- **Raymond Richards** • 14 days ago

  I will relay Bill's responses...

  - 2
  - •
  - Share ›

- 31 Comments
- **seL4 Summit**
- **Disqus' Privacy Policy**
- **Todd Humiston**
- **Recommend**

- **Sort by Oldest**

Join the discussion…

**Regan Robertson** Mod • 14 days ago

Good Morning,

The video will start on this page at 9:00am, and you may have to hit play or unmute. As a reminder this site works best in a Chrome Browser. You can write in comments through this feature to continue the conversation or ask questions.

- •
- Reply
- •
- Share ›

**Stuart Card** • 14 days ago

How about evolution in another sense: "Genetic Improvement of Software" using "Genetic Programming" -- combining this with formal methods -- who else is [interested in] doing this?

- 1
- •
- Reply
- •
- Share ›

**Raymond Richards** Stuart Card • 14 days ago

A number of researchers have revived old genetic techniques to support "automated bug repair" by mining large code bases and using genetic techniques to refine results. Claire LeGoues has been working in this area for a decade or so, and now it is well etablished. Recent work focuses on "quality" of patches, on more general approaches supporting transformation and synthesis. This is also enabled by large code repos such as GitHub (with its positive externalities) and the giant Google repo

- •
- Reply
- •
- Share ›

**mohit jangid** Stuart Card • 14 days ago

You mean re-designing programming languages which contains FM capabilities?

- •

- Reply
- Share ›

**Nathaniel Husted** • 14 days ago

Do you think there is value in FM folks expanding some of the various "technologies" such as "Contracts" and other more robust types of "in-the-loop" development techniques? Is this the path things are already going? The context of the thought is in spirit with the concept of "hiding the beautiful math".

- Reply
- Share ›

**Jason H Li** • 14 days ago

Bill - you mentioned the MSR success story about device drivers. The SLAM and SLAM2 works were great! Question - they realized a CEGAR-like refinement loop, which made total sense for the Microsoft device driver framework. Do you have some suggestions in terms of applicability of CEGAR-like approach to other domains and major systems?

- Reply
- Share ›

**Douglas Schafer** • 14 days ago

These dimensions are spot on. As a recent prior government sponsor, a challenge faced was when/how S&T funds can be "obtained" for the critical aspects of usability, tool chains, etc. that lower the technical expertise barrier to use. The core S&T tends to look to the core capability itself and then becomes incredibly competitive to gain the funds for any sustainability, etc.

S&T sponsors want to stop funding "support capabilities" and acquisition agencies have a hard time bridging that gap.

- 2
- •
- Reply
- •
- Share ›

**Nathaniel Husted** Douglas Schafer • 14 days ago

I've gathered that unless you're buying widgets, acquisition agencies have no interest in actually building up S&T into usable tools. Sadly, I think some of this is jus a fundamental hard cultural problem with a focus on material as capability vs. tooling as capability.

- •
- Reply
- •
- Share ›

**Douglas Schafer** Nathaniel Husted • 14 days ago • edited

Right, acquisition's 3600 S&T funding is (in my opinion) not capitalized on. Their "pull" is in "what" not "how," like "make it more secure" not "use FM." There needs to be a merge of knowledge and coordination of effort,

- 1
- Reply
- Share ›

**Douglas Schafer** • 14 days ago

This is important, these artifacts and justification should be a required deliverable....thus required, paid for, and owned by the government (in the DoD case).

- 1
- Reply
- Share ›

**Jason H Li** Douglas Schafer • 14 days ago

Agreed. Evidence artifacts should be brought along with dev.

- Reply
- Share ›

**Nathaniel Husted** Jason H Li • 14 days ago • edited

I think there's a lot of inspiration that can be found from the early open source business models here as well. I think there's a fear in large private companies that they loose leverage if they give up their IP to the Gov. In many ways I think there's bigger and better opportunities in the "developer as a service" business models that have been championed by RedHat and other early F/OSS orgs.

*steps off the soap box*

- Reply
- Share ›

**Douglas Schafer** Nathaniel Husted • 14 days ago

Agreed. I don't think the government "wants" the IP (or even would know what to do with it--though it needs to be protected). If we required specification and evidence of how implementation meets it (formally, for example) then IP itself is protected, but there is "some" assurance...?

- Reply
- Share ›

**Jerry Dussault** Jason H Li • 14 days ago

I don't believe we've addressed this issue with respect to the CoE Private Repo. Including evidence/artifacts for software we host should be an important consideration.

- Reply
- Share ›

**Renato Levy** Douglas Schafer • 14 days ago • edited

I could not agree more Doug. The power of Government acquisition in requesting evidence artifacts can significantly put pressure in wider FM adoption.

- Reply
- Share ›

**Raymond Richards** Douglas Schafer • 14 days ago

Keeping tool ecosystems alive is a huge challenge, even/especially open source tooling. There are no license fees, but there needs to be community engagement, which includes explicit effort by user teams. This is a cost of doing business.

- Reply
- Share ›

**Raymond Richards** Raymond Richards • 14 days ago

Rethinking the software deliverable is essential. Delivering a purely black box executable for a critical component will not support any credible T&E process.

How can providers protect their IP but also enable direct artifact-focused evaluation for critical security/safety/functionality properties?

Reply

Share ›

**Carl Nerup** • 14 days ago

Can you talk more on 5G, Formal Methods, and seL4?

Reply

Share ›

**Jason H Li** • 14 days ago

It seems that there are some issues in the systems. Some attendees can't see questions. Ray doesn't see any question, and Bill is having trouble with the Chat too.

Regan, can we collect these questions for Bill to answer a bit later?

- Reply
- Share ›

**June Andronick** • 14 days ago

Excellent presentation, many thanks for the overview and perspective on current focus and opportunities.

- 1
- Reply
- Share ›

**Jason H Li** June Andronick • 14 days ago

Thanks for support the event at such an early/late time in Sidney!

- Reply
- Share ›

**Renato Levy** • 14 days ago

i found an interesting synergy between Kevin's bottom up approach and the need to update our legacy systems. If we can lift what is out there and find critical issues using our techniques, then we can micro-patch them into better systems.

- Reply
- Share ›

**Jason H Li** • 14 days ago

Question - ACL2 was mentioned a couple of times. In terms of tool chain infrastructure, do you have other examples in mind to recommend? Maybe the Isabelle/HOL and Coq systems?

- Reply
- Share ›

**Raymond Richards** • 14 days agoFeatured by seL4 Summit

I will relay Bill's responses...

- 2
- Reply
- Share ›

**Stuart Card** • 14 days ago

I keep seeing indications that others are typing replies to my comment on integrating GP-based GI w/FM, but I never see the actual replies, despite frequent reloads using "Show new" button...

- Reply
- Share ›

**Raymond Richards** Stuart Card • 14 days ago

Stuart, I relayed Bill's response to your question

- Reply
- Share ›

**Stuart Card** Raymond Richards • 14 days ago

Thanks! That has now appeared. I will follow the lead therein. I am heavy on GP, familiar with GI, but have seen little activity integrating it w/FM.

- Reply
- Share ›

**Jerry Dussault** • 14 days ago

Great presentation! I didn't catch when/where we might look for a report on the results from the FM @ scale East- West- workshops. Will we be able to find that information soon?

Reply

Share ›

**Jason H Li** • 14 days ago

I particularly like the point of smaller proofs for large programs with great impacts. Avoid 'all-or-nothing'. Great insights and guidance! Will definitely think more into this.

Reply

Share ›

**Regan Robertson** Mod • 14 days ago

Bill Scherlis has sent in his comments to Ray to post. Please scroll down to see responses to earlier comments.

- Reply
- Share ›

**Regan Robertson** Mod • 14 days ago

Please join us for the next session that starts in 2 minutes. You can either go back to agenda to get to the next session or at the bottom of the page there is a next session button.

- Reply
- Share ›