Automated Reasoning Technologies Will Enable a Correct-by-Construction Approach to Systems Engineering

Abstract submitted to the
2023 MITRE DE and T&E Connect the Dots Workshop

Raheel S. Mahmood*, Jackson Mayo, Noah Evans, Rob Armstrong
Sandia National Laboratories†— Livermore, CA, USA

22 May 2023

High-consequence engineered systems, for which failure of specified requirements can result in loss of life or other unacceptable consequence, must implement a disciplined and rigorous systems engineering methodology from inception of the product development program. Such a methodology will necessarily include generation of evidence that the product will meet its requirements once fielded.

The utilization of digital components continues to increase in high-consequence engineered systems due to the desire for modern features such as flexibility, adaptability, and reuse. At the same time, the cybersecurity threat environment in which systems are required to operate safely will continue to evolve. The design complexity introduced by utilization of digital components mandates an engineering approach that incorporates trust and assurance earlier in the system design process, as requirements and design architectures are being derived. The assurance case constructed early in system design should be updated and preserved during development as component requirements and functional architectures are derived, which reduces the risk that defects will only be detected later as failures during testing and verification of component designs, or that vulnerabilities will manifest as undesired behaviors in the fielded system.

In this submission, the authors will describe how recent advances in formal methods, along with improved accessability and usability of automated reasoning technologies such as proof assistants and model checkers, can be used to enable a systems engineering approach wherein correctness of the system design with respect to requirements can be assessed early in the development lifecyle. The correct-by-construction systems engineering approach requires development of an executable abstract model of the system design along with a concise set of system requirements that are expressed as logical relationships about the executable digital model. The abstract executable system model is a mathematical construct that bounds the possible behaviors of the system and facilitates use of automated tools to reason about correctness of the system design. This allows systems engineers to provide evidence in the form of a mathematical proof that the system design, as described by its model, satisfies its specified requirements.

This method extends contemporary methods for system assurance by providing a means to formally and rigorously prove safety and security characteristics, often expressed as always/never requirements, for which testing or simulation provide limited assurance. As component requirements are derived during development, construction of component executable specifications will enable formal verification of the designed component with respect to its own specification. To ensure that the derived component specifications do not violate their design envelope as specified by system requirements, formal methods tools are used to generate evidence of mathematical refinement (correspondence) between the system-level and component-level executable specification models.

This approach aids engineers in eliminating defects in the specified system functional architecture and in derived requirements early in the development process, before the defects are realized as failures or vulnerabilities in the final design. The authors will discuss successes and challenges associated with implementation of this correct-by-construction systems engineering approach on current development programs for high-consequence systems designed at Sandia National Laboratories.

*raheel.mahmood@sandia.gov

†Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525. SAND2023-04064A.