- **Greg Shannon** • 15 days ago
  Good morning everyone, and especially Dr. Levy and Dr. Li.
- Reply
- Share ›

Renato Levy Greg Shannon • 15 days ago
Good Morning!

Reply

Share ›

Nathaniel Husted Greg Shannon • 15 days ago
Good morning! Looking forward to the keynote!

Reply

Share ›

Lenny Elliott Greg Shannon • 15 days ago

Good morning!

- Reply
- Share ›

This comment was deleted.

Renato Levy Guest • 15 days ago • edited

it will start right here on this page, at (9;00am EDT sharp). try refreshing your page to see the countdown

- Reply
- Share ›

Renato Levy • 15 days ago • edited

Just to remind everyone, you can ask questions directly to Greg while the presentation is rolling. It is pre-recorded, so you don't have to wait. You will not interfere with the presentation.

During Panels, you can ask questions by typing, and the moderator decides if wants to bring it before the panel. The panel may answer your question offline as well.

- 1
- Reply
- Share ›

Regan Robertson Mod • 15 days ago

Good Morning Everyone! The video will play right in your window and you can write comments or questions in this chat feature!

- Reply
- Share ›

Nathaniel Husted • 15 days ago

It is a bummer not being able to join you all in person this year. Here's to hoping for next year! Thanks to the organizers for making this possible given all the logistical and technical challenges.

- 4
- Reply
- Share ›

Greg Shannon • 15 days ago • edited

Just FYI to all, I changed my talk title after Jason recorded his intro. New title is Targeted Formal Methods. Sorry about that Jason.

- Reply
- Share ›

Greg Shannon • 15 days ago

There are now 16 of these Manufacturing Innovation Institutes. 5 funded by DOE, 1 by NIST, 10 by DOD.

- Reply
- Share ›

Nathaniel Husted • 15 days ago

Greg, do you still leverage the "full-scope" computational stack model with these modeling efforts? The notion of having the hardware levels down to the atom --> the traditional OSI model --> then the human bits?

- 1
- Reply
- Share ›

Greg Shannon Nathaniel Husted • 15 days ago

No, not initially. Full-scope tacks really aren't ready for us/CyManII to use/incorporate.

Reply

Share ›

Nathaniel Husted Greg Shannon • 15 days ago

Understood. It's a concept we're leveraging regularly philosophically but certainly difficult to put into practice in our internal efforts.

Reply

Share ›

Greg Shannon Greg Shannon • 15 days ago

however, if there are some stacks, especially on the asic side, I'd like to know about them

- Reply
- Share ›

Noah Evans Greg Shannon • 15 days ago

Can you talk about what you're interested in for ASICs? Automated reasoning about ASIC behavior?

- Reply
- Share ›

Greg Shannon Noah Evans • 15 days ago

can one have a "contract" for an asic that describes expected behavior at the interface level? in that way we split the problem. part 1 is using the asic correctly. the other is is the asic correct?

- Reply
- Share ›

Noah Evans Greg Shannon • 15 days ago

Greg, let's talk about this offline if you've got the time. Galois, Sandia and MIT all have interesting work in this space.

- Reply
- Share ›

Greg Shannon Noah Evans • 15 days ago

Yes, Please do. Sandia is one of our partners, but it's a huge org there.

- Reply
- Share ›

Noah Evans Greg Shannon • 15 days ago

Great thanks! I just sent a mail to your CMU email.

- Reply
- Share ›

Nathaniel Husted Greg Shannon • 15 days ago

I'll reach out to a colleague who is working in the general area though my (limited) understanding from the hardware assurance world is they aren't quite as "far along" as we are in the software world -- or at least are following different approaches with their own pluses/minuses.

Reply

Share ›

Greg Shannon Nathaniel Husted • 15 days ago

Hence, our targeted approach.

Reply

Share ›

Greg Shannon • 15 days ago

For e-PURE, formal methods are key to the resilience/robust/secure solutions for U.S. Industry.

Reply

Share ›

Renato Levy • 15 days ago

what about aluminum?

Reply

Share ›

Greg Shannon Renato Levy • 15 days ago

:)

Yes, metals, smelting.

Reply

Share ›

Greg Shannon Renato Levy • 15 days ago

With a project like this, it's key to use the words that the sponsors use. We all understand that other processes similar to iron/steel are important. So I/we think of "iron/steel" as a handle for what DOE wants

- Reply
- Share ›

Noah Evans • 15 days ago

Greg Shannon Can you talk a little more about the semiconductor part of the work? Are you guys interested in verified ASIC synthesis and place and route? Mask verification?

2

Reply

Share ›

Greg Shannon Noah Evans • 15 days ago

no. more about using an ASIC "correctly" in a secure automation solution

Reply

Share ›

Jerry Dussault • 15 days ago

Is there some coordinating body that works across the 16 Mfg Innov. Inst.? Or does each have a clearly defined scope that minimizes overlap?

Reply

Share ›

Greg Shannon Jerry Dussault • 15 days ago

Yes, congress watches that for sure. That's why we each "stay in our lane". That is each MII.

Reply

Share ›

Greg Shannon Jerry Dussault • 15 days ago

We/CyManII do anticipate working with our 15 peer MIIs to improve their operational security as well the security around/in their innovations

Reply

Share ›

Renato Levy • 15 days ago • edited

I do have Cyber technologies for manufacturing, but to be honest it does not use formal methods

- Reply
- Share ›

Greg Shannon Renato Levy • 15 days ago • edited

I'd like to hear more on what you have. We're watching and working with MxD, a DoD MII for digital manufacturing that is working to provide solutions for CMMC efforts by small and medium manufacturers (SMMs).

- Reply
- Share ›

Greg Shannon • 15 days ago

For my gov't colleagues listening in, I'm scheduled to talk about CyManII at the NITRD's CSIA working group meeting on December 3rd.

- Reply
- Share ›

Greg Shannon • 15 days ago

Also, cymanii.org is online now (though some testing today may have us bringing the site down a few times, just today).

Reply

Share ›

Nathaniel Husted • 15 days ago

I recall a lunch conversation I had with John Rushby about 10 years ago now where he figured there were about 1000 people in the world who really GOT formal methods. Hoping we've made strides over the past decade. *grin*

Reply

Share ›

Greg Shannon Nathaniel Husted • 15 days ago

I think there are 10x or 100x nay-sayers

- Reply
- Share ›

Jason H Li • 15 days ago

I like the approach, adequate but simple, etc. Can you explain a bit more on incremental properties? I was thinking about something similar but would like to hear more from you, Greg. It sounds like some composability may be needed.

- Reply
- Share ›

Greg Shannon Jason H Li • 15 days ago • edited

I'm pretty sure Bill Scherlis will address this and give a 100x better answer than I can.

- Reply
- Share ›

Greg Shannon Jason H Li • 15 days ago

And, this is what the FM teams in industry are doing.

1

Reply

Share ›

Jason H Li • 15 days ago

Efficient critical thinking and automatable analysis - these are great points. I personally would like to see a tool chain that can automate the efficient, increment FM. Any additional insights on this?

1

Reply

Share ›

Greg Shannon Jason H Li • 15 days ago

I see that CI/CD has been essential for the progress in ML/AI. Similarly I think CI/CD is/will be essential for incorporating FM into tool chains

Reply

Share ›

Jason H Li Greg Shannon • 15 days ago

Agreed on CI/CD. I am more curious on the tech base that can make CI/CD possible without losing the global soundness after incremental I&D. But this is very difficult of course. Sometimes in engineering we seek for 'almost', like you said in 'almost' counterexamples when talking about gaps between real systems and models.

- Reply
- Share ›

Greg Shannon Jason H Li • 15 days ago

you have to have a fast feedback loop. and the agile DevSecOps tools to take advantage of that feedback

- Reply
- Share ›

Ryan Craven Jason H Li • 15 days ago

Just curious (and apologies if covered in the talk), but what is the strategy for incremental FM? Target the low hanging fruit first, do the more "easily provable" stuff? or go after the

things that get the most use, have the most direct exposure to uncontrolled inputs from users?

Reply

Share ›

Greg Shannon Ryan Craven • 15 days ago

you didn't miss anything in the talk on this point. to me it starts will a very simple model, architecture & interfaces. it's how one gets some decomposability imho

Reply

Share ›

Jason H Li Greg Shannon • 15 days ago

Totally agreed Greg. Just to add 2 cents: incremental to me is 1) get the low hanging fruit; 2) prove something small but critical at the binary level, as Kevin H will talk about; and 3) try 1) and 2) in multiple places with different perspectives.

Reply

Share ›

Renato Levy Jason H Li • 15 days ago • edited

Maybe what we need is to use the Ci/CD process to verify the changes in proof from our last version. This way with incremental proofs, each proof is smaller and more tractable than proofing the whole system. Incorporate FM in the development process.

Reply

Share ›

Jason H Li Renato Levy • 15 days ago

Agreed, Renato. And this is related to what I replied to Greg - pasted here.

I am more curious on the tech base that can make CI/CD possible without losing the global soundness after incremental I&D. But this is very difficult of course. Sometimes in engineering we seek for 'almost', like you said in 'almost' counterexamples when talking about gaps between real systems and models.

Reply

Share ›

Renato Levy Jason H Li • 15 days ago

8^)

Reply

Share ›

Nathaniel Husted Jason H Li • 15 days ago

I'm curious if there's a way to build an FM process based around Test Driven Development processes? Perhaps Proof Driven Development? This would require languages to support a "simple" way to state these proofs and build the "hard stuff" on the back-end though. Ties in well to the "easy to use" tools bit I think...

Reply

Share ›

Greg Shannon Nathaniel Husted • 15 days ago

i like the PDD concept

Reply

Share ›

Douglas Schafer Jason H Li • 15 days ago

This starts to hit a great point, looking at this from an adopter and acquisition point of view, FM will have to hit three key marks: 1. Scale, 2. Conducted at the speed required (artifacts?), and 3. Meet economic constraints.

- Reply
- Share ›

Nathaniel Husted • 15 days ago • edited

I'm particularly interested in the training/trainable teams solutions that folks have. Are there any that have come up in your experience thus far? We certainly have a need/gap for folks who have some CS expertise but don't have Ph.D.s or M.S.s in the area already. There's a lot of excitement for formal methods but some of the standard tooling definitely scares folks.

- Reply
- Share ›

Greg Shannon Nathaniel Husted • 15 days ago

Nathaniel Husted please let me know what you find for answer to your question. I/CyManII needs those resources too

- Reply
- Share ›

Nathaniel Husted Greg Shannon • 15 days ago • edited

Will do! I've an internal R&D project going on this year -- if all goes well, we'll have a survey by non-experts for tools for non-experts.

I'm always happy to stand on the shoulders of giants. *grin*

- 1
- Reply
- Share ›

Olin Sibert Nathaniel Husted • 15 days ago

I'd sure like this gap to be smaller, too. It was a yawning chasm when I started doing security evaluations almost 40 years ago, and although the tools have improved dramatically in the succeeding decades, the chasm seems little better. Ordinary programmers today seem to have no better resources for understanding and updating proofs than they did then. As then, it seems like there may be opportunities to use literate programming techniques to tie specifications, proofs, and code together in a manner readily accessible to programmers. Such tools might provide as much benefit as better education.

- Reply
- Share ›

Greg Shannon • 15 days ago

All, it's 10:15am ET now. I'll be checking in on this chat/channel occasionally and respond to further questions. Thank you for listening.

Reply

Share ›

—

Jason H Li Greg Shannon • 15 days ago

Greg - thanks so much for the great keynote! Very insightful.

1

Reply

Share ›