Project DEPLOY
Grant Agreement 214158

“Industrial deployment of advanced system engineering methods for high productivity and dependability”

DEPLOY Deliverable D2

D14.06 Electronic Newsletter

Thierry Lecomte (ClearSy)

Public Document

31th January 2011

http://www.deploy-project.eu

SEVENTH FRAMEWORK PROGRAMME

DEPLOY PROJECT

Newsletter N° 6

Contents

Partners

Introduction

The goal of the DEPLOY project is to make Formal Methods ready for routine application in industrial practice and - by this - make industrial software engineering more efficient and the resulting software products more reliable. However, software engineering processes, methods, and tools in companies like those of the deployment partners in the project are well established and radical changes are often simply infeasible.

For SAP, this is the crucial challenge with respect to the adoption of Formal Methods: how easily can Formal Methods be integrated with existing processes, methods, and tools in a non-disruptive way? And since acceptance of new methods by developers is of greatest importance: how can we make Formal Methods so attractive for developers to use that they see a productivity increase in their daily work?

The DEPLOY project is an ideal opportunity for answering these questions. From the very beginning there has been an intensive exchange between the academic partners in the project and our research team at SAP. We very often base our exchange on simple but realistically sized examples from which academic partners learn how our problems look like and by which we can deepen our expertise in applying formal approaches.

What have we achieved in the first three years of DEPLOY? The goal of easy integration could be met to a large extent. From a tooling side the usage of Eclipse as the base platform of Rodin allowed for an easy integration with our modelling infrastructure, based on Eclipse as well.

We soon learned that the acceptance of developers could only be achieved if the modelling formalisms already in use, and more importantly the modelling content already available, could be re-used. This required the integration of our graphical in-house modelling languages and the import of modelling contents into Event-B and Rodin. From UML-B we could learn the seamless integration of Event-B and Rodin with graphical modelling. However, since our development is often based on domain-specific languages for various purposes (e.g. process modelling, business object modelling, service choreography modelling), we use our own translation to Event-B.

Another important point was to build on existing quality assurance (QA) methods for which processes and tooling infrastructure already exists. At SAP, testing is still the pre-dominant QA technique with dedicated environments and deep expertise. While the Event-B community mostly advocates a strict top-down model-based approach with interactive / automated proofs of correct refinement, we accepted the fact that testing will play an important role in the QA concept for business applications for a considerable time.

We therefore implemented – with the help of the Rodin-integrated model checker ProB – a model-based testing extension, which takes Event-B models translated from our in-house models and systematically generates checks, with guaranteed coverage control and high automation. With it, developers build models, have the benefit of good automated test cases, possibilities for model simulation (which we implemented on top of ProB) or consistency checks (again with ProB and with the Rodin provers). Luckily, the tools offered a lot of flexibility even if we did not follow the originally intended modelling process.

As to be expected in a research project, there are issues which are yet unsolved:

- How to deal with scalability issues of Rodin?
- How to improve the automation of consistency checks, which is crucial if we would like to use our in-house languages as the only interface to the user?
- How to match the refinement concept in Event-B better, which does not exist in our internal modelling languages?
- How to deal with issues of finding suitable test data in our model-based testing approach, when we are dealing with data-intensive software?

Our goals for the remaining time in DEPLOY is to find answers to these and many more research questions which need solution if we like to lay a foundation for Formal Methods within our company.

Moreover we would like to extend the reach of our approach towards business process models (realized in languages such as the Business Process Modelling Notation BPMN), which are the most important type of models for business applications. With the whole DEPLOY consortium we are sure to have excellent partners for making significant steps towards these goals.

Andreas Roth
SAP, Software Engineering Research

Electronic Dissemination

With the release of the Rodin platform 2.0 in October 2010, the number of 10 000 downloads has been reached by the beginning of January 2011. As seen on figure 1, each release has been regularly downloaded between 500 and 1 000 times since July 2007, except for the version 0.8.2 scoring more than 2 000 downloads. Most of the user base (61%) is running the platform on Windows computers, 25% on Linux and 14% on MacOS.

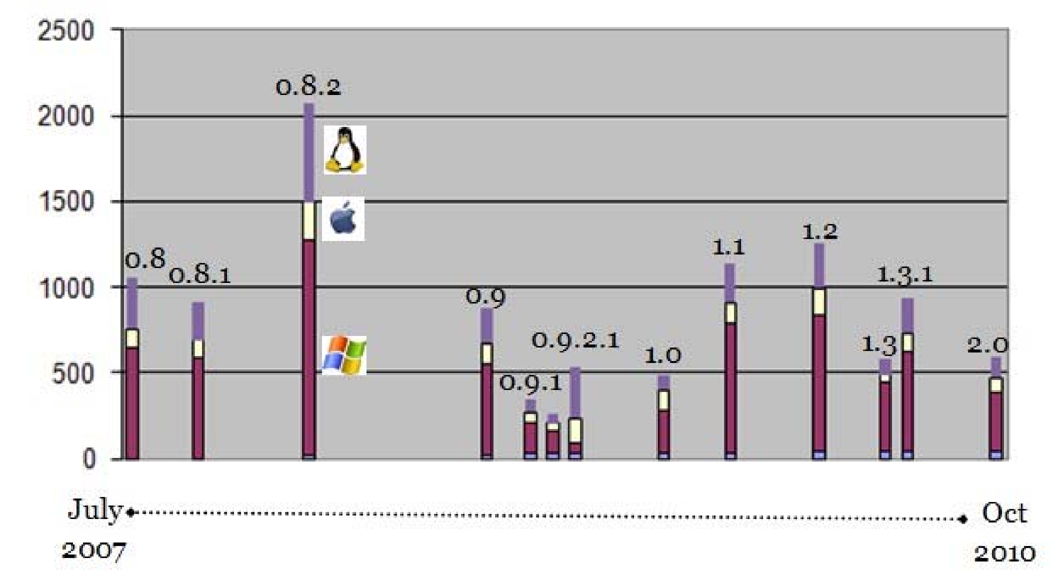

Figure n°1: number of downloads per version and per OS

During these 3 years, the number of visits of the 3 websites run by DEPLOY has slightly increased (see figure n°2) to reach a total of more than 330 000 visits. The www.deploy-project.eu website, presenting the project, the partners and offering all deliverables produced by the project, is the most visited site, especially during the third year of the project with a number of visits multiplied by 2 in the mean time. This situation is very likely caused by the increasing maturity of the project results and the improved quality of project reports.

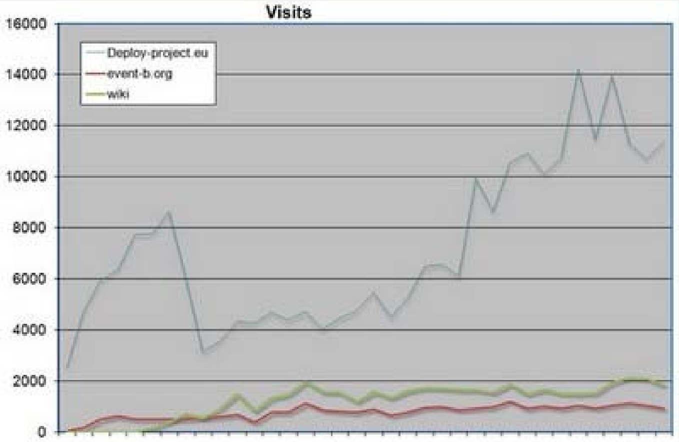

Figure n°2: number of visits during the first 3 years of the project

For the fourth and last year of the project, with the integration and finalization of the existing and new features, we are anticipating a better dissemination both in the industry and in the academic world.

Thierry Lecomte,
ClearSy

Update on the Rodin Platform

On the existing release page, the user can now learn more about the available plug-ins and their compatibility: http://wiki.event-b.org/index.php/Rodin_Platform_Releases. The most recent version of the platform is Rodin 2.0.1. The version 2.1 is currently under development.

Rodin Release 2.0 (released in October 2010)

See http://wiki.event-b.org/index.php/Rodin_Platform_2.0_Release_Notes. This release includes in particular the following new features:

- **Mathematical extensions.** They are available through the theory plug-in (http://wiki.event-b.org/index.php/Theory_Plug-in). Existing theories are collected on a dedicated page (http://wiki.event-b.org/index.php/Sharing_theories) and will be progressively enriched by users.
- **Auto-completion** has been added to wizards and to the proof control.
- **Rule Details view**. The details of a proof can now be displayed using this view, which shows up the various operations performed by a rule on a proof tree node. See http://wiki.event-b.org/index.php/Rodin_Proving_Perspective#Rule_Details_View.

Rodin Release 2.0.1 (released in November 2010)

See http://wiki.event-b.org/index.php/Rodin_Platform_2.0.1_Release_Notes. The version 2.0.1 of Rodin is a maintenance release which includes mainly bug fixes. The Rodin team aims to produce bug free platforms.

Rodin Release 2.1 (expected in January 2011)

See http://wiki.event-b.org/index.php/Rodin_Platform_2.0_Release_Notes. This minor version of the release contains corrections as well as evolutions. Some improvements are noteworthy:

- **General interface**. Improved general platform performance: one of the main tasks of scheduled future work is to increase platform's performances. Investigation is on the way and some early enhancements are already part of the release 2.1.
  In parallel, several tactic profiles (i.e. ordered lists) of tactics can be defined and used in post or automatic tactics at both workspace and/or project level. A mechanism is also provided in order to import/export and share these profiles. This is the first step of the evolution concerning proving strategies.
  See http://wiki.event-b.org/index.php/Preferences_for_the_automatic_tactics.
- **Proving**. Over 150 automatic rewriting rules have been added, making it easier to discharge proof obligations, and changing the proving experience. The proving interface now uses other graphical components to increase the responsiveness of the platform and avoid bugs related to large model proving.

Carine Pasca l& Thomas Muller,
Systerel

Update on the Rodin Plug-ins

Existing plug-ins have continued to evolve and two significant new plug-ins have been released.

- **Theory plug-in:** The Theory plug-in allows users to extend the mathematical language of Event-B and the Rodin proof support. New mathematical data types, operators and proof rules may be defined in a Theory component and then used in an Event-B model and in proofs for that model. Definitions and rules are constructed by the user in a similar manner to Event-B contexts and models. Proof obligations are generated from definitions and rule to validate their soundness. Basic theories for sequences and bags have been defined. Over time we will build up a standard library of mathematical theories that augment the in-built theories of Rodin.

- **Code generation:** A demonstrator for a code generation tool has been developed. The plug-in supports generation of multi-tasking Ada code. The plug-in provides an extension of an Event-B machine called a Tasking machine that includes additional information used for code generation such as event sequencing. The approach supported by the plug-in is designed to fit with the shared-event decomposition supported by the Rodin decomposition plug-in; a model is decomposed to separate tasks using the decomposition plug-in and these tasks are then translated to Ada tasks. The plug-in supports limited data types currently; we are working on developing a support for richer data types (to be included in a release later in 2011).

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

AeS Brazil

Aes have made good progress with their pilot deployment of Rodin. The target of the pilot is a "dead man control" for metros trains, responsible for applying emergency brakes in case of any problem with the train operator. UML-B was used for the specification. Several gaps were found in the natural language (NL) specification that required clarification with the specialists, resulting in an improved rewritten NL specification. They are currently formalising a safety function for hardware failure detection for the system. AeS are also working with DEPLOY partners on more research-oriented topics. They are working with The University of Dusseldorf on linking the WRSPM approach to requirements analysis with Event-B modelling. They are exploring extensions to UML-B for use cases, activity diagrams and sequence diagrams. AeS are also working on a Rodin plug-in that will use Event-B to validate safety boolean equations used in train signalling.

Critical Software Technologies

Critical Software have made good progress on their pilot. The system under analysis is an Integrated Secondary Flight Display (ISFD) used onboard commercial or military aircraft. The ISFD provides attitude, air and navigation information required to land the aircraft in the event of a primary display failure. Critical have developed a structured requirements document for the ISFD following guidelines provided as part of the DEPLOY Associate training. This structured requirements document has facilitated construction of a generic model of the ISFD in Event-B. The identification of a generic system has been facilitated by the abstraction capabilities provided by Event-B.

XMOS

XMOS recently became a DEPLOY Associate. XMOS is a UK-based “fabless” semiconductor company that develops multi-core, multi-threaded processors targeted at embedded systems markets. XMOS has developed several core pieces of technology, including a multi-threaded multi-core processor (XCore), an interconnect switch that can route messages between cores, and a link that can be used to interconnect these switches. Support for these features is integrated into the Instruction Set Architecture (ISA) of the XCore. XMOS have embarked on a project to construct a formal model of the ISA of the XCore microprocessor using Event-B. This builds on the methods developed by Dr Stephen Wright to model ISAs using Event-B and Rodin which makes extensive use of refinement to structure ISA models. The aim is to be able to manage future incremental upgrading of the ISA, by verifying the preservation of essential properties. This work is funded by a one year EPSRC Knowledge Transfer Secondment running since October 2010 under grant EP/H500316/1.

Michael Butler,

University of Southampton

Focus on a Past Event: Workshop on B Dissemination Natal, 8-9 November 2010

This two-day workshop, a satellite event of the Brazilian Conference on Formal Methods (SBMF), was held in Natal, 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 scope of presentations given by the DEPLOY project members or associated to the project results as well as contribution from external researchers and industrialists.

See http://www.bmethod.com/php/conference-sbmf-2010-en.php 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
- development of new plug-ins
- release of educational material (refer to the DEPLOY publications site http://deploy-eprints.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 10 000 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 users 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 spent few minutes to fill the form. A synthesis will be published when enough data have been collected. The survey is available 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/