Study on the Barriers to the Industrial Adoption of Formal Methods

September 2013
Jennifer Davis, Ph.D.
Rockwell Collins

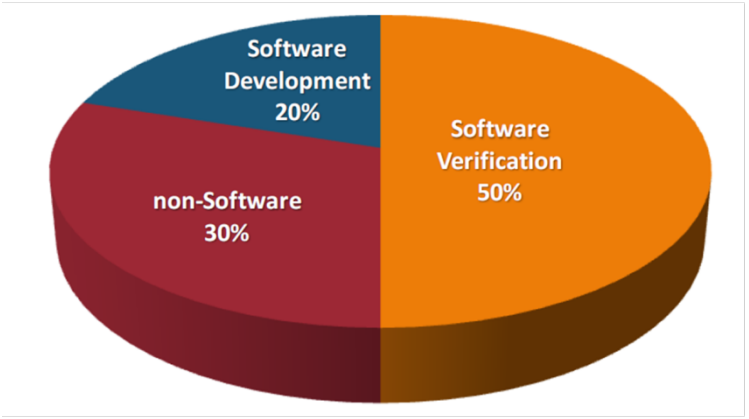
Rockwell Collins

Approved for public release. Case number 88ABW-2013-3892.

Motivation & Objectives

- United States (US) Air Force Research Laboratory (AFRL) funded this survey in order to:
  - Understand the current barriers to further adoption of formal methods in industry
  - Identify promising mitigations

Typical Recent Commercial Aircraft Cost Distribution



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

- Survey Objectives
  - Make current the knowledge about barriers.
  - Identify barriers specific to the US aerospace domain.
  - Provide the perspective of "novices."
  - Identify promising mitigation strategies.

"Formal methods" in this study includes static code analysis, model checking, theorem proving, and abstract interpretation

Approved for public release. Case number 88ABW-2013-3892.

Interviewees

- Surveyed 31 individuals from certification authorities, contractors, and customers in the US aerospace domain
- 14 experts, 9 novices, 5 users, and 3 managers of users

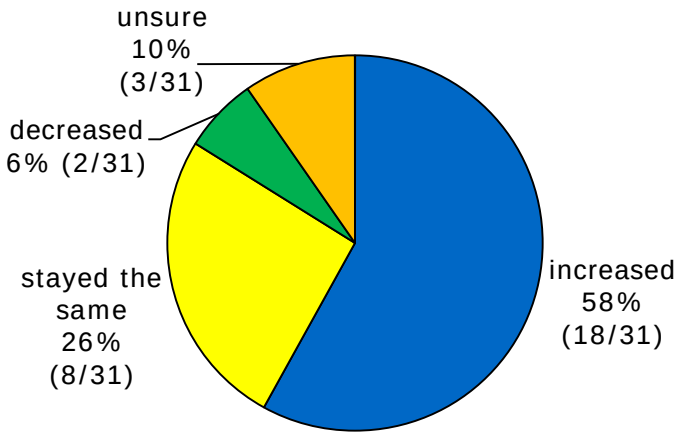
	NASA	US Army	FAA	Rockwell Collins	Honeywell	Galois	Wind River	Boeing	Lockheed Martin
Experts	5			5	1	2		1	
Novices		3	1		2		1		2
Users				4	1				
Managers of Users				2				1	
TOTAL	**5**	**3**	**1**	**11**	**4**	**2**	**1**	**2**	**2**

Approved for public release. Case number 88ABW-2013-3892.

Results—Use of Formal Methods

- The use of formal methods has increased in the last 5 years

"Has the use of formal methods in your organization increased, decreased, or stayed the same in the last 5 years?"

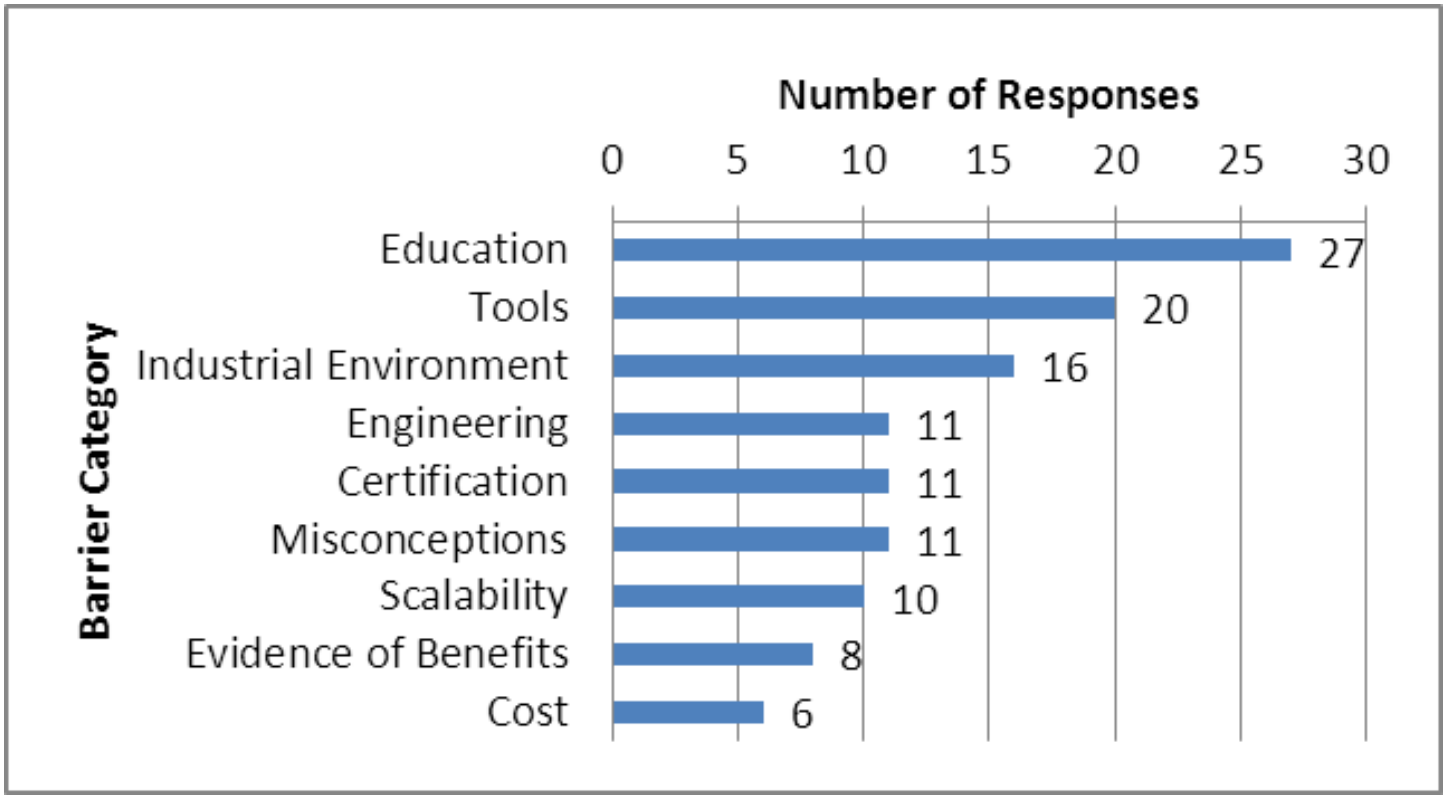


- 84% of survey respondents said the use of formal methods has increased or stayed the same

Approved for public release. Case number 88ABW-2013-3892.

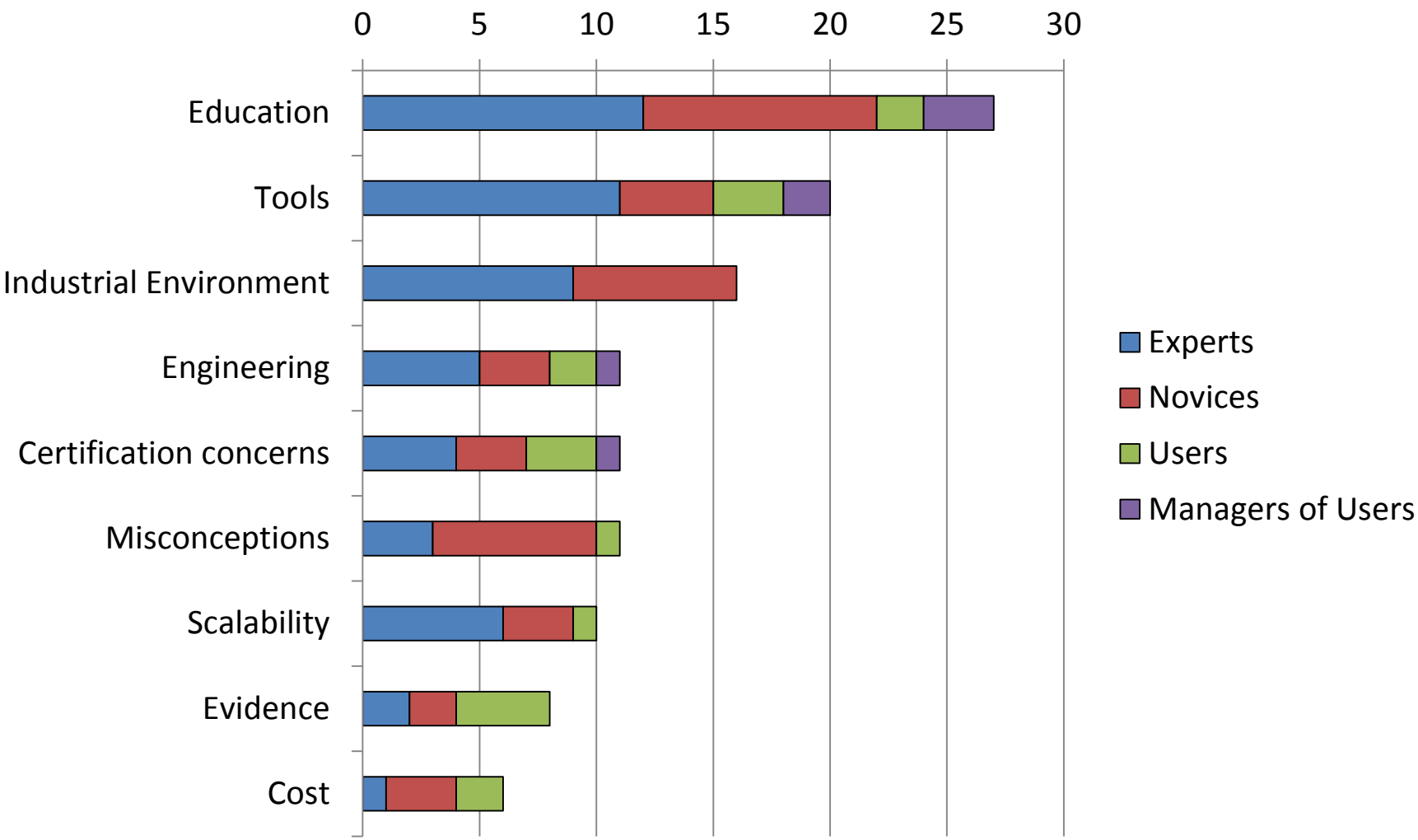
Results—Barriers

- Received 120 responses to the question "*What do you see as the current barriers to the industrial adoption of formal methods (especially in your organization)?*"



Approved for public release. Case number 88ABW-2013-3892.

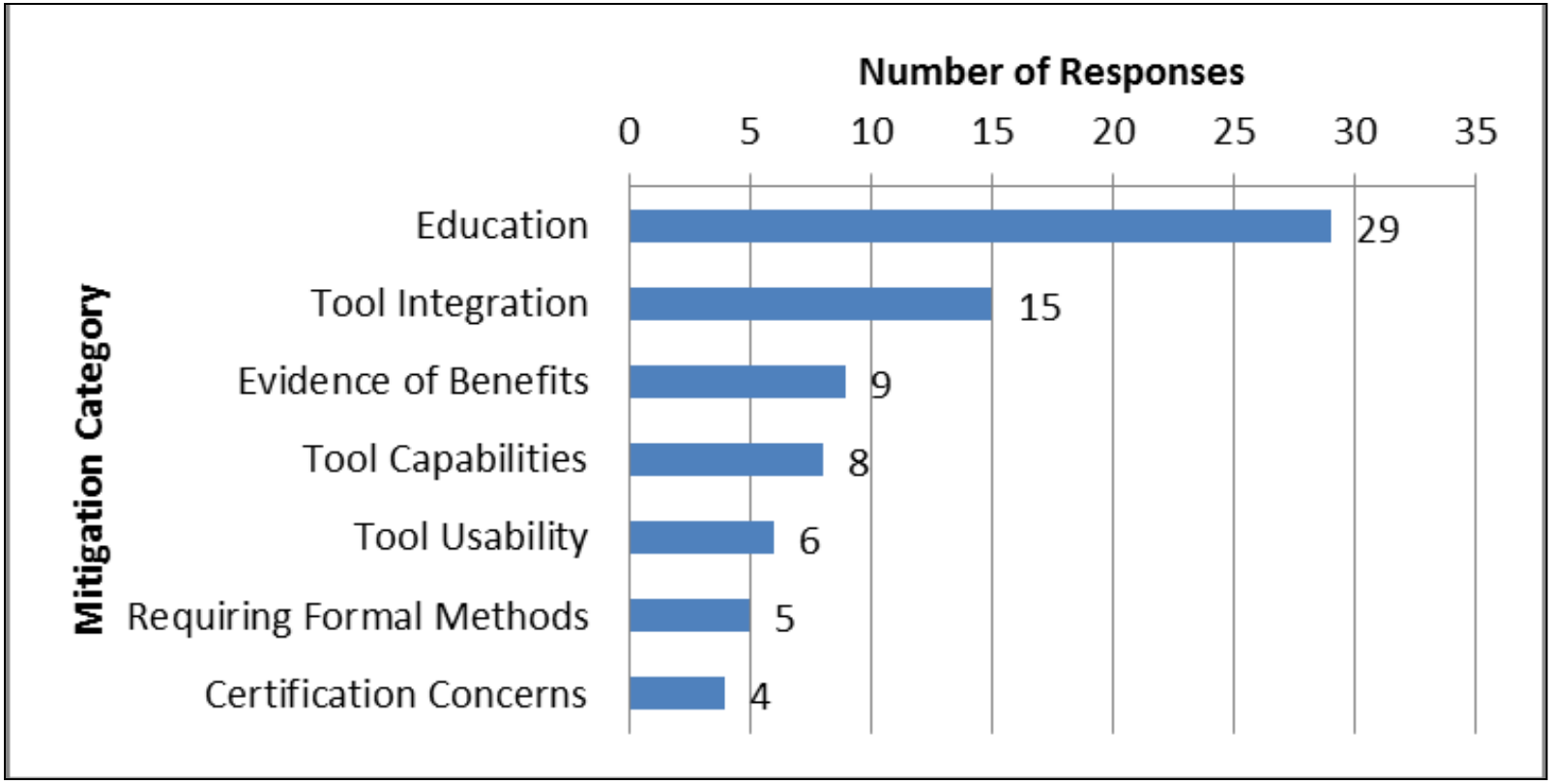
Barriers by Expertise



Approved for public release. Case number 88ABW-2013-3892.

Results—Mitigations

- Received 76 responses to the question "*Do you have any suggestions for removing [the barriers you mentioned]?*"



Approved for public release. Case number 88ABW-2013-3892.

Comparison with Prior Work and New Insights

- Our survey confirmed that several previously known barriers are still issues:
  - tools are not user-friendly
  - need for automation and scalability of tools
  - lack of evidence to support adoption decisions
  - skills deficiencies
- Lack of evidence on the reduced cost for second and subsequent use of formal methods is not a barrier.
- The need for education was the most frequently cited barrier; this was not emphasized in prior surveys.
- Non-technical barriers regarding project timelines and personnel changes are significant.

Approved for public release. Case number 88ABW-2013-3892.

Barriers Unique to the US Aerospace Domain

- No certification credit for formal methods.
- Certification authorities are reluctant to change.
- Need training on evaluating formal methods artifacts for certification.
- Certification authorities are not familiar with FM techniques or their benefits.
- Tool qualification of formal methods tools is uncertain.
- International certification authorities must agree on certification credit for FM.
- Uncertainty regarding whether certification based on formal analysis will stand up in court.
- US export control laws on technical data can make it difficult to collaborate internationally.

Approved for public release. Case number 88ABW-2013-3892.

Summary: Education

- A major theme 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
  - Host courses in formal methods for working engineers.

Approved for public release. Case number 88ABW-2013-3892.

Summary: 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.

Approved for public release. Case number 88ABW-2013-3892.

Summary: 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

Approved for public release. Case number 88ABW-2013-3892.