A FAQ Approach for Collecting Evidence on Formal Method Industrial Usage

Jean-Christophe Deprez[1], Christophe Ponsard[1], and John Fitzgerald[2]

1. Centre d'Excellence en Technologies de l'Information et de la Communication (CETIC),
2. University of Newcastle
{Jean-Christophe.Deprez, Christophe.Ponsard}@cetic.be and
john.fitzgerald@newcastle.ac.uk

Abstract. After several decades, formal methods are gaining ground in Industry. However, as pointed out by the results of Woodcock *et al*'s survey, formal methods still need significant additional effort in several areas, most notably in collecting evidence on the use of formal methods and tools in Industry. This article proposes an approach for building a repository of evidence material. The main benefits of the proposed approach are first to make it possible to integrate information for many Industry pilots that have tested diverse formal methods. The secondary benefit is that the current implementation of the approach has a 'project on a forge' and of the repository as a wiki of that project is simple yet efficient in managing access and contribution rights. Nonetheless, the shortcomings of the current implementation are also reviewed.

1. Introduction

Industry take up of formal engineering methods and tools gains ground as the number of critical systems in various Industry sectors are increasing. There is however potential to further increase take-up. Several survey results were published almost two decades ago [1, 2], and then Woodcock et al. published in 2009 a new survey and survey results on formal method (FM) uses in Industry [3, 4]. They collected input from 62 Industry projects over a 25-year span. The most important factors highlighted by the survey results are related to increasing the importance of tooling support and also to the need for a systematic collection of evidence on formal method use in Industry. Incidentally, they also pointed out that people only reported on first time uses of formal methods and very little information were gathered on subsequent usage. Finally, the psychological barrier and the skills were also advocated as inhibitors to formal method adoption in the survey.

This paper proposes an approach to collect evidence material. The main goal of an evidence repository is to help various people from Industry to understand what formal methods can best help their specific context and needs. Unfortunately, published results of Industry use cases often solely focuses on presenting their success stories or at best compares their work to a very few others hence it is quite hard for Industry

readers to deduce enough information to make an fully informed decision on the adequacy of formal methods to their particular cases.

An important challenge when creating an evidence repository is therefore to identify a structured approach for classifying various Industry cases in a coherent way easily understandable by actors from different industrial contexts (requirement 1). The proposed approach identifies a list of general themes of interest to all (or at least most) domains and sectors. The current themes are listed in Section 2.1.

Industry members interested on formal methods also have different roles in their companies ranging from top level management and project manager to safety analysts and research or production engineers. Although similar themes may interest several roles, the kind of information sought will differ. The evidence repository should then facilitate the browsing of information based on role (requirement 2). The list of roles, their characteristics and a sample of theme-specific role-based questions of the FAQ are presented in Section 2.2.

It is often believe that research and industrial viewpoints are disconnected. Thus, when possible, the approach used for building the evidence repository should help to close that gap between the two communities (requirement 3). For example, by explicitly pointing out what industry finds important including non-research topics related to formal method and how industrial needs can be satisfied. On the other hand, researchers who may struggle to identify Companies to conduct realistic pilots should easily find easily companies that have participated in pilots on a selected theme. Actions taken to satisfy this requirement are presented in Section 2.3.

Finally, it is important to put in place a recognized editorial board who oversees the content of the evidence repository and its evolution. Incidentally, an adequate publication procedure should also entice authors to easily propose new evidence material (requirement 4). This procedure should also manage potential confidentiality issues which are frequent in Industry and which could prevent evidence reporting.

This paper describes an initial attempt to implement the four requirements above using a FAQ approach on a set of themes important to Industry. The implementation of the proposed approach is in the form of a *project on a forge* publically available at https://fm4industry.cetic.be. The most interesting information is currently found on the wiki section. Summary statistics on the current repository of evidence material are given in Section 3. This paper concludes with Section 4 on the benefit and the limitation of the current implementation of the approach.

2. FAQ Approach based on Theme and Role-based Questions

The general suggestion of using a FAQ to present evidence came from Industrial partners of the DEPLOY project (www.deploy-project.eu) who believe that this format seemed the most appropriate for Industry readers. However, they would be too many questions to cover the topics on the use of formal methods in Industry and topics that influence the use of formal methods in Industry. Furthermore, the Industrial audience is in itself quite large and constituted of people filling different roles in their organizations. To facilitate the search of relevant information, the

presentation of evidence material should therefore be partitioned based on themes and roles respectively presented in Sections 2.1 and 2.2.

2.1 General Themes of the Repository

Theme partitioning can take different viewpoints. On the one hand, it may remain generic identifying topics of general concerns to all Industry sectors such as training, standard certification or on the other hand, themes can segment information on a sector basis such as aeronautics, space, automotive, mass transport, business information, banking, medical, etc. A repository should be opening viewpoints. So, instead of encapsulating information on sector-basis, we find it more relevant to emphasize potential use of formal methods across-sectors in particular since formal methods are rarely sector-specific. The following list of general themes below comes from cross-sector concerns expressed by DEPLOY Industry partners originating from four key sectors: automotive, business, mass-transport and space:

- Training scope and resourcing
- Impact on quality of a product through its various development stages and on productivity at the various development stages/disciplines
- Exploit formal models at various development stages or in the various disciplines/development processes,
- Reuse across development projects
- Phase the learning of a formal method in an organisation or eventually limit the scope of who must understand and become an expert in a formal method
- Phase the migration to using a formal method (given the existence of products not initially developed using formal methods)
- Known strengths and weaknesses of tools associated to a formal method as well as the quality of support by tool providers
- The external factors (from competition, standard bodies, laws) pushing take-up of formal methods

2.2 Roles and Their Questions of Interest

People with different roles in an organization may be interested by different aspects of the themes identified. Concerning formal methods, we found useful to clearly identify the following roles:

- High-Level Managers – taking enterprise's strategic decisions and their financial impact
- Project and QA Managers – supervising people who actively use FM (in production or R&D), planning projects and performing safety analysis and more traditional QA activities
- Engineers and Analysts – People actively using FM
- QA Practitioners – people who must understand documents involving FM notations but don't need develop the capabilities to produce them.

It may be that in a particular organisation, a role above does not fit with the profile described. The naming scheme presented is just for mnemonic use, it should not be taken literally.

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 lone concern of a single sector or even worst a single company.
- Specific enough so it is fairly easily to understand what results from Industry pilot should be proposed to what questions from the FAQ.

Due to space consideration, only a very short sample of question can be presented in this paper. The full list is available at the URL mentioned earlier.

Theme: Exploit formal models at various development stages or in the various disciplines/development processes

Question of Interest to ***Project and QA Managers***:
Can formal method help create or refine more accurate project plans?

Question of Interest to ***Engineers and Analysts***
Is it possible to take advantage of formal models to automate additional development tasks? (for example, to generate code or tests)

Questions of Interest to ***QA Practitioners***
Is it possible to take advantages of formal models to automate some QA tasks? (for example, ease in determining requirement coverage)

It is worth observing the most questions currently identified in the FAQ may be answered from diverse viewpoints and therefore, any single question can find several answers.

2.3 Connecting Research and Industry

Academic researchers' scientific interests can vary widely from Industry's pragmatic concerns. For this reason, our theme-specific and role-based questions are a first step to explicitly remind researcher of important considerations from an Industry's viewpoint. In addition, the approach proposed suggests that Industry members should specifically express their degree of interest in each question of the FAQ. In particular, Industry partners of DEPLOY were asked to rate each question based on interest: high, medium, low, or useless. The goal is not necessarily to identify an Industry wide trend as context, roles, and understanding of a question can make degree of interest vary drastically. However, if many Industry members explicitly find a question highly interesting, researchers will have to understand that the question deserves a proper treatment even if not extremely challenging or interesting from a scientific standpoint.

Conversely, every answer to a question will emphasize the companies involved in the Industry pilots. In this way, researchers in search for Industry partner for pilots in the same sector or on the same king of questions can search for potentially interesting industrial in the evidence repository.

3. Editorial Board and Statistics on the Current Evidence Repository

To guarantee the integrity and coherence of the repository of evidence, an editorial board must be appointed from relevant Industry and Academic individuals. Currently, this board is constituted from DEPLOY members from Industry, Academia and Research Centres throughout Europe well recognized in the world of formal methods. DEPLOY is currently creating a not-for-profit organisation that could potentially take the lead in electing and overseeing the editorial board's activities.

The editorial procedure is open to publishing evidence material from any relevant projects or published work. It currently already presents information from publications of case studies external to the DEPLOY project, this information was however selected and entered by DEPLOY partners. It is nonetheless possible for external people to propose new evidence material to the editorial board using the issue tracker of the project forge.

To further increase the credit of the evidence repository, new proposed material must have been published in a refereed event and FAQ answers must cite this publication in its reference section.

Overall statistics shows that the current evidence repository has

- 9 general, cross-sector themes
- 48 questions from the viewpoints of 4 roles
- 17 questions have been answered by at least one Industry case study

4. Conclusion and Future Work

The approach for building an evidence repository based on generic themes and roles based questions seems to provide an adequate mechanism to help industry members in their search for information on formal methods. The current implementation of this approach is done through a project on a forge.

The main advantage of this implementation is its simplicity. Furthermore, many are acquainted with the various tools offered by a forge. Consequently, the editorial procedure can express how the issue tracker can be used to manage the evolution of the evidence material. The main disadvantage is related to the wiki presentation of the FAQ and evidence material. Although flexible in how information can be structured along page hierarchy, it requires creating these pages. It is especially cumbersome for managing multiple views. Furthermore, it is always problematic to re-organize the hierarchy of a wiki. Consequently, the current hierarchy partitioned first on theme and second on role would not be easy to change. An evolution to address those issues could be through specific functionalities based on the underlying content management or database layers of the wiki. This would keep the flexibility of a wiki while facilitating modifications to the organisation and the search of the evidence material.

Finally, two issues remained to be solved: First, the FAQ answers should be presented in a more homogeneous way: a template is currently being developed to specify all information to include in a FAQ answer. Second, answers must remain concise while presenting all necessary information to understand the context of an

Industry pilot. Therefore, it seems important to provide a description of the context under which related Industry pilots took place. Since one pilot may answer several questions, it may be worth on developing a mechanism to avoid duplicating information related to a pilot context, for example, a separate wiki page which describes the overall context of a pilot can be created and all related FAQ answers can point to the corresponding context description of a Industry pilot.

References

1. Austin, S., Parkin, G.: Formal methods: A survey. Technical report, National Physical Laboratory, Teddington, Middlesex, UK (Mar. 1993)
2. Craigen, D., Gerhart, S., Ralston, T.: An International Survey of Industrial Applications of Formal Methods (2 volumes). U.S. National Institute of Standards and Technology, Computer Systems Laboratory (Mar. 1993)
3. Woodcock, J., Larsen, P.G., Bicarregui, J., Fitzgerald, J.: Formal Methods: Practice and Experience. ACM Computing Surveys (2009) in press.
4. VSR: Verified Software Repository. vsr.sourceforge.net/fmsurvey.htm (2009)