Framework for Trustworthy Lifecycle Modeling of Cyber Physical Systems using Formal Methods

Project Description

A significant factor that leads to compromised computer systems is design and implementation flaws in the software components, and the ways they are connected to create a system. Existing works in software fault detection face challenges in ad-hoc approaches and domain-specific requirements. This project aims to identify and detect security flaws in Programmable Logic Controller (PLC) software throughout the lifecycle of development. We design a framework, ***tfCPS***, that enables security property generation, automatic property verification (flaw detection), runtime data injection attack detection, and trustworthy maintenance in a decentralized network. The architecture of tfCPS is demonstrated in Figure. 1. PLCs take input from sensors, then use the input to execute the software logic, and finally produce output to control the physical plant. The lifecycle of each PLC contains four stages including specification generation, development, runtime testing, and maintenance. A remote supervisory component, e.g. SCADA, sends commands to monitor the PLCs.

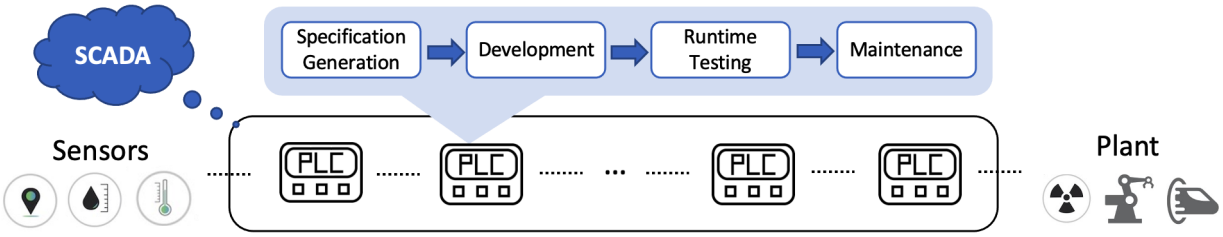

Figure 1. Overview of *tfCPS* architecture

Identified Needs Assessment

This proposal addresses the area of Secure Software Development and Lifecycle for Programmable Logic Controllers (PLC) with elements involving 1) the methodologies and testing that are used in the development of that system or software, 2) needs of vendors, and system integrators**,** and 3) a product lifecycle definition involving the specification generation, development, runtime testing, and maintenance.

Additional Needs Assessment

PLC devices become intensively involved in the Industrial Internet of Things (IIoT), relying on cellular communication with cloud-based systems such as SCADA platforms. Additionally, this proposal aims to investigate how Blockchain technologies should be integrated, and what are the benefits and (importantly) risks of that integration, towards trust and resilience of the system faced with cyber threats.

Broader Impacts

This research has the broader impacts of (1) Disseminate research findings through journal and top conference publications, (2) Community engagement, especially with local energy company collaboration, and (3) More secure and competitive OT system and software products.

Project Duration

24 months