Study on the Barriers to the Industrial Adoption of Formal Methods*

Jennifer A. Davis[1], Matthew Clark[2], Darren Cofer[1], Aaron Fifarek[3], Jacob Hinchman[2], Jonathan Hoffman[2], Brian Hulbert[3], Steven P. Miller[1], Lucas Wagner[1]

[1]Rockwell Collins, Cedar Rapids, IA 52402, USA
{jadavis4,ddcofer,spmiller,lgwagner}@rockwellcollins.com
[2]Air Force Research Laboratory, WPAFB, OH 45433, USA
{Matthew.Clark3,Jacob.Hinchman,Jonathan.Hoffman}@wpafb.af.mil
[3] LinQuest Corporation, an AFRL subcontractor, Beavercreek, OH 45431, USA
{Aaron.Fifarek.ctr,Brian.Hulbert.ctr}@wpafb.af.mil

Abstract. The authors conducted an informal survey of contractors, customers, and certification authorities in the United States aerospace domain to identify barriers to the adoption of formal methods and suggested mitigations for those barriers. We surveyed 31 individuals from the following nine organizations: United States Army, Boeing, FAA, Galois, Honeywell, Lockheed Martin, NASA, Rockwell Collins, and Wind River. The top three barrier categories were education, tools, and the industrial environment (i.e., non-technical barriers with respect to personnel changes, contracts, and schedules). The top three mitigation categories were education, improving tool integration, and creating and disseminating evidence of the benefits of formal analysis. Strategies to accelerate adoption of formal methods include making formal methods a part of the undergraduate software engineering curriculum, hosting courses in formal methods for working engineers, funding the integration of tools, funding improvements to tool interfaces, and promoting/requiring the use of formal methods on future contracts.

Keywords: formal methods, survey, barriers, education, certification, industrial, tools, benefits

1 Introduction

Aerospace systems, such as Unmanned Aerial Vehicles (UAVs), are becoming increasingly complex and non-deterministic by design. Advances in software autonomy are helping drive the development of future systems that will require greater levels of on-board, autonomous decision making as well as cooperative behaviors to achieve greater performance in their operational environment. With the complexity of these autonomous systems rising at an exponential rate, system integrators are beginning to

* Distribution Statement A. Approved for public release; distribution is unlimited. Case 88ABW-2012-6299.

reach the limit of their ability to exhaustively test the system. To make matters worse, many non-deterministic algorithms like adaptive control and neural networks will be impossible to fully test with traditional methods due to the enormous number of configurations the system may adopt. Whether or not these future system capabilities can be fielded safely and securely is dependent on the ability of developers to verify and validate the performance of highly complex systems. To do so requires a paradigm shift in the way system test and certification are conducted. Part of this shift, and a promising approach to mitigating this explosion in Verification and Validation (V&V) costs, is the use of advanced analysis techniques such as Formal Methods (FM). For the purposes of this paper, we include in the definition of formal methods all forms of formal analysis including static code analysis, abstract interpretation, model-checking, and theorem proving.

Formal methods have had V&V successes previously in communities such as computer hardware and software security [1] [2]. However, these techniques have made few inroads into the safety-critical software arena. The purpose of this study is to investigate why formal methods have been slow to be adopted in the aerospace domain. By identifying the largest barriers to the adoption of formal methods in the development of aerospace systems, as reported by respected domain leaders, it is easier to see which strategies would yield the greatest return on investment and maximize the adoption of these analysis techniques.

Several formal methods surveys have been conducted in the past. See, for example, [3], [4], and [5], which were published in the 1990s. Much has changed since then, especially with respect to tool performance. A fairly recent (2008) survey by Woodcock et al. [6] includes 62 applications of formal methods over 25 years in a wide range of application domains. The results were published in 2009 in both overview [7] and full report [8] forms. This and previous studies found the barriers to industrial adoption to be tool usability, lack of "ruggedized" tools, integration into the development processes, lack of evidence to support adoption decisions and appropriate cost models, perceived high entry cost of doing formal methods, lack of evidence of reduced cost for the second use of formal methods, psychological barriers, and skills barriers. Finally, The Formal Methods Manifesto 2010 [9] reports that there are still barriers (namely, the need for automation and scalability) preventing widespread use of formal methods in developing new software, despite 30 years of progress in methods and tools.

The contributions of this paper are:

1. Make current the knowledge about barriers to widespread adoption.
2. Identify barriers specific to the US aerospace domain.
3. Provide the perspective of individuals who are familiar with formal methods but have not used them.

2 Interview Process and Questions

Organizations and individuals were selected for the survey based on prior known interest or experience with the use of formal methods in the United States aerospace industry. An effort was made to identify individuals from a variety of roles in their organizations with diverse perspectives on formal methods. We sent email requests for participation to 37 individuals representing ten organizations. Of these requests, 31 individuals agreed to participate. These individuals are employed by the following nine organizations: United States Army (3 individuals), Boeing (2), FAA (1), Galois (2), Honeywell (4), Lockheed Martin (2), NASA (5), Rockwell Collins (11), and Wind River (1). Our respondents included 14 experts, 5 users, 9 individuals familiar with formal methods but not using them, and 3 managers of users.

Listed below are the first four questions that were asked of the interviewees. These questions were intended to be open-ended and avoid biasing the respondent toward any particular kind of barrier or mitigation. After question #4, we asked respondents to rate the barriers found in the 2008 formal methods survey by Bicarregui et al. [7]

1. Please describe (at as high a level as you like) the use of formal methods within your organization, if any.
2. Has the use of formal methods in your organization increased, decreased, or stayed the same in the last 5 years?
3. What do you see as the current barriers to further adoption of formal methods (especially in your organization)?
4. Do you have any suggestions for removing these barriers?

All interviews were conducted in person or by phone. Survey responses are anonymous in this paper. Furthermore, any conclusions drawn should not be attributed to any particular individual or organization.

3 Results

The following sections summarize the results of the survey, including the change in the amount of use of formal methods, the barriers to the adoption of formal methods, and the suggested mitigations to alleviate those barriers.

3.1 Use of Formal Methods

The Use of Formal Methods is Increasing. Eighteen out of 31 interviewees reported that the use of formal methods has increased within their organizations in the last 5 years. Five of these 18 individuals specified that the use of FM has increased slightly and one said that its use has increased dramatically. Another 8 respondents said the amount of use of formal methods has stayed the same (i.e., no noticeable change in the amount of use). Three of these 8 respondents said that their teams are using formal methods very little or not at all, so "stayed the same" means a continued lack of use. Two respondents reported that formal methods use has decreased. The remaining

three did not respond or did not know the answer. These results are depicted in Fig. 1. Note that 84% of survey respondents said the use of formal methods has increased or stayed the same. If we look at the relative majority of responses for each organization, six organizations have seen a growth in the use of formal methods, and the use of formal methods has stayed the same in the remaining three organizations.

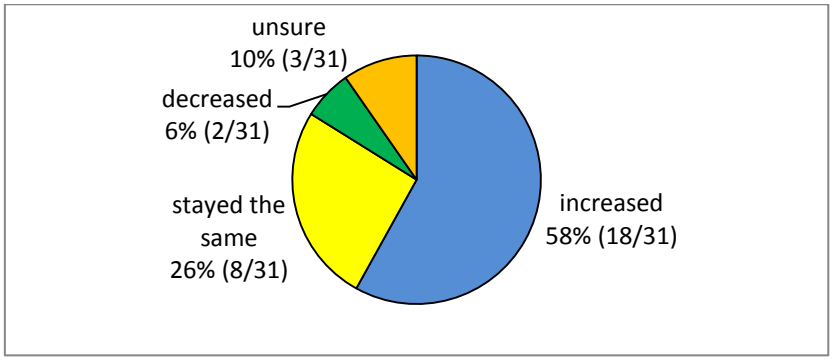

Fig. 1. Change in the Use of Formal Methods in the Last 5 Years

3.2 Barriers

Survey participants listed 120 items in response to the question "*What do you see as the current barriers to the industrial adoption of formal methods (especially in your organization)?*" The authors grouped these 120 responses into like statements (the barriers listed in this section) and then identified broad categories encompassing all of the barriers listed. These categories are: education, tools, industrial environment, engineering, certification, misconceptions, scalability, evidence of benefits, and cost. The Industrial Environment Category includes non-technical barriers with respect to personnel changes, contracts, and project schedules. The Engineering Category includes technical barriers to the use of formal methods that result from the manner in which projects are executed and how industrial problems are solved. Fig. 2 shows the number of responses for each category. Most interviewees listed more than one barrier, and many listed more than one barrier for some categories.

Next we will look at the specific barriers mentioned within each category. The barriers listed in the subsections that follow are the authors' restatements/groupings of the survey responses to the barriers question. While individuals may have multiple responses for a given category, care was taken so that each individual is counted at most once for a given barrier restatement.

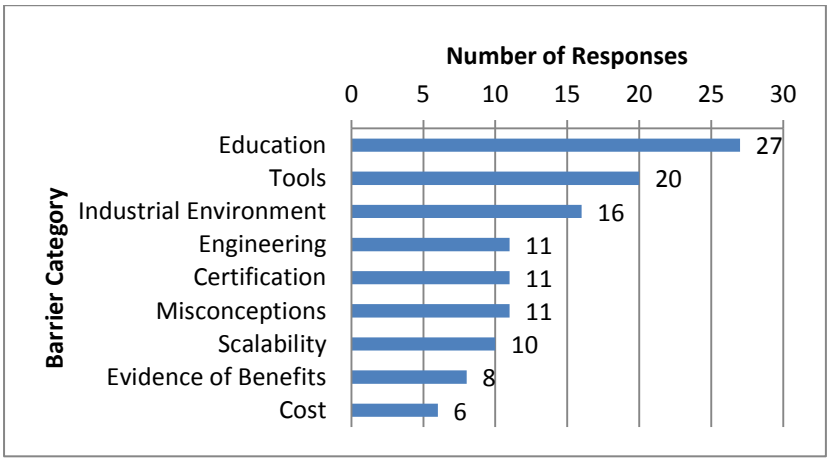

Fig. 2. Number of Responses for each Barrier Category

Education Barriers. Education barriers include all barriers regarding education of the individuals involved in the design, development, management, or certification of products. A major theme is the need to train the current workforce. Specific issues mentioned are that users do not know how to properly apply formal methods or how to properly interpret the results. Respondents also expressed the need for formal methods experts. At least three of the organizations we spoke with have an expert group of formal methods practitioners that are responsible for developing and maintaining the formal analysis tools used within the organization. The education barriers are listed next with the number of respondents indicating each barrier in parentheses.

- General education on formal methods techniques and tools is needed, especially for the working engineer. (7)
- Highly trained formal methods experts are needed. (6)
- Users do not know how to properly apply formal analysis. (6)
- Certification authorities need to be educated on how to evaluate FM artifacts. (3)
- Certification authorities are not familiar with FM techniques or their benefits. (2)
- Formal methods advocates do not have sufficient appreciation for the practical issues that the product engineers face. (1)
- Lack of awareness of resources. (1)
- Users do not know how to properly interpret the results of formal analysis. (1)

Tools Barriers. Tools barriers include all barriers with respect to tools including, but not limited to, usability, capabilities, and integration. The majority of responses in this category are on the need for improved usability and integration of tools, rather than improved capabilities.

- Tools are not user-friendly. (5)
- Tools are distributed and not integrated. (4)

- Formal methods tools are not compatible with development tools. (3)
- Tools are not sufficiently automated. (3)
- Lack of support for real-time embedded systems. (2)
- Uncertainty if or how long it will take for formal analysis to complete. (2)
- Inconsistencies between the mathematics behind the model and the mathematics of the real world. (1)

Industrial Environment Barriers. Industrial environment barriers include non-technical barriers with respect to personnel changes, contracts, and schedules. While there is not one major theme in this category, we note that both the third barrier about export restrictions and the sixth barrier about people changing positions frequently would be alleviated somewhat by educating more of the workforce on formal methods.

- Some projects operate on too short of a timeline for formal analysis. (3)
- Contractually requiring the use of formal methods can be difficult. (2)
- US export control laws on technical data make it difficult to hire foreign nationals and/or collaborate internationally. (2)
- Psychological: some engineers do not like to formalize things. (2)
- The benefits of formal analysis are not reaped by those who do the analysis but rather by those downstream in the development process. (2)
- Transitory nature of people (people change positions frequently). (2)
- Proprietary methods and tools that cannot be shared. (1)
- Uncertainty regarding how FM will affect system modification/maintenance. (1)
- Uncertainty with respect to how to adapt formal methods to legacy systems. (1)

Engineering Barriers. Engineering barriers are technical barriers to the use of formal methods that result from the manner in which projects are executed and how industrial problems are solved. The most common problem cited in this category is that requirements are informal, changing, and sometimes wrong. On the one hand, formal methods can help formalize and catch inconsistencies with requirements. On the other hand, it may not be cost effective to formalize the requirements until the informal requirements have stabilized.

- Uncertain requirements (i.e., requirements that are informal, incomplete, changing, or simply wrong). (4)
- Formal analysis is not integrated into the existing development process. (2)
- Validating a model in a new domain is difficult. (2)
- Designs are not organized with formal methods in mind. (1)
- FM often require a high level of expertise with the system being analyzed. (1)
- Sometimes unclear how to show that assumptions of analysis are being met. (1)

Certification Barriers. Certification barriers include barriers specific to airworthiness or airborne systems certification authorities. The most common barrier men-

tioned in this category is the need for certification credit for formal methods. This will be an option under DO-178C [10]. Two other issues mentioned include a reluctance to change on the part of the certification authorities and the uncertainty of how to qualify formal methods tools. One respondent listed "It is unknown whether certification based on formal analysis will stand up in court" as a barrier. We note that it is also unknown whether certification *without* formal methods will stand up in court. Michael Holloway's fictional court case presents a tongue-in-cheek examination of the possibilities [11].

- No certification credit for formal methods. (4)
- Certification authorities are reluctant to change. (3)
- Tool qualification of formal methods tools is uncertain. (2)
- International certification authorities must agree on certification credit for FM. (1)
- Unknown whether certification based on formal analysis will stand up in court. (1)

Misconception Barriers. Misconception barriers include barriers that result from poor publicity, misunderstandings about formal analysis, and questions about the trustworthiness of formal analysis tools. The first two barriers in this category show a need for evidence of successful applications of formal methods and dissemination of that information. Recall that six respondents said there is a need for formal methods experts (listed under the Education Category), and here two respondents said there is a false perception that a formal methods expert is needed to do the work. The primary difference is that the barrier listed here refers to the *user* of formal methods tools rather than the developers and maintainers of such tools.

- There is skepticism about formal methods, sometimes due to past failures. (3)
- Too much emphasis on the theory rather than the application. (3)
- Concern that a given FM tool might have a bug in it, in which case we would be placing our trust in something unreliable. (2)
- False perception that FM expert is needed to do the work. (2)
- Misconception that formal methods will replace all testing. (1)

Scalability Barriers. Scalability barriers are barriers regarding the limits on size and/or types of problems that formal analysis techniques and tools can handle. About half of those that said we need a means to scale the approach referred to the need for composability so that one can work at the system level, employing different kinds of analysis and testing (*not* all formal) to handle the different parts of the system.

- Need a means to scale the approach. (7)
- Formal methods research challenges remain. (3)

Evidence-of-Benefits Barriers. Evidence-of-benefits barriers relate to a lack of evidence (or perhaps lack of awareness of the evidence) for the benefits of formal methods. Benefits can be with respect to the business case (especially savings in schedule

or cost) or the improved quality of systems (i.e., fewer defects) when formal analysis is used. The number one barrier in this category is that decision makers do not see the advantage of formal analysis over testing.

- Decision makers do not see the advantage over testing. (7)
- Lack of evidence to support adoption decisions. (1)

Cost Barriers. Cost barriers include barriers with respect to the cost of doing formal analysis. Several projects report a savings in cost when using formal methods [8]. However, some types of analysis (e.g., theorem proving) are more expensive than others (e.g., static code analysis).

- Formal analysis can be expensive in actual cost or measured financial risk. (5)
- It is time-consuming to write robust properties. (1)

Non-Barriers. In addition to the responses we collected on barriers to the adoption of formal methods, some individuals wanted to highlight items they did **not** see as barriers. These responses are listed below.

1. More than one person said that evidence on savings during the second and subsequent use of formal methods is not that important. The reason is that program managers are thinking about their current program and how decisions will impact cost and schedule for that program.
2. A former formal methods group manager emphasized that the mathematical sophistication of product engineers is **not** a barrier. This manager pointed out that the complexity of building safety-critical systems exceeds the complexity of using formal methods.
3. A department head said that skills/training is **not** a barrier. He said that if there is a good business case for using formal methods, then his department would hire and/or train people as needed. He is not concerned with the skill set required.

3.3 Mitigations

We received 76 responses to the question "*Do you have any suggestions for removing [the barriers you mentioned]*?" The authors grouped these responses into like statements and then identified broad categories encompassing all of the mitigations listed. These categories are: education, tool integration, evidence of benefits, tool capabilities, tool usability, requiring formal methods, and certification concerns. Fig. 3 shows the number of responses for each category. Note that most interviewees listed more than one mitigation, and many listed more than one mitigation for some categories.

Next we will look at the specific mitigations mentioned within each category. The mitigations listed in the subsections that follow are the authors' restatements/groupings of the survey responses to the mitigations question. While individuals may have multiple responses for a given category, care was taken so that each individual is counted at most once for a given mitigation restatement.

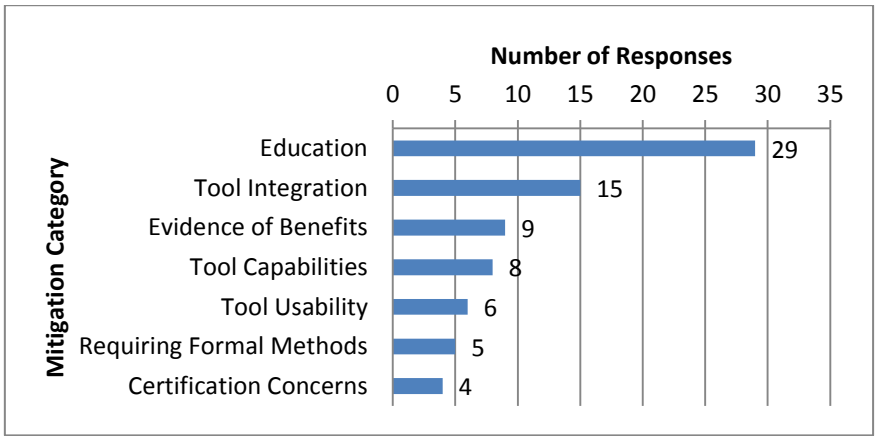

Fig. 3. Number of Responses for each Mitigation Category

Educational Mitigations. Educational mitigations are recommendations on how to improve education on formal methods. Two themes in this list of mitigations are that we need to include formal methods in undergraduate education and that we need training courses available for working engineers who will be using formal methods tools. The educational mitigations are listed next with the number of respondents indicating each mitigation in parentheses.

- Include formal methods in undergraduate education. (4)
- Caution that FM cannot solve everything; there is still a need for testing. (2)
- Get word out about the tools, expertise, and training available. (2)
- Attack the perception that a formal methods expert is needed to do the analysis. (1)
- Document how to demonstrate the analysis and how the assumptions are met. (1)
- Do not use the term "formal methods" in training classes for working engineers. Instead, show the engineers what the tools can do. (1)
- Education—need to convince people that doing this is a better way because it will help them downstream. (1)
- FAA-specific training on formal methods: one course at the familiarity level to provide top-level education on formal methods and another course at the expertise level to provide people the skill set necessary to evaluate a vendor proposing formal methods on a project. (1)
- Find more people interested in doing theorem-proving work. (1)
- Formal methods training at multiple levels: new users, users with some formal methods experience, and formal methods experts. (1)
- General education on FM for working engineers (e.g., via a university course). (1)
- Guidance on which pieces need formal analysis, which need semi-formal analysis, which do not need formal or semi-formal analysis, etc. (1)
- Include formal methods in an organization's systems engineering curriculum. Also, include training on using formal methods to gain certification credit under DO-333 in DO-178C training. (1)

- Need to get young people (starting in high school) interested in the notion of engineering safe systems. Make it attractive from an educational perspective. Make "engineering safe/secure systems" an engineering specialty one can choose in college. FM would come with the package and be part of the core curriculum. (1)
- Perhaps a professional society such as AIAA or IEEE could provide professional training in the use and application of one or more formal analysis techniques. (1)
- Required training for senior managers and developers of mission-critical SW. (1)
- Talk about the problems formal methods can and has solved in engineering newsletters (not just a sales pitch). (1)
- There is no way to remove the expertise barrier other than through education and getting people to use the tools (rewards in finding bugs). (1)
- Usability workshop. FM succeeding in Integrated Circuit community. (1)
- User education about when and where to apply formal methods. (1)
- We have to persuade people to use a different approach, especially those that have been working in their field for decades. Technical arguments are not sufficient to convince them. We need to show teams what the tools can do. (1)
- We need a way to explain FM that a jury can wrap their minds around. (1)
- We need FM related to domains and the interfaces that people are used to. (1)
- Work with teams on tool reviews to encourage the use of formal methods. (1)

Tool-Integration Mitigations. The mitigations listed in this section are recommendations for how to better integrate formal analysis tools, either with each other or with other development tools. A common theme among the mitigations listed is that we need formal methods tools to be integrated with existing tools. This includes system-level design tools, model-based design tools, and compilers.

- Automated process or guidance to constrain the way systems and software engineers do things, to enable the use of formal methods. (2)
- Coding standard with compliance checkers. (2)
- Bridge the gap to the dominant notation (UML, AADL, etc.). (1)
- Build static analysis into the development tool. (1)
- Develop open-source formal verification tools. (1)
- Emphasis on translation between tools. Then one can choose the right tool with the right strengths for the job. (1)
- Get FM early in chain, at the requirements level. (1)
- Integrate tools (e.g., compilers and formal methods tools). (1)
- Model checking the language people like to use in an automated fashion. (1)
- Model-Based Design (MBD) and simulation to address "getting the requirements right." (1)
- Need formal methods tools in sync with our development tools. (1)
- Strategy for what to do when FM tools fail. Combine analysis and testing into a global solution. (1)
- The opportunity for the most impact is for modeling tool vendors to embed FM. (1)

Evidence-of-Benefits Mitigations. Evidence-of-benefits mitigations include recommendations for the type of evidence that needs to be created and with whom it should be shared. Respondents cited a need for evidence of cost savings, time savings, and defects found on industrial-sized problems. The authors note that several published examples of formal methods applications and benefits do exist [8] [12].

- Insist that formal methods tools be applied to industrial-sized examples and disseminate those examples, including the cost and benefits data. (2)
- Demonstrating the value of FM and expanding the area where it can provide value. Show that higher quality SW can be produced in a more automated fashion. (1)
- Good, meaty, fully and publicly worked and documented formal methods examples beyond toy problems. (1)
- Highlight products that were fielded with defects that could have been caught with formal methods. (1)
- Need a direct measure / direct evidence of success when FM are used. (1)
- Need to convince program managers in DoD of savings of cost and time and that the quality is improved. (1)
- Solve practical problems with FM. (1)
- Use FM to debug and get systems to market faster rather than to get a proof. (1)

Tool-Capabilities Mitigations. The mitigations listed in this section are recommendations for what tool capabilities are needed. Responses vary from increased automation, composability to analyze system architectures, better support for continuous systems, and the ability to predict how much time it will take to do the analysis.

- Better tool support for continuous systems (e.g., more data types). (1)
- Continue to invest in research in these areas (FM tools and techniques). (1)
- Develop tools for composability to model and analyze system architectures. (1)
- We must provide sound abstractions automatically for data types we cannot handle (floating-point, etc.). There are function-based approximations (approximating the function) and data-based approximations (approximating the data types). (1)
- More automation, including automated test vector generation. (1)
- More robust tool (so analysis completes and/or makes it easier to make modifications to help analysis complete). (1)
- Predict how much time it will take to do the analysis. (1)
- Research on technical barriers such as floating point numbers and nonlinear mathematics. (1)

Tool-Usability Mitigations. The mitigations listed in this section are recommendations for how to improve the user-friendliness of formal methods tools.

- Better tool support for properties with respect to time. (1)
- Develop better tools to help people write their requirements more formally. Use a template-based approach with a built-in dictionary so that the requirements can be turned into logical-based expressions. (1)

- FM community needs to simplify tools and abstraction tools. FM theory (i.e., what the tools are doing) is very abstract. (1)
- Make theorem proving simpler or more amenable to complex systems. (1)
- Make tools easier to use. This is a difficult problem that will not be solved for a good while. (1)
- System-level tools and frameworks to help guide engineers on what needs to be done where. (1)

Requiring-Formal-Methods Mitigations. The mitigation mentioned here is simple: require the use of formal methods on new contracts. This implies a customer-driven decision to use formal analysis.

- Require the use of formal methods on new contracts. (4)
- Require and incentivize the use of FM. (1)

Certification-Concern Mitigations. The mitigations suggested here are giving credit toward certification for formal methods, and working an example to demonstrate how to certify a system with formal analysis.

- Certification authorities giving credit toward certification for the use of formal methods, or even requiring its use. (3)
- Need a small example (at the LRU level) to go through airworthiness certification to demonstrate how to certify a system with formal analysis. (1)

4 Discussion

4.1 Cross-correlations

In this section we investigate results for particular subgroups. One of the most interesting subgroups consists of what we will here call novices, i.e., those who are familiar with formal methods but have not yet used them. Our survey included 9 novices, which is 29% of the surveyed population. They provided 42 responses to the barrier question. Novices tended to be more concerned about misconceptions and less about tools compared to the rest of the survey respondents. They accounted for 7 of the 11 misconception barrier responses. Novices were also concerned about education (10 responses) and the industrial environment (7 responses). The top three specific barriers listed by novices were:

- General education on formal methods techniques and tools is needed, especially for the working engineer.
- Need a means to scale the approach.
- Formal analysis can be expensive, either in actual cost or measured financial risk.

Our survey included 14 individuals who are considered formal methods experts. Experts almost unanimously (13 out of 14) reported a growth in the use of formal methods. Much of this growth is the result of increased internal and external funding of formal methods research and development. The percentages of barriers listed in each category by experts were about the same as the percentages for the entire group. In other words, no particular kind of barrier stood out more for this subgroup.

Another subgroup of interest consists of the 18 individuals who reported seeing an increase in the amount of use of formal methods. The percentages of listed barriers in each category for these individuals were about the same as the percentages for the entire group.

Five individuals reported "Tools are not user-friendly" as a barrier. Three of these individuals listed no other barriers, from which we can deduce that they consider this to be the most important barrier to widespread adoption of formal methods. Mitigations suggested by these five individuals included the following:

- Work with teams on tool reviews to encourage the use of formal methods.
- Coding standard with compliance checkers.
- Model checking the language people like to use in an automated fashion.
- Make tools easier to use. This is a difficult problem.

4.2 Comparison with Prior Work and New Insights

Our survey confirmed that several previously known barriers are still issues: tools are not user-friendly, the need for automation and scalability of tools, a lack of evidence to support adoption decisions, and skills deficiencies. Our respondents did not, however, consider the lack of evidence on the reduced cost for second and subsequent use of formal methods to be a significant barrier. The need for education on formal methods was the most frequently cited barrier by our participants, and this was not emphasized in prior surveys. Our survey also found non-technical barriers regarding project timelines and personnel changes to be significant. Finally, we identified several barriers unique to the US aerospace domain, such as:

- No certification credit for formal methods. (4)
- Certification authorities are reluctant to change. (3)
- Certification authorities need to be educated on how to evaluate FM artifacts. (3)
- Certification authorities are not familiar with FM techniques or their benefits. (2)
- Tool qualification of formal methods tools is uncertain. (2)
- International certification authorities must agree on certification credit for FM. (1)
- Unknown whether certification based on formal analysis will stand up in court. (1)
- US export control laws on technical data make it difficult to hire foreign nationals and/or collaborate internationally. (2)

At the outset of our survey, we expected to see similar awareness of formal methods to what has been observed in the past. We expected to see modest use of formal methods by a few researchers in companies and government labs on most systems, and an increased use of formal methods on security applications. We were surprised

to see increased awareness and use of formal methods in companies and government labs overall (even though it is far from mainstream). Regarding barriers, we expected commonality between the barriers in our domain and those of industry at large. We were surprised by the importance of buy-in from an organization's management chain. This drives the need for management to be somewhat knowledgeable of formal methods so that they will help push the adoption and use of this technology.

5 Summary

Education. Based on the large number (27) of barrier responses in the Education Category, it is clear that the need for education is a significant barrier to further adoption of formal methods. A major theme among survey responses is the need to train the current workforce. Also, decision makers need to know what formal analysis is and its benefits. Three levels of education need to be addressed: general awareness, users, and experts. Suggested strategies for addressing Education Barriers are

1. Make formal methods a part of the standard software engineering curriculum, possibly within a course on "designing safety- and security-critical systems."
2. Develop and host courses on formal methods, designed for the working engineer at the user (i.e., non-expert) level.

Tools. Formal methods tools have come a long way in the last 5-10 years in terms of their performance and the complexity they can handle. Most research dollars continue to be invested in improving the scalability and the types of problems the tools can handle. However, significant issues remain that are not being funded: outdated user interfaces, lack of integration between formal methods tools, and lack of integration with other tools in the development process (e.g., compilers and tools for requirements capture). Improving tool integration and user interfaces is not that difficult from a research point of view, but it is time-consuming and requires both formal methods and engineering expertise. Suggested strategies to impact Tool Barriers are:

1. Fund improvements to FM tool interfaces.
2. Fund the integration of FM tools with each and other development tools.

Customer/Executive Support. Many barriers remain with respect to the industrial environment, the way projects are currently executed, certification concerns, and the cost of formal methods. Most of these barriers can be overcome by a top-level decision to use formal methods. Strategies for encouraging the use of formal methods on future contracts include:

1. Customer requirements. If customers and/or certification authorities require the use of formal methods on programs, then formal methods will be used.
2. Credit toward certification. If conducting formal analysis yields credit toward certification and saves some measurable (i.e., in both schedule and cost) effort down

the road, then contractor program managers are equipped to make that trade decision. Certification credit for formal analysis will be an option under DO-178C [10].

3. Creating and disseminating evidence of benefits. For years, formal methods advocates have shared the benefits of formal analysis to the quality of a system or product. There are even several published examples of its application to industrial-strength problems [8] [12]. However, it is very difficult to convince contractor program managers to use formal methods based on this evidence alone.

In summary, strategies to accelerate adoption of formal methods include making formal methods a part of the undergraduate software engineering curriculum, hosting courses in formal methods for working engineers, funding the integration of tools, funding improvements to tool interfaces, and promoting or requiring the use of formal methods on future contracts.

References

1. D. S. Hardin, Design and Verification of Microprocessor Systems for High- Assurance Applications, Springer, 2010.
2. J. Harrison, "Floating-Point Verification using Theorem Proving," in *Formal Methods for Hardware Verification, 6th International School on Formal Methods for the Design of Computer, Communication, and Software Systems, SFM 2006*, Bertinoro, Italy, 2006.
3. S. Austin and G. Parkin, "Formal Methods: A survey," National Physical Laboratory, Teddington, Middlesex, UK, 1993.
4. D. Craigen, S. Gerhart and T. Ralston, An International Survey of Industrial Applications of Formal Methods (2 volumes), U.S. National Institute of Standards and Technology, Computer Systems Laboratory, 1993.
5. E. M. Clarke and J. M. Wing, "Formal Methods: State of the Art and Future Directions," *ACM Computing Surveys*, vol. 28, pp. 626-643, 1996.
6. J. Woodcock, P. G. Larsen, J. Bicarregui and J. Fitzgerald, "The Industrial Application of Formal Methods: an International Survey," [Online]. Available: http://fmsurvey.org/. [Accessed June 2012].
7. J. C. Bicarregui, P. G. Fitzgerald, P. G. Larsen and J. C. P. Woodcock, "Industrial Practice in Formal Methods: A Review," in FM 2009: Formal Methods, Eindhoven, The Netherlands, Springer, 2009, pp. 810-813.
8. J. Woodcock, P. G. Larsen, J. Bicarregui and J. Fitzgerald, "Formal Methods: Practice and experience," ACM Computing Surveys, vol. 41, no. 4, pp. 1-40, October 2009.
9. J. Krieker, A. Tarlecki, M. Y. Vardi and R. Wilhelm, "Modeling, Analysis, and Verification - The Formal Methods Manifesto 2010," in *Dagstuhl Manifestos 1*, Schloss Dagstuhl, Germany, 2011.
10. D. Cofer, "Model Checking: Cleared for Take Off," in SPIN 2010, Berlin Heidelberg, 2010.
11. C. M. Holloway, "Issues in Software Safety: Polly Ann Smith Co. v. Ned I. Ludd," in Proceedings of the 20th International System Safety Conference, 5-9 August 2002, Denver, Colorado, 2002.
12. S. P. Miller, "Lessons from Twenty Years of Industrial Formal Methods," in Proceedings of HCSS (http://cps-vo.org/node/3434), 2012.