Introduction: Metrics, Modeling and Simulation for Cyber Physical Systems

Barry Charles Ezell
Old Dominion University
Virginia Modeling Analysis &
Simulation Center
bezell@odu.edu

Luanne Burns Chamberlain
JHU Applied Physics Lab
11100 Johns Hopkins Road
Laurel, MD 20723
luanne.chamberlain@jhuapl.edu

In recent years, there has been a massive increase in cyber crime. Cyber breeches have become ubiquitous. The US government is attempting to adapt through legislation and policy. For instance, businesses in the defense industrial base must be in compliance of NIST 80-71 by 31 December 2017. Insurance companies as well are beginning to build actuaries on cyber risk. Along with NIST, there are many cyber frameworks that exist, each with their own following. Recently, companies have sought mapping from one framework to another but this is imperfect solution because some frameworks are exclusively technical control measures with very little to do with risk governance. Along with these frameworks, assessment models have been and are under development.

Against this backdrop, the Metric, Models, and Simulation for Cyber-Physical Systems focuses on different frameworks that have been operationalized so that cyber-physical systems can be baselined in security. In addition, the minitrack focuses on innovations in decision support such as cost effective means to decide what metrics should be addressed to get the best value in cybersecurity. There are many challenges to overcome in cyber-physical systems. We ask: How should frameworks be operationalized? What methodologies are available to quantify cybersecurity frameworks while accounting for cyber-physical interactions into account.

In the first paper, *Analyzing the Instability of the Core Components of Software Projects,* authors Lerina Aversano, Daniela Guarda, and Maria Tortorella note that software architecture is an artifact of how the initial concept of a software system has been actually mplemented. Continuous changes imply the modification of the software system that could impact its architecture. Architecture stability information refers to a nonfunctional attribute that is significant for a software engineer, and measures the aptitude of a software system to evolve without changing its architecture. The authors use metrics for measuring the architecture instability of the core components of software system across different releases. They analyze how the architecture of a set of core components of a software system evolves with respect to the whole system and investigate the factors determining the instability. The aim is to verify if the architectural instability of the core components decreases across releases, and to determine which factors influence it.

In the second paper, *Semi-symbolic Simulation and Analysis of Deviation Propagation of Feature Coordination in Cyber-physical Systems*, authors Michael Rathmair, Christoph Luckeneder, Hermann Kaindl and Carna Radojicic present a semi-symbolic modeling approach based on Affine Arithmetic Forms. This approach allows the representation of uncertainty in terms of ranges. Simulations of such models directly include propagation of deviations within the defined ranges, and their traceability. This paper presents a semi-symbolic model of a cyber-physical system including the coordination of safety-critical and interacting features. This model includes two different behavioral modes and their integration (for feature coordination). This involves representing discrete uncertainty. Based on this model, a single simulation run is presented showing the effects of several deviations. The modeling approach presented facilitates specific analyses of deviations based on traceability information.

URI: http://hdl.handle.net/10125/50595
ISBN: 978-0-9981331-1-9