DEPLOY’s first Year

The DEPLOY project is addressing the most significant issue that faces developers of significant software-based systems: how can we build commercial and industrial systems that we know will satisfy their users, whilst minimising the costs and time-to-market?

Software dependability is increasingly important for both commercial and industrial companies. Software faults can be very costly, leading to security breaches, breakdowns in service or product recalls. Companies that develop safety-related software, for example for medical or transport applications, have to satisfy regulators that their systems will be safe in use. Meanwhile, applications are becoming more complex, and there is increasing pressure on costs and timescales.

Most companies seek to achieve dependable software through prototyping, expert reviews, structured methods and extensive testing but this approach can be slow and expensive, and many errors can easily survive even the most rigorous testing and lead to failures in service. Security weaknesses are particularly difficult to eliminate with a test-and-fix way of working.

As a software engineer with almost four decades of experience in industry and commercial applications, I know that we need methods that guarantee that our systems meet the needs of our users, and tools that make these methods straightforward and cost-effective for engineers to use. Recent R&D has created such methods and tools; in DEPLOY the researchers are working closely with major companies to explore the application of these methods to real commercial and industrial problems. By the end of DEPLOY, in 2012, we aim to release methods, tools, guidance and training that will allow companies to develop software and to know — and to be able to show — that it is dependable, all far more effectively than they can at present.

It is always a challenge to get researchers and professional software engineers to collaborate productively, because their motivations, goals and timescales can be very different. Software engineers want solutions that are good enough, whereas researchers want results that will withstand the critical scrutiny of review by their academic peers. Engineers need solutions that give them rapid benefits in a competitive marketplace, whereas researchers are used to projects that take the four or more years of a typical doctoral thesis. In the first year of DEPLOY, we have already built a team that has shared goals and a shared urgency. The academic technology partners are driven by a need to understand how their methods and tools will be used on industrial scale projects and by professional engineers: they are already getting practical feedback and are improving the scope and usability of their technology to meet industrial needs.

The DEPLOY project wants to reach out as widely as possible in industry and commerce so, if you find this newsletter interesting, please visit the project website and sign up for the DEPLOY Interest Group, download the tools and training materials, and let the project hear about your needs and your experiences.

Martyn Thomas CBE FREng
Chair, DEPLOY Executive Board

Getting Involved

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 [http://www.event-B.org/roadmap.html](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](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.
Progress

DEPLOY is a four year FP7 Integrated Project on Industrial deployment of system engineering methods providing high dependability and productivity started in Feb 2008. The overall aim of DEPLOY 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, initially in the five sectors which are key to European industry and society.

During the first half of the year the main focus of the consortium was on initial technology transfer to the deployment partners, identification of their major methodological and tooling needs, joint work on minipilots, and creating strong teams working on deployment in the specific sectors. The main areas of the ongoing work are medium scale pilot development, advanced training, advancing the tools, addressing the identified methodological challenges (focusing mainly on requirements and architecture) and developing measurement methodologies. The consortium realizes the needs for the deployment partners to reduce the risk for the project and pays special attention to identifying the risks as soon as possible (these issues are discussed during the Executive Board meetings).

During the first year the following major management steps have been undertaken: a management office was set in Newcastle University, the executive board meeting each 6 months was created and all procedures were defined, the project infrastructure was created (including mailing lists, BSCW file sharing/repository, as well as project, tool platform, publication, and technology transfer web sites) and the internal deliverable review/assessment procedure was set.

The project kickoff meeting was held in February 2008 (Newcastle), followed by an intensive training course for industrialists in April conducted at ETH in Zurich. During May all industrial partners organised sector specific kickoff meetings. Since then a number of project meetings have been held: on methods and tools, dependability, requirements, tool platform. The 1st annual plenary meeting was organized in Turku in November to discuss the ongoing work focusing on general issues crosscutting various workpackages and to plan the production of the 12M deliverables and the consortium work in year 2.

The chief project aims for the second year are to conduct project refocus (i.e. strategic changes in the Description of Work), to complete pilot deployment, to ensure real deployment by advancing methods and tools, to achieve wider (sector specific) dissemination and to produce the deployment strategy document.

More information about the project can be found in the project web site: http://deploy-project.eu

Alexander Romanovsky, Project Coordinator

RODIN Platform and Plug-ins

In the past semester, a lot of work has been devoted to improving the Rodin platform. Development has been carried concurrently along two axes: strengthening the platform core and implementing the features most wanted by users.

On the core side, the static checker and the proof obligation generator internal architecture has been completely revised to allow for easier and more powerful extensions of these tools. Also, the internal database API has been cleaned up and a major conceptual change has been introduced (root element of a Rodin file). As the event-B language evolves, database versioning has been implemented so that old developments can be automatically upgraded to the current language by the Rodin core. Finally, an
The indexing framework has been implemented, allowing plug-ins to compute an index of all names that are declared and used in models. This framework is the basis on which refactoring and browsing is implemented. All these changes, which are mostly invisible to the end user, build a solid foundation for future improvements of the platform.

On the user side, a lot of problems have been fixed and some features long requested have been implemented. The most outstanding user-visible changes of the platform are:

- **Undo and redo are now available in the event-B editor.**

- **The event-B language supported by the platform has been upgraded to the current version, as described in Jean-Raymond Abrial's coming book. This change introduces event parameters and event extensions.**

- **A new explorer view now combines the old project and obligation explorer. This new view is fully Eclipse-compliant and thus seamlessly integrated.**

- **The provers have been updated. Problems with too many provers running concurrently or provers running when not needed have been fixed. Also, new proof rules have been added and a few partially invalid ones fixed.**

- **New views and actions are now available for manipulating proofs (proof visualization and purging unused proof).**

- **The platform has been ported to the latest stable release of Eclipse (Ganymede), leveraging all the cool new features developed by the Eclipse Community.**

- **A detailed log of all the changes to the Rodin platform is available on SourceForge on the download page (just click on the little notepad icon next to the software release).**

**Caution:** There is a major change between releases 0.8.2 and 0.9.0. This means that all models opened with release 0.9.0 or later are not backward compatible with previous releases. When you plan to move to release 0.9.0, please backup all your workspaces before opening them with the latest Rodin platform. The procedure for upgrading one workspace to release 0.9.0 or later is fully explained in the release notes of the platform.

For more information on the current developments, please visit our wiki (http://wiki.event-b.org/index.php/Current_Developments). The wiki is also the reference site for all documentation (both user and developer) about the platform. Do not hesitate to visit it and contribute.

As a final note, three mailing lists have been created for the Rodin platform and plug-ins. You can register to any of them by clicking on the appropriate link below:

- http://lists.sourceforge.net/lists/listinfo/rodin-b-sharp-announce (important announcements (mostly new software releases), very low traffic)
- http://lists.sourceforge.net/lists/listinfo/rodin-b-sharp-user (user discussions, tips and tricks, help, ...)

**Contact and Further Information**

Laurent Voisin (laurent.voisin@systerel.fr) is responsible for WorkPackage 9, the tooling work package in DEPLOY. 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

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

A number of improvements to existing plug-ins have been achieved and several prototype plug-ins have been developed. The most up to date information can be found on the Event-B wiki: http://wiki.event-B.org/index.php/Current_Developments

The Atelier B Provers plug-in has replaced the B4free prover plug-in. This provides additional automated proof capabilities based on the separate Atelier B tool.
The UML-B plug-in has been improved to provide better support for refinement of UML-B models. This allows a statemachine to be recognised as a refinement of another one and to be treated in an appropriate way during translation to Event-B. The states and transitions of a refined statemachine can be elaborated by adding more detailed hierarchically nested statemachines. Better support for synchronisation of parallel state machines has also been added.

The UML-B Plug-in

The ProB plug-in has been improved to make the full model-checking capabilities of the original ProB tool available within the Rodin plug-in.

A prototype Requirements Management plug-in has been developed that allows requirements to be edited in separate documents then viewed within Rodin and linked with Event-B elements.

A prototype Parallel Composition plug-in is available that supports the parallel composition of several Event-B machines into a composite machine. The machine composition uses a shared event style, where separate machines operate on disjoint variables and machines interact by synchronising on events that may share parameter.

Other ongoing developments include a text editor for Rodin based on EMF technology (Eclipse Modeling Framework) and a refactoring framework for propagating basic modifications, such as name changes, through models and 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 devoting to tooling issues both within the DEPLOY project and outside (external contributors).

ProB: Industry-size Railways Application

We report on a successful application of the ProB validation tool on an industrial case study within Work Package 2 of Deploy. The case study centres on the San Juan metro system installed by Siemens. The control software was developed and formally proven with B. However, the development contains certain assumptions about the actual rail network infrastructure which have to be validated separately in order to ensure safe operation. For this task, Siemens had developed custom proof rules for Atelier B. Atelier B, however, was unable to deal with about 80 properties of the deployment. These properties thus had to be validated by hand at great expense (and they need to be revalidated whenever the rail network infrastructure changes).

In recent weeks, we have been able to validate all of the properties required in the San Juan deployment, around 400 in number. We detected the same faults that were uncovered manually, but taking around 15 minutes. This achievement required the extension of the ProB kernel for large sets as well as an improved constraint propagation phase.

Other features were required in moving from a tool capable of dealing with medium-sized examples towards a tool able to deal with actual industrial specifications. Notably, a new parser and type checker were developed for ProB.
Contact and Further Information

Please contact Michael Leuschel (leuschel@cs.uni-duesseldorf.de) for further information concerning ProB in general or this application in particular.

ProB can be downloaded at http://www.stups.uni-duesseldorf.de/ProB/. The site contains also contains documentation. The ProB plugin for Rodin can be obtained using Eclipse’s update feature (Rodin is preconfigured with the proper update site).

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)
- Keesda (France)
- University J.E Purkyne (Czech Republic)
- Qinetiq (UK)
- Sysart Oy (Finland)

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

Workshop on Formal Methods for Service-Oriented Architecture

The Working Group “Formal Methods for Service Oriented Architecture”, run by DEPLOY, is now organising a one-day event on February 16th in Düsseldorf at the iFM conference on the theme of the working group. Ten talks are planned (see below) as well as a panel on the future of SOA and funding opportunities for research in formal methods for SOA and Internet of the Future.

- From compliant business process specifications to code, Natalia Kokash, CWI
- Using Reo for Composition of Web Services, Farhad Arbab, CWI
- Formal Modeling for Service-based Process Integration, Andreas Roth, SAP
- Specification, Partitioning, and Composition Techniques for Web Application in the Context of Event-B, Abdolbaghi Rezazadeh, Univ. Southampton
- ProTest - property based testing for Erlang, John Derrick, University of Sheffield
- REST: SOA without Contracts?, Stefan Tilkov, innoQ
- Verification and Certification using rewriting logic, Santiago Escobar, University of Valencia
- Formal Modelling and Analysis of SOA-based Business Information Applications with Fault Tolerant Middleware, John Fitzgerald and Jeremy Bryans, Newcastle University
- Title to be announced, Manuel Mazzara, Newcastle University
- Adding domain-specific constructs to (Event) B for developing and reasoning about grid applications, Pontus Bostrom, Åbo Akademi
We need to know who you are!

The Rodin platform has been downloaded more than 8500 times, the event-b.org website has 650 unique visitors a month, and up to 1400 for the wiki.event-b.org website.

Because sourceforge downloads are anonymous, we have only limited knowledge about the growing user community. So that we can develop relevant and tailored resources, we need to know more about potential users, so a short survey has been set up; please take a few moments to complete the form at:


A synthesis of the results will be published. Thanks for your help!