Deployment of Formal Methods in Industry: the Legacy of the FP7 ICT DEPLOY Integrated Project

Alexander Romanovsky
Deployment of Formal Methods in Industry: the Legacy of the FP7 ICT DEPLOY Integrated Project

A. Romanovsky

Abstract

The work of the major EU-funded ICT DEPLOY Integrated Project (February 2008 – April 2012) on Industrial Deployment of Advanced System Engineering Methods for High Productivity and Dependability was driven by the tasks of achieving and evaluating industrial take-up, initially by DEPLOY industrial partners, of DEPLOY methods and tools, together with the necessary further research on methods and tools. Our previous SEN paper introduced the project. The project has been one of the most significant efforts ever focusing on understanding the issues researchers and engineers face during the deployment of formal methods. This paper briefly reports on the project legacy and provides pointers to the various sources of information produced by the project.
Bibliographical details

ROMANOVSKY, A.

Deployment of Formal Methods in Industry: the Legacy of the FP7 ICT DEPLOY Integrated Project
[By] A. Romanovsky


(Newcastle University, Computing Science, Technical Report Series, No. CS-TR-1351)

 Added entries

NEWCASTLE UNIVERSITY

Abstract

The work of the major EU-funded ICT DEPLOY Integrated Project (February 2008 – April 2012) on Industrial Deployment of Advanced System Engineering Methods for High Productivity and Dependability was driven by the tasks of achieving and evaluating industrial take-up, initially by DEPLOY industrial partners, of DEPLOY methods and tools, together with the necessary further research on methods and tools. Our previous SEN paper introduced the project. The project has been one of the most significant efforts ever focusing on understanding the issues researchers and engineers face during the deployment of formal methods. This paper briefly reports on the project legacy and provides pointers to the various sources of information produced by the project.

About the authors

Alexander (Sascha) Romanovsky is a Professor in the Centre for Software and Reliability, Newcastle University. His main research interests are system dependability, fault tolerance, software architectures, exception handling, error recovery, system structuring and verification of fault tolerance. He received a PhD degree in Computer Science from St. Petersburg State Technical University and has worked as a visiting researcher at ABB Ltd Computer Architecture Lab Research Center, Switzerland and at Istituto di Elaborazione della Informazione, CNR, Pisa, Italy. In 1993 he became a postdoctoral fellow in Newcastle University, and worked on the ESPRIT projects on Predictable Dependable Computing Systems (PDCS), Design for Validation (DeVa) and on UK-funded projects on the Diversity, both in Safety Critical Software using Off-the-Shelf components. He was a member of the executive board of EU Dependable Systems of Systems (DSoS) Project, and between 2004 and 2012 headed projects on the development of a Rigorous Open Development Environment for Complex Systems (RODIN), and latterly was coordinator of the major FP7 Integrated Project on Industrial Deployment of System Engineering Methods Providing High Dependability and Productivity (DEPLOY). He now leads work on fault tolerance in Systems of Systems within the COMPASS project and is Principal Investigator of Newcastle’s Platform Grant on Trustworthy Ambient Systems.

Suggested keywords

FORMAL METHODS
TOOL SUPPORT
DEPENDABILITY
FAULT TOLERANCE
REUSE
REQUIREMENTS
ECLIPSE
EVENT-B
REFINEMENT
RODIN
Deployment of Formal Methods in Industry: the Legacy of the FP7 ICT DEPLOY Integrated Project

Alexander Romanovsky
Newcastle University
Newcastle upon Tyne
UK
+44 191 222 8135
alexander.romanovsky@ncl.ac.uk

ABSTRACT
The work of the major EU-funded ICT DEPLOY Integrated Project (February 2008 – April 2012) on Industrial Deployment of Advanced System Engineering Methods for High Productivity and Dependability [1] was driven by the tasks of achieving and evaluating industrial take-up, initially by DEPLOY industrial partners, of DEPLOY methods and tools, together with the necessary further research on methods and tools. Our previous SEN paper [2] introduced the project. The project has been one of the most significant efforts ever focusing on understanding the issues researchers and engineers face during the deployment of formal methods. This paper briefly reports on the project legacy and provides pointers to the various sources of information produced by the project.

Categories and Subject Descriptors
D.2.1 [Requirements/Specifications]
D.2.2 [Design Tools and Techniques]: Computer-aided software engineering (CASE)
D.2.4 [Software/Program Verification]: Correctness proofs, Formal methods, Model checking
D.2.6 [Programming Environments]: Integrated environment

General Terms
Design, Reliability, Theory, Verification.

Keywords
Formal methods, tool support, dependability, fault tolerance, reuse, requirements, Eclipse, Event-B, refinement, Rodin.

1. INTRODUCTION
Formal engineering methods enable greater mastery of complexity than do traditional software engineering processes. It is the central role played by mechanically-analysed formal models throughout system development that enables mastery of complexity. As well as leading to big improvements in system dependability, greater mastery of complexity leads to greater productivity by reducing the expensive test-debug-rework cycle and by facilitating increased reuse of software.

The successful three-year FP6 STREP RODIN project on Rigorous Open Development Environment for Complex Systems (2004-2007) [3] 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 [4] (the platform, called Rodin, supports the Event-B [5] stepwise development combined with the use of a number of other modelling techniques – such as CSP, UML, π-calculus and B, integrated using the plugins), along with a body of work on formal methods for dependable systems. DEPLOY exploited and built on these results.

In FP7 DEPLOY Integrated Project (Industrial Deployment of Advanced System Engineering Methods for High Productivity and Dependability, fifteen EU partners, €17.5M) four leading European companies, representing major sectors: transportation (Siemens), automotive (Bosch), space (Space Systems Finland), and business information (SAP), worked on deploying advanced engineering approaches to further strengthen their development processes in order to improve competitiveness.

The overall aim of DEPLOY was to make major advances in engineering methods for dependable systems through the deployment of formal engineering methods. The work was driven by the tasks of achieving and evaluating the industrial take-up of the DEPLOY methods and tools, initially in the four sectors which are key to European industry and society.

Paper [2] written when the project just started, introduces the project objectives, describes the consortium, outlines the project methodology and summarises the results the project was set to deliver. The DEPLOY project was successfully completed in April 2012. The overall aim was achieved with a coherent integration of scientific research, technology development and industrial deployment of the technology. The project public deliverables downloadable from the main DEPLOY web site [1] report on its outcomes, experience, results and achievements.

This paper serves several purposes. Firstly, it reports on the project unique experience in dissemination and exploitation. Secondly, it briefly introduces all major sources of information describing project scientific and technological results to help ensure their wide dissemination.

2. DEPLOY ECOSYSTEM
As part of the dissemination and exploitation work the consortium promised to create a functioning DEPLOY ecosystem that would help engineers, academics, managers, educators, students, researchers, policy makers and certifiers to understand, use and apply the methods and tools developed in the project. The DEPLOY ecosystem that has been created to provide continuing support for the growing community of people and organisations with various interests in the project results. In particular, these include companies already using Event-B and Rodin. One of the purposes of the ecosystem is to allow an industrial company to adopt new methods as the basis for product development and support possibly over decades of service lifetime. This ecosystem includes

- the deployment partners of the project and the DEPLOY Associates,
- the DEPLOY Interest Group,
- a number of already on-going and completed research projects with strong industrial participants,
- a not-for-profit company Rodin Tools Ltd,
- an active community of tool developers ensuring that the new releases of the tools are regularly issued and that reported bugs are corrected,
- various sources of training, educational and scientific
materials developed and enhanced during DEPLOY.

3. DEPLOYMENT PARTNERS AND DEPLOY ASSOCIATES

The work of the four deployment partners (Bosch, Siemens, SAP and Space Systems Finland) has been instrumental to the success of DEPLOY as they applied the Rodin technology in their domains during the lifetime of the project. In the last two years of the project three companies (Xmos Ltd, Grupo AeG and Critical Software Technologies) became the DEPLOY Associates and were involved in the assessment and the deployment of Event-B/Rodin. These seven companies represent the following application domains: aerospace, transportation, business information, railway, avionics and semiconductor design. The experience gained during their involvement in DEPLOY has helped them to improve their development in various ways and provided them with the knowledge and experience that will be helping them in further deployment and use of formal methods. Some of these companies are already getting involved in new R&D projects related to Event-B and Rodin.

With the first hand experience gained during DEPLOY these companies, as well as other DEPLOY partners, such as technology developers and consultants from Systereel, ClearSy and CETIC, will be in the core of future development and transfer of the Rodin technology.

4. DEPLOY INTEREST GROUP

The DEPLOY Interest Group (DIG) was created at the beginning of the project. It was composed of companies, universities and individuals interested in the DEPLOY objectives and results. The project established tight bidirectional links with the DIG members and ensured that the group grew substantially during the project lifetime.

They received regular updates on the project progress and development, as well on plans and their changes. Special attention was given to DIG as dedicated means were allocated in the project to help the DIG members to gain experience with the Rodin tools. By the end of DEPLOY the DIG was composed of around 70 members from all continents and with an equal participation from academia and industry. Several R&D projects have been initiated with the participation of the DIG members. The members also provided many useful comments and insightful feedback related to the tool, plug-ins, documentation and other materials developed in the DEPLOY project.

Several DEPLOY events have been organized with the help and contribution of the DIG members, including

- Workshops on B Dissemination in Salvador de Bahia, Sao Paulo, Eindhoven, Natal and Tokyo, gathering up to 80 attendees each.
- Rodin Users and Developers Workshops in Southampton (2009), Dusseldorf (2010) and Fontainebleau (2012).
- DEPLOY Industry Day in Fontainebleau (2012) with more than 80 participants.

Yet another event will be held in late 2012 with the aim to expand the community of researchers and practitioners working with Event-B/Rodin: Workshop on the Experience of and Advances in Developing Dependable Systems in Event-B, November 2012, Kyoto, Japan in conjunction with IFCEM 2012 [6].

Rodin Users and Developers Workshops will be held annually with the next workshop planned for earlier 2013.

The DIG members attended various workshops and tutorials organised by the DEPLOY members as well as the final project Federated Event held in February 2012 in Fontainebleau.

It is expected that the DIG members will be strongly involved in the future development and industrial application of the Rodin technology via its use in product development, industrial or public projects, open tool development and maintenances, sharing deployment experience or academic research.

5. PROJECTS OUTSIDE DEPLOY

Event-B and Rodin are currently being used in Industry in various application domains, as well as in several close-to-application R&D projects. Outside the DEPLOY project, several application cases have been reported, some of these are briefly described below.

For the automation of Flushing and Culver metro lines in New York, Event-B is being used by ClearSy to formally model the whole system, including a Communication-Based Train Control. This modelling will ensure that all the equipment specifications have a high degree of consistency and correctness, thereby contributing directly to Independent Safety Assessment and improving confidence in the overall safety of the system.

The new EU-funded ADVANCE (Advanced Design and Verification Environment for Cyber-physical System Engineering project [7], which involves Alstom Transport, Critical Software Technologies, Systereel and two universities, Southampton (project coordinator) and Dusseldorf, aims to deliver methods and tools for formal modelling, verification and validation, which will make it possible to produce precise models for embedded systems and help eliminate design errors before projects go into the manufacturing stage. This will improve the design of embedded software systems in automated railway signalling and smart energy distribution. The project will result in further improvements and extensions to the Rodin platform.

STMicroelectronics and ClearSy have collaborated during several years on modelling and generation of a VHDL code for a smartcard-based microcircuit, based on the Event-B models.

Systereel has used Rodin and Event-B in a number of railways projects: interlocking modelling, Communication-Based Train Control (CBTC), CBTC train tracking, security barrier and in some other safety critical case studies.

The PARSEC project, funded by French Research Administration, aims at providing development tools for critical real-time distributed systems requiring certification according to the most stringent standards such as DO-178B (avionics), IEC 61508 (transportation) or Common Criteria for Information Technology Security Evaluation. The approach proposed by PARSEC provides an integrated toolset, including the Rodin platform that helps software engineers to meet the requirements associated to the certification of critical embedded software. Distributed applications are being modelled with Event-B.

The OISAU project, funded by French Defence Administration, aims at defining the standard of architecture of future autonomous systems for military applications (more commonly called robots or drones). This standard's primary aim is to ensure interoperability of these systems within the community of systems of similar or various origins, referred to as the system of systems. This will enable designers and the like to define software and hardware architectures, which are independent of the carrier (air, land, sea) and reusable. ClearSy is in charge of modelling the functional and functional needs of the systems. By modelling the behaviour of the system in its environment, Event-B enables the system to be characterised by successive refining of its properties and functions within the various operational scenarios and to validate the final generic model, which is deduced from it.

In the SafeCap project (Overcoming the Railway Capacity Challenges Without Undermining Rail Network Safety [8]) Invensys Rail with the help of Newcastle University is working on transferring the Event-B technology into in-house industrial railway projects. This project focuses on developing modelling techniques and tools for improving railway capacity while ensuring that safety standards are maintained. The project team (Newcastle University, Swansea University, Invensys Rail) works on integrating proof-based reasoning about time in state-based models, exemplified by Event-B and CSP-Prover, and on providing an open tool support for verifying timed systems. The toolset to be created is based on Rodin and uses a specially developed domain-specific language (DSL) to describe track layouts. SafeCap is supported
by EPSRC UK and RSSB UK.

Since April 2010 the Åabo Akademi University team has been involved in the EU funded ARTEMIS JU project RECOMP (Reduced Certification Costs Using Trusted Multi-core Platforms) [9]. The project is industrially-driven. The team is working on developing methodologies for component-based design of safety-critical real-time systems using Event-B targeting and developing trusted multi core platforms.

The Dependable Systems Forum (DSF) project involves several Japanese companies namely NTT-Data, Fujitsu, Hitachi, NEC, Toshiba and SCSK. The DSF project applied several formal methods including Event-B and Rodin in an industrial development. One of the conclusions drawn was that “Event-B/Rodin is definitely one of the industrial-strength formal methods today” - see [10].

QNX Software Systems Ltd, a leading vendor of operating systems, development tools and professional services for connected embedded systems, has been applying the Rodin toolset to the design of software for a simple medical device. The aim is to use the evidence provided by the tool to support a safety case and to help in the approval process, see [11].

6. RODIN TOOLS LTD, RODIN TECHNICAL COMMITTEE AND TOOL DEVELOPERS

The development and coordination efforts, initiated during DEPLOY, will be continued in the following ways.

Rodin Tools Ltd [12] was set up by Newcastle University in early 2012 in accordance with the project dissemination and exploitation plan. It works with a community of members and is in charge of organizing the following activities around the Rodin platform:

- New platform and plug-in releases: new versions may be available on beta-release to members.
- Bug fixing: with a priority service for members.
- Consultancy services: including plug-ins to order, with preferential rates for members.
- Training: the organization will run training courses for all, with preferential rates for members. It also advertises training being run by others.
- Organisation of workshops: including the Rodin Users and Developers workshops, and other events, with preferential rates for members.
- Participation in conferences: including organisation of tutorials and of associated dissemination events.

This organization will be funded by members fees, set at several levels to enable individuals, PhD students, SMEs, large companies, STREP and IP projects to subscribe.

Rodin Tools Ltd works together with the Rodin Technical Committee that is in charge of defining the strategic development of the Rodin platform and the technical programmes of the Rodin Users and Developers workshops. The Committee is also responsible for running the event-b.org website [4] supporting users and developers of the Rodin toolset. The source code and tool development is overseen by the Committee and will continue to be hosted on the SourceForge facilities. The two organisations, Rodin Tools Ltd and the Rodin Technical Committee, will continue to sustain and enlarge an active community of tool developers ensuring that the new releases of the tools are regularly issued and reported bugs are corrected.

7. HOW COMPANIES AND UNIVERSITIES CAN GET INVOLVED WITH THE TECHNOLOGY

The development and coordination efforts, initiated during DEPLOY, will be continued in the following ways.

The DEPLOY project established clear ways to learn about the technology, install it, study (and share) the experience, get support during development of small and medium size projects and organise training at various expert levels. All these steps are supported by various elements of the DEPLOY ecosystem that ensures that new and already existing users of the technology are always supported in their work, the technology is maintained and there is a community of users sharing their experience.

These are the main sources of information about the technology:

- Material related to the book with some examples and slides - see [13].
- The main DEPLOY web site [1] providing access to the project description and all project results, including public deliverables and Newsletters.
- The DEPLOY publication repository [14] contains various training materials, models, tutorials, training courses, as well as research papers and reports (more than 300 entries by the end of the project and growing). This includes material developed and used during a 3 day block course run in the first months of DEPLOY for the project deployment partners.
- The Event-B and Rodin Documentation wiki [15], the main portal for material related to the Event-B modelling method and the Rodin platform, including documentation for users of the platform and all its plugins.
- Rodin users handbook [16] was developed during the last year of DEPLOY, the final release was issued before the project end. The handbook is intended to help in getting acquainted with the tool platform and provides the basics of modelling. It can also be used as a companion guide for experts. It will remain available after the project end.
- A repository of evidence for adopting of formal methods in industry [17] was developed in the project for providing answers to recurring concerns of companies wanting to investigate the usage of formal methods. It initially included the evidence collected in DEPLOY. The intention is that this repository will become widely used by organisations outside DEPLOY for collecting evidence and sharing experience in adoption of formal methods.

The Event-B/Rodin site [4] provides pointers for downloading recent releases of the tools and links with the dedicated SourceForge site [18]. There is information about the procedures for bug reporting and various mailing lists to discuss the experience in using the tools and receive announcements about new releases.

8. ACKNOWLEDGMENTS

The DEPLOY project was supported by the ICT within the 7th Framework, Strategic Objective IST-2007.1.2 on Service and Software Architecture, Infrastructure and Engineering (Grant Agreement 214158). My sincere thanks go to all people who contributed to this work. I am particularly grateful to Martyn Thomas for helping me to coordinate this major project. I would like to acknowledge Thierry Lecomte for providing me with some information about the projects that use Rodin and Event-B.

9. REFERENCES


