Virtualizing Industrial Control Systems Testbeds for Cybersecurity Research

ACSAC ICSS 2016

Rishabh Das
Thiago Alves
Dr. Tommy Morris

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Overview

Problems:

- Industrial Control Systems are too big to fit in a lab
- ICS Cybersecurity researchers rely on small testbeds to collect data
- Small testbeds may not have all the data required for cybersecurity research

Accomplishments:

- Create a high fidelity virtual copy of a physical SCADA system
- Compare results between the physical and virtual testbeds during normal and attack conditions
- Scale up the virtual testbed to model a full-size ICS

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

SCADA Components

Physical System
(sensors and actuators)

Wire bridge
Analog and
digital I/O

Programmable Logic Controller
(PLC)

Network /
SCADA Protocol

Human-Machine
Interface

THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

First Example
Gas Pipeline Testbed

THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

Physical System

Characteristics:

One inch diameter pipeline network

Four 90° pipe bends

Two T-joints.

Positive displacement pump connected to a 0.5 Hp 1Φ 120 Volts induction motor

Sensors:

Analog pressure sensor

Actuators:

Relay - Turn pump on and off

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Wire Bridge - Analog and Digital I/O

- Sends sensor signals to the controller
- Sends controller commands to the actuators
- Electrical communication between the controller and its physical interfaces

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

PLC - Programmable Logic Controller

- Digital computer used on automation
- Input modules read data from sensors
- User program decides what to do based on the input data
- Output modules control actuators on the industrial plant

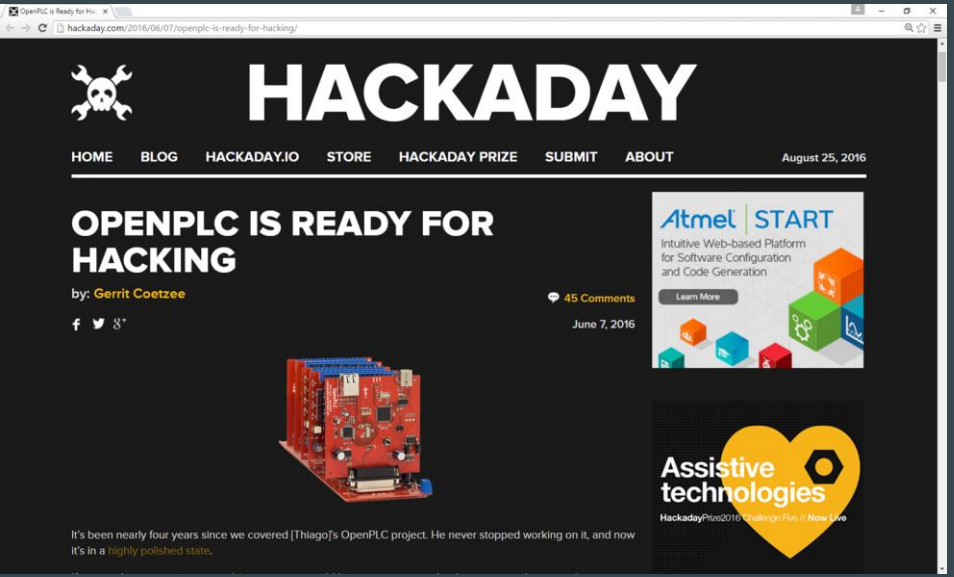
THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

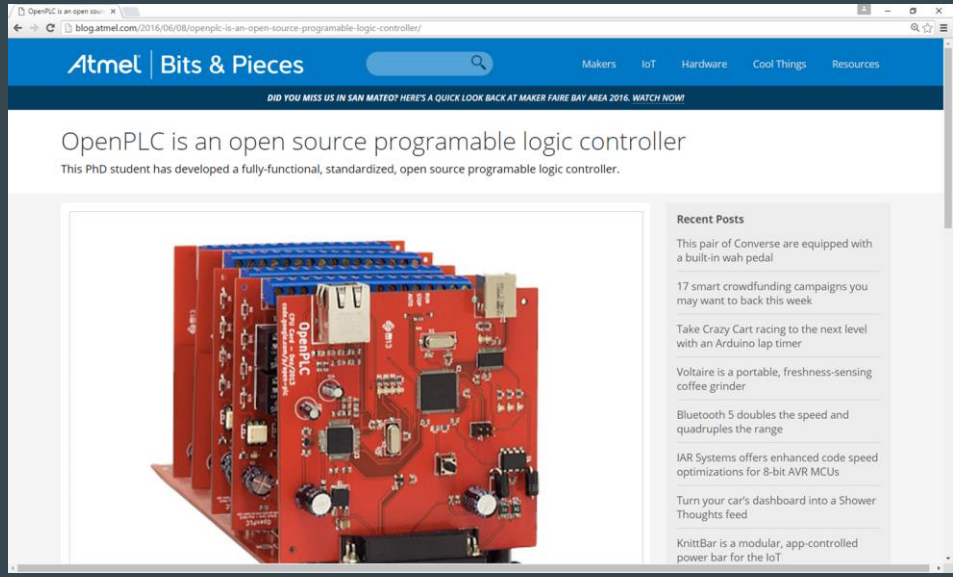
OpenPLC - An Open Source Industrial Controller

http://www.openplcproject.com

Valuable research tool since entire source code is available online

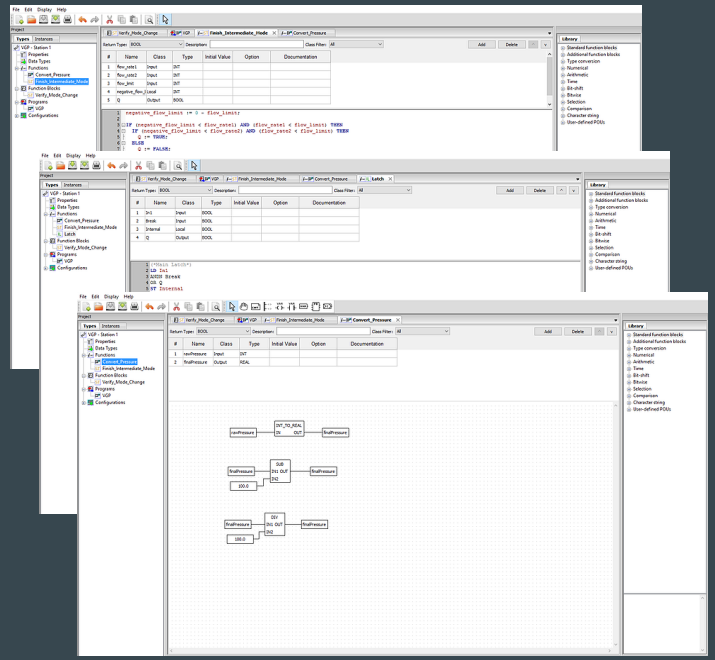
OpenPLC - An Open Source Industrial Controller

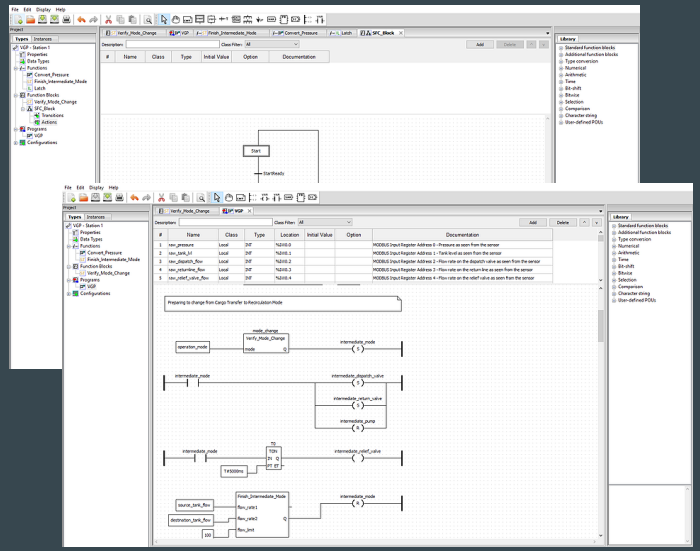




THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

OpenPLC - An Open Source Industrial Controller





Supports all five IEC 61131-3 programming languages

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

OpenPLC - An Open Source Industrial Controller

Compatible with Modbus/TCP SCADA

THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

OpenPLC - An Open Source Industrial Controller

Supported platforms

Raspberry Pi

UniPi

PiXtend

ESP8266

Arduino

Windows (soft-PLC)

Linux (soft-PLC)

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

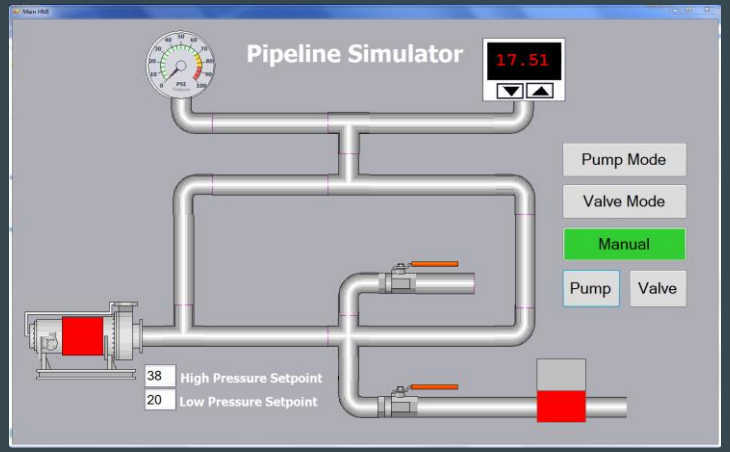
OpenPLC - Multiple platform support

Very easy to port to another platform

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

HMI - Human Machine Interface

- Built in C# using the EasyModbusTCP library
- Uses Modbus/TCP to communicate with the PLC
- Queries PLC for data every 100ms
- Display status on the screen



THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Virtualizing the Gas Pipeline Testbed

THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

SCADA Components Virtualized

Physical System
(sensors and actuators)

Wire bridge
Analog and
digital I/O

Programmable Logic Controller
(PLC)

Network /
SCADA Protocol

Human-Machine
Interface

SCADA Components Virtualized

Physical System
(sensors and actuators)

Wire bridge
Analog and
digital I/O

Programmable Logic Controller
(PLC)

Network /
SCADA Protocol

Human-Machine
Interface

MATLAB
SIMULINK

Model with virtual
sensors and actuators

UDP Packets

OpenPLC
(on a Virtual Machine)

Network /
SCADA Protocol

Human-Machine
Interface

SCADA Components Virtualized

Physical System
(sensors and actuators)

Wire bridge
Analog and
digital I/O

Programmable Logic Controller
(PLC)

Network /
SCADA Protocol

Human-Machine
Interface

MATLAB
SIMULINK

Model with virtual
sensors and actuators

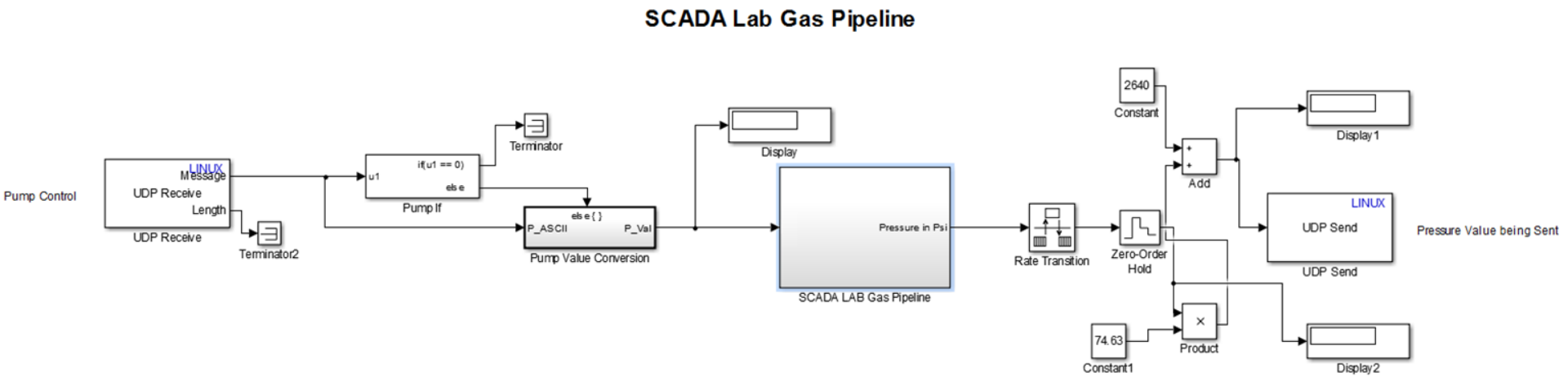
UDP Packets

OpenPLC
(on a Virtual Machine)

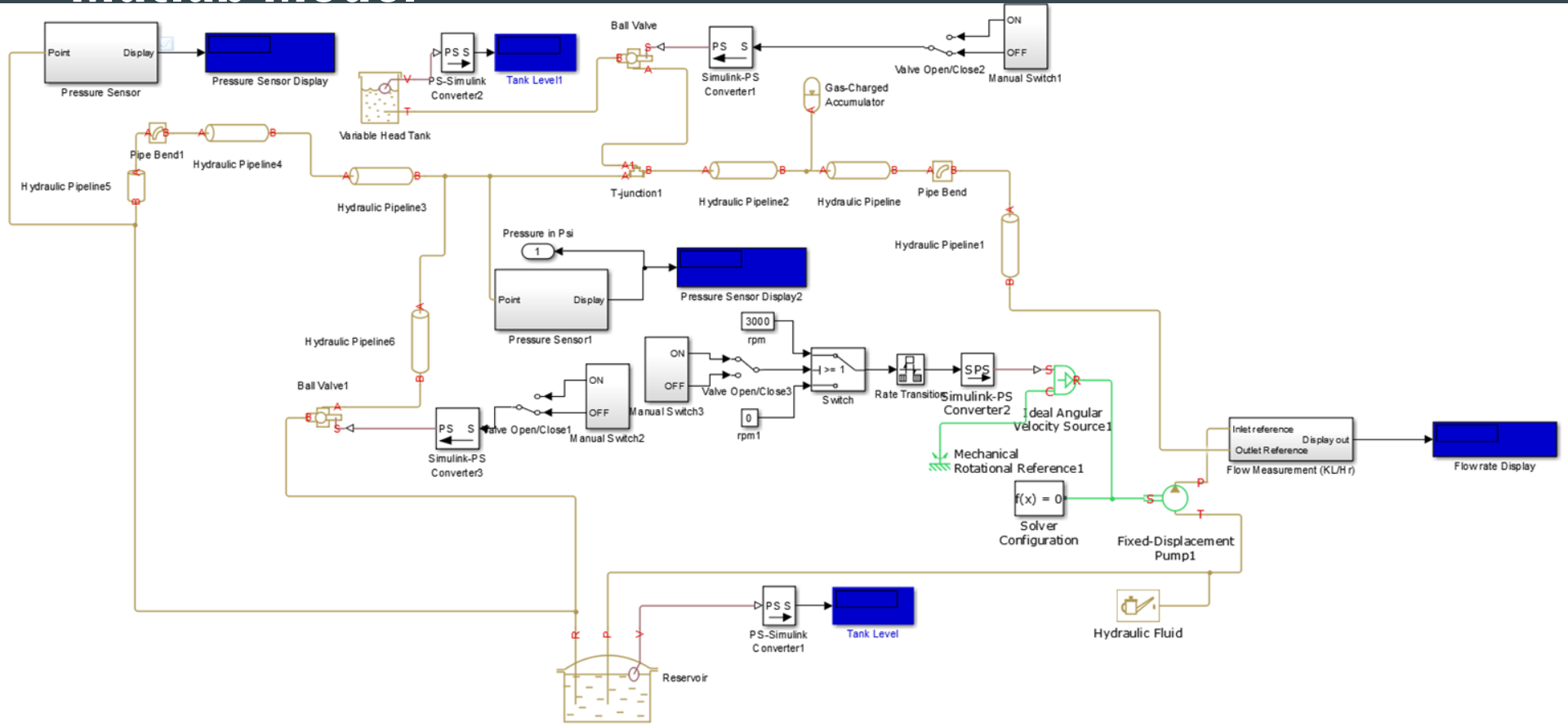
Network /
SCADA Protocol

Human-Machine
Interface

Matlab Model



Matlab Model



Other Examples Using the Same Approach

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

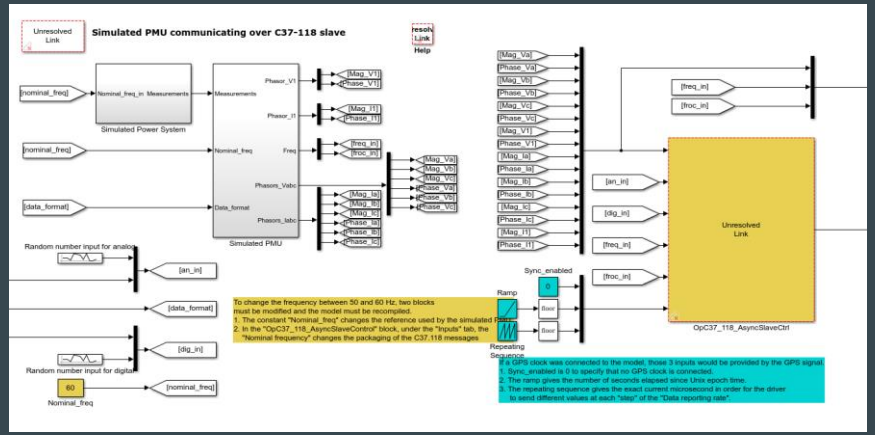
Water Storage Tank Testbed

- Tower: 40cm height x 20cm diameter
- Total volume: 0.0126 m^3
- Constant flow rate pump to fill the tower
- One outlet valve for water distribuition

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Power System

- 9 Bus Standard IEEE Power System
- 18 Simulated Relays with auto reclose
- Each relay can be controlled over Modbus
- 1 PMU Unit with C37-118 protocol support



THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Virtual Gas Pipeline Testbed Fidelity Evaluation

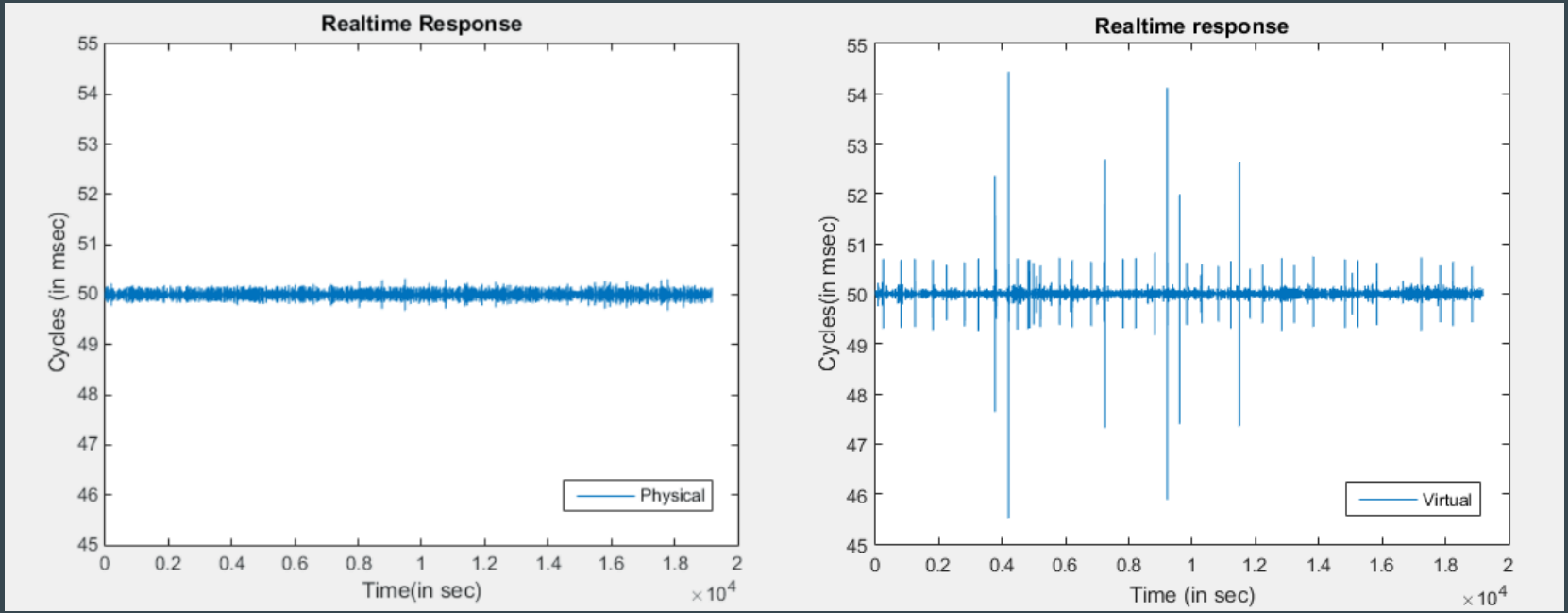
THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

Performed Tests

- Real-time response
- Pressure rising curve
- Pressure discharge curve
- Man-in-the-middle attack

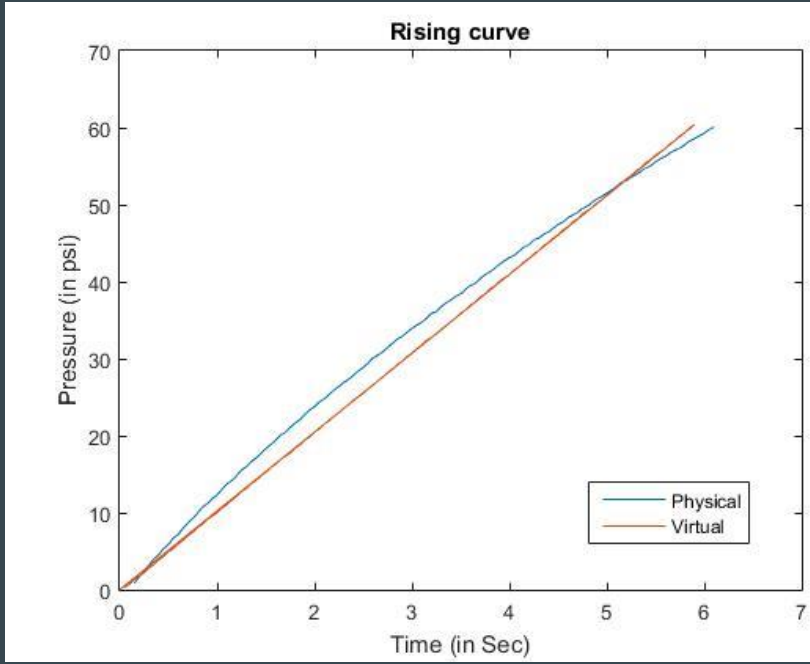
THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

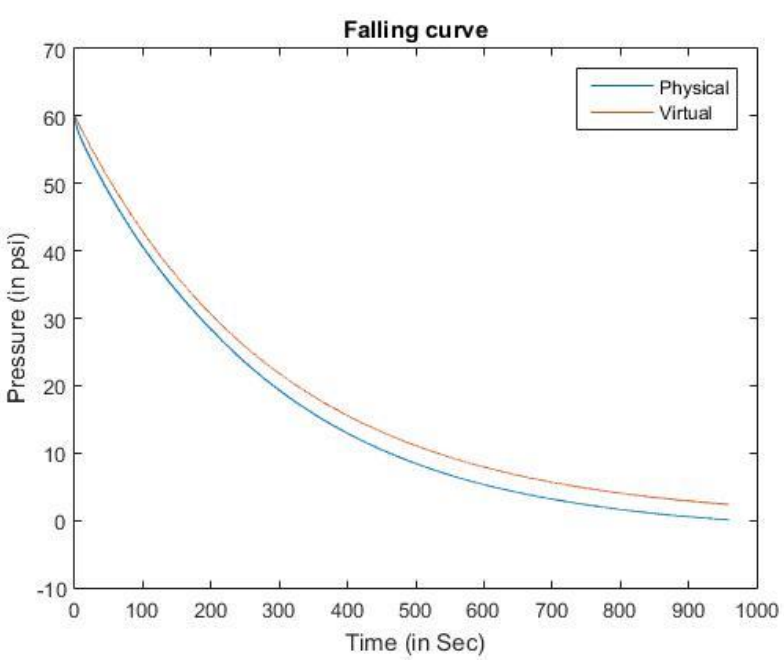
Real-Time response of the OpenPLC



THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

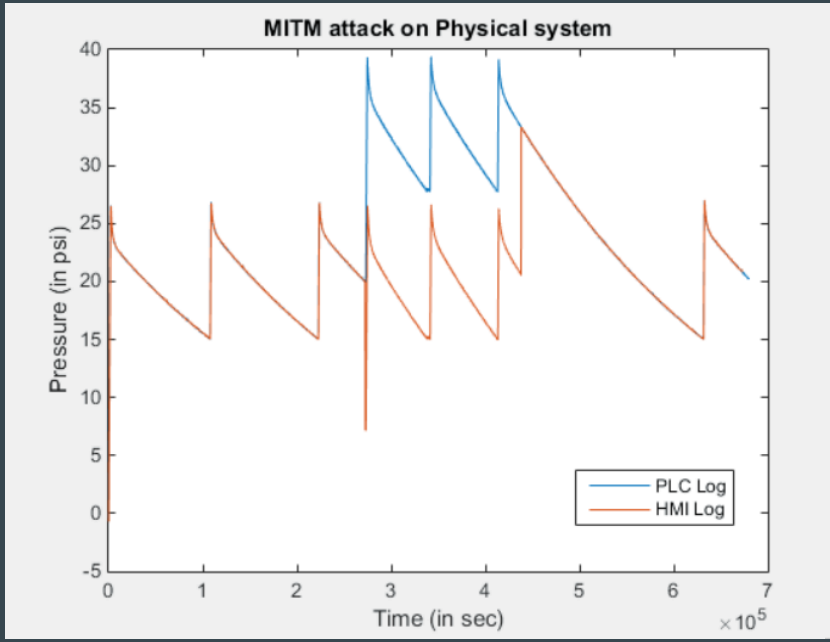
Comparison Results - Pressure Characteristics

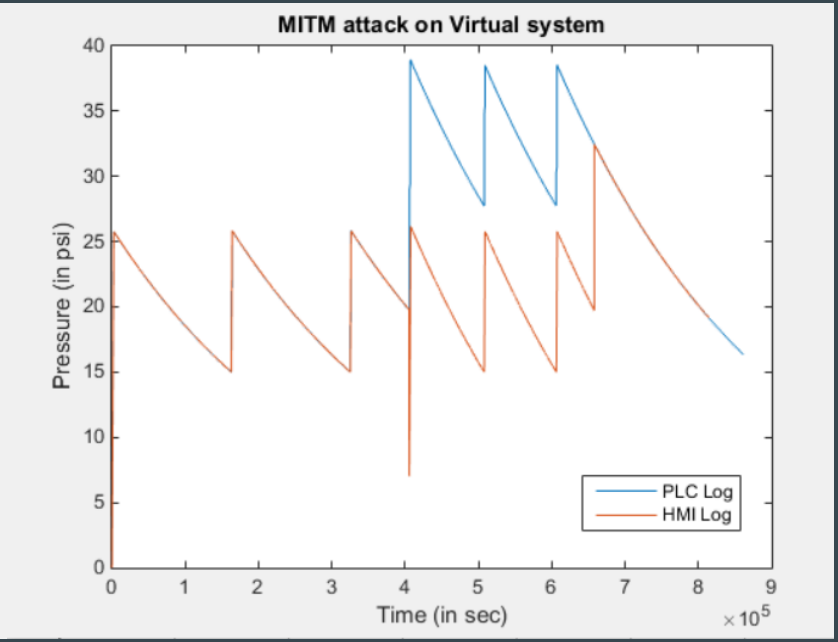




THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Comparison Results - Attacks (MiTM Injection)



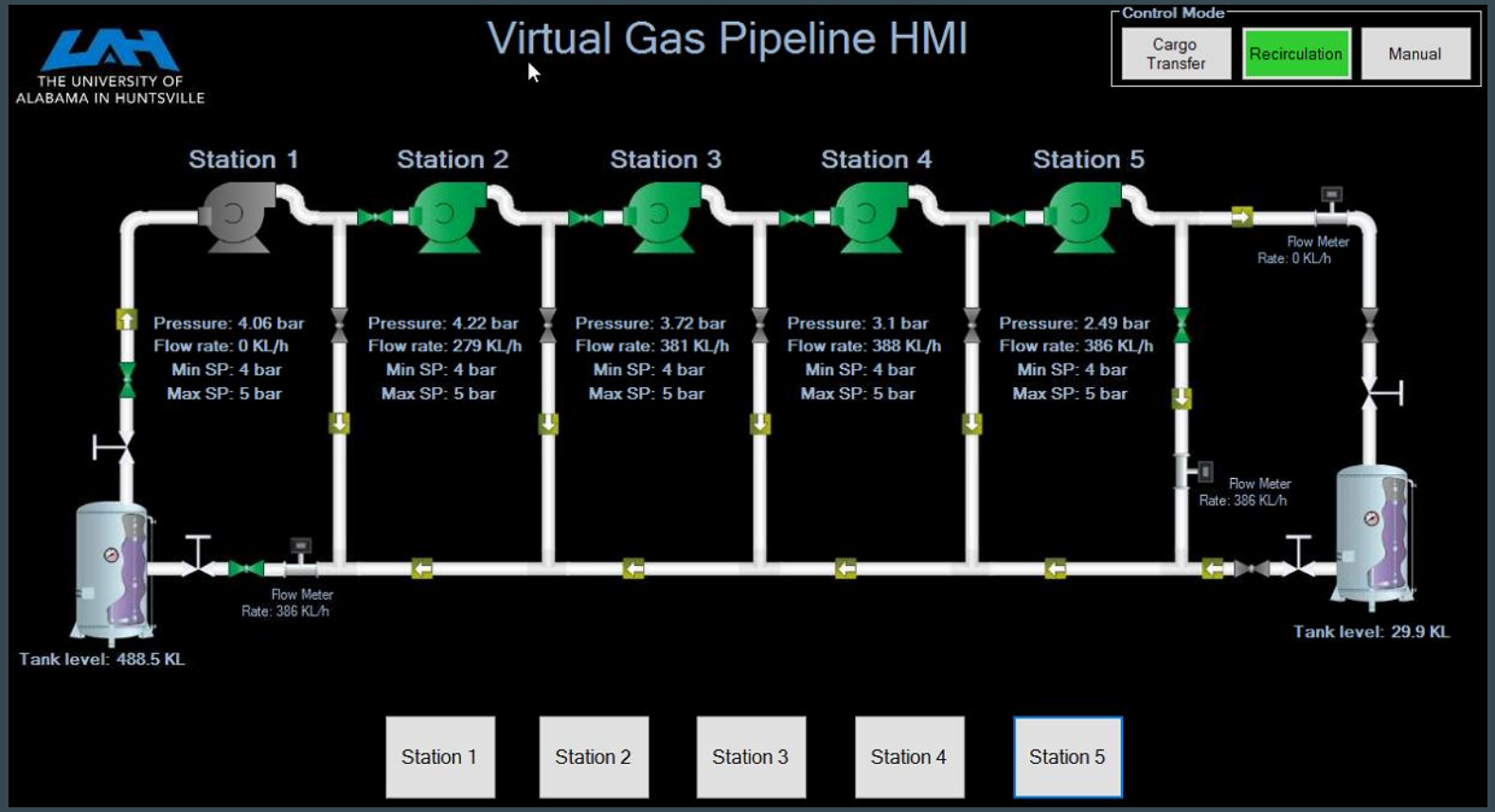


THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Expansion of the Virtual Gas Pipeline

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

Virtual 15km Pipeline Testbed



Questions

?

THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE