Contents

About Deploy
The RODIN Platform
Progress
Meetings
Deploy Interest Group
Future Events
Call for Contribution

Partners

About Deploy

The overall aim of DEPLOY 1 is to make major advances in engineering methods for dependable systems through the deployment of formal engineering methods. The work is driven by the tasks of achieving and evaluating the industrial take-up of the DEPLOY methods and tools. The aim will be achieved with a coherent integration of scientific research, technology development and industrial deployment of the technology. The complementary expertise and technological base of the industrial deployment partners and the technology provider partners will be combined to achieve a set of challenging scientific and technological objectives.

The DEPLOY consortium sees the problem of building dependable, well-architected and evolvable computer-based systems as crucial to the future of European industry at large and not just its IT industry. From its considerable experience of building large complex systems, the consortium has strong evidence that dependability can be achieved for such systems through the use of formal engineering methods that are grounded in mathematical modelling and analysis. Moreover, we believe that to build trustworthy systems developers need to incorporate appropriate resilience mechanisms in their design in a systematic way to ensure that these systems continue providing the expected service in spite of various erroneous conditions in the systems and their environments.

The successful three-year STREP 2 RODIN project researched and developed industrial strength methods and tools paving the way for the technology to be deployed. In particular, RODIN delivered an extensible open source platform, based on Eclipse, for refinement-based formal methods along with a body of work on formal methods for dependable systems. DEPLOY exploits and builds on these results.

The project is coordinated by Newcastle University with a dedicated Project Office set at the School of Computing Science.

I would like to welcome you to the first issue of the 6-monthly Newsletter reporting on the implementation of our project and to encourage you to follow our work and to apply our results in developing your systems.

Alexander Romanovsky
Project Coordinator

1 FP7 ICT Integrated Project (February 2008 - January 2012) on Industrial Deployment of Advanced System Engineering Methods for High Productivity and Dependability

2 Specific Targeted Research Project

The RODIN Platform

The Rodin platform is an extensible open source platform that was developed during the FP6 RODIN (Rigorous Open Development Environment for Complex Systems, 2004-2007) project, as well as some plug-ins that contribute to extend its functionality. Within DEPLOY, this platform is being strengthened and made ready for industry, by delivering improved or new services applicable to large, complex models.

The Rodin platform is an open platform based on Eclipse and specialized for formal modelling. It provides all the tools needed to support system modelling with the event-B notation (static checker, proof obligation generator and prover), and many more additional tools which are deemed useful in the area of system modelling.

Main Objectives
A reactive platform

In order for formal modelling to be used safely and effectively in engineering practice, good tool support is necessary. Present day integrated development environments used for programming do carry out many tasks automatically in the background and provide fast feedback when changes are made to a program text. In particular, there is no need for the user to start processes like compilation. A program is written and then run or debugged without explicitly compiling it (everything happens in the background, without the user noticing it).
The Rodin platform is a transposition of this approach to formal modelling. Instead of compilation, we are interested in proof obligation generation and automatically discharging trivial proof obligations. Instead of running a program we reason about models or analyse them.

**An open platform**

Our view is that no one tool can solve all our modelling problems and that it is important to apply a range of tools in a complementary way. For example, it makes sense to apply model checking as a pre-filter, before applying a theorem prover to a proof obligation. Similarly the use of a diagrammatic views (e.g., UML) of a formal model can aid with construction and validation. Many analysis tools, such as model checkers, theorem provers, translation tools (e.g., UML to B and code generators), have been developed, some of which are commercial products and some research tools. However a major drawback of these tools is that they tend to be closed and difficult to use together in an integrated way. They also tend to be difficult for other interested parties to extend, making it difficult for the work of a larger research community to be combine.

One objective of the Rodin platform is to greatly extend the state of the art in formal methods tools, allowing multiple parties to integrate their tools as plug-ins to support rigorous modelling methods. This is likely to have a significant impact on future research in formal methods tools and will encourage greater industrial uptake of these tools.

As well as supporting the combination of different complementary tools, openness and customizability is very important in that it will allow users to customize and adapt the Rodin platform to their particular needs. For example, a car manufacturer using event-B to study the overall design of a car information system might be willing to plug some special tools able to help defining the corresponding documentation and maintenance package. Likewise, a rocket manufacturer using event-B might be willing to plug a special tool for analysing and developing the failure detection part of its design.

**Architecture**

The architecture of the Rodin platform is given in the schema below. The platform is decomposed in two parts: the Eclipse part and the Rodin specific part. The Eclipse part provides basic functionality for building IDEs. The Rodin part, built on top of it, adapts this general framework to the specific needs of formal modelling.

In the center of the Rodin part lies the core of the Rodin platform. It consists of one plug-in that implements a database (repository) of modelling items organized hierarchically, and a builder that is the mechanism that runs all tools in the background without user intervention. This latter mechanism is at the core of the platform reactivity.

On the left, appear the Kernel plug-ins which are specific to event-B. These plug-ins are:

- The AST library that allows manipulating mathematical formulas.
- The Sequent prover that provides a general framework for performing, storing and retrieving proofs in the Sequent Calculus. This proving framework is extensible, so that people can contribute new “reasoners” that become an integral part of the prover.
- The core event-B tools that support the modelling activity: Static Checker, Proof Obligation Generator and Proof Obligation Manager.
- The event-B user interface, which supports the two main activities of modellers: entering a model and proving it correct.

On the right appear all external plugins which are not part of the basic platform itself, but interface with it to provide additional tools or user interfaces to the user.

**Current extensions**

At the time of writing, the extensions available publicly for the Rodin platform are:

- B4free provers: Provide additional automated proof facilities to the existing Rodin provers (based on the B4free tool for the B Method).
- UML-B: Provides a UML-like graphical front-end for event-B modelling. It adds class oriented
and state machine modelling capabilities. UML-B is automatically translated into event-B for analysis and verification.

- **ProB**: Provide automatic animation of EventB models and can be used to systematically check a model for errors. In addition, it can assist the proving process and can be used as a disprover on individual proof obligations. The plug-in is based on the ProB model checker for the B Method.
- **B2Rodin**: Enables importing Atelier B models into Rodin. Only event B compliant models are supported.
- **B2LaTeX**: Produces latex printing of event B models
- **Brama**: Animates B models. Animation capabilities are twofold: first, debugging B models: the designer can verify by experiment that a model and a system have similar behaviour. Second, connecting B models with a flash animation: B models are used to trigger a flash animation.
- **Mobility**: Provides automated verification of mobile agent systems. Implements a newly developed high level programming notation, hybrid of event-B combined with constructs inspired by two process algebras (KLAIM and pi-calculus). Furthermore, the tool is capable of model checking event-B specifications (deadlock detection and invariant checks). The model checking engine is based on Petri nets unfoldings.

**Work in progress**

The 2008 work-program for the DEPLOY project concentrates on the following topics:

- Enhancing documentation. Some documentation exists, targeted at both end-users and plugin developers. However, it is currently incomplete and partially obsolete. We're working hard at improving it. Any help in this area is welcome. Just have a look to the platform Wiki and do not hesitate to contribute. Contact the Tool Coordinator if you would like to contribute.
- **UI**: some major improvements are in the works: providing undo/redo in the modelling interface, and implementing some simple refactoring (for instance renaming of variables, events or components). Also, the classical editor will become easier to use and a new text based editor is in development.
- **Animation and model-checking**: tighter integration of the ProB plug-in is in development, as well as a new interface for model animation (connected to flash interfaces)
- **UML-B integration**: being improved to provide better support for refinement in UML-B
- A prototype plug-in for requirements management is being developed.
- Various improvements to the prover are planned, especially incorporation of new reasoners for enhancing user experience.

For all these tasks, help from external contributors is much welcome. Please contact the Tool Coordinator for further details.

A major release of the platform is planned for 15 September. This release will incorporate some non-backward-compatible changes to the database and the mathematical languages. However, a transition solution will be provided so that users do not loose their models or proofs.

**Contact and Further Information**

Michael Butler (mjb@ecs.soton.ac.uk) is the Tool Coordinator of the DEPLOY project. He is in charge of coordinating efforts devoted to tooling issues both within the DEPLOY project and outside (external contributors).

Laurent Voisin (laurent.voisin@systerel.fr) is responsible for WorkPackage 9, that is the tooling workpackage of the DEPLOY project. He is also the reference person for all technical issues regarding platform development and coordination at the technical level (API evolution, coding guidelines, etc.)

More information about the Rodin platform can be obtained from the web site: [http://www.event-B.org](http://www.event-B.org)

All documentation related to the Rodin platform (User Manual, Developer’s Guide) is available from the wiki: [http://wiki.event-B.org](http://wiki.event-B.org)

**Progress**

During the first six months of the project, the partners were mainly involved in training and specifying the pilots that the Rodin platform and its related methods will be checked against. This is briefly reported below as well as the occasions where the project or the platform was presented.

**WP1 (Deployment in the automotive sector)**

The Bosch project members have taken part in an introductory event-B course held in Zurich in April 2008.

The WP1 pilot application has been defined and initially discussed with the WP1 partners. The
requirements specification of the WP1 pilot application has been translated into English and will be distributed to the WP partners shortly. It has been agreed on complementing the textual requirements specification with problem frames diagrams.

As a first step in applying event-B and the RODIN tools, a mini-pilot has been specified and modeled in event-B.

WP2 (Deployment in the transportation sector)

Three people from Siemens attended the event-B meeting held in Zurich from April 9 to April 11. Siemens issued a first version of the mini-pilot specification, and an event-B model of this specification has been developed, that enabled to discover some mistakes in the specification. A second version of the specification and an enriched version of the event-B model is currently under review by WP2 Partners.

WP3 (Deployment in Space sector)

Before the formal kick-off meeting that was held in May in Finland, SSF project participants attended an Event B training in Zurich in April 2008. In June, SSF attended an Event B training arranged by AABO. The goal was to build upon the foundation laid in Zurich. The next steps of the project are to arrange a progress meeting in September 2008 to report on the progress of the pilot modeling. A workshop on modeling the pilot will be arranged in conjunction with the plenary meeting in Turku in November 2008.

WP4 (Deployment in the business information sector)

SAP participated in the Event-B course in Zurich in April. Based on this various experiments with Rodin and the UML-B plugin have been conducted at SAP. In preparation of the WP4 kick-off and as follow-up, SAP has issued two mini-pilots. These have been the basis to investigate the applicability of Event-B patterns to the problem of interacting process components. This research has been conducted in close collaboration with the WP4 partners. A generalization of the mini-pilots to a full pilot is in preparation.

WP12 (DEPLOY Management)

The DEPLOY Management office at Newcastle is now fully staffed. The Project Manager is Jon Warwick who has managed 10 EU projects in the last 8 years. He is assisted by Jodi Hossbach, the Project Administrator who has responsibility for day to day project matters and Shelly Henderson the Project Secretary. DEPLOY Management Staff can be contacted using deploy-coordinator@jiscmail.ac.uk

The project infrastructure is also fully operational and includes a web page www.deploy-project.eu, an internal BSCWE site and a presence on Sourceforge, as well as a suite of mail lists. Further information on the project can be obtained by contacting the management office.

WP14 (Dissemination of the results)

- August 5th-17th 2008: (Marktoberdorf, Germany) Lectures on Event-B and Rodin at the NATO Summer School on Engineering Methods and Tools for Software Safety and Security
- June 16th 2008: (Nantes, France) "Presentation of event-b and the Rodin Platform" - Special day on B organized by the Nantes University
- June 13th 2008: Berlin (Germany) A general presentation about the DEPLOY project at Intern. Symposium on Quality Engineering for Embedded Systems
- May 26th-27th 2008: Turku (Finland) A tutorial "event-B and the Rodin Platform" was given at the occasion of the FM 2008 conference. DEPLOY project was presented at the exhibition of research projects and commercial tools
- April 23th-26th 2008: Kirovograd (Ukraine): A Rodin platform demo at Third International Conference on Dependable Systems, Services and Technologies
- April 21th-25th 2008: Tunis (Tunisia) presentation "event-B and the Rodin Platform" was given
- March 30th-31th 2008: (Bled, Slovenia) DEPLOY is represented at the BLED Conference
- March 29th 2008: (Budapest, Hungary) A talk entitled "Teaching Formal Methods: an experience with event-B" was given at ETAPS 2008, FORMED workshop

Meetings

Plenary workshop

The plenary kickoff meeting was held on February 18-20, 2008 in Newcastle upon Tyne. This was an important event when all project members met for the first time to discuss the implementation plan and to establish closer collaboration. All workpackage leaders had dedicated slots to present the work planned. The focus was on deeper discussions of the work in the industrial deployment packages. A special session was organized to look into the RODIN heritage, including the methods and the platform. During the kickoff meeting informal groups working on specific workpackages, tasks and problems started to appear. The Executive Board met for the first time to plan the
project work in the coming 6 months and to establish the main project procedures. To actively engage the industrial partners into technology transfer the Board agreed to organize a 3 day intensive training course on the RODIN platform and methods in Zurich. It was decided that DEPLOY would have annual plenary meetings in November each year, the first one will be held in Turku (Finland) in 2008 and organized by Aabo Akademi.

WP1 (Deployment in the automotive sector)

The WP1 kick-off meeting was held 13th-14th of May 2008 in Schwieberdingen, Germany with participants from University of Zurich, Newcastle University, University of Southampton, Aabo Akademy, University of Dusseldorf, and CETIC joined the meeting. Goals of the workshop were to give the project partners introductory information about the system development process and the tools applied within the automotive industry in general and Bosch in particular. Furthermore, the partners were introduced into the WP1 pilot application (cruise control). Challenges concerning the application of the event-B method and the RODIN tools, in particular handling real-time requirements, have been initially discussed. Measurement concerns have been discussed briefly. An initial collaboration plan has been developed and was accepted by the participants.

WP2 (Deployment in the transportation sector)

The WP2 kick-off meeting was held on April 30 at Siemens office, in Châtillon (France), with participants from university of Newcastle, university of Southampton, university of Zürich, Systerel, Aabo academy, CETIC. Current Siemens development process (both at system and software level) was discussed, as well as the new development process that includes event-B. Siemens expressed tool requirements to support this new development process. The mini-pilot specification has been presented to the participant, with a focus on time constraints. An animation of the corresponding event-B model has been performed.

WP3 (Deployment in Space sector)

The kick-off meeting for WP3 was held 20-21st of May in Espoo, Finland, with participants from Newcastle University, CETIC, Aabo Akademy, University of Southampton and University of Dusseldorf. During the meeting the pilot strategy was discussed. It was decided that the pilot would be done in several steps. A mini-pilot was completed for the kick-off. The goal is to complete a more realistic pilot for the end of the year, and the full pilot by next year.

WP4 (Deployment in the business information sector)

The kick-off meeting was held 6th-7th of May at the SAP headquarters in Walldorf, Germany in, with participants from SAP, Newcastle University, University of Zürich, Aabo Akademy, University of Southampton, and University of Dusseldorf. together, The concrete objectives of this work package were discussed. SAP gave insights into the kind of software SAP is developing and into the software development practice at SAP. This was the basis to discuss in which areas opportunities for formal methods can be expected, and what a promising pilot case study can be. For preparing the latter, event-B specifications of a mini-pilot provided by SAP in advance were presented in detail. Finally, concrete next steps, especially in the direction of pattern development, graphical front-ends, and models for fault tolerance, were identified and assigned to WP4 contributors.

WP8 (Achieving and demonstrating dependability)

All four kick-off meetings with industry partners gave the Dependability researchers something to think about! Work on techniques for deriving specifications has been inspired by the challenge of describing timing behaviour in the Siemens Transportation Systems and Bosch mini-pilots. A study on resilience, a collaboration between Newcastle University and SAP, has the aim of supporting developers in selecting between design alternatives. Work on stochastic and logical reasoning has begun to address the incorporation of failure rates and probabilities into event-B models using examples from the Siemens Transportation Systems mini-pilot.

WP9 (Tooling research and development)

The kick-off meeting was held 5th-6th of June 2008 in Aix-en-Provence, France. This meeting defined both short-term and longer-term issues that will be dealt with. An action plan for year 2008 has been agreed on as a result. A public roadmap has been made available on the event-B.org website.

WP11 (Measurements)

The WP measurement team is led by CETIC (Belgium) with involvement of partner having experience in the industrial application of formal methods. During each of the four industrial kick-offs (WP1-WP4), a special session was devoted to identifying the main measurement goals to assess the success of the transfer. Based on this, a goal catalogue is now being elaborated, as well as short term measurement plan to assess the first pilot of the project. This will among other focus on the impact of modelling activities on the quality of requirement and architectural documents. Besides this, the impact of initial training held in Zurich in April was also assessed using before and after questionnaires.
WP14 (Dissemination of the results)

DEPLOY attended two events organized by the Software and Service Architectures and Infrastructures Unit, on March 4th-5th 2008 in Brussels, Belgium. During the first one were presented the “Priorities for the Workprogramme 2009-2010”. The second was the Public launch of the 28 projects resulting from Call 1. Collaboration among projects was initialized on the “Internet of Services” topic.

Deploy Interest Group

This group (DIG) is composed of companies/universities/individuals interested in the DEPLOY objectives and results. The DIG has privileged access to information (bi-annual newsletter, dedicated hands-on sessions, etc.) and we are looking for further collaboration with DIG members (feedback, new case-studies, new contributing plug-ins, etc).

Special attention is given to DIG: dedicated means are allocated to help DIG members getting educated / gaining experience with the Rodin tools.

Current members are:

STMicroelectronics (France), Nokia (Finland), AT Engine Controls (UK), Cyber Defense Agency (USA), Formal Methods Europe, National Aerospace University (Ukraine), Acesso e Segurança (Brazil), University of South Wales (Australia)

Joining the DIG is simple. Please send an electronic letter of intent to the Dissemination & Exploitation Manager (thierry.lecomte@clearsy.com)

Future Events

- **August 26th 2008**: Salvador de Bahia (Brazil) - B Dissemination Day at SBMF 2008 Conference [http://www.lasid.ufba.br/sbmf2008/events.html] - Presentation of the Rodin platform
- **August 28th 2008**: Sao Paulo (Brazil) - B Dissemination Day at the IPT [http://www.grupo-aes.com.br/site/home/?id=95] - Presentation of the Rodin platform
- **November 17th-19th 2008**: Newcastle upon Tyne (UK) - Dedicated session reporting DEPLOY initial results and general presentations about the project SERENE 08 - RISE/EFTS Joint International Workshop on Software Engineering for Resilient Systems [http://serene2008.uni.lu]

Call for Contribution

We are inviting anyone interested in DEPLOY to contribute to its success. Expected contribution 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 [http://www.event-B.org/roadmap.html])
- 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.