Project DEPLOY

Grant Agreement 214158

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

DEPLOY Deliverable

D46 (D11.4) Consolidated evidence report (covering the whole project)

Report – Public (with restricted Appendix)

FINAL

V1.0 – 26 April 2012

http://www.deploy-project.eu

Contributors:

Christophe Ponsard, CETIC, BE

J.C. Deprez, CETIC, BE

Reviewers:

Ravi Ramdoyal, CETIC, BE

Thomas Muller, SYSTEREL, FR

Cliff B. Jones, University of Newcastle, UK

Executive Summary

An important goal of DEPLOY was to improve the maturity of formal engineering methods and tools in order to raise the level of industry interest and increase take-up. Many industrial deployments took place, firstly from DEPLOY industrial partners, and followed by DEPLOY associate partners. Other successful applications also took place among industrial organisations involved in the DEPLOY interest group and service-oriented partners.

This deliverable presents the project achievement of the work of collecting and structuring pieces of evidence identified in all those deployments in order to help potential industrial companies in their decision and deployment process about formal engineering methods.

The form taken by the evidence repository evolved across the project:

- In order to best fit the need of the industrial audience it finally took the form of a wiki combining a "Frequently Asked Questions" with a set of illustrating "Success Stories".

- In order to ease the navigation, it is structured using both a theme-based and a role-based logic.

- In order to attract contributions about deployments and lessons learnt by others, the wiki is open to external contributions. The ultimate goal is to create a community that keeps the knowledge repository up-to-date with quality data.

At the end of DEPLOY, the content of the repository covers the whole range of themes and roles. It also covers seven domains which goes well beyond the four initially defined in DEPLOY.

The wiki infrastructure was also improved and migrated to a fully-fledged wiki (media-wiki) and hosted on the following well-referenced URL:

<div align="center">

http://www.fm4industry.org or http://www.fm4industry.eu

</div>

Document History

Date	Version	Author	Description
30/1/2012	0.1	C. Ponsard	Writing plan and structure
17/2/2012	0.2	J.C. Deprez	Usage scenarios
5/3/2012	0.3	C. Ponsard	Repository evolution
25/3/2012	0.4	C. Ponsard	Statistics
31/3/2012	0.5	C. Ponsard	Future sections
2/4/2012	0.6	R. Ramdoyal, C. Ponsard	CETIC internal quality review
24/4/2012	0.7	C. Ponsard	Update after Systerel's review
26/4/2012	1.0	C. Ponsard	Update after U. Newcastle's review

Acronyms

DIG	DEPLOY Interest Group
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 IC-MOL	Siemens Société par Action Simplifiée, Infrastructure & Cities sector, Mobility and Logistics division.
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 numerous 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. DEPLOY was a unique opportunity in this regard since DEPLOY industrial partners (referred to as Deployment Partners) could experiment with the whole process of introducing formal engineering methods in their organisations during the course of the project. They had to face 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 were 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 was also a part of this work.

To increase the impact of the assessment results, it was 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 wanted to identify those methods that were beneficial to their contexts. In addition to the set of initial industrial partners, a **second wave of associated industrial partners** also joined the project to conduct specific experiments with the formal engineering methods. For the subsequent objective analysis of their experimentation with the various formal engineering methods, all those industrial partners needed to have a repository where facts of their various interactions with different formal engineering methods can be consolidated.

- **Academic partners**: DEPLOY Academics also needed to record information on their interaction with the deployment partners while helping them out. In a larger perspective, this information can be used to identify potential improvement paths for certain formal engineering methods. Therefore setting up a repository gathering information on deployment experiences is also useful in this perspective.

- **Wider engineering community**: This segment of potential adopters did not experiment the formal engineering methods during the course of DEPLOY project. Nonetheless, they have now access to the information repository where they can find authentic information on what to expect when using formal engineering methods. It also allows

them to determine if their context can benefit from formal engineering methods. Furthermore, centralizing generic information on the usage of various formal methods facilitates their comparison. As people with different roles in an organization want to find different kinds information on formal methods, it is also important to address their specific needs in terms of content and depth of answers.

In practice, this work took 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.

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] and [D29] by further answering the role-based questions listed in the "frequently asked questions" (FAQ) and by updating and providing more "success stories".

This document will not detail the evidence material that is best experienced through the online wiki but as the final deliverable related to our evidence collection work, it gives a comprehensive and self-contained summary of what was achieved. In complement to this deliverable and to the public wiki, the [D47] public deliverable named ("HOWTO guide for managers") gives a focused view of guidelines helping managers considering the adoption of formal methods.

The present document has the following structure:

- Section 2 will detail the structure and the practical form of the repository (FAQ, success stories...),

- Section 3 will present typical usage scenarios,

- Section 4 will give a consolidated analysis of the repository content, showing its evolution over time,

- Section 5 will explain how this repository will continue to live after the end of the DEPLOY project.

This document reflects the cooperation effort of all the DEPLOY partners towards the goals described in the previous section. In this respect, the repository was also very good collaborative tool to consolidate and validate the material that is now being made more widely available.

2   A Method for Collecting and Presenting Evidence

General surveys such as [Woo09] confirm the need to provide evidence to support the adoption process by companies considering the use of Formal Methods (FM). However, the concept of evidence needed to be further analysed in order to define how it could best provide information about formal methods to Industry and in particular, on formal methods explored during the DEPLOY project. Although evidence was first collected to help Deployment Partners in their adoption process, the main target audience is organizations not involved in DEPLOY.

2.1 Success (and Failure) Stories

Success stories have shown to be an efficient way of collecting evidence of successful Industry adoption. They often take the form of a white paper. In some cases, they are published in Industry tracks of conferences. The nature of such publications rarely allows sufficient space. Consequently, success stories often lack details of the very specific context in which they took place, for example, little information is usually provided about the overall innovation cycle of the enterprise involved in the success story, or on how researchers and production engineers collaborated during the transfer project.

To address this issue, success stories must be augmented to provide readers with additional contextual information as well as links to other related efforts. Consequently, a specific "success story" template was designed to enhance and systematize the presentation of success stories emerging from the DEPLOY project. This template is as follows:

Name	A short meaningful identification to use as title of the story
Keywords	A list of keywords helping in the classification of the success story
Short description	A description in a few lines of what the story is about and what claims are supported
Source	Organization that contributed to the work of this story and a contextual description of the company's structure and research and innovation process.
Benefits	The positive impacts that can be inferred from the success story. (NOTE: Themes/questions from the FAQ propose the important points on which impacts are sought hence one should review them when listing the benefit highlighted in an success story.
Limitations	Limitations identified (not definitive if on-going story), those are potential show stoppers and barriers to overcome.
Elaboration	Complete description of the work done to document the success story.
Consolidation	Additional arguments reported in the scientific literature corroborating this success story including citations to scientific publications presenting these arguments.
Further work	Specific work still to be done by DEPLOY partners to make the story a success.
References	List of publications or reports related to the success story.
Related FAQ	List of questions in FAQ to which this success story provided material.

Table 1 – Success Story Template.

The template above contains information on the context. In particular, the Source section asks

that an organization describes its structure as well as its research and innovation process. Usually, this context information can be lengthy. Hence it is recommended for the Source field to only provide the organization name and a link to another document that describes the full company context. This approach also has the added benefit that an enterprise with several success stories may often be linked to the same context document.

Although initially restricted to DEPLOY, the reported success stories evolved to wider project contributions coming also from associate partners and are now open to external consolidation, based on the above template. All success stories 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.

2.2 A role-based FAQ

Success stories provide evidence of formal method transfer and usage in Industry from a very specific viewpoint. By their specific nature, success stories do not however address high-level cross concerns of various Industry sectors, or at least, they do not present information so that cross concerns can easily be deduced.

This means that success stories should be complemented by another technique for presenting topics of general concerns to many readers from various Industries. During the DEPLOY project, researchers and Industry partners proposed to structure this cross cutting information in a **Frequently Asked Question format (FAQ)**. Industry partners are accustomed to this type of format where generic questions are answered in a fairly short space. During DEPLOY, the average length targeted for answers was about one page as illustrated in the next section. The resulting structure of our evidence repository is shown in Figure 1.
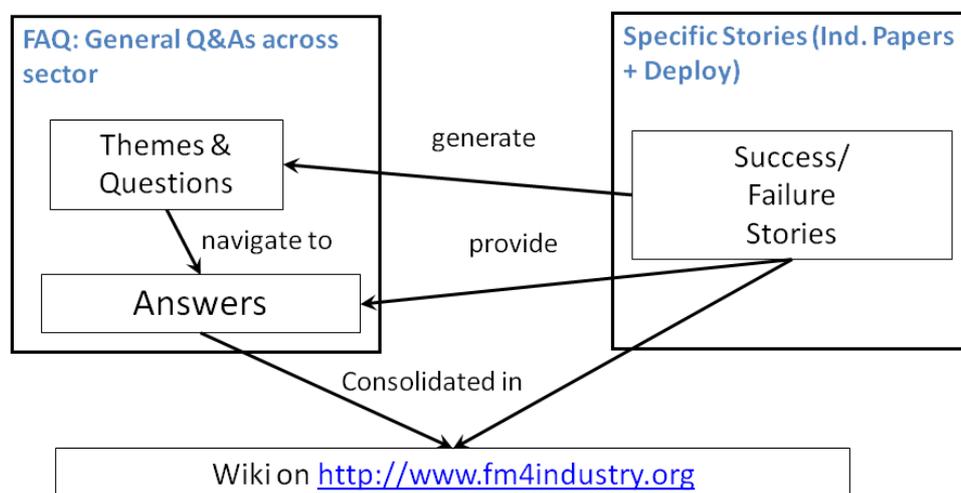

Figure 1 – Structure of the Evidence Repository.

2.2.1 FAQ Themes

At this point, an approach is needed to identify a fairly exhaustive list of common concerns from different Industry sectors. In order to identify common high-level concerns across domains, many documents provided by the DEPLOY Industry partners as well as by the Academic researchers and the tool providers were analysed. The high-level topics identified

are:

- The impact on an organisation with regards to training scope and resourcing,

- The impact on the Software/System Development Process, further refined in:

  - 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 with 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.

These various themes validated by the DEPLOY Industry and Academic partners provide the initial categories for which FAQ needs to be formulated.

2.2.2 Industry Roles

Pieces of evidence are labelled with the notion of **Industry Roles** to specifically target the relevant types of audience, and increase the impact of answers. The organisations involved in DEPLOY were quite different, ranging from the technological SME with highly polyvalent roles to large companies with a specific R&D unit and very well defined roles. Based on a careful study of the innovation cycle of the involved companies and on our experience in technology transfer, it was however possible to identify a set of key roles common to the DEPLOY partners, namely, high level managers, project managers, engineers and technical analysts, and quality assurance staff.

For a transfer project to be successful, many of these roles must be involved and supportive of the proposed transfer of research results. Thus, to obtain clear and concise answers, each FAQ should always explicitly target a single role. This does not necessarily mean that other roles will not be interested in the question but rather that the named role is the primary target hence the answer is provided to match with this primary role. For instance, the wording of an answer targeted to engineers is different from answers to questions whose primary audience is high level management. Thus, if a high level manager is interested to read a FAQ answer primarily targeting engineers, he will understand that the answer is presented from the engineer's viewpoint. Making the targeted audience explicit, by stating their roles, definitely helps the reader.

In the context of transferring formal method engineering techniques to Industry, the following roles were put forth:

- **High-Level Managers**: managers of production departments or R&D departments have to take an enterprise's strategic decision 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 issues.

- **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 of resources 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 FAQ approach suggests identifying questions of interest to each role for each theme. The important subtlety is that a question in the FAQ must be:

- Generic enough to interest enough readers and not be the sole concern of a single sector or even worse a single company.

- Specific enough so it is fairly easy to understand which results from Industry pilot should be proposed to which questions from the FAQ.

2.3 Presentation issues

At the presentation level, the most adequate and commonly used media is an Internet wiki which gives wide access to the material. Wiki technology also enables feedback from the people accessing the material, ranging from comments to more active contributions, with a degree of control/moderation that can easily be tuned.

Many Open Source wiki implementations exist. After an initial period on a simple RedMine wiki, we finally opted for Mediawiki [MediaWiki] (initially developed for Wikipedia) and which is made very powerful through many extension plug-ins. Figure 2 shows the homepage, accessible at http://www.fm4industry.org.
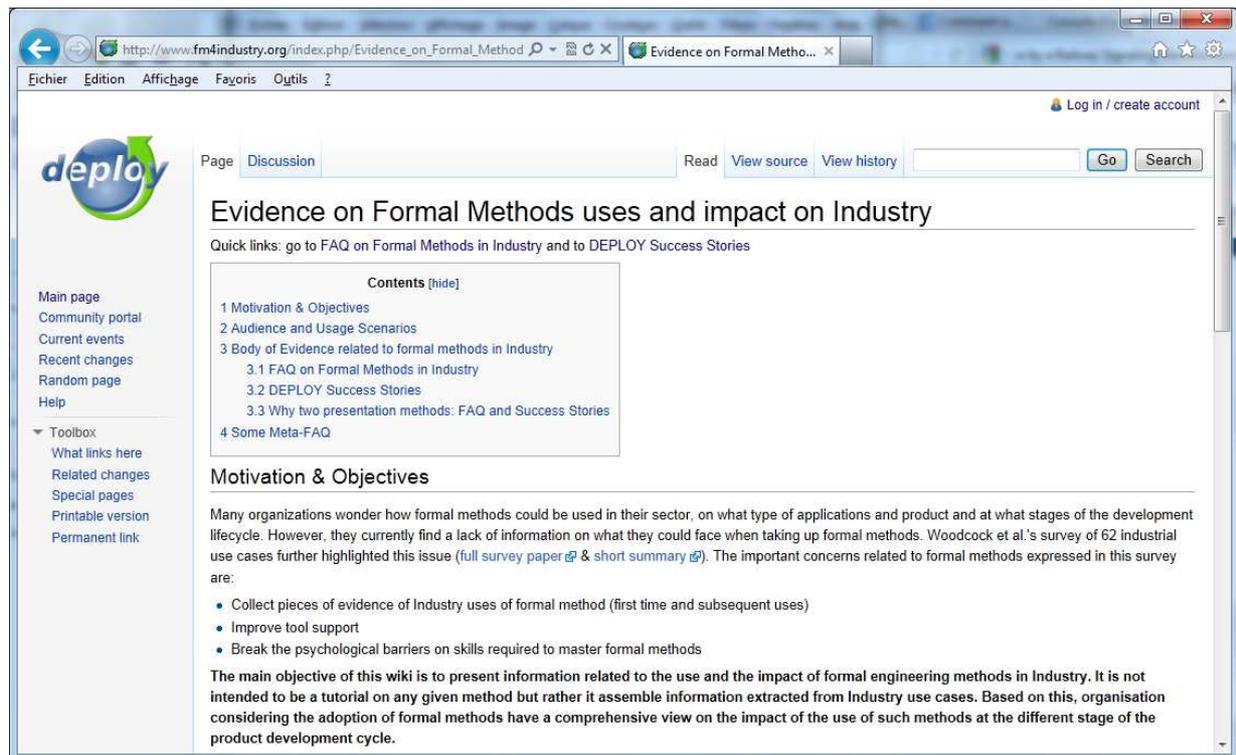
Figure 2 – Homepage of the Evidence Wiki.

3   Usage scenarios

A few customary situations faced by professionals with different roles in software-intensive system development in Industry are presented, along with the kind of specific questions each usually wonder about formal methods and their usage in actual Industry development. Subsequently, a brief explanation shows how they can browse the evidence repository to find elements of answers to their questions.

- **Scenario I - I am a High level manager who has heard that others in the sector have successfully used formal methods**. My staff has no prior experience on formal methods. My question is now "How should I proceed in the evidence repository to better understand if FM could also be used in my company?"

- **Scenario II - I am an Engineer in an SME, our development team has successfully used advanced static analysis tools during the debugging and testing phased of product development**. However, in a recent project, important requirements remained implicit until the customer validation phase. Subsequently, a significant overhaul of the architecture was needed to handle these requirements. Static analysis was clearly of no help. My question is now "How should I proceed in the evidence repository to better understand how our development team could start using formal methods earlier in the development lifecycle to increase the chances to have identified all important requirements after the design phase?"

- **Scenario III - I am a QA engineer, at a conference I saw a presentation from another company where QA and safety engineers in another fields have used tools to generate test cases for various coverage**. My question is now "Does your repository contain information on test generation formalism, approaches and tools and their eventual applicability to my sector?"

- **Scenario IV - I am a product (line) manager. I have heard of several success stories on the use of formal methods** but in my company's case, we already have well-tested components that fulfil their quality requirements. Our project mostly consists in configuring these existing components and integrating them. My question is "Does your evidence repository elaborate on the use of formal method to ease the integration of components, even if these components were not developed using formal methods?"

- **Scenario V - I am a QA manager in a SME. I have little experience of formal methods, in particular I ensure that my QA staff verifies our software product with renowned analysis tools.** However, I am completely unclear on how using formal methods at the requirement and design phase of product development could impact the QA process in my company. My question is not "Where does your evidence repository present pertinent information on the impact on QA process?"

These example situations traditionally faced by Industry help to illustrate how to navigate in the evidence repository to find FAQ and success stories with information relevant to one's context. For each of the scenarios above, a suggested navigation approach will be explained. In general, there are only two ways to start navigating in the evidence repository. In particular, the top-down approach starts from the FAQ while a bottom-up approach starts from success stories. In general, most readers will come with a general question and therefore, a top-down approach will be more suitable. However, in few cases, one may learn about a specific success story at a conference or while reading an article, for example in Scenario IV. In this case, it may be more appropriate to find if this success story is present on the Wiki with the evidence repository or if a similar success story exists in the evidence repository. Below, the two navigation approaches are briefly discussed and then applied to each of the above scenarios.

- **I - Top-down Navigation Approach** - When one has a general question about formal methods and searches how it could be answered for their specific organisational context, it is assumed that one is then in a rather non-focused exploratory search. In this case, the most appropriate way to find relevant information is as follows:

  o Identify the Themes in the FAQ that are of interest to your question,

  o For each theme of interest, review the questions specific to one's role, identify a subset of relevant questions.

  o While reading answers, the reader will find pointers to specific reference papers and success stories. The reader according to her context can then deepen the search by reading success stories in evidence repository or even the referenced scientific literature.

  It is important to note that questions are sometimes worded to highlight broad cross-industry concerns. Such questions can be answered from quite different viewpoints taking into account different sectors, different types of formal methods and even different phases of the lifecycle. Thus, when initially reading the FAQ, readers must understand that an answer may not only focus on their topic of interest. This broad coverage for some questions is selected on purpose so that a reader will find more general answers than the one initially anticipated. In turn, readers will be free to limit their interest to a part of the answer or to explore the other information proposed in the answer. In general, the various dimensions considered in an answer are specifically identified and usually yield subsections in an answer, for example, an answer that considers different formal methods usage at different phases of the development lifecycle will explicitly be broken down with one subsection per phase of the lifecycle.

In other words, when initiating a search from the FAQ, the reader must keep an open exploratory mind and not search for direct answers tailored to their only context. Obtaining tailored answers would require a specific study that can only be achieve through a dedicated subcontract, which goes much beyond this evidence repository.

- **II. Bottom-up Navigation Approach** - One may start an investigation by reading a success story that closely matches one's specific need. Although one may be tempted to stop the investigation at that point and to start implementing the approach described in the success story, appropriate caution should be exercised. Firstly, one's specific context will likely not completely match the context in which the success story developed. Secondly, continuing the investigation may highlight new possibilities not initially anticipated by the reader on formal method usage. It is therefore worth spending a little additional time navigating from the success story to its context description. To search for a success story and identify those potential similar to the one read or heard elsewhere, a full browsing is needed to review the complete title list of success stories, which are currently organised by Industry sectors. At the moment, the list is still short enough for full browsing to remain efficient. Alternate (sub-)classifications will be developed when the number of success stories grows larger than 30 or 40. Success stories in the evidence repository include cross references to FAQ questions where they are cited. It is then possible to navigate to a FAQ question linked to the success story and identify other potential questions of interest in the same FAQ theme. Finally, the success stories are classified by sectors, thus, it is also appropriate to review other success stories applied in one's sector.

4   Evolution of the Evidence Repository during DEPLOY

During the whole project life, continuous improvements to make the evidence collection work more effective were identified and implemented. Some were already reported in previous WP11 deliverables [D29][D30]. This section gives a summary of the main evolution of the Evidence repository during the whole DEPLOY project.

4.1 Full theme and role coverage

Until year 3, theme coverage was only partial because a number of specific themes had yet to have a second deployment achieved, for example the capability to reuse artefact and to internalise the expertise (trainings by the "first generation of deployers"). The second phase of deployment was successful to address this. In addition to providing answers to already identified FAQ, a number of new questions were also identified at this time (about ten).

Role coverage was also improved. At the start of DEPLOY, questions were often driven by technical concerns and addressing engineers and project managers. In the second half of DEPLOY, most companies started to think about internal adoption strategies and partial transfer to production, leading to the consolidation of a number of interesting FAQ related to high level managers. This material was also important to compile our HOWTO guide for manager [D47].

In terms of domain covered, the project was also very successful because at the end of DEPLOY, seven domains are covered (aerospace, automotive, business information, chip design/smart cards, operating systems, space and transportation). Among those, only four were

initial DEPLOY domains (automotive, business information, space and transportation). Other domains were contributed by DEPLOY associates or even the DEPLOY Interest Group (see http://www.deploy-project.eu/html/exploitation_dissemination.html).

Some statistics of the global evolution of our FAQ is provided in the following table.

	Year 2 (Month 24)	Year 3 (Month 36)	Year 4 (Month 51)
Number of themes and sub-themes	9	9	9
Number of role categories	4	4	4
Number of role-based FAQ defined	37	48	55
Number of FAQ of interest addressed so far	Interest not yet validated	28	38
Number of success/failure stories	7	9	14
Domains	4	5	7

Table 2 – Evolution of FAQ statistics

4.2 Broader scope than DEPLOY

The evidence repository work stated as a purely DEPLOY internal work based on material consolidated from the deployment experiments (WP1-4). The scope was progressively enlarged to the DEPLOY Associated partners and the DEPLOY Interest Group which contributed to a significant number of success stories. In addition, technology transfer partners such as ClearSy and Systerel were also successful in the development of business application scenarios of the DEPLOY methods and tools.

In the second half of the project, the repository evolved towards an online FAQ, it also became important to make connections with industrial experience case studies reported by others, e.g. in the scientific literature and in industrial tracks of conference. This is particularly important in the perspective of the long term evolution of the repository, beyond the end of DEPLOY. This objective was achieved at the FAQ level by including a strong reference section through which published material is consolidated together with DEPLOY internal material. A specific FAQ section is related to this consolidation.

Note that the purely external success stories have not yet been added to our success story section. A template is however provided and proposed for others to report about the success story they wish to include (see section 4.4).

4.3 Better external visibility

The evidence material is meant to be public and [D29] implemented 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.

In year 3, a simple Redmine-based wiki was used and showed a number of limitations such as the management of users, references, images and the interaction with contributors. In the final project year, it was decided to move the content to a more advanced wiki. The choice was MediaWiki, which is the Open Source wiki powering Wikipedia. It is very widely adopted as wiki engine, well supported and has a large number of potentially useful extension plug-ins.

The following features are now available:

- Media management, with good resize and placement support,

- Quick self registration of users with anti-spam control (email confirmation, captchas),

- Threaded discussions pages,

- Citations modules,

- Quick overview zone and content maturity assessment zone.

In order to have good visibility on the World Wide Web, the following improvements were also implemented:

- Final wiki URL http://www.fm4industry.org and http://www.fm4industry.eu ,

- Explicit referencing from other DEPLOY websites and from external web sites such as the FM wikia (http://formalmethods.wikia.com) managed by Pr. Bowen,

- Wiki keywords support improved referencing.

4.4 Open to external contributions and collaborative management

In order to prepare for after DEPLOY, several actions were taken to opening the repository to external contributors but also to enable a collaborative form of review with the ultimate goal to create a community ensuring the long term maintenance of this work:

- **Reading**: the wiki is fully public and free of charge.

- **Subscribing** to the wiki is easy and immediate (fully automated). It only requires a valid email address which helps fighting spam bot. The account creation process takes about 1 minute and enables both passive and active contributions.

- **Passive contributions**: discussion page provide a management space for each page were the content can be discussed. A user friendly module is used not requiring any knowledge on the wiki syntax.

- **Active contributions**: pages can be edited by all contributors but no new page can be created/move, so the structure is maintained. It is however possible to suggest such evolutions. It is up to the contributor to decide if they feel their level of expertise is enough w.r.t. the page subject to implement a contribution or just leave a comment.

This move also implies a rethink of the quality procedures to ensure the content quality. The previous procedure relied on a private wiki where the content was matured before being published. It was also a necessary step for managing possible confidentiality issues. This resulted in a limited visibility of a number of topics partially elaborated. In the after DEPLOY perspective, it is important to make all the useful information available and install a community-oriented process that still provides enough quality assurance. The evolution to reach this balance was to:

- Set up an editorial board managing the structure and monitoring the content. Technically it is also possible to review all modification to a page and even to filter out low quality contributions.

- Introduce quality tags on the articles, giving a clear indication of the level of quality of an article pointing out some flaws (incomplete, lack of references, requiring cleanup), or qualities (approved by the board, positive comments from visitors).

> Quality improvement actions are discussed in the related discussion page.

- Push more content on line, especially content for which DEPLOY could only provide partial answers but which can be further elaborated in a larger perspective. The use of the quality tags is also important here to mark the need for further elaboration.

About the content licensing, in order to be aligned with an open contribution scheme, a creative commons licence was selected. The selected licence is: "share alike" (CC BY-SA: http://creativecommons.org/licenses/by-sa/3.0). This choice is also consistent with other DEPLOY content such as the Rodin handbook. It allows the user to:

- **to Share** — to copy, distribute and transmit the work,

- **to Remix** — to adapt the work,

- to make **commercial** use of the work.

under the condition of:

- **Attribution** — You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

- **Share Alike** — If you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

5 Future of the Evidence Repository

To summarise, the DEPLOY evidence repository evolved from a closed project repository to an wiki open to all not only for consultation but also for contribution. It also evolved from quantitative measurements to a more practical work taking the point of view of different industry roles on different key themes related to the adoption of formal engineering methods. Its final form adopted is an industry-oriented FAQ providing practical answers to questions those different roles will naturally ask when considering the adoption of such methods. It is complemented with a set of success stories giving concrete illustrations supporting specific FAQ.

A number of approaches have also been taken in order to ensure the long term evolution of this work. In addition to the community-based process that was implemented, there are other commitments from the current DEPLOY partners on the future:

- **Review board**: the current DEPLOY evidence board will form the core of the evidence wiki editorial board. It will enforce the defined quality procedure and make it evolve as required.

- **Infrastructure**: CETIC will ensure the maintenance of the hosting and the mediawiki, keeping it available and up-to-date.

- **Support** will also be provided by formal methods organisations such as Formal Methods Europe and the RodinTools LTD.

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.

[D29] DEPLOY, JD2 – Initial Assessment Results, September 2012.

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

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

[D47] DEPLOY, HOWTO Guide for Manager – April 2012

[D49] DEPLOY, Fourth Year Project Assessement – April 2012

[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.

6 Restricted Annex

The restricted appendix is empty: all the relevant material was published on the on-line repository at http://fm4industry.org