Project DEPLOY

Grant Agreement 214158

"Industrial deployment of advanced system engineering methods for high productivity and dependability"

DEPLOY Deliverable

D29 (JD2) – Initial assessment results

Public Document

14 September 2010 – V1.0

http://www.deploy-project.eu

Contributors:

J.C. Deprez, CETIC, BE
Christophe Ponsard, CETIC, BE
Renaud De Landtsheer, CETIC, BE
Jérôme Falampin, Siemens SAS I MO, FR
Timo Latvala, Space Systems Finland, FI
Andreas Roth, SAP, DE
Rainer Gmehlich, Bosch, DE
John Fitzgerald (Newcastle University)

Editor:

Christophe Ponsard, CETIC, BE

Reviewers:

Cliff Jones (Newcastle University)
Michael Butler (University of Southampton)

Executive Summary

Although formal methods have developed for several decades in research laboratories, up to now they have had only little breakthrough in Industry. However, two factors have emerged in this decade. First, formal methods and tools have grown in maturity thanks to projects such as Rodin. Second, Industrial systems have grown to much higher degrees of complexity than ever before. Anticipating every interaction between all the electronic and software sub-components of a system is beyond the scope of Human capabilities alone. Formal engineering methods therefore offer a powerful mechanism to help engineers in crafting more dependable systems. In particular, formal methods impose to engineers to state explicitly the important aspect so that important properties and behaviours of the modelled systems can be guaranteed. The DEPLOY project now pushes further the argument for formal methods. First, by increasing the maturity of formal methods and tools; and second, by showing the applicability of formal methods and tools to solve real industrial problems.

To achieve these goals, the first part of the DEPLOY project conducts pilot projects where Industry partners (referred to as Deployment partners in the context of DEPLOY) learn to apply formal methods and tools to real industrial problems. The particular sectors targeted by DEPLOY are automotive with Bosch, public transport with Siemens SAS-I-MO, space with Space System Finland, and business with SAP. The second important part of the project consists in improving the maturity and functionality of formal tools to better address the need of Deployment partners.

To determine the extent to which the main goals of DEPLOY are achieved, a whole portion of the project is dedicated to assess the important issues encountered during the industrial pilots. For all European businesses to leverage on the DEPLOY experience, the assessment effort presents its findings in a generic way. In particular, Frequently Asked Questions related to formal engineering methods and tools have been identified and are being answered during the project using the information learned from the industrial pilots. In addition, success stories on significant accomplishments by each Deployment partner are presented. This assessment work is ongoing and will last until the end of the project. This report presents a summary of public information captured up until the middle of the third year of DEPLOY. Furthermore, the assessment plan for the remaining one and a half year of DEPLOY is presented.

This report provides a summary of the assessment efforts. The detailed information on the FAQ and its answers as well as the success stories are published on a wiki at the following address:

https://forge.pallavi.be/wiki/formalmethodevidence

The wiki structure provides a better navigation experience and also enables easier collaborative work for anyone to contribute answers. The contribution rights are restricted to the DEPLOY internal partners for the moment. However, in longer term, it will be accessible for external contributors and will eventually be released on a renowned web hosting by the formal method community and easy to find for industrial organisations looking for information about formal methods.

Document History

Date	**Version**	**Author**	**Description**
05/05/2010	0.1	C. Ponsard	Writing plan and structure
29/6/2010	0.2	C. Ponsard	Draft summarizing main lines
14/7/2010	0.3	C. Ponsard J-C. Deprez	Update based on internal discussion and the newsletter article
28/7/2010	0.4	C. Ponsard	Finalisation of review version
30/7/2010	0.5	C. Ponsard	Assessment and future work chapters
2/8/2010	0.6	R. De Landtsheer C. Ponsard	Corrections.
3/8/2010	0.7	S. Naqvi C. Ponsard	Internal proof reading and corrections
3/9/2010	0.8	J-C Deprez	Improvements, integration of reviewers comments (industry and academic partners)
9/9/2010	0.9	C. Ponsard	Consolidation of reviewer comments
14/9/2010	1.0	S. Naqvi R. De Landtsheer	Final proof reading

Acronyms

DoW	DEPLOY Project Description of Work
DP	Deployment Partner
DSL	Domain Specific Language
FAQ	Frequently Asked Questions
FLOSS	Free-Libre / Open Source Software
FM	Formal Methods
FMEA	Failure Mode and Effects Analysis
PO	Proof Obligations
QA	Quality Assurance
RAMS	Reliability, Availability, Maintainability, Safety
ROI	Return On Investment
SME	Small-to-Medium Enterprise
SOA	Service Oriented Architecture
SRS	Software Requirements Specification
SSF	Space Systems Finland
SIL	Safety Integrity Level, SIL4 is very high level of integrity
SAS I MO	Siemens Société par Action Simplifiée, division Industry, branche Mobility
TS	Technical Specification
UML	Unified Modelling Language
WP	Work Package

Table of Contents

1 Introduction

1.1 Context and Goals

Formal methods have been successfully applied in a number of industrial case studies and are even adopted in specific industrial fields. However, they are still not widely used in commercial software development, even in safety/security/business-critical sectors such as automotive, mass transport, aerospace or business information systems. The reasons for this situation have been widely studied over time, and a number of obstacles and often misconceptions ("myths") are identified such as the difficulty of the mathematics, their acceptance by customers, the effect on costs and duration, the incompatibility with traditional development methods, the lack of support and tools, etc. [Hall90, Bow95]. Guidelines (stated as "commandments") have also been suggested to address these obstacles [Bow95, Bow06]. With a partial sponsorship of the DEPLOY project, ACM conducted a survey in 2009 to gather the state of the art of industrial use of formal methods. The findings of this survey mainly at the specification and design stages give highlights based on industrial project [Woo09].

To foster the adoption of formal methods in the industrial domain, it is necessary to gather and consolidate information about industrial deployment experiences. The DEPLOY controlled effort offers a unique opportunity in this regard since DEPLOY industrial partners (referred to as Deployment partners) are experimenting with the whole process of introducing formal engineering methods in their organisations during the course of the project. They are facing issues such as deciding the scope of what to formalise, how to adapt the development process to ease formalisation and gain value from it, how to train people on formal methods, tools and techniques. These industrial pilots at each Deployment partner are therefore closely monitored to identify and collect evidence on the impact of deploying formal methods in various industrial contexts. A consolidation of experiences reported by non-consortium members of DEPLOY is also a part of this work.

To increase the impact of the assessment results, it is necessary to present evidence in a way that answers direct concerns of different kinds of audience:

- **Deployment partners**: Based on the first hand experience with various formal engineering methods used during DEPLOY; deployment partners want to identify those methods that are beneficial to their contexts. In addition to the set of initial industrial partners, a **second wave of associate industrial partners** are also now experimenting with the formal engineering methods and are providing some valuable feedback on their usefulness. For the subsequent objective analysis of their experimentation with the various formal engineering methods, all those industrial partners need to have a repository where facts of their various interactions with different formal engineering method can be recorded.
- **Academic partners**: Academics also need to record information on their interaction with the deployment partners while helping them out. Later, this information can be used to identify potential improvement path for certain formal engineering methods. Therefore academic partners also need a repository to collect information on deployment experiences.
- **Wider engineering community**: This segment of potential adopters will not be able to experiment the formal engineering methods during the course of DEPLOY project. Nonetheless, they will have access to the information repository where they can find authentic information on what to expect when using formal engineering methods. It will

also allow them to determine if their context can benefit from formal engineering methods. Furthermore, centralizing generic information on the usage of various formal methods will facilitate their comparison. We also recognize that people with different roles in an organization want to find information on formal method. It is therefore also important to address the various needs of different roles in terms of content and depth of answers.

In practice, this work is taking place in the evidence work packages (DEPLOY WP11) with the strong involvement of the industrial work packages (DEPLOY WP1-5) which also involve the technology transfer work of many academics and tool developers. It directly feeds to the assessment work package (DEPLOY WP13.1).

1.2 Scope and Structure of this Deliverable

This deliverable is the logical continuation of the previous deliverable of the related work package on evidence collection (WP11). It follows the methodology defined in the [D7Bis] and elaborates on the evidence repository described in [D30] by further answering the role-based questions listed in the “frequently asked questions” (FAQ) and by updating the “success stories” already presented in [D30].

This document is also a joint deliverable of the project showing a collaborative effort of all the DEPLOY partners towards the goals described in the previous section. This document is mainly an introductory and explanatory part to our evidence repository which contains the complete and up-to-date information.

A number of audience specific goals are also driving this deliverable:

- **For the DEPLOY industrial partners, it is a mid-project assessment deliverable** based on the evidence material produced during the initial learning period and the first phase of “pilot” deployments in the four industrial sectors. It will also describe **how each sector plans to further elaborate** this material. The way new DEPLOY associates will join this effort will also be described.
- **For the academic partners, it is important to clearly define how their contributions can improve DEPLOY methods and tools can address specific industrial needs**. In the defined methodology, they are stated as working hypothesis that related to some FAQ. In this deliverable a set of new working hypotheses are defined in order to answer the new strands of work.
- **For the wider engineering community, this public deliverable is an important step towards the production of public material** that will help them out to make an informed decision about the opportunity to adopt formal engineering methods and how to best address the major issues that often arise when formal methods are taken-up.

This deliverable is structured as follows:

- Chapter 2 gives an overview of the structure of the evidence repository.
- Chapter 3 focuses on the publication objective by presenting the evolution of the evidence repository since the release of D30 in order to address the needs of an industrial audience. It shows the various improvements and the way it is made public.
- Chapter 4 presents the assessment results focusing on evidence from each industrial sector. This chapter summarizes and gives some updates of the assessments presented in the first and second year assessments [D12][D25]. The link with evidence material is also highlighted.

- Chapter 5 describes the ongoing evidence collection work. It addresses the objectives of the industrial and academic partners of DEPLOY.

A complete snapshot of the evidence FAQ is not included in this deliverable because it is continuously evolving and hence the presented snapshot will become obsolete very quickly especially given the time interval between the submission and the review. Moreover, the original format is a wiki offering hypertext navigation and multiple indexing schemes. This aspect is important but cannot be experienced by a linear document.

2 Presentation of the Evidence Repository

A quick summary of the structure and the contents of evidence repository is presented in this section. The contents of this chapter are also presented in the fifth DEPLOY newsletter (August 2010) which focused on our evidence work.

2.1 A role-based FAQ approach

To draw the attention of an industrial audience, a FAQ (Frequently Asked Question) structure listing important questions is used to present DEPLOY's key results. Furthermore, it is also observed that different roles in an organisation are interested in different types of questions. Thus, FAQ are grouped by Themes and Roles. Specific key themes of interest are:

- The impact on an organisation with regards to training scope and resourcing,
- The impact on the quality of a product developed using formal methods,
- The capability to exploit formal models at various stages of the development process,
- The capability to perform reuse across development projects when formal methods are used, including reuse of formal and proven artifacts
- The capability to phase the learning of a formal method in an organisation and eventually to restrict the scope of who must understand and become an expert in a formal method
- The capability to phase the migration to using a formal method, given the existing context
- The known strengths and weaknesses of tools associated to a formal method as well as the support quality of the tool providers
- The external factors such as competition, standard bodies, or legislations, pushing the take-up of formal methods

To make sure that the essential points on these themes are covered, questions are raised from four different viewpoints roughly corresponding to the following organisational roles:

- **High-Level Managers**: managers of production department or R&D department have to take an enterprise's strategic decisions and assess the financial impact of using new methods and techniques. Furthermore, this role includes product and product line managers who are concerned with the commercial aspects of products.

- **Project and Quality Assurance Managers** directly manage engineers, analysts, and QA practitioners. They have to determine project feasibility and they directly manage staff working on system development projects. They do not perform technical tasks but often need to have a good understanding of the methods and tools used by their teams so they can determine the feasibility of a project, decide about the profile to allocate on the project and possibly identify the associated training, and adapt quality assurance procedures.

- **Engineers and Analysts** represent people who directly work on system development projects. They are among those who apply the engineering methods selected and who use the associated tools.

- **QA Practitioners** perform the QA tasks such as document review, traceability checks, integration and system testing. In general, QA practitioners do not need to apply formal methods but they need to understand them because work products that they review and use are expressed in the selected formalisms.

The four roles presented above cover a large panel with diverse needs. Therefore, identifying questions that interest all of these roles on all the themes listed earlier will cover all the important aspects related to the impact of deploying formal methods in a company.

The natural way to structure this information is a web-based FAQ. It provides the appropriate mechanism to structure information along different dimensions: themes, roles, and industrial sectors. A partial example of a question/answer is presented hereafter. In addition to the question/answer, the theme and the role associated to the question are also listed.

Theme	Exploiting formal models at various stages of the development process
Roles	• Engineer and Analyst • QA practitioner
Question	Is it possible to take advantage of formal models beyond using them to guarantee certain properties of a system, for example, to automate certain development and QA tasks?
Answer	Siemens SAS I MO is showing how Engineers can generate FMEA and system documentation from Event-B models and to connect those to their existing B development chain. SAP showed how Engineers could help QA practitioners by generating integration test cases for testing business processes. Formal models were developed to prove certain properties of the business processes and then these formal models generated interesting test cases not yet imagined by QA practitioners.

2.2 Success and Failure Stories

In addition to a question oriented approach, it is also useful to provide complete stories detailing key topics, explaining in detail how a real world industrial situation benefited or not from formal methods. Not only success should be reported as one should also learn from the mistakes. Examples of success stories elaborated within the project were reported by industrial sector and also related to major training and tooling challenges. Among them:

- the use of requirements models to prepare the formalisation (Bosch)
- the improved capacity to model and prove complex systems in the space sector (SSF)
- the use of model-checking techniques to perform time-consuming data validation (Siemens SAS-I-MO)
- the use of domain specific notations to hide formal methods and foster adoption (SAP)
- the benefits of formal models for model-based test automation (SAP)
- the risk and benefits related to the use of open-source tools for formal methods (Systerel)
- the technology transfer and training needed to reach autonomy in the application of formal methods (ETHZ)

The reported success stories are not restricted to the internal project contributions but are also consolidated with similar experience reported by others in the literature or from the collaboration activities DEPLOY is organising through its associate program, interest group and dissemination events.

2.3 Contributors

The DEPLOY evidence work is currently open to external contribution. A call to join the work has been published in the DEPLOY newsletter 5 and is also posted on the DEPLOY evidence wiki presented later in this document.

3 Summary of Recent Evolutions of the Evidence Repository

A number of improvements were identified in [D30] to make the evidence collection work more effective. The status of identified issues is given in this section.

3.1 Extending the scope

New themes and questions have to be identified as the current deployments have mainly focused on the early development phases and not considered reuse issues.

Status: Chapter 5 describes the new topics to supervise to collect evidence items as well as the proposed approach to monitor them. Some statistics are provided hereafter. They depict the FAQ size and the current level of completion.

	January 2010 (Month 24)	**August 2010 (Month 31)**
Number of themes and sub-themes	9	9
Number of role categories	4	4
Number of role-based FAQ	37	48
Number of FAQ of interest addressed so far	Interest not yet validated	17
Number of success/failure stories	7	7
Number of working hypothesis identified	Not yet identified	97
Number of working hypothesis of interest	Interest not yet validated	59

3.2 Providing more complete answers

D30 presented only partial answer to a number of FAQ because currently on-going evidence items depend on some research work being implemented.

Status: D29 is close to D30 from the content point of view. Most industrial partners are working on sector specific issues that will consolidate evidence but new material is still not mature enough to be integrated. Current work is reported in [D31] and will derive the related evidence collection work (see Chapter 5). The work of the current two associate partners is still in early the early stages. Most of the new material related to some new training sessions and to parallel literature review work which is taking place to identify similar experiments reported by other peers.

3.3 Systematising the consolidation and validating the work

In order to stimulate contributions and the information collection to be used as evidence, CETIC is implementing the following means:

- Monitoring active mailing lists where interesting topics can be discussed. e.g. on specific method and tools issues. An important topic being discussed is the performance level of the Rodin tool

- Interactions between academic and industrial partners: currently industrial workshops and discussions on mailing lists are visible. CETIC asked academic researchers to more systematically inform the measurement team when they initiate a new interaction on a new topic with industrial partners. In this way CETIC can now engage in the dialogue so the evidence collection work is performed on the basis of explicit objectives and targeting specific questions of the FAQ.
- A new series of visits/teleconferences was initiated for improving the current FAQ, discuss the new questions and their answers in the second half of the project related to the new topics being deployed and more systematically plan the collection of evidence information in relation with the issues identified in the questions.
- Interactions are taking place with the measurement panel composed of senior scientists (John Fitzgerald, Martyn Thomas) who can provide guidance in the direction where the work can be extended.
- Finally, the executive board of DEPLOY is also kept informed of the status so it can input to this work if necessary.

3.4 Ensuring external visibility of the FAQ

The evidence material is meant to be public and a major goal of D29 as public deliverable is to make a significant step in this direction.

D29 implements the idea of publishing the FAQ on the popular form of a wiki that can provide useful return channel to collect improvement suggestions and also to facilitate collaborative work, including from external partners of the DEPLOY project.

During the course of the project, the FAQ’s and answers (of public distribution level) are published on the wiki at the following URL:

https://forge.pallavi.be/wiki/formalmethodevidence

This wiki only contains carefully validated public material. The elaboration and validation of the material is performed in another wiki which is kept internal to the project where all DEPLOY partners can contribute.

So far the collaborative dimension is kept internal to the project. However call for contributions have already been issued (see section 3.3) through the DEPLOY newsletter. This mean will also be used to draw the attention on the FAQ evolution over the last two years of the project.

A plan to make the wiki more visible and durable beyond the end of the project is being elaborated, for example through the formal methods wiki or the web site hosting the FM survey set up by Woodcock and Fitzgerald [Woo09].

4 Assessment Summary at Project Month 30

The main assessment of the DEPLOY project is provided by the evidence material documented in the FAQ repository. According to the feedback received from the Deployment partners, this presentation format provides them information in a more suitable and convincing format than previously envisioned formats. The FAQ not only presents questions whose answers have already been collected, but also additional questions that will be answered in the second half of the project. These questions will drive the evidence collection activity.

This chapter highlights the process of connecting our comprehensive assessments (reported yearly in restricted deliverables [D12][D25]) to the FAQ repository. There are two main activities:

1. **the identification of relevant FAQ's and success stories** in our repository and the documentation in a more generic form as a consolidation of already existing evidence material.

   For example the success of generating tests from Event-B models in the business information deployment contributed to the question about "Is it possible to take advantages of formal models to automate part of QA tasks?"

2. **the identification of future consolidation work**. The current achievement in each task in general has not yet covered all the industrial expectations. Analysing the industrial feedback is important to better identify important success factors that should be reflected in the FAQ. From there onward working hypotheses can be formulated to define precise piece of evidence that each task should try to provide to further elaborate the FAQ.

   For example: a working hypothesis is made on the time taken to train a person with (or without) prior knowledge of performing some productive tasks such as writing a simple model, structuring a more complex model, etc. The training periods of a person joining the project can be observed with respect to those tasks and the claim about the amount of training can be consolidated from this observation.

In the rest of this chapter, we review sector by sector a set of relevant aspects regarding formal methods and the current achievements made in DEPLOY from the perspective mentioned above. Although the presentation structure is based on the division in industrial sectors, a number of cross domain issues are also present. Such cross-domain views are best presented in the on-line FAQ (for example about training, tooling, integration strategies…)

4.1 Assessment of the Automotive Deployment

The objective within DEPLOY is to provide evidence that refinement-based methodologies such as Event-B can be adapted to the needs of the automotive sector. The automotive sector has not yet adopted formal engineering methodologies in production environments.

4.1.1 Requirements Engineering Phase

Goal: the proposed formal methods should be integrated and supported by requirements engineering phase enabling the systematic structuring of the requirements and the building of formal models from those.

Achievements: a formal engineering method based on the problem frames approach [Jack01] was designed and adapted to make it more scalable. This semi-formal method was successfully applied on a large cruise control specification.

FAQ support:

- This work directly supports the questions about Understanding Impact on the System Development Process, more specifically about Quality Improvements related to Requirements Engineering activities.
- A specific success story was developed entitled: "Requirements Quality Improvements through Requirements Modelling".

Remaining Issues:

- The approach lacks some tool support.
- The mapping of problem frames to Event-B is incomplete (e.g. derivation of invariant) and is not yet validated.

4.1.2 Effective Reuse of Formal Models and Analysis

Goal: not only the process but also parts of the developed models should be reusable across projects.

Achievements: There is some evidence that the requirements analysis process is reusable (see previous goal). The reuse of model parts could not yet be assessed as it requires a second deployment.

FAQ support: A specific FAQ section dedicated to the Reuse across Development Projects was created. However, it is not yet well developed as the reuse is planned for the second half of the project (see Chapter 5).

Remaining Issues: reuse of (component) models.

4.1.3 Ability to Manage Close-to-Production Industrial Problems

Goal: the proposed approach should be able to manage close-to-production industrial problems

Achievements: a large model of a cruise control system could be specified with a number of remaining issues related to methods and tools.

FAQ support: requirements on the tool performance are captured in the on-line FAQ section about Known Strengths and Weaknesses of Tools and Tool Providers

Remaining Issues:

- Lack of tool support for problem frames,
- Lack of modelling support for real time and event flows
- Lack of distinction between the Problem frame concepts of "machine" and "environment" in Event-B.
- Serious Rodin performance issues

4.1.4 Impact on the Development Process

Goal: Identifying the required changes with respect to the current processes.

Achievements: the impact on the process was mostly explored upstream, in connection with the requirements (see previous sections).

FAQ support: a specific FAQ section is dedicated to Understanding the Impact on the System Development Process.

Remaining Issues: exploring the connection with other development steps downstream the development cycle such as code generation and testing.

4.1.5 Quick start training session

Goal: provide engineers a short intensive course to get started

Achievements: the initial block training proved adequate to reach a first level of expertise. The next training steps based specific workshops centred on small scale sub-problems (called "mini-pilots") also proved adequate.

FAQ support: there is a specific FAQ section dedicated to Training Scope and Pace capturing training-related questions for different target audiences.

Remaining Issues: there is a lack of industrially oriented documentation, especially manuals for various profiles (beginners, experts), teaching concepts, teaching material, how to's ("cookbook").

4.1.6 Availability of training material

Goal: provide reusable material.

Achievements: the training material of the blocked course is available through the website. It was reused a number of times during large sessions (Zurich training, Dusseldorf training and Bucharest training) and more regularly by DEPLOY associates.

FAQ support:

Remaining Issues: some issues regarding the training material are:

- There is a lack of industrially oriented documentation, especially manuals for various profiles (beginners, experts) and how to's ("cookbook").
- There is also a need to show intermediate developments with various modelling decisions and their impact. Showing final developments are not enough.
- Material is scattered over different locations.

4.2 Assessment of the Transportation Deployment

The DEPLOY industrial partner of the transportation sector is Siemens SAS I MO. It has a large experience in formal methods, more specifically for the development of software components of railway systems with the B method.

The main objective within the DEPLOY project is to extend the use of formal engineering methods to system engineering, in order to address system's safety using Event-B and Rodin tools. Presently, this part of the design does not rely on formal methods. The B method is heavily used for component development, not at system level. The target users are therefore people without any background in formal methods.

A more specific objective is to improve the efficiency of specific time-consuming tasks in the B-development chain.

4.2.1 Method Integration at System Level

Goal: define an industrial process, necessary for large scale deployment. This means connecting system level modelling with existing activities such as requirements engineering, FMEA, development of B models, etc.

Achievements: STS has progressed in the design of a model-based methodology where a system level Event-B model integrates with the requirements engineering stage based on the definition of a refinement plan covering the informal system requirements.

FAQ support: STS work helped understanding the Impact on the System Development Process especially for questions related to development and quality assurance tasks.

Remaining Issues:

- The global gain of using Event-B has only been assessed qualitatively at the task level but not globally, also taking into account the need to train system analysts who are not familiar with formal methods.
- Alternatively to reduce the need for training, part of the complexity of Event-B could be hidden behind commonly used modelling notations by the systems analysis: namely state machines or tables.
- The Event-B model still needs to be connected to the B tool chain.

4.2.2 Validation on a Realistic Problem

Goal: develop a realistic (but not necessarily complete) model of a system using Event-B to capture all the key aspects of such systems.

Achievements: a realistic model of train system was produced based on an informal specification of 15 pages composed of 80 requirements. The Event-B model was composed of 7 machines and 7 contexts. Its size is more than 6000 lines of Event-B resulting in more than 1000 proof obligations of which 40% were automatically discharged. The model covered key aspects such as safety invariant, timing properties and probabilities.

FAQ support: this contributes to an important general question: whether formal methods can cope with industrial size and complexity? A directly related question is about the tooling performance.

Remaining Issues: some languages' limitations where encountered such as lack of transitive closures, the limited way to model probabilities, the absence of decomposition/recomposition (in July 2009). Prover limitations related to set cardinalities also limited the level of proof automation.

4.2.3 Automated Data Validation of B Models

Goal: proof-based tools are not efficient for data validation required when deploying a train line. It results in long manual validation sessions. The approach is to explore if alternative model-checking techniques can help here.

Achievements: the use of an adapted version of the Pro-B model checker proved very successful as it improved the productivity of the problematic task over an order of magnitude (from 1 month to a few minutes, not taking into account some preparation time).

FAQ support: this directly contributes to highlight the importance of the choice of the right verification technique with respect to the problem considered. It is documented in the FAQ category "Known Strengths and Weaknesses of Tools and Tool Providers".

Remaining Issues: the resulting tool has to be certified for industrial use.

4.3 Assessment of Space Deployment

The goal of SSF in the project is to integrate the DEPLOY methods and tools in their development process. This covers specific sub-goals related to the elicitation and management of requirements, the way of modelling space systems in Event-B (relevant aspects to capture for Event-B, abstractions to use to cope with complexity) and the acquisition of knowledge on modelling typical architectures.

4.3.1 Defining a Reusable Method to Model Space Systems in Event-B

Goal: find out reusable techniques to efficiently model space systems using Event-B and carry out the proof process with Rodin.

Achievements: two complementary pilot projects were developed, both modelling satellite systems. The first pilot is a model of the BepiColombo command and control software. The second is a generic model of an Attitude & Orbit Control System (AOCS). Several versions were developed especially for the first system and with major rewrite. The resulting models were quite complex, but most of the efforts were spent in proving them rather than in producing them. The final versions have several refinement steps (resp. 8 and 13) and over 1000 PO. About 70% of them proved automatically.

FAQ support: this contributes to quantify the industrial suitability of the method and to some extend the productivity benefits of using formal models. The complete assessment should however take into account more models to assess the reuse effect.

Remaining issues:

- Event-B: readability, typing problem, control flow modeling, modularity
- Prover: the current level of automated proof is not enough
- Tool: lack of teamwork (December 2009)

4.3.2 Use of Event-B and Rodin for Low-Level Modelling

Goal: assess if Event-B and Rodin can be used to low-level close to the code models.

Achievements: two models were developed with different approaches, both by SSF and Abo Academy. The Abo approach was top-down from the specification and did not succeed to produce a full model. The SSF approach started from an ADA based model and failed to yield interesting model diagnostics.

FAQ support: this contributes to show the limitation of the application scope of Event-B and could contribute to a general question about how to make a good choose of formal method.

Remaining issues: none, as the approach was dropped.

4.4 Assessment of Business Information Deployment

Formal methods are not used routinely in the development of business software. Even though this domain is not safety critical, it is mission critical. Consequently, it could benefit from formal techniques and tools especially building on business models and model-driven engineering techniques [D21].

4.4.1 Hiding Formal Models behind Domain Specific Notations to Ease Adoption

Goal: Adoption in the e-business sector is only possible if using the existing domain specific notation. Event-B should provide the underlying semantics and Rodin should support a model verification process.

Achievements: Automatic translation of business process models to Event-B has been defined and implemented. Models for different middleware configurations enable specific checks on the way the communication channel works with respect to message delivery such as Exactly Once (EO) and Exactly Once in Order (EOIO).

FAQ support: this directly contributes to an important question reflecting a strategy to control the introduction of formal methods in an organisation by hiding it behind existing notations for a given class of users.

Remaining issues:

- Prover: the degree of proof automation is not sufficient
- Providing explanation to failed properties is still challenging

4.4.2 Improving Testing using Model-Based Testing

Goal: Model-based testing can reduce the time to produce integration tests, improve the coverage and guarantee complex coverage criteria. Moreover they are compatible with traditional development process. In the assumption a model is already available and suitable for test generation, the productivity gain can be important.

Achievements: A feasibility study was carried out as part of the pilot project. It was successful in producing transition coverage with minimal length tests on a message choreography state machine. Concrete tests could be produced and understood by validating users. Reuse also proved effective as there were only minor changes to the test adaptation layer.

FAQ support: this contributes to the question related to the exploitation of formal models by quality assurance practitioners and also by to the automation of tedious tasks (testing) by formal tools.

Remaining issues:

- Limitation to specific test classes and of the size of the model
- Not transparent: formal modelling skills required, model directed towards the test
- Significant effort to write the adaptation layer required for running abstract tests on a concrete environment

5 Planned Evidence Collection Activities

The current version of the FAQ repository has a well shaped and validated structure; however, a number of questions are still partially answered. The main goal of the second half of the DEPLOY project is to continue to elaborate those answers. This will be driven by:

- **Tasks related to sector specific challenges** identified as major impediment in each industrial sector such as tool performance, documentation, and code generation.
- **Reuse oriented tasks**. Those will contribute to the consolidation of existing FAQ answers. They will also help in the development of the specific section devoted to 'reuse' that is crucial to assess the level of productivity gain across projects. This is taking place in the second pilot. The WP8 research work package is also directly supporting it.
- **Tasks related to the exploitation of models** and directed towards the implementation level such as code generation and model-based testing. New strands of related work have been clearly defined in the refocused description of work [D18].

As presented in section 4, the practical way to organise the evidence consolidation work is based on the definition of working hypotheses. Based on the interaction with the academic and industrial partners, a number of such hypotheses have been attached to the FAQ (about 100). About half of these were evaluated interesting to the track. These working hypotheses have a simple formulation and represent explicitly agreed success factors of the related deployment tasks. Consequently, they become a good driver for the evidence collection work which becomes more natural and is also more easily kept in mind by all the deployment partners.

References

[Bow95] Bowen, J. P. and Hinchey, M. G. Ten Commandments of Formal Methods. *Computer* 28, 4, Apr. 1995.

[Bow06] Bowen, J. P. and Hinchey, M. G. Ten Commandments of Formal Methods. Ten Years Later. *Computer* 39, 1, Jan. 2006).

[BSI00] Bundesamt für Sicherheit in der Informationstechnik, Formal Methods Diffusion: Past Lessons and Future Prospects, Version 1.0, Adelard London, September 2000.

[Crai99] Craigen, D. Formal Methods Adoption: What's Working, What's Not! In *Proceedings of the 5th and 6th international SPIN Workshops on theoretical and Practical Aspects of SPIN Model Checking*. D. Dams, R. Gerth, S. Leue, and M. Massink, Eds. Lecture Notes In Computer Science, vol. 1680. Springer-Verlag, London, 77-91, Sept. 1999.

[DoW] DEPLOY Consortium, "Industrial deployment of advanced system engineering methods for high productivity and dependability - Description of Work", http://www.deploy-project.eu, October 2007.

[D7bis] DEPLOY Consortium, "Measurement Methodology (second version)", August 2009.

[D12] DEPLOY, First Year Project Assessment, January 2009.

[D16] DEPLOY, Pilot Deployment in Transportation, July 2009.

[D18] DEPLOY, Amended Description of Work (Project Re-focus), July 2009.

[D19] DEPLOY, Pilot Deployment in Automotive, January 2010.

[D20] DEPLOY, Pilot Deployment in Space, January 2010.

[D21] DEPLOY, Pilot Deployment in Business Information, January 2010.

[D25] DEPLOY, Second Year Project Assessment, January 2009.

[D30] DEPLOY, Initial Evidence Repository, January 2010.

[D31] DEPLOY, Tackling Industry Specific Challenges, July 2010.

[Gar09] Gartner Consulting Japan, Worldwide Trends of Formal Methods Application and the Issues in Information Systems to Secure Software Dependability. March 31, 2009.

[Hall90] Hall, A. 1990. Seven Myths of Formal Methods. *IEEE Softw.* 7, 5 (Sep. 1990), 11-19.

[Jack01] Michael Jackson. Problem Frames, Analysing and Structuring Software Development Problems. *Addison-Wesley*, 2001.

[Lar96] Larsen, P. G., Fitzgerald, J.S., and Brookes, T. Applying Formal Specification in Industry. *IEEE Software.* 13, 3, May 1996.

[Lar08] Larsen, P.G., Fitzgerald, J. S., Recent Industrial Applications of VDM in Japan*, in P. Boca, J.P. Bowen and P.G. Larsen (eds.) Proc. BCS-FACS Workshop on Formal Methods in Industry, Electronic Workshops in Computing, The British Computer Society*, 2008.

[Lec07] Lecomte, T and Servat, T, *Formal Methods in Safety-Critical Railway Systems.* In: 10th Brasilian Symposium on Formal Methods, Ouro Preto (Brazil), 29-31 August 2007.

[Sti03] Stidolph Donna C., Whitehead James, Managerial Issues for the Consideration and Use of Formal Methods In *Stefania Gnesi, Keijiro Araki, and Dino Mandrioli (eds.), FME 2003, International Symposium of Formal Methods Europe*, 2003.

[Woo09] Woodcock, J., Larsen, P. G., Bicarregui, J., and Fitzgerald, J. 2009. Formal methods: Practice and experience. *ACM Comput. Survey.* Vol 41, nr 4, October 2009.