# Mitigation of Industrial Control System Attacks Using A Boosted Filter Ensemble

{ Kelvin Ly, Andrew Hughes, Jacob Hazelbaker, Orlando Arias and Faculty Advisor: Yier Jin}
University of Central Florida, Department of Electrical and Computer Engineering

## Objectives

Industrial Control Systems (ICS) are all too often composed of legacy hardware which was not designed with security in mind. The goal of our research is to create a defense system which will will be compatible with the majority of the ICS hardware utilized in power plants, water facilities, and other industrial settings.

## Introduction

The ICS defense system we developed interfaces with multiple Programmable Logic Controllers (PLC) in parallel for redundancy. Communications to the PLCs are analyzed by the defense system to determine if signal is valid or is indicative of a cyber attack. This is done via a variety of machine learning algorithms.

## High-Level Architecture

OpenPLC was installed on a Raspberry Pi to simulate how a real PLC might respond to inputs. MATLAB Simulink was installed on the laptop computer to simulate the various sensors which would be found throughout an ICS.

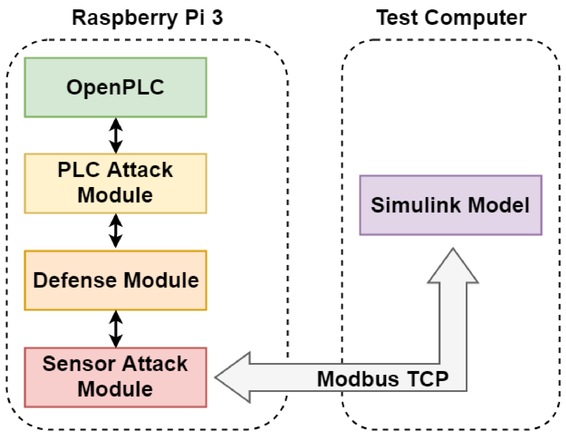


**Figure 3:** Overview of Test Framework

Communication between the laptop computer and the Raspberry Pi was moderated by the Intrusion Detection System we developed which uses machine learning to determine if the input data to the PLCs are valid or potentially indicate a cyber attack is underway.

## Intrusion Detection System

The IDS consists of several machine learning classifiers, with final result being adaptively weighted based on the IDS learning which classifiers are most accurate for a given control system. This allows the IDS to adjust itself to provide good accuracy for a large variety of control systems.

Three PLCs are used to provide triple redundancy, and allows the system to be at least as effective as triple redundancy, as any detection capabilities will augment the security provided by the redundant PLCs.

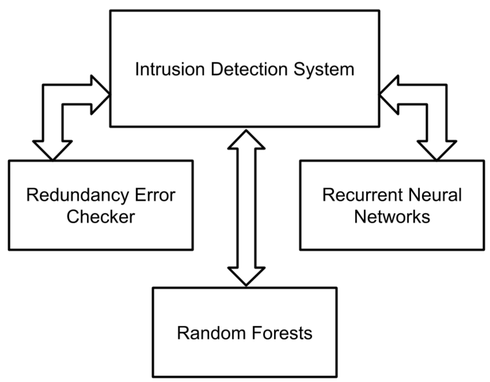


**Figure 4:** IDS Architecture

## Simulation Model

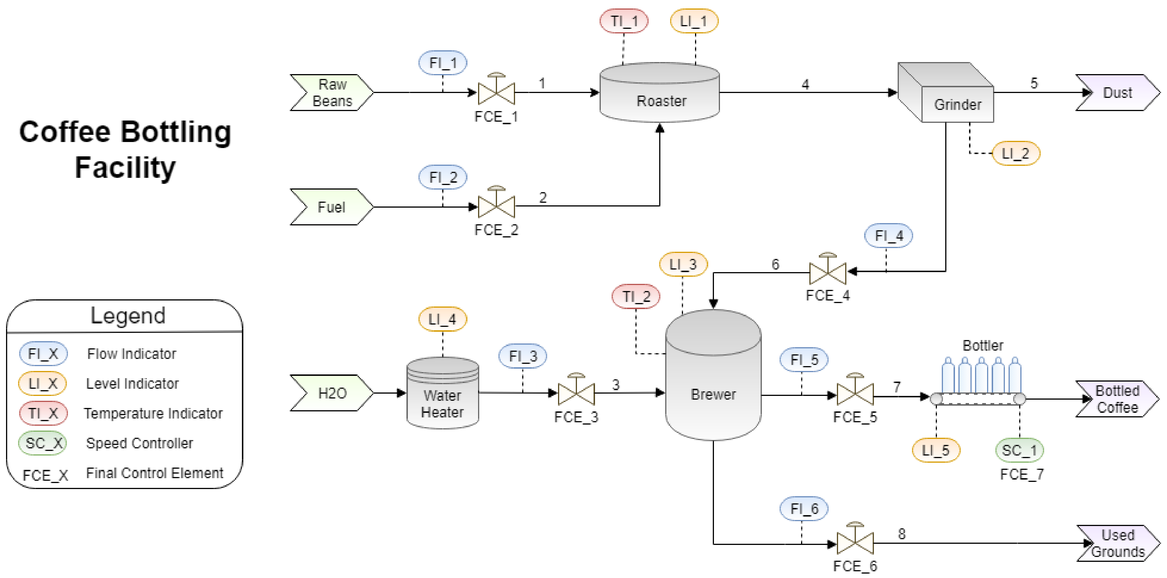


**Figure 1:** Process Flow Diagram (PFD) for the ICS

To provide a realistic simulation of a real-world ICS, we designed a coffee bottling facility. The PFD in Figure 1 above illustrates the industrial process of roasting raw coffee beans, grinding up the beans, brewing the grounds with hot water, and lastly filling bottles with coffee to sell in grocery stores and gas stations. This design is meant to serve as a modern alternative to the classic Tennessee Eastman chemical plant example problem. [1]

## Future Research

Beginning in January of 2018, we will transition our test environments to be more hardware-based and include far more PLC units.

We have recently purchased 20 UniPi 1 units for our future research. The UniPi 1 provides additional I/O for the Raspberry Pi 3, closely resembling the functionality of a PLC.

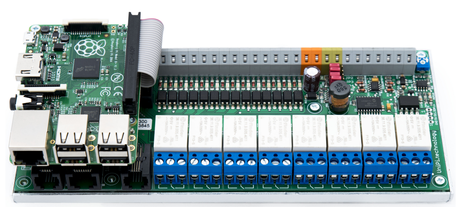

**Figure 2:** UniPi 1 Peripheral for Raspberry Pi [2]

## References

[1] J. J. Downs and E. F. Vogel. A plant-wide industrial process control problem. *Computers Chemical Engineering*, 17(3):123–456, 1993.

[2] Unipi-1.1-starter-kit. https://www.unipi.technology/unipi-1-1-starter-set-p122?categoryId=7. Accessed: 2017-11-09.

## Security in Silicon Lab

We are members of the Security in Silicon Lab (SSL) located at the University of Central Florida (UCF) and the University of Florida (UF). Our focus is on hardware security, specifically smart device security, IP core security, and cross-layer protection.

## Contact Information

**Web** http://jin.ece.ufl.edu
**Name** Yier Jin
**Email** yier.jin@ece.ufl.edu