CYBERSECURITY MODELING OF NON-CRITICAL NUCLEAR POWER PLANT DIGITAL INSTRUMENTATION

TREVOR MACLEAN

MICHAEL HANEY, PHD

R. A. BORRELLI, PHD

BACKGROUND

INTRODUCTION AND STATEMENT OF THE PROBLEM

- Nuclear Power Plants are experiencing digitization of control systems.
  - Controls are being updated from old analog to new digital methods opening up plant to cyber-attack.
- Nuclear Power Plant security tends toward the use of a multiple layered defense approach to plant operations.
  - “Defense in Depth” maintains safety at an increased cost or risk of lost energy production.
- Plant operations could be secured for any and all equipment deficiencies to maintain safety at all costs.
- A more efficient and operationally safe method would be to operate with real time detection and repair of system failure.
  - We will approach “Defense in Breadth” by using multiple Programmable Logic Controllers in a concurrent redundancy.

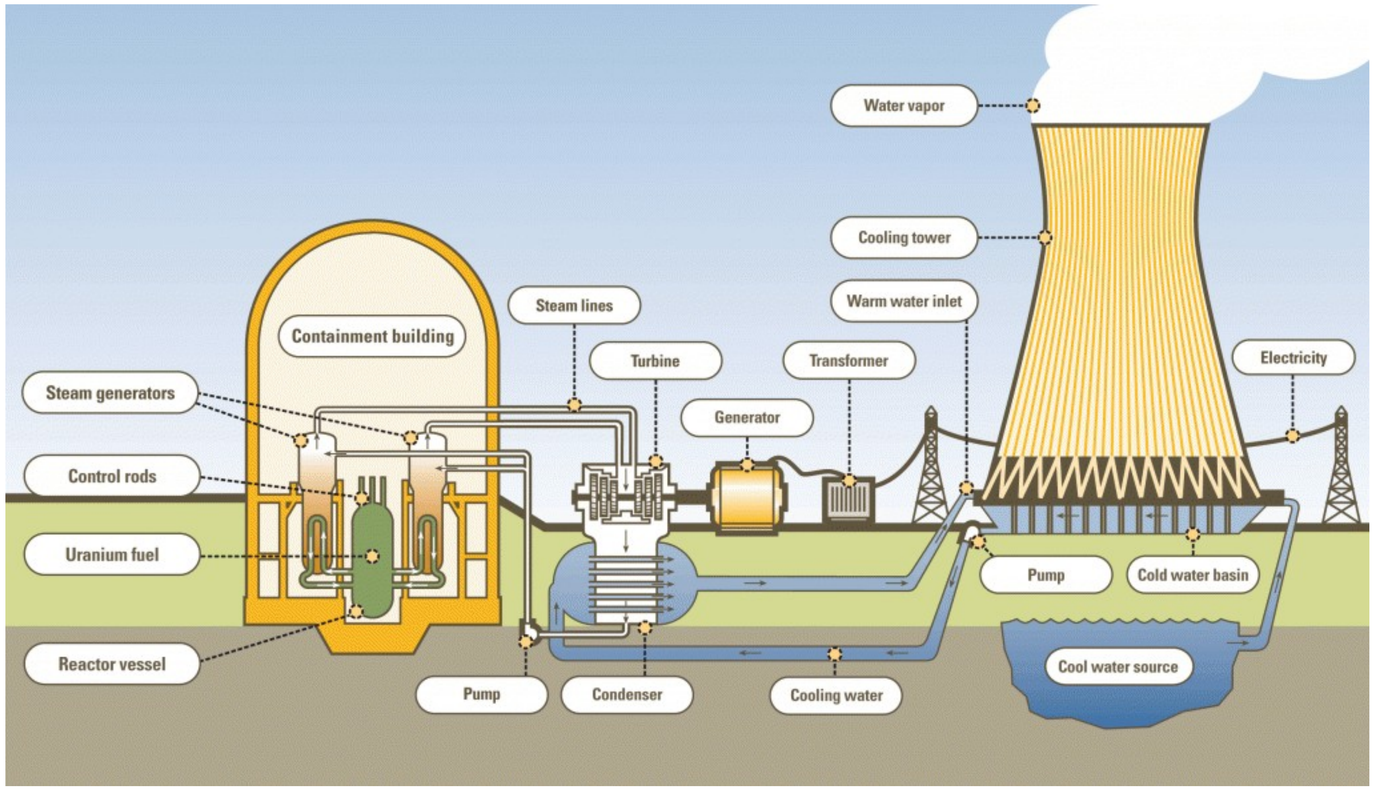
LITERATURE REVIEW

INITIAL REVIEW

- Methods of attack on Modbus and DNP3 communication protocols – 4 categories of attack
  - Intercepting Data
  - Interrupting Data
  - Modifying Data
  - Fabricating Data
- Zero-Day Vulnerabilities – Unknown vulnerabilities that can be exploited against a system with minimal warning.
- Historical cyber-attacks on Nuclear Power Plant industry
  - Davis-Besse Nuclear Power Plant
  - Browns Ferry Nuclear Power Plant
  - Iranian Nuclear Program – Stuxnet (Modifying Attack)

RISK ANALYSIS

RISK INFORMED SELECTION OF ATTACK PATH



Began with an initial overview of a Nuclear Power Plant identifying potential components and control systems.

Some systems identified:

- Condenser
- Plant Balance
- Turbine
- Electric Generator
- Steam Generator
- Nuclear Reactor
- Pressure Vessel
- Boron Monitoring
- Radiation Monitoring
- Spent Fuel Pool
- Switch Yard
- Cooling Tower

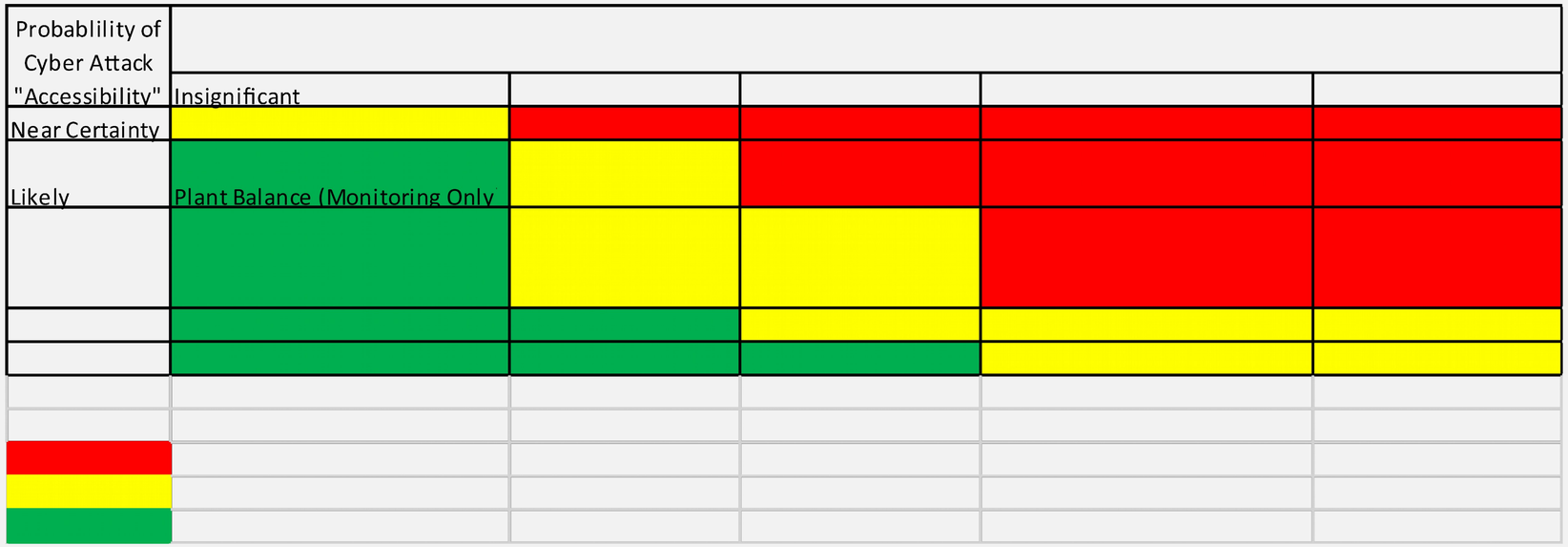
RISK ANALYSIS

RISK MATRIX

Through the use of a risk matrix comparisons between the different identified components and control systems can be made.

Our risk matrix compares the Probability of Cyber Attack (Accessibility) to the Severity of the impact the proposed event would have.

Once organized, Plant Systems with High Risk are identified in Red, in upper right side of the matrix, and became the focus of the project.



LITERATURE REVIEW

FOCUSED SCOPE ON HIGH RISK SYSTEMS

With a large emphasis on critical systems, non-critical systems can be left vulnerable to cyber-attack.

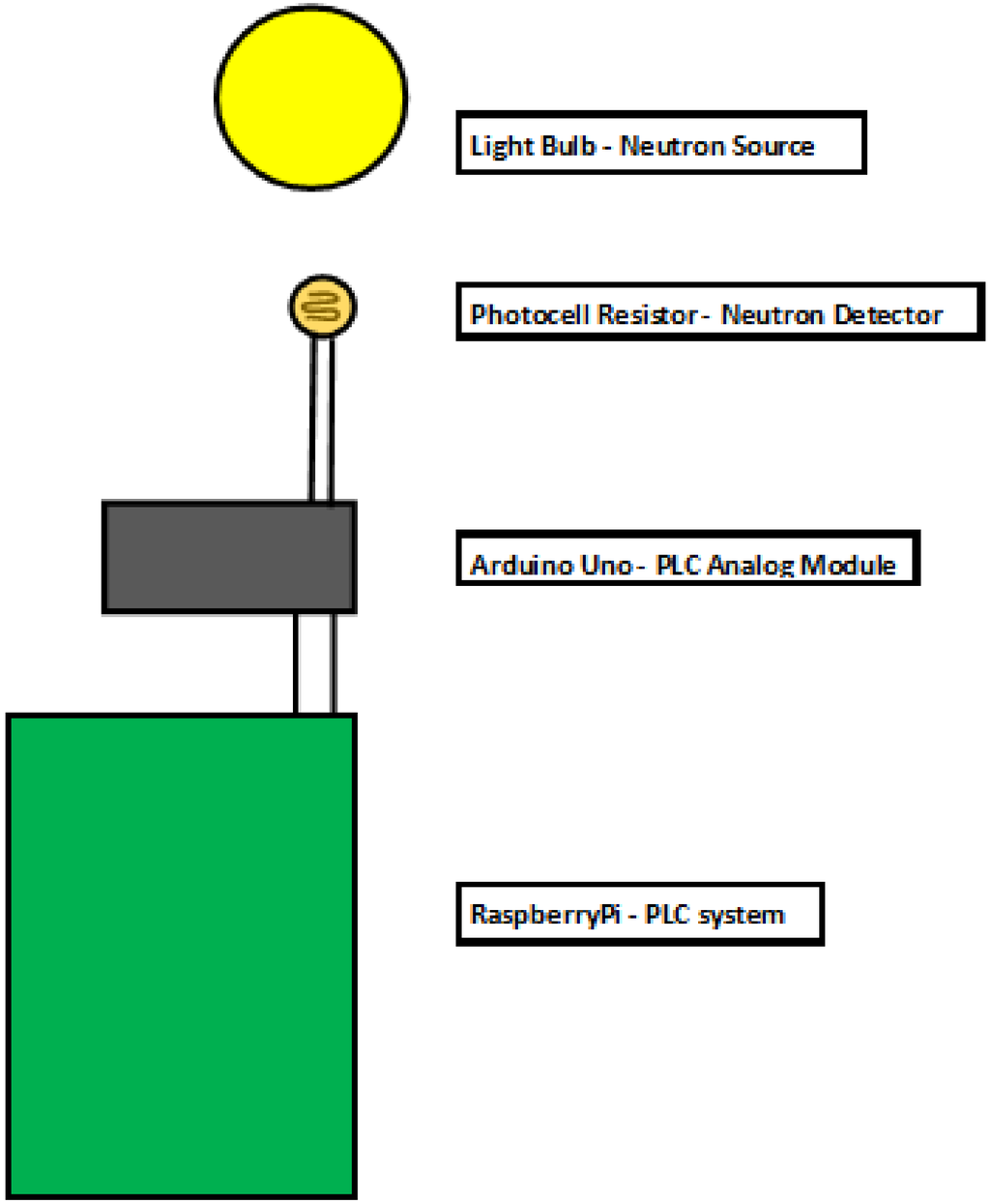
With this in mind we examined systems that would have low impact on the environment but could have a severe impact on plant operations.

Through this analysis we narrowed scope to 4 systems and reviewed publicly available information about each systems.

- Spent Fuel Pools
  - Found passively cooled pools and therefore no control system needed.
- Boron Monitoring System
  - Identified commercially available systems from Rolls-Royce and Mirion Technologies.
- Balance of Plant
  - Reserved for future analysis
- Switchyard
  - Reserved for future analysis

BORON MONITORING SYSTEM

SYSTEM BREAKDOWN

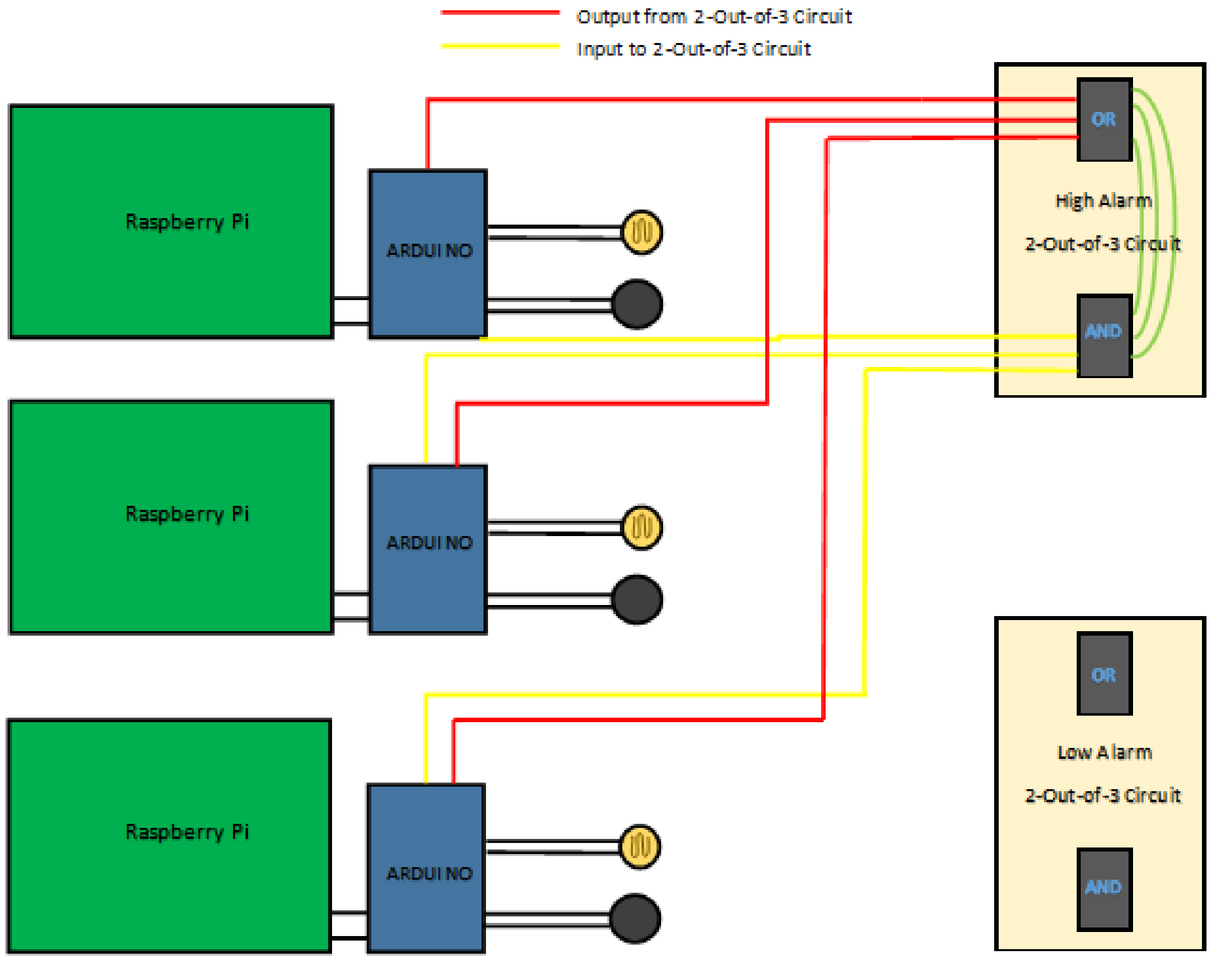


The basic components of the Boron Monitoring Systems reviewed consisted of:

- PLC control system
- Neutron Source
- Neutron Detector

For our model we decided on Opensource hardware and software. Hardware used were RaspberryPis and Arduino Unos. The software used is a combination of OpenPLC and ScadaBR

EXPERIMENTAL SETUP



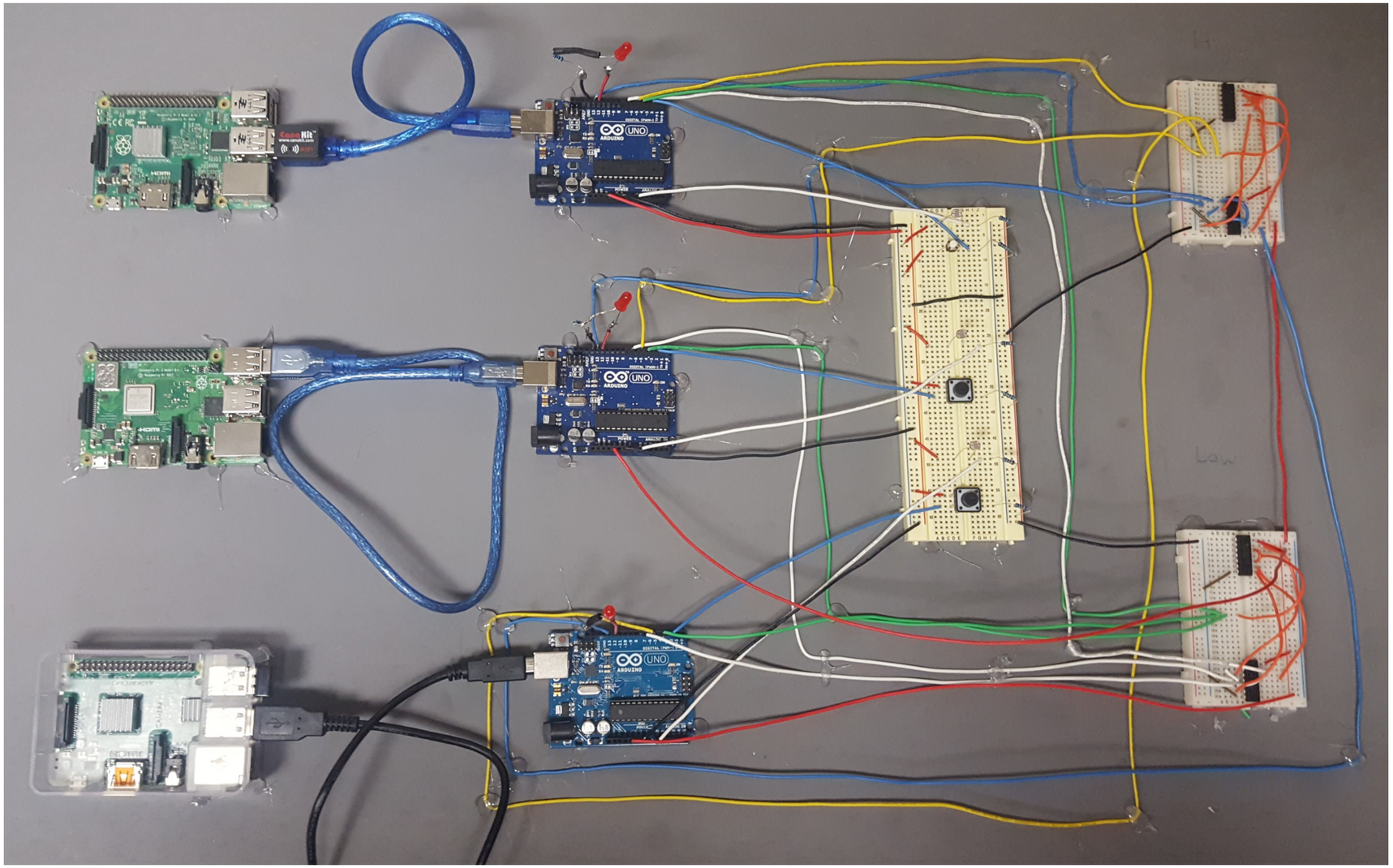
2-OUT-OF-3 CIRCUIT PROOF OF CONCEPT

To mitigate the risk of cyber-attack implementation of digital-analog hybrid systems have been implemented.

To demonstrate the effectiveness of a digital-analog system we implemented a 2-out-of-3 circuit on our proposed Boron Monitoring System.

EXPERIMENTAL SETUP

PHYSICAL TESTBED



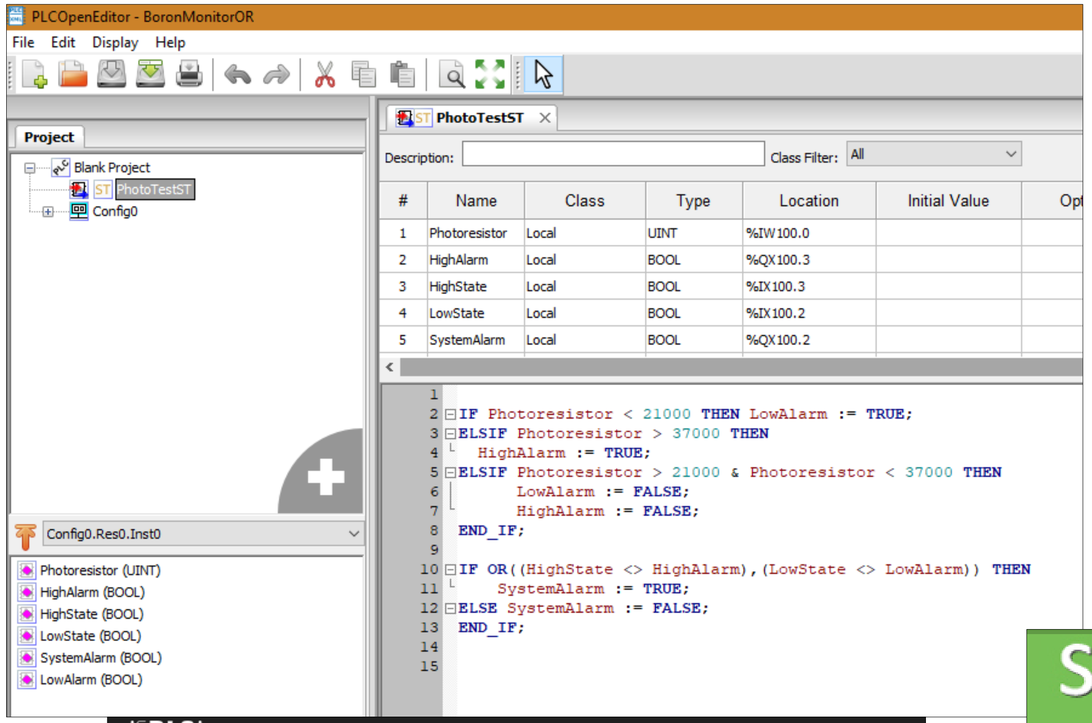
SOFTWARE

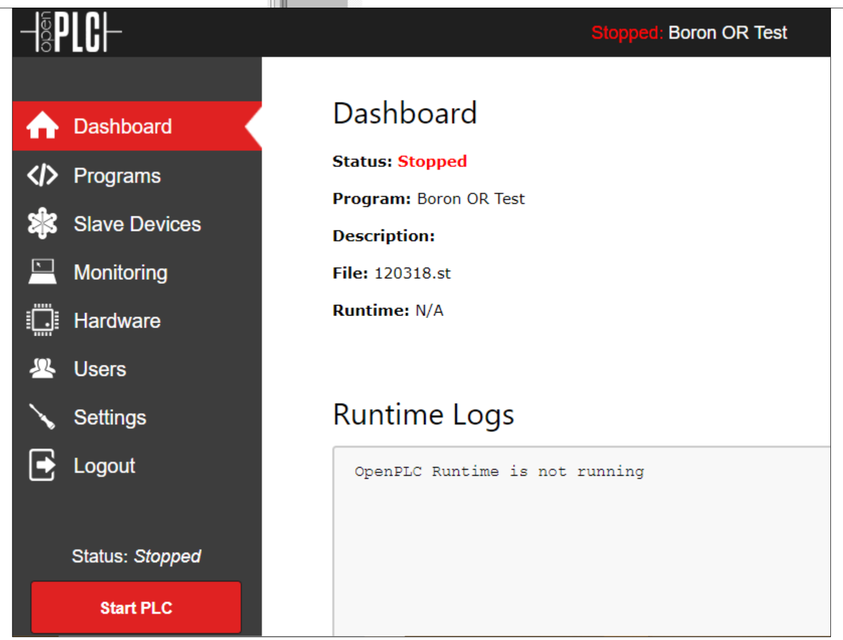
PROGRAMS USED FOR ANALYSIS

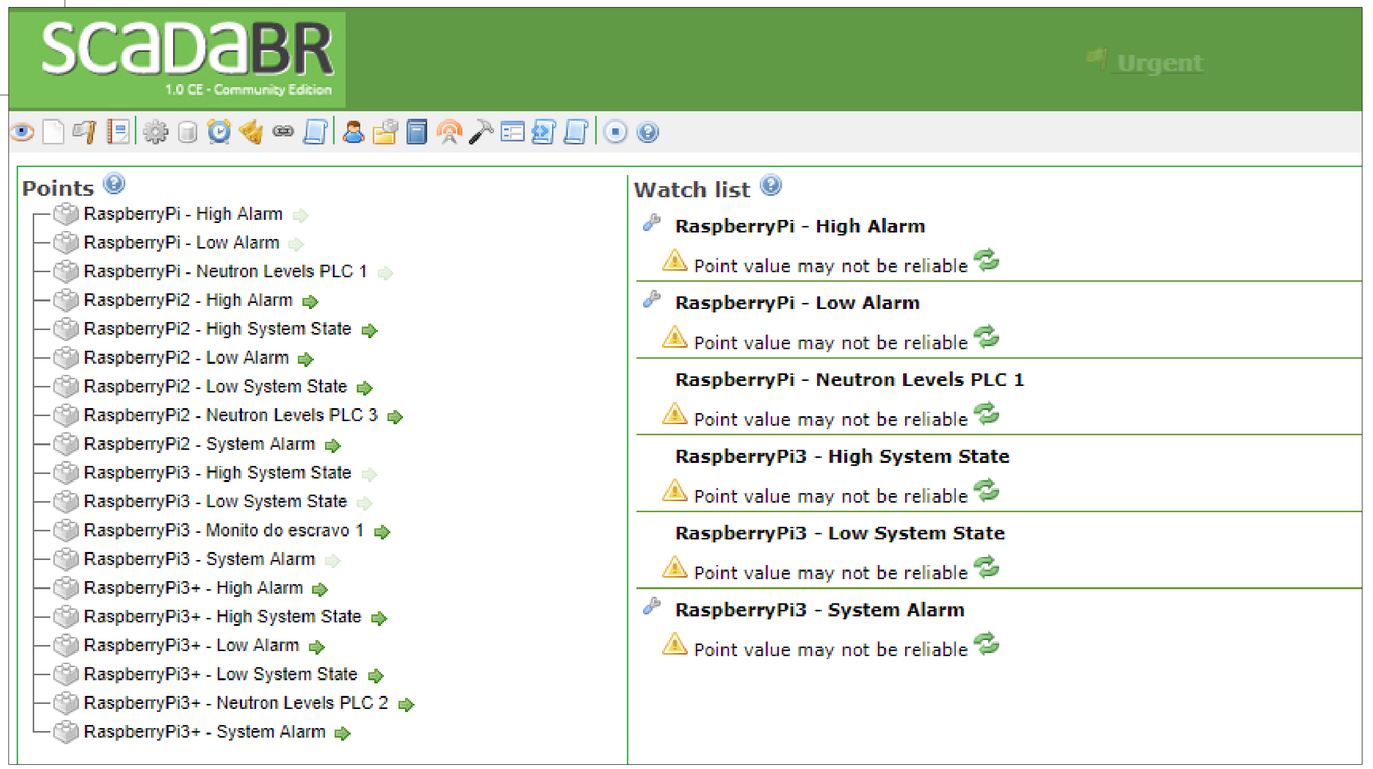
Top Left – PLCOpenEditor (PLC program text editor)

Bottom Left – OpenPLC (Control environment for RaspberryPi PLCS)

Bottom Right – ScadaBR (used for HMI and data collection)

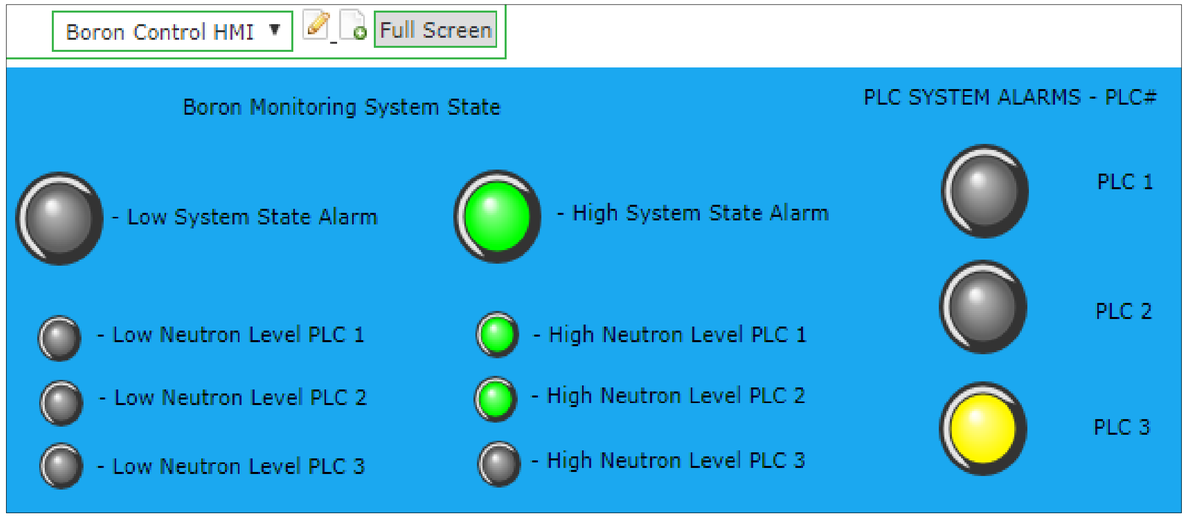




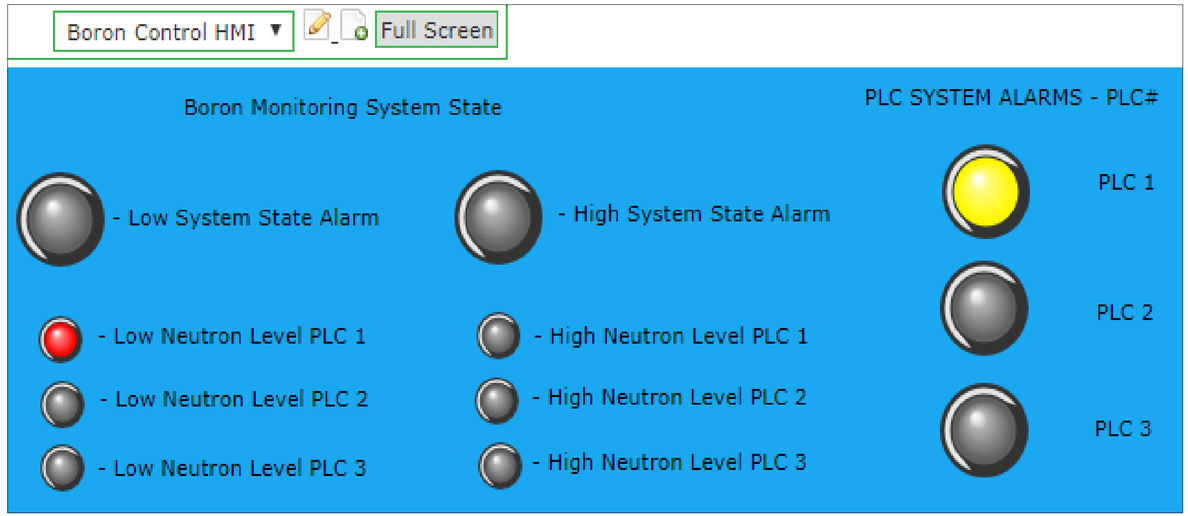


HUMAN MACHINE INTERFACE (HMI)

EXAMPLE HMI FOR SYSTEM STATE ALARMS



Two High Alarms. PLCs 1 and 2 received extra light. PLC 3 did not match the other PLCs therefore PLC 3 System Alarm triggered.



Active Cyber-Attack. PLC 1 has an active cyber-attack causing a Low Neutron Level alarm on PLC 1. Rather than the BMS diluting the boron concentration, the System Alarm for PLC 1 is triggered due to the disparity between PLC 1 and PLCs 2 and 3.

FUTURE WORK

- Develop testbed on a commercial PLC system. (Repeat current experiment for validation)
- Model other cyber-attacks against the identified Non-critical Nuclear Power Plant Systems
- Implement other cyber-attack mitigation methods
- Develop a self-healing protocol for identified compromised systems