TCCOE Summit Technical Program

May 11-12, 2023

Theme: Modern Software Development vs Current Assurance Policies

Thursday May 11, 2022	**Chair & Time**
	Dr. Ray Richards
Day One Keynote Tim Booher, Vice President Combat Systems, Lockheed Martin	09:00AM – 10:00AM
U.S. Army DEVCOM-GVSC Vision and Progress– Leonard Elliott, U.S. Army DEVCOM-GVSC	10:00AM – 10:30AM
Break (30 minutes)	10:30AM – 11:00AM
Secure and Resilient Systems Programs at ONR – Dr. Ryan Craven, ONR	11:00AM – 11:30AM
Scaling Formal Methods for Software Assurance – Dr. Natarajan Shankar, SRI International	11:30AM – 12:00PM
Lunch (on your own)	12:00PM – 13:30AM
MINDing the GAPS: A Next Generation Tactical Cross Domain Solution – William D. Smith, GE	13:30PM – 14:00PM
ACVIP in support of Airworthiness Certification – Dr. John Hudak, CMU/SEI	14:00PM – 14:30PM
Assurance of Learning-enabled Software Systems – Prof. Sandeep Neema, Vanderbilt University	14:30PM – 15:00PM
Privacy Enhancing Technology – Joe Kovba, Leidos	15:00PM – 15:30PM
Break (30 Minutes)	15:30PM – 16:00PM
Panel Discussion – Software and Assurance (Moderator: Ray Richards)	16:00PM – 17:00PM
• Tim Booher, Lockheed Martin • Dr. Mallory Graydon, NASA Langley • Joe Kovba, Leidos • Dr. Robert Denz, Riverside Research	
Adjourn for the day	17:00PM

Friday, May 12, 2023	**Chair & Time**
Correct by construction approaches for high consequence hardware – Noah Evans, Sandia Labs	08:30AM – 09:00AM
Model-based High Assurance Development – Todd Carpenter, Galois	09:00AM – 09:30AM
Day Two Keynote Dr. Jimmy "Rev" Jones, NH-IV SAF/AQLV, PEM, STITCHES Warfighter Application Team Lead	09:30AM – 10:30AM
Break (30 Minutes)	10:30AM – 11:00AM
seL4 updates and Foundation – seL4 Foundation (Recorded video)	11:00AM – 11:30AM
Overview of TCCOE - Patrick Hurley, TCCOE	11:30AM – 12:00PM
Closing Remarks (Brad Martin, DARPA; Dr. Paul Ratazzi, Air Force Research Laboratory)	12:00AM – 12:30PM
Summit Adjourned	12:30PM

Keynote Presentations

Tim Booher, Vice President Combat Systems, Lockheed Martin

Dr. Jimmy "Rev" Jones, PEM, STITCHES Warfighter Application Team Lead

Government & Labs Efforts

Dr. Ryan Craven, ONR: Secure and Resilient Systems Programs at ONR

Leonard Elliott: U.S. Army DEVCOM-GVSC Vision and Progress

Mr. Elliott has been an electrical engineer in the Combat Capabilities Development Command (DEVCOM) Ground Vehicle System Center (GVSC) Vehicle Electronics & Architecture (VEA) Division since September 2010. He has participated in the development of various military ground vehicle Modular Open System Approach (MOSA) initiatives and supports research and development in the areas of middleware, open system architectures, and secure embedded systems. Mr. Elliott holds a B.S. degree in Electrical and Computer Engineering from the University of Massachusetts Amherst, and an M.S. in Electrical and Computer Engineering from Worcester Polytechnic Institute.

Noah Evans, Sandia Labs: Correct by construction approaches for high consequence hardware

Building Assured Systems

Todd Carpenter, Galois: Model-based High Assurance Development

Dr. John Hudak, SEI: ACVIP in support of Airworthiness Certification

In this presentation we demonstrate that the Architecture-Centric Virtual Integration Process (ACVIP) provides value for military aircraft airworthiness qualification. Military aircraft airworthiness criteria describe aviation airworthiness processes and the criteria, standards, and methods of compliance necessary for airworthiness assessment of manned and unmanned military aircraft systems. The U.S. Army Military Airworthiness Certification Criteria (AMACC), for example, includes elements from many existing civilian standards and is used to define airworthiness requirements for existing and new acquisition programs. Software safety of complex systems is assured by compliance with formal development processes and testing of essential elements. The AMACC also allows for verification by analysis to detect defects in the evolving software design. Going forward, the U.S. Department of Defense's (DoD) Digital Engineering Strategy will improve aircraft requirements, design, and development through model-based engineering. ACVIP provides the foundation needed for effective model-based verification by analysis.

Dr. Hudak is a Principal Engineer at the Software Engineering Institute, Carnegie Mellon University.

Joseph Kovba, Leidos: Privacy Enhancing Technology

Joe Kovba is the Leidos Cloud Center of Excellence Practice Lead and an Adjunct Professor at John Hopkins University.

Dr. Sandeep Neema, Vanderbilt University

Abstract: Significant advances have been made in the last decade in constructing autonomous systems, as evidenced by the proliferation of a variety of unmanned vehicles. These advances have been driven by innovations in several areas, including sensing and actuation, computing, modeling and simulation, but most importantly deep machine learning, which is increasingly being adopted for real-world autonomy. In spite of these advances, deployment and broader adoption of learning techniques in safety-critical applications remain challenging. This talk will present some of the challenges posed by the use of these techniques towards assurance of system behavior, and summarize advances made in DARPA's Assured Autonomy towards establishing trustworthiness at the design stage and providing resilience to the unforeseeable yet inevitable variations encountered during the operation stage. The talk will also discuss related work in creating frameworks for assurance driven software development.

Speaker Bio:
Dr. Sandeep Neema is a Professor of Computer Science at Vanderbilt University since August 2020. He also holds courtesy appointment as Professor of Electrical and Computer Engineering at Vanderbilt University. He was a Program manager at DARPA's Information Innovation Office (I2O) from July 2016 till September 2022. In his tenure at DARPA he conceived, developed, and managed influential programs at the intersection of Artificial Intelligence and Cyber Physical Systems, that included programs such as Assured Autonomy, Symbiotic Design of Cyber Physical Systems, and Assured Neurosymbolic Learning and Reasoning. His research interests include Cyber Physical Systems, Model-based Design Methodologies, Artificial Intelligence and Machine Learning, and Distributed Real-time Systems. Dr. Neema has authored and co-authored more than 100 peer-reviewed conference, journal publications, and book chapters. Dr. Neema holds a Doctorate in Electrical Engineering and Computer Science from Vanderbilt University, and a Master's in Electrical Engineering from Utah State University. He earned a Bachelor of Technology degree in Electrical Engineering from the Indian Institute of Technology, New Delhi, India.

Dr. Natarajan Shankar, SRI: Practical Formal Verification Tools

Speaker: Natarajan Shankar, SRI International Computer Science Laboratory

Abstract: Right from its formative years, the field of formal methods has faced the skepticism that rigorous software verification might be a bridge too far. Advances in the last few decades in static analysis, model checking, SAT/SMT solving, and theorem proving have yielded technologies that are now widely and

even routinely used in industrial settings. There are now several significant case studies where these technologies have been employed in developing complex and useful software artifacts. However, we face several serious barriers to the broader adoption of formal techniques. We survey the challenges for high-assurance software development using formal methods and enumerate some concrete steps toward creating an ecosystem within which software can be economically developed and maintained hand-in-hand with a rigorous assurance argument.

Bio: Dr. Natarajan Shankar is a Distinguished Senior Scientist and SRI Fellow at the SRI Computer Science Laboratory. He received a B.Tech. degree in Electrical Engineering from the Indian Institute of Technology, Madras, and Ph.D. in Computer Science from the University of Texas at Austin. He is the author of the book, "Metamathematics, Machines, and Godel's Proof", published by Cambridge University Press. Dr. Shankar is the co-developer of a number of technologies including the PVS interactive proof assistant, the SAL model checker, and the Yices SMT solver. He is a co-recipient of the 2012 CAV Award and the recipient of the 2022 Herbrand Award.

William (Bill) D. Smith, GE - MINDing the GAPS: A Next Generation Tactical Cross Domain Solution

This presentation covers the work that GE Research is performing on the DARPA Guaranteed Architectures for Physical Systems (GAPS). GE is developing the Monitoring & INspection Device (MIND) to serve as a tactical Cross Domain Solution for embedded real-time SWaP-constrained applications. We are developing software tools and FPGA IP libraries to build high performance CDS filters featuring deterministic 10+ Gbps throughput at microsecond scale latency. We are using Data Format Definition Language (DFDL) schemas to specify application wire protocols and associated security policies. We have extended the open-source Apache Daffodil project to generate embedded C code as well as FPGA-based hardware-synthesizable VHDL code from DFDL schemas for CDS filter pipeline stages. We have demonstrated the MIND technologies on a variety of application protocols, and we are working with GE Aviation Systems to build a 3U VPX CDS card for the US Army's Ground Vehicle Survivability's Vehicle

Protection System. We will also highlight how the MIND technologies can be matured and integrated with the systems engineering environments used in avionics applications such as the Future Vertical Lift program.

Bill is a Principal Engineer at GE Research and worked with many current and former GE businesses – including critical infrastructure, avionics, healthcare, transportation, media, and military / aerospace. Bill has led the development of the edge security technologies used in a variety of GE products and is currently the PI on the DARPA Guaranteed Architectures for Physical Security (GAPS) program focused on next generation tactical cross domain solutions. Bill has undergrad and master's degrees in electrical engineering from RPI in Troy, NY.

Panelists

Tim Booher, Lockheed Martin

See Keynote presentation.

Dr. Robert Denz, Riverside Research

Dr. Robert Denz serves as the Director of the Secure and Resilient Systems group at Riverside Research. In this role, he leads a team of researchers who ensure software provenance, security, reliability, and resilience in systems. To achieve these objectives, the Secure and Resilient Systems group conducts innovative research in formal methods, AI-driven secure waveform design, and secure operating system implementations for the Department of Defense (DoD) and Intelligence Community (IC).

Dr. Denz has over 15 years of experience working on and leading cybersecurity and anti-tamper research programs for DARPA and the DoD. He was recently the Principal Investigator for DARPA Dispersed Computing, where he oversaw a multi-disciplinary team that delivered distributed resilient mesh routing protocols to the tactical edge. Dr. Denz also served as a research lead for DARPA Mission Resilient Clouds (MRC), contributed to the DARPA Clean-slate design of Resilient, Adaptive Secure Hosts (CRASH), and was an original designer of the Air Force Cross-Domain Access SecureView Hypervisor. Through these efforts, he gained extensive knowledge of x86 processor internals and secure operating systems.

Dr. Denz received his PhD in secure hypervisor and kernel design from the Thayer School of Engineering at Dartmouth College in 2016.

Dr. Mallory Graydon, NASA Langley

Dr. Graydon is a Research Computer Scientist at NASA Langley Research Center. She has worked as a Software Design Engineer building software for medical devices and for test and measurement applications, as a Research Associate at the University of York (UK), and as a Researcher at Mälardalen University (Sweden). Mallory's research on safety assurance for software-intensive systems has covered safety process planning, review of safety arguments, assurance of changes to legacy systems, safety cases for component-based systems, mixed-criticality hard real time scheduling, formal argumentation, and argument confidence.

Her work explores the efficacy and appropriateness of argument-based approaches to civil aviation safety assurance. Mallory co-organized the 2014 workshop on Planning the Unplanned Experiment: Assessing the Efficacy of Standards for Safety Critical Software.

Joe Kovba, Leidos

See technical presentation

TCCOE

Patrick Hurley, TCCOE: Overview of TCCOE

Raymond Richards, Leidos: Panel Moderator