Industrial Practice in Formal Methods: a Review

J. C. Bicarregui[1], J. S Fitzgerald[2], P. G. Larsen[3], and J. C. P. Woodcock[4]

[1] STFC Rutherford Appleton Laboratory (Juan.Bicarregui@stfc.ac.uk)
[2] Newcastle University (John.Fitzgerald@ncl.ac.uk)
[3] Engineering College of Aarhus (pgl@iha.uk)
[4] University of York (Jim.Woodcock@cs.york.ac.uk)

Abstract. We examine the the industrial application of formal methods using data gathered in a review of 62 projects taking place over the last 25 years. The review suggests that formal methods are being applied in a wide range of application domains, with increasingly strong tool support. Significant challenges remain in providing usable tools that can be integrated into established development processes; in education and training; in taking formal methods from first use to second use, and in gathering and evidence to support informed selection of methods and tools.

1 Introduction

The successful transfer of formal methods technology into industrial practice has been a goal of researchers and practitioners for several decades. Indeed, by the early 1990s questions were being raised about whether formal methods could ever be viable in industrial settings. Several reviews in that decade [1–4] reported significant successes but also identified challenges to formal methods adoption including a lack of good tooling and objective evidence for the commercial benefits. Opinions diverged on whether formal methods were delivering hoped-for improvements in practice. Standards, tools, and education would "make or break" industrial adoption [5] and some saw a chasm between academics who "see formal methods as inevitable" and practitioners who "see formal methods as irrelevant" [6].

Following a decade of advances in both methods and tools, it seems appropriate to undertake a new review of industrial experience, including past as well as current projects, with the aim of developing an ongoing, updated resource using a consistent review format for each project. Here we present a short summary of the review, its findings, our observations and suggested challenges. We focus on aspects relevant to developers and users of industry-strength formal methods and tools. Further detail on the review can be found at [7, 8].

2 A Review of Industrial Applications of Formal Methods

Using a structured questionnaire, data was collected on 62 industrial projects known from the literature, mailing lists, and personal experience to have em-

ployed formal techniques. Data on 56 of the projects were collected from individuals who had been involved and data on the remainder were gathered from the literature. This initial collection may be biased to those with whom we had the strongest contacts. However, the uniform way in which the data was collected does allow comparison between projects, and gives some insight into current practice. It should be stressed that the review is not a statistical survey and so does not form a basis for general inferences about formal methods applications.

The largest application domains were transport (16 projects) and the financial sector (12). Other major sectors were defence (9), telecommunications (7), and office and administration (5). Some 20% of responses indicated that the projects related to software development tools themselves, suggesting that developers are to some extent taking their own medicine. The most strongly represented application types were real-time (20), distributed (17), transaction processing (12) and high data volume (13). 30% of responses indicated that certification standards applied, notably IEC 61508, Common Criteria and UK Level E6 for IT Security Evaluation. Half of respondents estimated the size of the software: the split was roughly equal between 1–10, 10–100, and 100–1000 KLOC. Two projects are from the 1980s, 23 are from the 1990s and 37 are from 2000-2008.

Mild correlations were observed between techniques and software types, indicating higher than average use of model checking in consumer electronics and of inspection in transaction processing software. The use of model checking has increased greatly from 13% in the 1990s to 51% in the present decade. No significant change was apparent for proof, refinement, execution or test case generation.

Some 85% of responses indicated that project staff had prior formal methods experience. Of those reporting no previous expertise, half were in teams with mixed experience levels and half introducing techniques to a novice team. Over half the responses indicated that training had been given.

Respondents were asked to comment on the time, cost and quality implications. The effect on time was, on average, seen as beneficial: three times as many reported a reduction in time as reported an increase. Several projects noted increased time in the specification phase. Of those reporting on costs, five times as many projects reported reductions as reported an increase. 92% of projects reported enhanced quality compared to other techniques; none reported a decrease. Improvement was attributed to better fault detection (36%); improved design (12%), confidence in correctness (10%) and understanding (10%).

3 Observations and Challenges

Trends in Tooling In spite of the observation in 1993 that tools are "neither necessary nor sufficient" [2], it is now almost inconceivable that an industrial application would proceed without tools. Nevertheless, one respondent saw tools as a potential source of rigidity:

> "... not having a tool allowed us to modify the notation ... to appeal to the target audience. This was crucial to the success of the project.... Had we been locked into an inflexible tool, the project would have failed."

Although tool capabilities have increased, almost all previous surveys and about a quarter of the responses in our review report a lack of "ruggedised" tools. Particular challenges include: support for human interaction in automated deduction, common formats for model interchange and analysis, the lack of support for tools offered on a "best efforts" basis and the need to integrate heterogeneous tools into tool chains. Expectations from tools are also high. One respondent commented:

> "... formal methods need to provide answers in seconds or minutes rather than days. ... model-checking has to be tightly integrated into the ... tools that developers are already using."

Tools usability was poorly rated by many respondents: "Tools don't lend themselves to use by mere mortals." Such comments challenge the community to ensure that potential industry users are communicating their requirements effectively to tools providers, and that the tools providers are responding by ensuring that usability is gaining adequate attention in tools research and development.

Evidence Previous surveys have noted the lack of evidence to support adoption decisions [1] and appropriate cost models [2]. Only half the projects that we reviewed reported the cost consequences of using formal methods. Some cost data may be sensitive but nonetheless this suggests that pilot studies are not always gathering relevant evidence. In our view, the decision to adopt development technology is often risk-based and convincing evidence of the value of formal techniques in identifying defects can be at least as powerful as a quantitative cost argument. We conjecture that it would be more effective for methods and tools developers to emphasise the de-risking of the development process than to make cost arguments. Pilot applications should observe factors relevant to the needs of those making critical design decisions. This would suggest that the construction of a strong body of evidence showing the utility and ease of use of formal techniques is at least as high a priority as the gathering of more evidence on development costs.

Second Use Responses to the review questionnaire suggest that the entry cost for formal methods is perceived as high, although the cost can drop dramatically on second use [9]. It is noticeable that very few published reports of formal methods applications describe second or subsequent use, though 75% of respondents in our study indicated that they will use similar methods again. This may be a lack of reporting, or it may represent a challenge to the community to secure and report on series of applications.

Skills and Psychological Barriers Several responses identify psychological barriers to the use of formal techniques: "people like making things work; lack of early visible progress"; "many developers are 'builders' who do not want to specify everything"; "Barriers: formal methods people ... Too much emphasis

on properties and refinement rather than actually constructing something". Respondents also identified skills deficiencies as a major impediment to formal methods adoption. We do not believe that it is not possible to de-skill the verification process entirely, so the challenges remain of improving education/training and providing provide technology that is readily adopted by engineering teams, taking account of skills, psychology and even the social context.

4 Conclusions

Our review paints a picture in which a substantial range of application areas have been shown to benefit from formal modelling and verification technology. Some of the impediments identified a decade ago have been addressed, notably in the focussed use of methods supported by strong tools. Many challenges remain, particularly in ensuring tools' usability, integration into development processes, providing evidence to support second and subsequent use, and overcoming skills and other barriers to adoption. Initiatives such as the Verified Software Repository offer a basis for well-founded experiments that, it is to be hoped, will help to address these challenges in the next decade. We intend to continue with the collection of data regarding on industrial practice in formal methods[5] and intend to produce new survey reports at 5-year intervals.

Acknowledgements: We are grateful to all the contributors to our review and to the EU FP7 Integrated Project *Deploy* for support.

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. Clarke, E.M., Wing, J.M.: Formal methods: State of the art and future directions. ACM Computing Surveys **28**(4) (1996) 626–643
4. Bloomfield, R., Craigen, D.: Formal methods diffusion: Past lessons and future prospects. Technical Report D/167/6101, Adelard, London, UK (Dec. 1999)
5. Hinchey, M.G., Bowen, J.P.: To formalize or not to formalize? IEEE Computer **29**(4) (Apr. 1996) 18–19
6. Glass, R.L.: Formal methods are a surrogate for a more serious software concern. IEEE Computer **29**(4) (Apr. 1996) 19
7. VSR: Verified Software Repository. vsr.sourceforge.net/fmsurvey.htm (2009)
8. Woodcock, J., Larsen, P.G., Bicarregui, J., Fitzgerald, J.: Formal Methods: Practice and Experience. ACM Computing Surveys (2009) in press.
9. Miller, S.P.: The industrial use of formal methods: Was Darwin right? In: 2nd IEEE Workshop on Industrial Strength Formal Specification Techniques, Boca Raton, FL, IEEE Computer Society (1998) 74–82

[5] Potential contributors are invited to contact the authors.