Computing Science

Newcastle Experience of Coordinating the FP7 DEPLOY Integrated Project

Alexander Romanovsky and Jon Warwick
Newcastle Experience of Coordinating the FP7 DEPLOY Integrated Project

A. Romanovsky and J. Warwick

Abstract

In the paper we discuss one of the largest ever projects on industrial deployment of formal engineering methods called DEPLOY. This 50 months FP7 Integrated Project successfully completed in May 2012, was coordinated by Newcastle University. The paper presents our experience and lessons learnt in building the project consortium, preparing the proposal and running this project. We describe in detail the motivations for the project, its objectives and scientific and technological outcomes. The DEPLOY ecosystem was created by the end of the project to ensure that its results would be widely used, extended and applied after the project end.
**Abstract**

In the paper we discuss one of the largest ever projects on industrial deployment of formal engineering methods called DEPLOY. This 50 months FP7 Integrated Project successfully completed in May 2012, was coordinated by Newcastle University. The paper presents our experience and lessons learnt in building the project consortium, preparing the proposal and running this project. We describe in detail the motivations for the project, its objectives and scientific and technological outcomes. The DEPLOY ecosystem was created by the end of the project to ensure that its results would be widely used, extended and applied after the project end.

**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.

Jon Warwick has been Research Manager in the School of Computing Science for 12 years. In that time, he has been responsible for the management of 10 EU projects of varying size. He has extensive experience of EU research and the issues surrounding it and has worked with Prof. Romanovsky for some 8 years, building, writing and delivering the EU projects, Rodin and Deploy.

**Suggested keywords**

- FORMAL METHODS
- DEPENDABILITY
- EVENT-B
- INDUSTRIAL DEPLOYMENT
- TECHNOLOGY TRANSFER
- FP7
- INTEGRATED PROJECT
Newcastle Experience of Coordinating the FP7 DEPLOY Integrated Project

Alexander Romanovsky, Jon Warwick

School of Computing Science,
Newcastle University, Newcastle upon Tyne, UK
(Alexander.Romanovsky, Jon.Warwick}@ncl.ac.uk

Abstract. In the paper we discuss one of the largest ever projects on industrial deployment of formal engineering methods called DEPLOY. This 50 months FP7 Integrated Project successfully completed in May 2012, was coordinated by Newcastle University. The paper presents our experience and lessons learnt in building the project consortium, preparing the proposal and running this project. We describe in detail the motivations for the project, its objectives and scientific and technological outcomes. The DEPLOY ecosystem was created by the end of the project to ensure that its results would be widely used, extended and applied after the project end.

Keywords. Dependability, formal methods and tools, dependability, Event-B, industrial deployment, technology transfer, FP7, Integrated Project

1 Introduction

The work of the major FP7 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. The project focused on formal engineering methods and supporting tools because they allow greater mastery of complexity than do traditional software engineering processes. The Event-B formalism [2] was used as the foundation of the formal engineering methods developed in DEPLOY. Even though this was not a technology transfer project, DEPLOY centred on, and was driven by, the tasks of achieving and evaluating industrial take-up, initially by DEPLOY industrial partners, of the DEPLOY methods and tools, together with the necessary further research on methods and tools.

Seven of the fifteen DEPLOY partners were involved in the FP6 RODIN (Rigorous Open Development Environment for Complex Systems, 2004-2007) targeted project [3] which developed an extensible open source platform called Rodin, for
refinement-based formal methods along with a body of work on formal methods for
dependable systems. DEPLOY exploited and built on these results.

DEPLOY, successfully completed in April 2012, has made significant contribu-
tions into both, computer science and our understanding of how formal engineering
methods should be deployed in industry. Newcastle University led the preparation and
the execution of both projects RODIN and DEPLOY. The authors of this paper were
involved in this work from the very beginning: Alexander Romanovsky was the Pro-
ject Coordinator of RODIN and DEPLOY, Jon Warwick was the Project Manager in
both projects assisting Alexander Romanovsky in dealing with management, financial,
and legal issues. DEPLOY was a very large Integrated Project that involved about
100 people from 15 partners.

2 How to build a consortium for an EC project

In order to build a successful consortium, it is important to adhere to both EU guide-
lines and some internal “rules”. Of course the Consortium must have at least the min-
um number of Organisations from the minimum number of EU territories and it
must have an appropriate mix of Academic and Industrial partners, with, for example,
stronger industrial representation in an IP than a STREP. Even the most basic mix
however, allows for many variations and it is vital for the success of the proposal that
the Consortium ahhs the correct mix of expertise and balance of sectors. There is no
“magic consortium” that guarantees funding and no point in “window dressing; bring-
ing in partners to fulfil some spurious EU quota. The only valid factors for inclu-
sion in the Consortium are technical competencies and excellence in the field.

The start point of your consortium, even if it is to be a large IP (Integrated Project)
or NoE (Network of Excellence), is a small core group, usually of people you know
well and have worked with in the past. This group will agree on the Coordinator. This
is not a job that should be forced upon any Organisation. The Coordinator, both
Technical and Management, must be fully motivated and committed. They must be
prepared to take unpopular decisions and to take on jobs that other partners are doing
poorly or not at all, in order to guarantee the success of the project. Ideally, and espe-
cially for an IP, they will have had experience of Coordinating EU projects already.

Having agreed on a Coordinator, the core group then focus on defining the project
and its aims, and in turn on defining the missing skills and sectors. The core group are
then in a position to trawl their contact lists for suitable partners who fulfil the criteria
now set. In this way all partners in the project have worked with at least one other
partner before, integration is much easier to describe and a certain amount of trust
already established. Any partner brought in this way must have a specific role in the
project since there is no scope for significant overlap between interests or for Organis-
sations who simply pad out the project. These “fillers” are all too obvious at evalua-
tion and will result in the Consortium being marked down.

As the Consortium grows, plenary meetings should be organised in order to meet
physically and to get a feel for the expertise, commitment and personalities being
brought to the table. All core partners should probably have the power of veto over
additions and of course prospective new partners have the right to say no at any stage. Care should be taken when, for example, inviting more than one Company from the same Industrial sector, especially if they are in direct competition. As the project grows and is defined, it is entirely possible that its technical direction may change. If it does and the expertise of a particular Partner is no longer valid, they must be removed from the Consortium. This is often a difficult decision to come to and to action but it is essential that it is done, ideally with as little fuss as possible.

Finally, it is best if the Consortium is fixed and committed by the time the proposal is submitted. For Academic Partners this is usually straightforward. Most Research focussed Universities understand EU Framework research and already have a clear position on it. For Industry though it is often not so clear cut. Usually, although you could have contact with the Company at a fairly senior level, an approval process involving senior management will be required. As well as being prepared to assist in the process by supplying relevant information, the significant time it will inevitably take must be factored into discussions and planning.

3 How to write proposals

It is usually necessary for proposal writing to be taking place whilst the consortium is being built. It is not often that these activities can take place in series. However, all partners should be involved in the writing phase at some point. As they join, partners should write up their expertise and involvement. If they do not need to do so then you should seriously question the reasons for having them in the project, since self evidently, they are bringing nothing new to the table.

The starting point for proposal writing is, of course, the Commission template. This gives full guidance in what to include and indeed the volume of information required, via section titles and suggested page limits. From the start, clear responsibilities should be designated for each section, even if all that can be said at this point is that it will be written by a partner still to be announced. Those people responsible for each section will often act both as writer and editor, eliciting contributions from others as well as writing text, then forming into a coherent whole.

As with other tasks, the coordinator will retain overall control of the document. He will ensure that all sections are allocated, that new partners understand their writing responsibilities as soon as practical and that the document overall is taking shape. Most importantly, he will set clear, hard deadlines for contributions, based on an agreed overall schedule for the production of the final document. All partners must buy into any set schedule, however, it will often evolve as work goes on rather than being set in stone from the start.

Despite the many and varied virtual meetings which can now take place, we still believe that a small number of face to face meetings, probably three of four during the writing cycle, are necessary, to resolve major issues, to validate or alter the project focus and to agree technical and financial contributions.

As the document takes shape and arrives at, or very near to, a first full draft then a series of review and revision cycles should be instigated, involving each section being
looked at by someone who was not closely involved in its production. These new pairs of eyes give a fresh view of the text and can ensure that it is in keeping with the most recently agreed project direction.

During this time, the consortium will have to establish a requested budget for the proposal. The way we suggest is to ask partners to produce a budget and effort envelope for their participation. It should be made clear though, that at this stage it is only effectively a wish list. As the proposal refines and completes, the effort required from each partner should be easier to scope and adjustments to budget made. Also in terms of budget, valuable intelligence can be gleaned from the EU proposal documentation since it often tells us how many projects they intend to fund, together with the expected budget split between IP/STREP/Support Actions. With a little thought this gives enough to scope the Commission’s expected size of projects and allows some further thought to be given to the overall budget. Where the efforts have been finalised and the total budget is still too high, then project cuts need to be made. Check again that all partners are essential to the project and that all effort figures are in line with expected contribution. If either is not the case, then the solution is obvious. Assuming they are in line then a flat percentage cut across all partners is the only sensible way forward.

When the proposal is at “final draft” stage, ideally at least a week before the submission deadline, then it should be turned over to a small sub-group within the project, usually containing the most fluent or native English speakers. It is the job of these (three of four) people to go through the whole proposal and check its consistency, grammar and spelling so that by the end, it truly reads as one coherent document, not a number of loosely connected sections. Once ready, the aim should be to submit a full readable, and fundable proposal early, at least a couple of days before deadline. From there, the Consortium can submit after every non trivial edit right up until deadline. The comfort of having a full acceptable proposal in early, after several months work should not be underestimated. When coupled with the ability to then submit after every change, it would be negligent not to.

4 DEPOY aims and outcomes

Aim and challenges. The overall aim of the DEPLOY Project was to make major advances in engineering methods for dependable systems through the deployment of formal engineering methods [4]. 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 the system development that enables mastery of complexity. As well as leading to big improvements in system dependability, greater mastery of complexity also leads to greater productivity by reducing the expensive test-debug-rework cycle and by facilitating increased reuse of software.

The consortium saw the need to address 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. We realised that to achieve the re-
quired level of dependability, systems must be engineered in such a way that they deal with both accidental and malicious faults that come from within the system or from the system environment. From its considerable experience of building large complex systems, the consortium had 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:

- Modern formal methods support modelling and reasoning at multiple levels of abstraction enabling a systematic engineering flow from requirements specification, via architecture to detailed design and implementation
- An engineering flow based on formal methods can exploit powerful automated validation and verification technology to ensure consistency between levels.

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. Complex modern applications constantly face a wide variety of such conditions (caused among others by malfunctioning infrastructures, environmental hazards, malicious intentions, software defects, degradation of services provided by components and component mismatches) that can have potentially damaging consequences if these mechanisms are not in place.

Achieving industrial deployment involves a synergistic mix of scientific research, technology development and technology deployment. Deployment activities were planned to be conducted throughout the lifetime of the project in such a way that the needs and experiences of the deployment activities drove the research and development activities. Technology development underpinned by scientific research and both was validated through deployment. As well as playing the role of research and development drivers and validators, the deployment activities also played the role of technology demonstrators in the later phases of the project.

**Consortium.** DEPLOY offered a balanced interplay between industrial deployment, scientific research and tool development, where companies in four sectors join their forces with eight technology providers to meet the goal. The industrial sectors, transportation (Siemens), automotive (Bosch), space (Space Systems), and business information (SAP), comprised a palette of important European base industries of today. The companies possess different maturity levels when it comes to deploying formal approaches. The five academic partners (Newcastle University, University of Southampton, Åbo Akademi University, Dusseldorf University and ETH Zurich) are world leaders in formal methods research, that have considerable experience in developing and applying resilience 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 will be in charge of the assessment activities. In the middle of the project two universities joined the consortium (Pitesti and Bucharest) with a help of a newly opened program in FP7. The project was coordinated by Newcastle University with a dedicated Project Office set at the School of Computing Science.
Measurable outcomes. By the end of the project each industrial partner achieved deployment of formal engineering methods and tools in their development and became self sufficient in the use of formal engineering methods.

The deployments enable us to provide scientifically valuable artefacts including formally developed dependable systems and numerous results of systems analysis including a rich repository of models, proofs and other analysis results. The deployments also enabled us to provide a thorough assessment of formal engineering methods through assessing the tools and methods and collecting experiences both positive and negative.

By extending the mathematical foundations of formal methods the consortium delivered research advances in complex systems engineering methods that enable high degrees of reuse and of dependability, and effective systems evolution that maintains dependability.

The project delivered a professional open development platform (Rodin) based on Eclipse that provides powerful modelling and analysis capabilities, is highly usable by practising engineers and is tailored to sector-specific engineering needs.

Through the experience and insights gained in the industrial deployments we identified strategies that enable the integration of formal methods and tools with existing sector-specific development processes.

We put in place an organisation (Rodin Tools Ltd) which will be the home of the open platform: its role is to provide central support of the documentation, the training for and the maintenance of the platform. We have set up a body made of industrial users and technology providers whose role will be to coordinate technical decisions on the open platform. The project delivered training material and courses covering general and sector-specific formal engineering methods.

Deployment partners and DEPLOY Associates. Deployment was in four sectors. The initial phase of DEPLOY involved intensive training for the industrial partners state-of-the-art formal methods and tools. The training was followed by a phase of pilot deployment on industrial products in each sector. The experiences of the pilot deployment fed directly into the further advancement of methods and tools. These advances then supported the second phase of extensive deployment in each sector addressing production-level challenges. After each deployment there was a phase involving rigorous evaluation of the industrial impact of the deployments along with the development of strategies for future deployment.

In the middle of the project three companies became associated with the project work: AeS Group, Critical Software Technologies and XMOS. The project partners helped in training their engineers and were involved in developing several case studies using DEPLOY methods and tools. This lighter deployment helped the consortium to get more experience in deployment.

Four deployment partners and three DEPLOY Associate partners have achieved industrial deployment of the Event-B based methods and tools developed in the DEPLOY Project. This work involved the following specific areas:

• Bosch (Automotive): Formal development of a cruise control system and a engine stop/start system
• Siemens (Rail): The use of Rodin tools (ProB) for data validation of physical properties of network topologies for metro systems
• SAP (Business): Development of a method and a tool linking graphical modelling of BPMN models with Event-B formal modelling; development of a model-based testing test suite that includes some Rodin tools
• Space Systems Finland (Space): Formal development of an instrument management and mode management systems for space crafts
• AeS Group (Rail): Formal development of a platform door control system and ist safety analysis
• Critical Software Technologies (Critical systems): Formal development of an aircraft secondary display system
• XMOS (Processor design): Formal modelling of an instruction set of processor family.

**Rodin toolset.** The Rodin was architected as an extendable tooling environment based on Eclipse. It is an open-source project. This decision tremendously helped the project in achieving its aim of involving external users and developers in our work.

The tools developed in DEPLOY consist of the core Rodin platform based on Eclipse together with a range of integrated plug-ins. Highlights are as follows:
- The core Rodin platform providing support for model construction, syntax checking, proof obligation generation and proof management
- Modelling plugins that support refactoring, flow and mode control, team-based development
- Powerful proof support is provided through a range of internal automated provers together with plug-ins for using external provers including Atelier-B, SMT and Isabelle
- Model checking and animation is provided through the ProB tool which is fully integrated with Rodin
- Mathematical extension facilities means users can extend the in-built mathematical language of Event-B with libraries of new mathematical theories
- Tools for composition and decomposition of formal models enable better scaling of the methods (parallel composition, modularisation, decomposition)
- Tools for linking Event-B with other formalisms (UML-B, BPMN, UPPAAL, CSP) and with informal requirements (ProR, Problem Frames, UML-B)
- Tools for automatic code generation from Event-B models (JML, Dafny, C, C++, C#, Ada and VHDL) and tools for automatic model-based testing.

By the end of the project several plugins were developed and fully integrated into the platform by the external developers.

We would like now to briefly outline some of the successes achieved and difficulties identified in the DEPLOY work in the four domains represented by the project deployment partners. Full information could be found in the DEPLOY public deliverables. All these partners reported dramatic improvement of the Rodin toolset, in particular, by on-demand adding new functionalities and by improving its usability, reliability and scalability.

**Bosch experience.** A significant progress was made in formal development of industry-size automotive applications. Several traceable approaches were developed
and applied to support disciplined and structured mapping of the informal (natural language) requirements into abstract formal models; these were based on Problem Frames and RSML. At the same time the team found that the Rodin/Event-B technologies do not have full support for modelling closed loop controllers and time, as well as for development process (configuration management, variant management, team development and version management).

**Siemens experience.** At the time when DEPLOY started Siemens had had considerable experience in using formal methods (but not the Rodin/Event-B technologies). A medium-size application was successfully developed using these technologies, the company is now prepared to move to their wider use provided they are further improved to allow them to be applied in the development of safety critical applications (e.g. SIL4). The main success came in applying ProB for validation of on-board and wayside data – this approach was used by Siemens in several industrial projects. To achieve this ProB was validated to be used in a SIL4 development.

**Space Systems Finland experience.** Substantial experiments were carried out in formal development of typical space applications. The aim was to identify a model-driven approach to developing critical embedded systems. The importance of identifying the parts of systems for which the technologies are suitable became clear very early in this work. The focus was on formal modelling of behavioural requirements: modelling modal, distributed and reconfigurable systems and on fault tolerance modelling based on linking Event-B with the FMEA analysis. The achieved results meet the initial expectations of Space System Finland and form a solid base for further application of technologies within the company.

**SAP experience.** The main premise of this work was that the application of formal methods should be completely hidden from designers and developers of business applications. The main results were in successful development of tools and checkers for service choreography modelling, BPMN translation to Event-B and formal model-based testing. In the first two directions a substantial progress was made in understanding how to achieve the right interplay between applying proofs and model-checking, how to ensure consistency among different modelling layers and how to select invariants that a model must preserve during runtime. Achieving highest possible degree of automation played a crucial role in this work. At the end model-based testing received a wider acceptance of developers than formal verification. More efforts need to be invested into increasing the degree of automation, to make tool usage and feedback more user’s friendly and to improve tool efficiency when dealing with large software models.

**Technology transfer.** Ensuring successful transfer of the technologies developed in DEPLOY was one of the main focus of our work. Technology transfer served several purposes, including providing an earlier high-quality feedback on the application DEPLOY results in developing industrial applications in industrial settings and making sure that the companies gain the required sustainable experience and expertise in using these results. The technology transfer started with a 3-day block course and continued with on-demand training of the individual teams and engineers. Training was organised when the new tools and methods were developed in the course of the project. This was helped by the fact that each deployment partner had an experienced academic with a designated role of an adviser and the main contact point. Public tool tutorials were organised three times in association with the Rodin users and
developers workshops in 2009, 2010 and 2012. Various training materials were developed and made publicly available during DEPLOY.

5 DEPOY management

Management tasks in EU projects are funded at a higher rate than technical tasks leading to the temptation to pad out budgets as an easy win in terms of bringing in funding. This should certainly be discouraged. As with all other parts of the work, the Management budget is reserved for those carrying out the work of the project. Any partner requesting Management budget must be taking on management tasks on behalf of the whole consortium, not just a little local administration.

As already mentioned, the Consortium Coordinator will ideally already have experience in the role. The same applies to Management in that experienced staff who will be dedicated to the task, as opposed to working on technical tasks too, are undoubtedly the way to go. The Project Manager should also be able to work closely with the Technical lead, indeed they should be located close together physically too, and should both be committed to ensuring project success. Both must work to develop relationships with both EU and the Consortium and, although the Project Manager has no legal responsibility at sites other than his own, it’s important that he is seen as a source of advice and help by all partners. In this way he must truly manage the project not simply the interests of his own site. The trust and goodwill created by this management style are significant aids to the smooth running of the whole venture.

The key body in the management of any EU FP research project is the Management Board. This should consist of representation from all work streams and Partners. The Board should meet at least twice per year, taking advantage, where possible, of technical or other meetings already being attended by (at least some) partners. The Board will receive reports from all Work Packages and will advise on issues arising from the work. It is the Board’s primary purpose to keep the project on track with regard to technical focus and to ensure both the quality and timing of project outputs. In the DEPLOY Project we decided at proposal stage to appoint a neutral Chair of the Management Board, where previously, the role would probably have been the Coordinator’s. This departure from our norm was an outstanding success! Partly, this was due to our good fortune in securing the services of someone with wide experience in both Academia and Industry in the area of DEPLOY, Formal Methods, however, having someone who could be a bridge between interests and sectors was invaluable, and well worth considering in major industrial deployment projects.

With regard to the mechanics of managing a major deployment project, we instigated a review and refocus stage at month eighteen of the four - year project. The rationale behind the timing was to allow us to present our plans for years three and four at the second annual review. The rationale behind the event itself was that it is virtually impossible to know the trajectory of the work in the later stages a full year before the project actually begins, at the proposal stage. Having the checkpoint allowed us to look at what was working and at what needed to be done and re-develop
our plan for the latter stages of the project based on the changing needs of our indus-
trial partners, thus giving the project the best possible chance of success.

The nature of DEPLOY was that it focussed strongly on our industrial partners. Industrial uptake of the methods and tools was identified as the major potential suc-
cess of Deploy. In order to achieve this, it was necessary to integrate the industrial partners fully into the project process. One way we achieved this was to appoint an academic “buddy for each industrial partner (Newcastle/Bosch, Southampt-
on/Siemens, Åbo/SSF and ETHZ/SAP). It was the role of the academic partner to ensure that the needs of industry were kept at the forefront of all project decisions and to ensure that the work of DEPLOY was phased in such a way as to produce success. The buddy system was also important in providing early warning of changes in our industrial partners. Over a four - year period, management decisions and market forc-
es bring changed circumstances for industry much more than academia, and this can result in reduced commitment to the project. It is best to be prepared for this in ad-
vance. Similarly, in a four year, fifteen - partner project, it is almost certain that the consortium will be not remain constant throughout. It is, of course, possible to replace partners if the right organisation can be found. One alternative to a straight replace-
ment is to bring in an associate partner of partners. Associates, bring a much smaller level of involvement and smaller classes of problem. This can be easier to negotiate quick-
ly with management and also allows the project to spread into other domains and conduct initial experiments within them.

Finally, the project must make results easily accessible. DEPLOY did this by hav-
ing a number of repositories. For code writing and tool development, we used SourceForge. For internal documents, BSCW and as our external face, www.deploy-
project.eu, which also has links to the others mentioned. We were also fortunate to be able to use the, fully searchable, Southampton repository for papers.

6 DEPLOY Legacy

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 in-
clude companies already using Event-B and Rodin. One of the purposes of the eco-
system is to allow an industrial company to adopt new methods as the basis for prod-
uct 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 in-
dustrial 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.

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, automotive, 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 Systere, ClearSy and CETIC, will be in the core of future development and transfer of the Rodin technology.

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. 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.

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 (more information could be found in [5]).

In the SafeCap project (Overcoming the Railway Capacity Challenges Without Undermining Rail Network Safety) Invensys Rail with the help of Newcastle University is working on transferring the Event-B technology into in-house industrial rail-
way projects. This project focuses on developing modelling techniques and tools for improving railway capacity while ensuring that safety standards are maintained. The toolset to be created is based on Rodin and uses a specially developed domain-specific language to describe track layouts.

Event-B is being used by ClearSy to formally model the automation of the Flushing and Culver metro lines in New York, 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), which involves Alstom Transport, Critical Software Technologies, Systerel, Southampton 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.

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 Dependable Systems Forum (DSF) 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”.

Systerel 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.

Since April 2010 the Åbo Akademi University team has been involved in the EU funded ARTEMIS JU project RECOMP (Reduced Certification Costs Using Trusted Multi-core Platforms). The project is driven by industry. 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.

QNX Software Systems Ltd 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 help in the approval process.
**Rodin Tools Ltd and Tool Developers.** The development and coordination efforts, initiated during DEPLOY, will be continued in the following ways.

Rodin Tools Ltd [6] was set up by Newcastle University in early 2012 in accordance with the project dissemination and exploitation plan. It has a community of members and will offer several training courses per year free to members but available to the whole community. Rodin Tools will also advertise other training offerings available. As well as providing training, the company will oversee 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.
- 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.

Rodin Tools will be funded by members fees, set at various levels to enable individuals, PhD students, SMEs (Small and Medium Enterprises), large companies, STREP (Strategic Targeted Research Project) and IP projects to subscribe. Rodin Tools Ltd works 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/Rodin website [7] supporting users and developers of the Rodin toolset. The source code and tool development is monitored 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.

**Sources of training, educational and scientific materials.** These are the main sources of information about the technology developed in DEPLOY:

- Material related to the book with some examples and slides - see [8].
- 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 [9] 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 [7], 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 [10] 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 [11] 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 deployment book [12].
- The Event-B/Rodin site [4] provides pointers for downloading recent releases of the tools and links with the dedicated SourceForge site [13]. 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.

7 Conclusions

This paper summarises our experience in preparation and coordination of a major EC FP7 Integrated Project. We report on the main challenges the project addressed, its objectives and outcomes. Deployment of formal engineering methods is difficult; it requires special dedicated efforts and skills. The huge gap between the motivations of academics and the needs of industry is still there but the project demonstrated a way forward. The consortium work showed that it is possible and practical to train engineers in formal methods, the rigour required to formally model the systems helped industry in improving understanding of their systems and uncovering various problems, the gap between the informal world of customer requirements and formal models need a special support that is often underestimated.

Academic tools will be very rarely useful for industry; any attempt to make industry to try them often decreases the chance of later industrial uptake. During the project the consortium transformed a research experimental toolset into an industry-strength development environment used by industry and ready to be applied by interested industrial partners.

DEPLOY clearly showed that Rodin/Event-B are not a panacea, the choice of the right tools for the problems in hand is crucial for the successful deployment. But making various advances in developing methods and tools the consortium demonstrated the power of the technology, and at the same time identified its limitations. Future work on improving and extending them will help to address these issues.
8 Acknowledgement

DEPLOY has been a life-changing experience for us, we are grateful to all project members for their enthusiasm, cooperation, help and commitment to the project success. The project was supported by the EC Framework 7 Programme.

9 References

3. FP6 STREP RODIN project on Rigorous Open Development Environment for Complex Systems - http://rodin.cs.ncl.ac.uk/
5. Industrial and research projects that use and develop Event-B/Rodin: http://wiki.event-b.org/index.php/Industrial_Projects
9. DEPLOY repository - http://deploy-cprints.ecs.soton.ac.uk