Survey on the Barriers to the Industrial Adoption of Formal Methods

SURVEY DESCRIPTION

Our survey contacted contractors, customers, and certification authorities in the United States aerospace domain to identify barriers to the adoption of formal methods and to capture suggested mitigations for those barriers.

- Surveyed 31 individuals at 9 organizations.
  - Galois, Honeywell, Rockwell Collins, Wind River
  - US Army, FAA, NASA
  - Boeing, Lockheed Martin
- Organizations and individuals were selected based on prior known interest or experience with the use of formal methods in the US aerospace industry.
- Individuals surveyed included some who are aware of formal methods but have not used them.

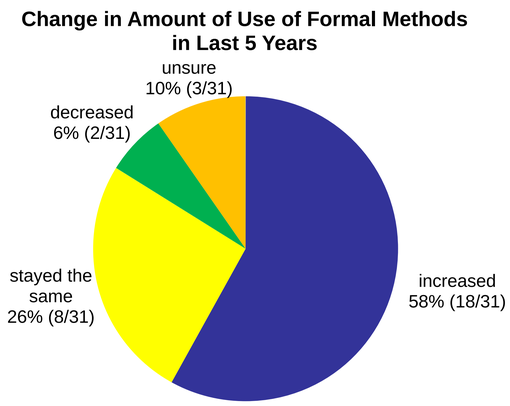
INTERVIEW PROCESS

- All interviews were conducted in person or over the phone.
- Survey responses are anonymous in published results.
- Interview questions included the following:
  1. Has the use of formal methods in your organization increased, decreased, or stayed the same in the last 5 years?
  2. What do you see as the current barriers to further adoption of formal methods (especially in your organization)?
  3. Do you have any suggestions for removing these barriers?

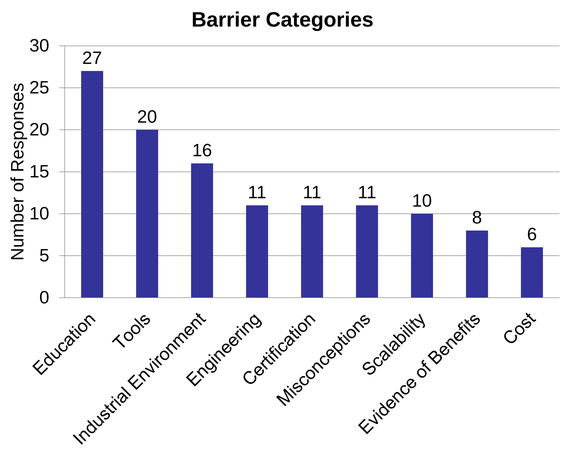
FORMAL METHODS GROWTH

- 84% of survey respondents said the use of formal methods has increased or stayed the same in their organization.
- Six organizations have seen a growth in use.*
- Three organizations have not seen a change in the amount of use.*

*Based on a relative majority of responses for each organization



BARRIERS



Commonly Listed Barriers (Number of Responses)

Education
- Need general education on formal methods. (7)
- Need formal methods experts. (6)
- Need training on the application of formal analysis. (6)
- Need training on evaluating formal methods artifacts for certification. (3)

Tools
- Not user-friendly. (5)
- Not integrated with each other. (4)
- Not compatible with development tools. (3)
- Not sufficiently automated. (3)

Industrial Environment
- Formal analysis too time consuming. (3)

Engineering
- Uncertain requirements. (4)

Certification
- No certification credit. (4)
- Certification authorities are reluctant to change. (3)

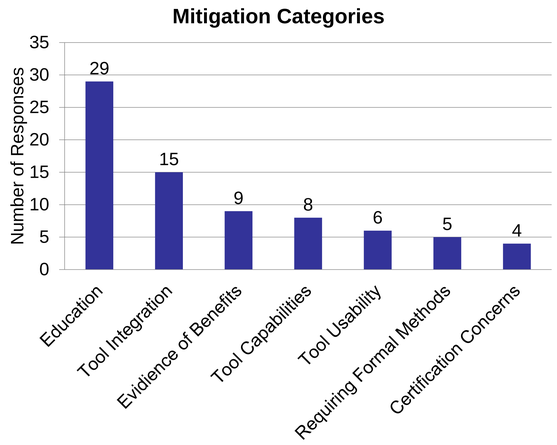
Misconceptions
- There is skepticism about formal methods. (3)
- Too much emphasis on the theory rather than the application. (3)

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

Evidence of Benefits
- Decision makers do not see the advantage over testing. (7)

Cost
- Formal analysis too expensive or too risky. (5)

MITIGATIONS



Selected Mitigations (Number of Responses)

Education
- Include formal methods in undergraduate education. (4)
- Offer general education on formal methods for working engineers. (1)
- Make "engineering safe/secure systems" an available engineering specialty in college. (1)

Tool Integration
- Develop translations between tools. (1)
- Embed formal methods in modeling tools. (1)

Evidence of Benefits
- Apply formal methods to industrial-sized examples and disseminate those examples, including the cost and benefits data. (2)
- Highlight products that were fielded with defects that could have been caught with formal methods. (1)

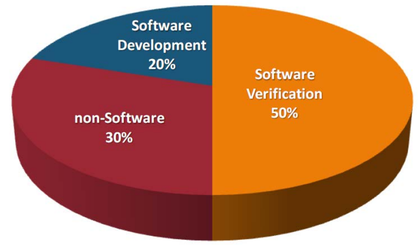
Tool Capabilities
- Develop tools for composability to model and analyze system architectures. (1)
- Provide automatic abstractions for data types we cannot handle. (1)

Tool Usability
- Develop tools for writing requirements more formally. (1)
- Develop system-level tools and frameworks to help guide engineers on what needs to be done where. (1)

Requiring Formal Methods
- Require the use of formal methods on new contracts. (4)

Certification Concerns
- Give credit toward certification for the use of formal methods, or even require its use. (3)

Typical Recent Commercial Aircraft Cost Distribution



Verification will become an even larger challenge as systems become more highly integrated

SUMMARIES

EDUCATION

- A major theme among survey responses is the need to train the current workforce.
- 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:
  - Make formal methods part of the undergraduate software engineering curriculum (e.g., as part of a course on "Designing safety- and security-critical systems").
  - Host courses in formal methods for working engineers.

TOOLS

- Last 5-10 years have seen a great improvement in both performance and the complexity that can be handled.
- Most research dollars continue to be invested in improving the scalability and the types of problems the tools can handle.
- Significant issues remain that are not being funded:
  - outdated user interfaces
  - lack of integration between formal methods tools
  - lack of integration with other tools in the development process
- Suggested strategies for addressing Tools Barriers:
  - Fund the integration of tools.
  - Fund improvements to tool interfaces.

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.
- Encourage the use of formal methods on future contracts via
  - Customer requirements
  - Credit toward certification (DO-178C)
  - Creating and disseminating evidence of benefits

Rockwell Collins