Chapter 2
Integrated Project DEPLOY

Alexander Romanovsky

Abstract This chapter introduces the four-year DEPLOY (Industrial Deployment of Advanced System Engineering Methods for High Productivity and Dependability) project to overview the context in which industrial deployment was conducted and explain how it was organised and managed.

2.1 DEPLOY Objectives, Consortium and Outcomes

The overall aim of the FP7 (EC Seventh Framework Programme) Integrated Project DEPLOY, run between February 2008 and April 2012 [6], 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.

Four leading European companies representing four major sectors: transportation (Siemens Transportation Systems), automotive (Bosch), space (Space Systems Finland) and business information (SAP AG) worked in DEPLOY on deploying advanced engineering approaches to further strengthen their development processes and thus improve competitiveness.

The overall aim of DEPLOY was achieved with a coherent integration of scientific research, technology development and industrial deployment of the technology. The complementary expertise and technological bases of the industrial deployment partners and the technology provider partners were combined to achieve a set of challenging scientific and technological objectives.

DEPLOY offered a balanced interplay between industrial deployment, scientific research and tool development, where companies in four sectors joined their forces with ten technology providers to meet the goal.

The industrial sectors (transportation, automotive, space and business information) comprised a palette of important European base industries of today. Before entering the project the companies possessed different maturity levels when it came to deploying formal approaches.

A. Romanovsky (✉)
Newcastle University, Newcastle upon Tyne, UK
e-mail: alexander.romanovsky@ncl.ac.uk

A. Romanovsky, M. Thomas (eds.), *Industrial Deployment of System Engineering Methods*, DOI 10.1007/978-3-642-33170-1_2,

The seven academic partners (Newcastle University, Åbo Akademi University, ETH Zurich, University of Düsseldorf, University of Southampton, University of Bucharest and University of Pitesti) are world leaders in formal methods research, with considerable experience in developing and applying dependability methods as well as a wide range of formal approaches.

The tool vendors, Systerel and ClearSy, have long-standing experience in developing tool support for formal engineering methods. CETIC has considerable experience in industrial quality measurement and was in charge of the assessment and evidence collection and analysis activities.

DEPLOY was set to deliver methods and tools that

- support the rigorous engineering of complex resilient systems from high-level requirements down to software implementations via specification, architecture and detailed design;
- support the systematic reuse and adaptation of models and software, thus addressing the industry's requirement for high productivity and requirements evolution;
- have been field-tested in and adapted for a range of industrial engineering processes;
- are accompanied by deployment strategies for a range of industrial sectors;
- are based on an open platform (Eclipse) and are themselves open.

By the end of DEPLOY, each industrial partner planned to achieve real deployment of formal engineering methods and tools in the development of products and to become self-sufficient in the use of formal engineering methods. The project plan focused on deployment that would enable the consortium to provide scientifically valuable artefacts (including formally developed dependable systems) and results of systems analysis (including a rich repository of models, proofs and other analysis results).

The description of work aimed to extend the mathematical foundations of formal methods in order to deliver research advances in complex systems engineering methods that enable high degrees of reuse and dependability and ensure effective systems evolution that maintains dependability. The DEPLOY work was planned with the aim of developing a professional open development platform based on Eclipse [7] that provides powerful modelling and analysis capabilities, is highly usable by practising engineers and is tailored to sector-specific engineering needs. It was in the project plan to use the experience and insights gained in the industrial deployments of DEPLOY to identify and report on the strategies that enable the integration of formal methods and tools with existing sector-specific development processes.

The consortium planned to put in place an organisation which would be the home of the open platform and which would serve as a body of industrial users and technology providers whose role would be to coordinate technical decisions on the platform and deliver training material covering general and sector-specific formal engineering methods. Åbo Akademi (Kaisa Sere, Elena Troubitsyna), ETH Zurich (Jean-Raymond Abrial) and the University of Southampton (Michael Butler) came together to work on FP6 STREP (Strategic Targeted Research Project) RODIN, Rigorous Open Development Environment for Complex Systems (2004–2007) [12], with the goal of creating a methodology and supporting open tool platform for the cost-effective rigorous development of dependable complex software systems and services. This project mainly focused on building a methodology and tool support for the Event-B Method [2], which was created at about the same time by Jean-Raymond Abrial.

While the B Method [1], developed by Abrial in the early 1990s, is focused on supporting formal development of software, Event-B broadens the perspective to cover systems. Rather than just modelling software components, Event-B is intended for modelling, analysing and reasoning about systems that may consist of physical components, electronics and software. An essential difference between Event-B and the B Method is that Event-B allows a richer notion of refinement in which new observables may be introduced in refinement steps. This means that complex interactions between subcomponents may be abstracted away in modelling at an early stage and then incrementally introduced through refinement.

The RODIN project was extremely successful as it researched and developed advanced engineering methods and tools that were extensively validated and assessed through industrial case studies from various domains, which paved the way for the technology to be deployed. In particular, RODIN delivered an extensible open source platform (called Rodin), based on Eclipse, for refinement-based formal methods along with a body of work on formal methods for dependable systems. DEPLOY has exploited and built on these results.

DEPLOY used the Event-B formal method as a basis but also explored various extensions and other formal approaches where appropriate. There were several reasons for choosing Event-B, and the success of the RODIN project was one of them. This project produced promising research results well received by the scientific community, and an open tool environment built on innovative principles and appreciated by the RODIN industrial partners and the project industry interest group. RODIN demonstrated the need for formal modelling at the system level. The RODIN team worked very well together and formed the core of the DEPLOY project consortium. It was very important for the consortium to have the creator of Event-B, Jean-Raymond Abrial, on board. It should be noted, however, that the consortium did not plan or have the resources to use multiple formal methods as a basis for its work.

The results of RODIN prompted several companies, which later became part of the DEPLOY consortium, to become interested in formal modelling at the system level, and in particular in Event-B and the Rodin platform. In addition to the academic partners well known for their research in formal methods, two French companies developing tools for B and Event-B joined DEPLOY. These formed the core of the DEPLOY consortium.

2.2 Event-B

The B Method [1] is a state-based formal approach that promotes the correct-by-construction development paradigm and formal verification by theorem proving.

The Event-B formalism [2] is a specialisation of the B Method. It enables modelling of event-based (reactive) systems by incorporating the ideas of the Action Systems formalism [3] into the B Method. In Event-B, a system specification (model) is defined using the notion of an abstract state machine. An abstract state machine encapsulates the model state, represented as a collection of model variables, and defines operations on it. Therefore, it describes the dynamic part (behaviour) of the modelled system. Usually a machine also has an accompanying component, called context, which contains the static part of the model. In particular, a context can include user-defined carrier sets, constants and their properties, which are given as a list of model axioms. Event-B employs a top-down refinement-based approach to system development. Development starts from an abstract system specification that models the most essential functional requirements. While capturing more detailed requirements, each refinement step typically introduces new events and variables into the abstract specification. These new events correspond to the steps that are not visible at the abstract level. The variables of a more abstract model in the refinement chain are called the abstract variables, whereas the variables of the next refined model are called the concrete variables. Event-B formal development supports data refinement, allowing us to replace some abstract variables with their concrete counterparts. In that case, the invariant of the refined machine formally defines the relationship between the abstract and concrete variables. To verify correctness of a refinement step, one needs to prove a number of proof obligations for the refined model. Intuitively, those proof obligations allow us to demonstrate that the refined machine does not introduce new observable behaviour, or more specifically, that concrete states are linked to the abstract ones via the given (gluing) invariant of the refined model. In general, these proofs guarantee that the concrete model adheres to the abstract one, and thus all proved properties of the abstract model are automatically inherited by the refined one. Appendix A provides a full introduction to Event-B.

2.3 DEPLOY Implementation

The work on DEPLOY had a cyclic nature and was conducted in two phases: pilot deployment and full deployment. The first phase started with an initial transfer of the technology developed during the RODIN project and intensive training of the deployment partners' engineers (in particular, we ran a three-day block course for all deployment partners' engineers). The pilot deployment was started in parallel; it consisted in the formal development of small- to medium-size systems typical of the application domains of the deployment partners. This allowed the consortium to assess the domain-specific deployment issues and to feed them back to the methodological and tooling work. The first phase was successfully completed after 1.5 years. The implementation plan included a project refocus at this point.

During the refocusing stage, the project Board analysed the major methodological and tooling needs identified in the pilot phase. In addition to this, an improved understanding of the DEPLOY methods and tools prompted the deployment partners to adjust their priorities and to clearly identify new needs. This resulted, in particular, in the creation of three new strands of work: code generation, model-based testing, and modelling and analysis of real-time systems.

During the second phase a full deployment was conducted in parallel with the improvement of the DEPLOY methods and tools. Regular meetings were held to insure that the feedback from deployment quickly came to the attention of the technology developers. The project assigned an experienced academic, who worked very closely with the deployment engineers, to each deployment partner; in some situations even becoming part of their team, s/he was responsible for reporting all deployment-related issues identified in the partner's work to the project method and tool development teams.

At the core of the DEPLOY project implementation was a triangle with industrial deployment, methodological and tooling work as the three corners. These three elements were always closely connected to and influenced each other, so that the needs of deployment drove the development of methods and tools, which in their turn were fed into the industrial deployment. The importance of the link (and the tension) between tools and methods was realised very early in the project; this allowed the consortium to find the right balance between advancing methods that could be supported with tools and those that could not, focusing more on advancing the tool-supported ones.

Building on the success of project dissemination and exploitation at phase one, the Board identified new opportunities for working with external users and developers. During the refocusing stage, we introduced the mechanism of DEPLOY Associates in order to allow selected companies interested in applying DEPLOY tools and methods in their settings to work together with the project partners. The aim was to gain more experience in deploying DEPLOY results in new application domains and for new types of applications. As the project supported only training and exchange visits, DEPLOY Associates significantly contributed to this work. The three companies (XMOS, Grupo AeS, Critical Software Technologies) that became DEPLOY Associates provided valuable feedback to the project work on methods and tools, and helped the project demonstrate wider applicability of its results. The work of the DEPLOY Associates is reported in Chaps. 7–9.

During the third year of the project, two new partners (University of Pitesti and University of Bucharest) joined the consortium, supported by a special grant available as part of FP7. This was intended to allow the ongoing FP7 projects to be extended by integrating new partners from the enlarged EC. The project Board added the two new academic partners in recognition of their concrete plans to closely work on methods and tool deployment with one of the deployment partners (SAP), and their excellence in research.

The initial plan was to work on measuring the impact of formal methods deployment, by focusing on defining metrics and collecting data showing quantitative improvements. During the first phase of the project, the consortium realised the importance (especially for the industrial partners) of qualitative measurement and collection of evidence. At the refocusing stage, a shift was made to gathering evidence that would help industrial organisations decide whether to adopt formal engineering methodologies, and to what extent. We created a methodology for collecting and structuring the evidence collected during the work of the deployment partners and DEPLOY Associates. Appendix B describes how CETIC created an evidence repository as the main mechanism for collecting and structuring evidence in order to make this information available to the various stakeholders (top-level managers of the industrial organisations, industrial managers working on specific projects and products, industrial engineers, academics, etc.).

As part of the project, we worked on building an ecosystem of people and organisations engaged with the tools and methods developed in the project by advancing and extending these tools and methods, deploying them in industrial settings and training engineers in using them. This ecosystem included universities that incorporated the methodological and tooling materials developed in the project in their courses. Over the lifetime of DEPLOY, it consisted of the project team (about 100 people from 14 organisations were involved in the project during its four-year work), the DEPLOY Associates and the DEPLOY Interest Group. The Interest Group consisted of more than 70 organisations and individuals that received regular updates on our work and took part in our public events, such as Rodin developer and user workshops and Industry days.

In the final year, the project worked not only on full deployment, finalisation of the tools, preparation of the documentations, and summarising of the project results and the lessons learnt, but also on building DEPLOY legacy and ensuring that its ecosystem will be operational and active after the project ends.

2.4 Legacy and Results

The DEPLOY project successfully achieved its main goal: it made major, substantial advances in developing advanced engineering methods for constructing dependable systems. This was done in response to feedback from industrial deployment of formal engineering methods on realistic problems.

The project legacy includes the main DEPLOY web site [6]; this will be maintained after the project end, but no new information will be added. The site includes all public project deliverables and newsletters [5].

The home of Event-B and the Rodin platform at [11] will be actively used after the project end. All participants involved in tool development will use it for dissemination of their results; this includes activities conducted in various public (both national and European) and industrial projects. This site allows free downloads of all tools and plug-ins [13] and the up-to-date Event-B and Rodin documentation wiki [10]. The Rodin handbook developed in DEPLOY is made publicly available at [14]. The Rodin platform development will continue at SourceForge [9].

All DEPLOY publications, reports, tutorials, training materials, presentations, papers, and models can be freely downloaded from [4]. This site will be used and maintained by the follow-up FP7 ADVANCE STREP on Advanced Design and Verification Environment for Cyber-physical System Engineering [8].

The open repository of evidence for adopting formal methods in industry created by the DEPLOY team is made available at http://www.fm4industry.org. It will be maintained in the foreseeable future, to be used by a wider community for collecting evidence on formal method application in and impact on industry.

As part of the project we created a not-for-profit company called Rodin Tools Ltd., which will take over the responsibility for the Rodin toolset at the end of DEPLOY (see http://www.rodintools.org). The company consists of

- a Strategy Committee of external advisers responsible for the development strategy,
- a Platform Development and Maintenance partner to carry out the wishes of the Strategy Committee and Company members, and
- a Coordination partner to manage the Company, run workshops and training, etc.

The main outcomes of the project include industrial deployment of advanced systems engineering methods at SAP, Bosch, Siemens Transportation and Space Systems Finland. In the course of the project, each deployment partner became self-sufficient in using these methods. DEPLOY developed an extensive set of scientifically valuable artefacts, including models, theories, methods, architectures, patterns and tools, which were thoroughly assessed during industrial deployment. The DEPLOY team made substantial research advances in complex systems engineering methods. We developed a professional industry-strength open development platform based on Eclipse (the Rodin platform), as well as a large number of high-quality training materials, courses and tutorials. We developed strategies for integration of formal methods and tools with existing sector-specific development processes. One of our outcomes is an organisation which will be the home of the open platform (Rodin Tools Ltd.). We ensured that the results of the project would be widely used and extended after the project end by building an ecosystem that comprises a substantial number of industrial users and technology providers (including the members of the project consortium, DEPLOY Associates and members of the DEPLOY Interest Group).

Acknowledgements I would like to express my deepest gratitude to everybody who has been involved in the preparation and implementation of the project since its idea was first discussed with Cliff Jones in April 2006. Cliff helped me enormously in negotiating and establishing DEPLOY. Martyn Thomas, who has chaired the project Board, was instrumental in steering the consortium towards its successful completion. Jon Warwick, the project Manager, has been with the team since the very first day of our work on the proposal, shielding me from dealings with various financial, legal and funding authorities.

References

1. Abrial, J.-R.: The B-Book: Assigning Programs to Meanings. Cambridge University Press, Cambridge (1996)
2. Abrial, J.-R.: Modeling in Event-B: System and Software Engineering. Cambridge University Press, Cambridge (2010)

3. Back, R., Sere, K.: Superposition refinement of reactive systems. Form. Asp. Comput. **8**(3), 1–23 (1996)
4. DEPLOY e-prints. http://deploy-eprints.ecs.soton.ac.uk/
5. DEPLOY project deliverables and newsletters. http://www.deploy-project.eu/html/deliverables.html
6. DEPLOY project web site. http://www.deploy-project.eu/
7. Eclipse modeling framework. http://www.eclipse.org/emf
8. FP7 ADVANCE project. http://www.advance-ict.eu/
9. Rodin development repository. http://sourceforge.net/projects/rodin-b-sharp/
10. Rodin documentation wiki. http://wiki.event-b.org/index.php/Main_Page
11. Rodin platform. http://www.event-b.org/
12. RODIN project web site. http://rodin.cs.ncl.ac.uk/
13. Rodin tools and plug-ins. http://wiki.event-b.org/index.php/Rodin_Plug-ins
14. The Rodin Handbook. http://handbook.event-b.org/

http://www.springer.com/978-3-642-33169-5

Industrial Deployment of System Engineering Methods
Romanovsky, A.; Thomas, M. (Eds.)
2013, X, 262 p., Hardcover
ISBN: 978-3-642-33169-5