S5 Enhanced Analysis Breakout Session
14 June 2012

Format

Mr. Jon Hoffman of AFRL/RBCC, the Enhanced Analysis Lead, developed a number of discussion points to begin the conversation of the current challenges that the attendees see in the adoption and use of Formal Methods outside the academic environment. Specifically, how do we implement Formal Methods (FM) into the standard development cycle for future platforms?

Attendees

Jon Hoffman – Lead
Lucas Wagner
Arie Gurfinkel
Mark Lawford
Natalie Posada
Tim Wang
Aaron Fifarek

Discussion Points

The AF research group is strongly considering building a fully open challenge problem to represent the type of certification challenges that are present in new aircraft systems. What are the key software components, documentation, and system models that should be generated to allow effective demonstration of the analysis tools?

The conversation on this point began with some brainstorming on how to develop an appropriate challenge problem for the community on the whole. One of the themes expressed in this regard was the need to build a problem that is complex enough to spark a level of interest but modular enough that differing levels of outside personnel could effectively examine. A first example of this type of scoped idea that was produced in the medical field was the open challenge problem on the pacemaker that Dr. Oleg Sokolsky and Dr. Insup Lee have posted. This example provided not only a modular design but also allowed for an end-to-end challenge where advancements from contributors could be seen in the completed overall result. Currently, people working the pacemaker challenge problem are attempting to get the hardware platform improved to better satisfy the needs of the posted problem set.

The most common agreed upon challenge subject material was one with an UAV (Unmanned Aerial Vehicle) basis. The upcoming requests to further implement Unmanned Aerial System(s) (UAS) into the National Air Space (NAS) offers a significant opportunity to implement Formal Methods (FM) into the development, testing, and certification of these future systems. It was mentioned that should the government advocate the use of FM in these portions of system development, the use (and maturity advancement) of enhanced analysis would significantly grow as a unified requirement outside of the academic environment. Complex systems that can be examined in this regard were that of a UAV autopilot or a UAV cruise control. These examples produce challenges in system control as well as in

mode switching. Image processing for ISR (Intelligence, Surveillance, and Reconnaissance) was mentioned to be past the scope desired for a challenge problem. It was also mentioned that Arduino-based controllers could be used.

Ultimately, there was a consensus that taking advantage of graduate work in universities and leveraging industry to contribute to the challenge problem is central to any future advancement. The university environment is rich with graduate students eager to research real-world problems as they see it as a stepping stone into more exciting and complex areas. Starting from something like ArduPlane (http://diydrones.com/) may provide enough of the foundation that is desired. Furthermore, there was a consensus that in such an environment, there are aspects of this challenge problem that do not yet exist. Therefore, development of those capabilities would likely not be accomplished for free. A suggested approach is to allow the DoD to lead the way to coordinate and assemble the various aspects of the problem to generate the complete result.

What does certification evidence look like? Will this evidence change depending on the tool? Are there standard formats that evidence can be formed so that non-SME personnel can understand the evidence? (Tabular Expression Toolbox, etc)

This topic first opened a discussion on what would be expected of an employee personnel mix that would be necessary to properly deploy FM into the development cycle. Some of the attendees felt that it was unrealistic for integration of such tools without formal training much less deciding what the certification evidence would entail. Others in the group believed that making the certification evidence/FM evidence able to be understood by the standard engineer would allow for better integration into development processes.

No matter the level of expertise required to understand the output, approving the results to classify for certification evidence may prove to be more of a challenge due to an overall lack of understanding of FMs with the agencies responsible for acquisition and flight approval. It was suggested that the DoD take the lead to make in-roads to those agencies (e.g., ASC, FAA, etc.) to describe to them the advantages of FMs implementation to the airworthiness testing that they conduct. This will become increasingly important as complete matrix testing becomes more complicated as systems continue becoming more complex.

How do we come to an agreed upon set of tools that can unify analysis results? If we develop an agreed upon toolset, who will need to be responsible to ensure the latest techniques are incorporated? (Government mandate / individual development group)

The group did not directly answer this topic but moved on to discuss the next topic. Portions of the next topic touch on some of the aspects of this topic.

Why haven't formal methods been adopted more in flight safety critical software?

There was some sediment in the group that many of the reasons that FMs have not been more widely adopted in flight and safety critical software are the same reasons that they have not been accepted in other fields; a lack of general knowledge and understanding of FMs and the upfront increased cost that

this process might entail. Many groups across various domains are using static analyzers currently and that is comfortable for the current engineers. It was discussed that approximately ten years ago, static analyzers were the new development technology and now it is widespread so there is a parallel that may be established on implementation of FMs. Ultimately, it will progress into the development process with better establishment of good commercial tools.

Increased college undergrad education of FMs and their use is another barrier in the current environment. Many programs focus too little on FMs and maintain this subject for graduate work. The reality is that many engineers are not completing graduate level certification prior to starting to work in the field. To compound that education gap, engineers who are already established also do not know of the capabilities provided by FM. These engineers train the next generation internally and, if they are not familiar with new enhanced analysis techniques, then they do not stress that they do not know about them.

Which portion of the barriers is most suited for the Government / Industry / Academia to tackle?

The government, when requesting proposals, could mandate a preference to program bids that utilize FMs would go a long way to accelerate the acceptance and distribution of these new techniques. This would "kick-start" the industry sector to investigate the existing tools out of academia or to develop tools that resolve the gaps that the tools do not cover. As the budget environment becomes even tighter, this capability could provide cost savings after the initial tool implementation into company processes.

Safety Cases. Will the increased use in Formal Methods lead to a greater use of safety cases or similar evidence-based certification processes?

What came to mind here were assurance cases which have their own problems. To start off, it is important to prevent cases where people will sign off on these just to "check the box." What an assurance case does provide is an answer to why you are doing a test. Ultimately, FMs will help to fill in some of the evidence in conjunction with test cases. Use of FMs may be able to better focus physical testing thereby improving the efficiency of spending dwindling development funds.

What will be the key advances needed in analysis techniques to integrate them into commonly used tool-chains?

The consensus of the session was that progress is being made on the advances of FMs into today's tool-chains. The community will need to develop a way to analyze the tools to figure out a way to qualify them as valid certification tools while maintaining a responsible cost point. Current FMs tools are known to be fairly expensive per seat. As adoption of approved tools increase, the cost breakdown may be more conducive due to greater volume. By looking to open-source tools, the DoD could also help to drive down the cost of commercial generated tools.

Other thoughts/concerns/topics that should be discussed?

The common theme that was discussed was that both academia and industry is looking to the DoD to develop examples to test their FMs tools against and that there are some companies attempting to aid the government in that respect. The idea was expressed of generating an open website (like AFRL/RI's Spruce portal—https://www.sprucecommunity.org/) to post challenge problems that the public could visit and attempt to solve. These solutions, although they may not be complete, may further spawn further development and advancement.