High Assurance Systems @ GE Research

Introduction

The High Assurance Systems team at GE Research in Niskayuna, NY is focused on addressing the technical challenges associated with the exponential growth of scale and complexity of software in critical infrastructure, which are also exposed to significant cybersecurity threats and increasing demand to support artificial intelligence and autonomy. The team is focused on requirements modeling (structured natural language) and analysis (automated theorem proving), automated test case generation (model checkers), compositional verification (SMT Solvers), synthesis, and assurance case-based verification. Accomplishments and experience include development of the ASSERT™ toolchain, development of the SOTERIA fault tree modeling & synthesis tool for NASA, 2017 AFRL Summer of Innovation - applied formal verification to UxAS code, currently participating in the DARPA Cyber Assured Systems Engineering (CASE) program and AFRL Team Enabling Architecture for Manned-Unmanned Systems (TEAMS) and soon to start the ARCoS rapid certification project. We are also developing technical solutions for continuous assurance cases including run time assurance to support autonomy and other untrusted components, formal verification of AI algorithms and to provide analysis and corrective action services.

ASSERT™

The size and complexity associated with software that monitors, controls, and protects flight critical products continues to grow. This is compounded by the increased use of autonomous systems which can be more complex as many operator responsibilities are supported and replaced by software in unmanned systems. Further, these systems are subject to cyber-attacks, thereby necessitating another level of complex software to ensure security. General Electric devoted a team to research and develop of a new suite of tools to address the challenges with design, development, and verification of these software-intensive products. The goals were to develop technology, processes, and tools that result in more efficient software and system development as measured by cost and cycle time, and to support new capabilities such as autonomy and the fourth Industrial revolution. The GE team created the ASSERT™ tool chain (Analysis of Semantic Specifications and Efficient generation of Requirements-based Tests) and an approach to formal requirements capture, requirements analysis, and auto test generation. More details on ASSERT™ are available in the following publications [1] [2] [3] [4] [5].

AFRL Summer of Innovation

During the summer of 2017, AFRL in Dayton, Ohio invited a team of experts from government, academia and industry to participate in their Summer of Innovation program. The team focused on applying state of the art formal verification tools on the AFRL UxAS software. GE High Assurance Systems team members applied ASSERT™ to capture, analyze requirements and generate test cases in the Requirements Group [6] and led the Systems Safety Group [7]. The work was presented at the AFRL Safe and Secure Software and Systems Symposium (S5).

SOTERIA

The GE High Assurance Systems team led a NASA program to create a tool named SOTERIA which stands for **S**afe and **O**ptimal **T**echniques **E**nabling **R**ecovery, **I**ntegrity, and **A**ssurance. The team developed a model-based framework for modeling, visualizing, and analyzing the safety of system architectures. The framework includes a modeling language for defining libraries of components that include information on component reliability, connectivity, and fault propagation, and automatically synthesizes fault trees and cutsets from the architecture model. The team applied the tool to safety analysis of an Integrated Modular Avionics (IMA) architecture. To address changes in the lifecycle of a product, as often

Contact Michael Durling for more information - durling@ge.com

happens during the course of development, our tool can also synthesize well-formed architectures that meet the safety requirements [8]. The source code is available on our GitHub site [9].

DARPA Cyber Assured Systems Engineering (CASE)

The goal of the DARPA Cyber Assured Systems Engineering (CASE) research program is to develop revolutionary technology and tools that enable systems engineers to design-in cyber resiliency while evaluating and trading off other properties of the system such as safety. The GE team, led by GE Research, including GE Aviation Systems and the University of Iowa is creating tools and process under technical area 2, *Design for Resiliency* on the program. The GE team's Model Based Architecture Synthesis (MBAS) tool will enable system engineers to model, jointly analyze safety and security based on architectural models and mission scenarios, generate fault and attack\defense trees, then synthesize an architecture that meets all the design constraints. Once the architecture is in place, the second thread of the GE tool, the Cyber Resiliency Verifier (CRV), will perform an analysis of the architecture and design models to see if they satisfy formal resiliency properties. After the analysis, the CRV tool returns proof evidence that the system is resilient, counter examples that highlight vulnerability, or run-time monitor location recommendations. The team started the 4-year program in February of 2018. [10, 11, 12, 13]

Teaming-Enabled Architectures for Manned-Unmanned Systems (TEAMS)

TEAMS is an architectural definition and prototyping program led by GE Aviation Systems aimed at enabling transformation of manned-unmanned teaming (MUM-T) systems development. The program is using an architecture-centric model-based system engineering approach to define the scope for the MUM-T domain, generate a Reference Architecture, provide assurance guidance and create multiple prototypes to validate the approach. The GE High Assurance Systems team will focus on formal requirements capture and analysis, and assurance methods for MUM-T systems that include run time assurance capabilities. GE Research will create and analyze models, contribute to the design of a reference architecture, specify a component assurance case profile and deliver prototype instantiations for evaluation and analysis [14].

NASA V&V Program

GE and NASA kicked off a 3-year program intended to evaluate formal methods tools applied to aerospace software and systems. On the program GE will apply a suite of formal methods-based tools developed at GE and at NASA to a relevant GE Aviation Systems application and compare the results of the traditional approach with the formal methods technology-based approach. The program will include use of the GE ASSERT™ requirements capture, analysis and test generation tool and the NASA AdvoCATE assurance case tool.

DARPA Automated Rapid Certification of Software (ARCoS)

The goal of the Automated Rapid Certification of Software (ARCOS) program is to automate the evaluation of software assurance evidence to enable certifiers to determine rapidly that system risk is acceptable. Two factors support the acceleration of software certification through the automation of evaluations. ARCOS will explore techniques for automating the evidence generation process for new and legacy software; create a means of curating evidence while maintaining its provenance; and develop technologies for the automated construction of assurance cases, as well as technologies that can validate and assess the confidence of an assurance case argument. The evidence generation, curation, and assessment technologies will form the ARCOS tools and processes, working collectively to provide a scalable means of accelerating the pathway to certification. The ARCoS program started in March 2020.

Contact Michael Durling for more information - durling@ge.com

References

[1] Kit Siu, et al, "Flight Critical Software and Systems Development Using ASSERT," in *Digital Avionic Systems Conference (DASC)*, St. Petersburg, Florida, 2017.

[2] A. Crapo and A. Moitra, "Requirements Capture and Analysis in ASSERT," in *25th IEEE Requirements Engineering Conference*, Lisbon, Portugal, 2017.

[3] A. Moitra, K. Siu, A.W. Crapo, H. Chamarthi, M. Durling, M. Li, H. Yu, P. Manolios, M. Meiners, "Towards Development of Complete and Conflict-Free Requirements. IEEE Requirements Engineering Conference (RE'18)," in *IEEE Requirements Engineering Conference 2018*, Banff, Canada, 2018.

[4] Craig McMillan, Abha Moitra, Andy Crapo, Michael Durling, Meng Li, Panagiotis Manolios, Mark Stephens, Daniel Russell, "Increasing Development Assurance for System and Software Development with Validation and Verification Using ASSERT," in *SAE Aerotech Americas*, Charleston, South Carolina, 2019.

[5] Meng Li, Baoluo Meng, Han Yu, Kit Siu, Michael Durling, Daniel Russell, Crig McMillan, Matthew Smith, Mark Stephens, Scott Thompson , "Requirements-based Automated Test Generation for Safety Critical Software," in *IEEE DASC*, San Diego, 2019.

[6] D. C. Anthony Aiello, "Summer of Innovation Requirements Group Report Out," in *AFRL Safe and Secure Software and Systems Symposium*, Dayton, Ohio, 2017.

[7] M. Castillo-Effen, "http://mys5.org/Proceedings/2017/Day_3/2017-S5-Day3_1005_SoI_System_Safety_Group_Castillo-Effen.pdf," in *Safe and Secure Software and Systems Symposium*, Dayton, Ohio, 2017.

[8] Panagiotis Manolios, Kit Siu, Michael Norman, Hongwei Liao, "A Model-Based Framework for Analyzing the Safety of System Architectures," in *The 65th Annual Reliability & Maintainability Symposium (RAMS)*, Orlando, Florida, 2019.

[9] "Soteria source code on GitHub," [Online]. Available: https://github.com/ge-high-assurance/safety-analysis.

[10] Michael Durling, Kit Siu, Abha Moitra, Meng Li, et al, "DARPA CASE VERDICT Phase 1 Final Report," 2109.

[11] Kit Siu, Abha Moitra, Meng Li, Michael Durling, Heber Herencia-Zapana, John Interrante, Baoluo Meng; Cesare Tinelli, Omar Chowdhury, Daniel Larraz, Moosa Yahyazadeh, M. Fareed Arif, and Daniel Prince, "Architectural and Behavioral Analysis for Cyber Security," in *IEEE DASC*, San Diego, 2019.

[12] Kit Siu, Heber Herencia-Zapana, Daniel Prince, Abha Moitra , "A Model Based Framework for Analyzing the Security of System Architectures," in *Reliability and Maintainability Symposium (RAMS 2020)*, Palm Springs, California, 2020.

[13] "VERDICT GtiHub," [Online]. Available: https://github.com/ge-high-assurance/VERDICT.

[14] [Online]. Available: https://www.airforce-technology.com/news/ge-aviation-teams-prototype-programme/.

Contact Michael Durling for more information - durling@ge.com