COMPUTER SCIENCE

MoDELS 2021 Special Issue

March 28, 2022

Shiva Nejati and Dániel Varró,

My name is Dr. Eric Mercer, and I am one of the corresponding authors on a recently published paper in ACM/IEEE 24th International Conference on Model Driven Engineering Languages and Systems (MoDELS 2021). On behalf of my coauthors, I would like to submit the enclosed manuscript entitled ”Synthesizing Verified Components for Cyber Assured Systems Engineering” for consideration for publication in the MoDELS 2021 special issue of the Journal of Software and Systems Modeling (SOSYM). I confirm that the enclosed manuscript is an original work and has not been published nor has it been submitted simultaneously elsewhere. Also, all authors have checked the manuscript and have agreed to the submission.

The published manuscript in MODELS 2021 describes a Model Based Systems Engineering (MBSE) environment developed as part of the the DARPA Cyber Assured Systems Engineering program. The environment enables systems engineers to design-in cyber-resiliency through automated model transformations that introduce high-assurance components into a system; in particular, filters that guard against malformed input, as well as monitors that guard against spoofing and other malicious behavior. A formal specification defines each high-assurance component and is used to verify that the component addresses system-level cyber requirements. Implementations for these high-assurance components are directly synthesized from their specifications. The model transformations are integrated into the Open Source AADL Tool Environment (OSATE). The manuscript discusses a real-world case study by verification experts and reports on their experience working in the environment.

The new manuscript submitted here for consideration expands on the MODELS 2021 manuscript with the following original contributions:

- A new, heavily revised to be more intuitive, example to motivate and explain the MBSE environment, the need for cyber-assurance, and the role of formal verification is synthesizing high-assurance components to cyber-harden a system.
- A section that formally defines the assume-guarantee reasoning used to prove cyber-requirements of a system design with its requisite verification conditions that are dispatched by a model checker.
- A new section that formally defines the syntax and semantics of the specification language to describe contract specifications on components and systems.
- A new section that formally defines a code contract that is a specialized specification for high-assurance components, such as filters and monitors, that are sufficient for proving cyber-properties of the system and for synthesis to an actual implementation.
- A heavily revised section on the synthesis process that starts with a code contract and ends with CakeML code describing is some considerable detail how the synthesis works and is proved correct.
- A new real-world case study with system developers that are not expert with assume-guarantee reasoning to show feasibility with such developers.

The authors feel this submitted manuscript represents a new and original contribution over the prior publication.

I hope that you find this manuscript of interest to your readers. Thank you for your consideration and your generosity in working with me, and my coauthors, in extending the submission deadline.

Sincerely,

Eric G Mercer
Associate Professor