model-based test automation (SAP)
- the risk and benefits opportunities related to the use of open-source tools for formal methods (Systerel)
- the technology transfer and training needed to reach autonomy in the application of formal methods (ETHZ)

The reported success stories are not restricted to the internal project contributions but are also being consolidated with similar experience reported by others in the literature or from the collaboration activities DEPLOY is organising through its associate program, interest group and dissemination events.

How you can contribute

The DEPLOY evidence work is currently being opened to external contribution. The developed FAQ will be published on-line in the form of an interactive wiki during year 3. The URL of the public wiki will be announced in a future newsletter and on the DEPLOY website. An early public report is however already available at: http://www.deploy-project.eu/pdf/d7-revised-final.pdf.

If you wish to join our effort and contribute material on the impact of formal methods on your organization or on your products, please contact us at: christophe.ponsard@cetic.be. CETIC is the leading partner on the Evidence collection and dissemination effort.

Christophe Ponsard and Jean-Christophe Deprez

DEPLOY: Current State

During the last 6six months the main focus of the consortium has been on conducting the initial work on full deployment of DEPLOY methods and tools in the four deployment partners, and on strengthening the Rodin platform to enable and support the full deployment.

Issue 3 of this Newsletter informed the reader about the project refocus conducted in Spring 2009. The refocus was largely driven by the needs of the deployment partners. During the last six months we have seen the appearance of its first positive results. These include industrial applications of the model based testing plugin, development of the first version of the code general features ready now for the internal evaluation and a close integration of the two DEPLOY Associates into our work. A substantial refocus of project work on measurement is reported in the leading article of this issue. We are now putting more focused efforts on ensuring that the deployment partners will have strong concrete evidence of the benefits the technology brings to their engineers and managers.

Following our successful proposal aiming at enlarging DEPLOY, submitted in call 9.5 in 2009, from June 1, 2010 we have been expanding our work on model composition and model-based testing, specifically focusing on improving the component-based design using the interactive system paradigm, and on advancing model-based testing by using search-base evolutionary approaches. This work will be carried out with the involvement of two new DEPLOY partners from Romania: University of Bucharest and University of Pitesti.

The most important area of our ongoing work is enhanced (full) deployment of DEPLOY methods and tools in the four sectors, specifically focusing on their full integration into the existing development environments of the project deployment partners. We are now making substantial methodological and tooling advances, which will enable us to achieve this. In this work we are expanding the scope of our work by addressing complex combinations of real issues typically raised in the development of medium/large scale applications in industry. During the coming months the consortium will be continuously reassessing the needs of the deployment partners to reduce the risk for the project.

The project partners have now in place a plan for preparing an edited book in which we will summarise our experience and results in deploying advanced formal methods in industry. The book will be completed after the end of the project and will be written by all industrial and academic partners with first hand experience in such deployment.

Alexander Romanovsky, Newcastle University
Project Coordinator

Update on the Rodin Platform

New features have been added and several bugs have been fixed in each new release of the Rodin platform. Thus, users are encouraged to check the calendar of releases and to keep their Rodin tool up-to-date (see http://wiki.event-b.org/index.php/Rodin_Platform_Releases).

The most recent version of the platform is Rodin 1.3.1. The major version 2.0 is currently under development.

Rodin Release 1.3 (released in May 2010)

See http://wiki.event-b.org/index.php/Rodin_Platform_1.3_Release_Notes. This release aims to improve the Rodin platform, and target the different underlying tasks:

- **Proving.** A new Proof Replay command has appeared which tries to prove undischarged POs by reusing older proofs. This command is accessible when right-clicking in the Event-B explorer.
- **Modelling.** The creation of new projects and Event-B components has been homogenised and now rely on the same wizard (File > New in menubar, button in the toolbar or in the Event-B explorer, context menu, etc). Moreover, the label prefixes may be customised, either globally (workspace scope) or locally (project scope).
- **Developing.** It is possible to extend the Pretty Print page, with the same kind of mechanism used to extend the structured editor.

Rodin Release 1.3.1 (released in June 2010)

See http://wiki.event-b.org/index.php/Rodin_Platform_1.3.1_Release_Notes. This release fixes three critical bugs (#2995930, #2999977 and #3006807) in the prover. The Rodin team is proud to be able to react quickly to major issues and to produce intermediate releases if necessary.

Rodin Release 2.0 (expected in September 2010)

See http://wiki.event-b.org/index.php/Rodin_Platform_2.0_Release_Notes. This major release will be an answer to several user requirements:

- **Modelling.** The mathematical extensions will allow defining basic predicates, new operators or new algebraic types. Moreover, it will be possible to use the same name for independent quantified variables (Previously declared bound identifier redeclared as bound identifier). Beyond that, some cumbersome behaviours will be improved (statistic view, selected hypotheses view), and some performance issues will be addressed (the navigation through the proof tree nodes will be faster).
- **Proving.** The Proof Replay, Retry Auto Provers and Recalculate Auto Status commands now run in the background, and the user can continue to work on a model and to perform interactive proofs while they are running.
- **Developing.** This release will be based on Eclipse 3.6 (Helios). It will allow a simplified addition of tactic providers for the proving UI and will provide a new mechanism to collect information while traversing formulas.

Only a 64-bit version of Rodin 2.0 will be provided for Mac platforms. In other terms, Rodin 2.0 will support Mac OS X Snow Leopard, but will not support PowerPC or 32-bit Intel Macs any longer.

Only a 32-bit version of Rodin 2.0 will be provided for Windows and Linux.

Thank you to help us to improve the Rodin platform

The Error Log view is now available (release 1.3 and newer) among the other General views. It is accessible from Window >Show view> Error Log. This information is very useful for developers, and it is intended to be copied/pasted by users when posting bug reports:

http://sourceforge.net/tracker/?group_id=108850&atid=651669

Carine Pascal, Systerel

Update on the Rodin Plug-ins

Some new plug-ins have been released since the last newsletter:

- **Structured Records:** The Records plug-in introduces a new modelling construct to provide a notion of structured types in Event-B Contexts. The plug-in supports the notion of record extension (extending record structures with new fields) and record subtyping: http://wiki.event-b.org/index.php/Records_Extension
- **Team-based Development:** The team working plug-in enables Event-B models to be stored in a repository (e.g. SVN). Models can be compared with versions in the repository and differences can be merged back into the local version. This relies on the Event-B EMF framework and serialisation into an XMI copy of the model: http://wiki.event-b.org/index.php/Team-based_development

Existing plug-ins include the Camille text editor, Decomposition, UML-B, ProB, Modularisation, and the Rule-based prover.

There are also some upcoming extensions under development:

- **Mathematical extension:** Currently the rule-based prover uses a new theory component in which users can define rewrite rules that are used in automatic and interactive proof modes. The core platform and plug-in are being extended to support users to define new polymorphic operators and predicates as well as inductive datatypes (lists, trees, etc) and general inference rules.
- **Code generation:** We are working on generation of code from refined Event-B models. This will support generation of concurrent implementations in Ada and C. Support for explicit control structures in refined models is being added and these models will then be automatically transformed into a specially developed intermediate language. A back-end is being developed to translate the intermediate language to Ada. Later a back-end for C will be added.

The most up to date information on all plug-in developments can be found on the Event-B wiki:

See http://wiki.event-b.org/index.php/Current_Developments

Michael Butler, University of Southampton

DEPLOY Associates

As reported in the last Newsletter, two Deploy Associates have joined the Deploy Associates Scheme:

- **Automação E Systémas (AeS) - Sao Paulo (Brazil):** A very successful one week Event-B and UML-B training session was held in Sao Paulo in May with trainers from the University of Southampton. 15 People participated including one from Alstom Brazil. AeS have commenced work on their Event-B and Rodin pilot, which is an automatic platform door system for metros.
- **Critical Software Technologies (CSWT) - Southampton (U.K.)** A series of half-day Event-B training sessions have been held between CSWT and the University of Southampton. CSWT have commenced work on their Event-B and Rodin pilot, which is an avionics subsystem.

Michael Butler, University of Southampton

Focus on a Past Event: B Dissemination Day workshop (Tokyo, 17 March 2010)

This workshop, a satellite event of the GRACE International Symposium on Advanced Software Engineering, aimed at providing a clear picture of B/Event-B current status of development and exploitation, focusing on the support tools as well as the industrial applications.

The workshop included a large range of presentations given by the DEPLOY project members or associated to the project results.

Around 80 persons attended the workshop, with a massive participation from industry.

See http://www.bmethod.com/php/conference-grace-2010-en.php for details.

Future Events

Workshop on B Dissemination, Natal (Brazil) 8-9 November 2010

This workshop, a satellite event of the SBMF 2010 conference, held in Natal (Brazil), is organized within the framework of the DEPLOY project. Its objectives are to present current status, ongoing research and development related to B and Event-B languages, as well as applications to industry size problems. Topics addressed by the workshop are many:

- Tool development (language extensions, external provers, code generation, etc.)
- Modeling challenges (real time properties, probabilistic refinement, high order logic, etc.)
- Deployment (methodology, cases-studies, return of experience, scaling up, etc.)

The workshop lasts two days:

- The first day is devoted to DEPLOY speakers. General presentation of the project and tools are supported by focused talks on scientific/technical matters (modeling time, code generation, model animation, model checking, etc.) that are being researched in DEPLOY. Reports on industrial applications (space, railways, automotive, information systems, etc.) complete the day.
- The second day is open to any presenter, through an international call for papers. Expected contributions would range from theoretical research to practical applications of B/Event-B.

See http://www.bmethod.com/php/conference-sbmf-2010-en.php for details.

Second Rodin User and Developer Workshop, Dusseldorf (Germany), 20-22 September 2010

Invited speakers:

- Jean-Raymond Abrial, Consultant, Marseille, France
- Joseph Kiniry, IT University of Copenhagen, Denmark

After the First Rodin User and Developer Workshop in July 2009 at the University of Southampton was well received by users and developers of Rodin, this year's workshop is going to take place at the University of Duesseldorf. The workshop is going to be colocated with AVOCS 2010, the 10th International Workshop on Automated Verification of Critical Systems (www.formal-methods.de/avocs10), September 21-23, 2010. While much of the development and use of Rodin takes place within the EU FP7 DEPLOY Project (www.deploy-project.eu), there is a growing group of users and plug-in developers outside of DEPLOY. The purpose of this workshop is to bring together existing and potential users and developers of the Rodin toolset and to foster a broader community of Rodin users and developers.

For Rodin users the workshop will provide an opportunity to share tool experiences and to gain an understanding of on-going tool developments. For plug-in developers the workshop will provide an opportunity to showcase their tools and to achieve better coordination of tool development effort.

The format will be presentations together with plenty of time for discussion. On Day 1 a Developer Tutorial will be held while Days 2 and 3 will be devoted to tool usage and tool developments.

If you are interested in giving a presentation at the workshop, send a short abstract (1 or 2 pages of A4) to rodin@ecs.soton.ac.uk by 9 August 2010. Indicate whether it is a tool usage or tool development presentation. Plug-in presentations may be about existing developments or planned developments.

Workshop registration details will be available in due course. Check www.event-b.org for details.

Call for Contributions

We are inviting anyone interested in DEPLOY to contribute to its success. Expected contributions are diverse:

- feedbacks from using the Rodin platform and its related documentation
- experience while using the DEPLOY formal approach on academic/industrial case-studies
- integration to the open-development team (refer to the roadmap www.event-B.org/roadmap.html
- development of new plug-ins
- release of educational material (refer to the DEPLOY publications site http://deployeprints.ecs.soton.ac.uk)

If you are interested in joining, send an email to thierry.lecomte@clearsy.com who will connect you with the right person.

We need to know who you are

The Rodin platform has been downloaded more than 9.000 times, the event-b.org website has 650 unique visitors a month, and up to 1400 for the wiki.event-b.org website. But, as sourceforge downloads are anonymous, we have almost no clue about the user community that is being set up. In order to know who you are and what is your usage of the Rodin platform, a very short survey has been set up. We invite you to spend a few minutes filling the form. A synthesis will be published when enough data have been collected. The survey is reachable at: www.deploy-project.eu/html/enquiry-001.php

Edited by ClearSy www.clearsy.com - Editor: Thierry Lecomte thierry.lecomte@clearsy.com
www.deploy-project.eu/ - www.cordis.europa.eu/fp7/ict/