CAREER: Formal TOols foR SafEty aNd Security of Industrial Control Systems (FORENSICS)

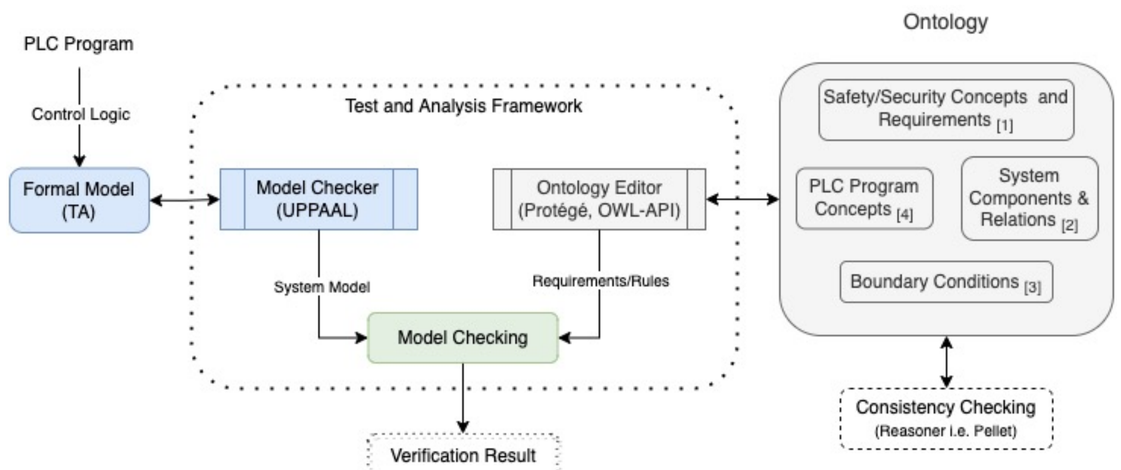
BOISE STATE UNIVERSITY
COLLEGE OF ENGINEERING
Department of Computer Science

Dr. Hoda Mehrpouyan Boise State University

The research provides algorithms and tools to improve the safety and security of Industrial Control Systems (ICS), which are complex and highly interconnected software and hardware systems. These systems are considered critical and essential for the well-being of the society. Hence, any type of cybersecurity threat can result in significant destruction, affecting millions of people. Considering the seriousness of the consequences, it is essential to develop an understanding of: 1) how to integrate safety and security requirements into the control software, 2) how to design and develop tools that are capable of observing large data streams of the physical processes and detect anomalous behavior.

<u>Formal Verification and Validation of Safety and Security Requirements of Industrial Control Software:</u>

The development of the security knowledge-base that can serve as a reference security ontology for the security requirements of the industrial control software and an automatic verification and validation engines that are able to check the correctness of the logic with regards to these requirements will result in a safe and secure industrial process



An ontology that is based on Description Logic (DL) is designed and developed. The proposed ontology is designed to include 1- safety/security concepts and requirements, 2- system components (sensors, actuators, etc.) involved in the control logic, 3- several boundary values and conditions, and 4- PLC program concepts (input/output, variables, etc.). The consistency check of safety and security specifications are check by the reasoners such as Hermit or Pellet.
The second part of the solution is utilizing a model checking framework in which the PLC program is modeled as networks of Timed Automata (TA) and the security specifications are modeled in Timed Computational Tree Logic (TCTL) formulas. Translation of the specifications from ontology to the TCTL is based on Specification Pattern System (SPS) via *Semantic Web Rule Language.*

This work will provide knowledge base and tools for understanding how safety and security could be integrate into industrial processes and critical infrastructures, a question of increasing public concern in both the U.S. and abroad.

We have been able to *train a cross-disciplinary (computer Science, Electrical Engineering, and Mechanical Engineering) undergraduate/graduate students in cybersecurity with emphasis on Industrial Control Systems*

This work will enhance examination of attack/defense impacts in other fields such as electrical engineering, control engineering, and system theory studies. Methods and findings will be extensible to additional applications such as cyber-physical systems and Internet of Things (IoT).

Award ID#: **1846493**