Contract No:

This document was prepared in conjunction with work accomplished under Contract No. 89303321CEM000080 with the U.S. Department of Energy (DOE) Office of Environmental Management (EM).

Disclaimer:

Portable Industrial Control Systems Simulator

Project Start and End Dates
Project Start Date: 10/1/2019
Project End Date: 10/30/2021

Project Highlight
To develop a virtual industrial control system environment model that can be utilized for both training, research, and development for critical infrastructure cyber protection. The system will be used for optimizing and improving network mapping of OT networks for future cyber security projects.

Project Team
Principal Investigator: Klaehn Burkes
Team Members: Harrison Howell, Ajay Tiwari, Dillon Tauscher
External Collaborators:

Abstract
Industrial Control Systems (ICS) are more integrated than they have ever been before, but also the division between IT (Information Technology) and OT (Operational Technology) is becoming a grey area. As the integration of IT and OT occurs more often, cyber attack will also increase. Cyber attacks on Critical Infrastructure can be highly detrimental to society, notably via compromised Industrial Control Systems (ICS). Virtual and physical simulation has been used in medical fields, mathematics, architecture, aeronautics, space, and many more. Virtualization & Simulation in a lab environment is ideal because there is a need for the ability to test theories and designs is a safe and cost-effective way without risking equipment damage or, more importantly, human life. Furthermore, OT and ICS are some of the most difficult systems to use for research and development. They are either committed to operations or widely expensive to set up in a life-like environment. Virtualization and simulation will allow these otherwise accessible systems to be a test bed for the training, development, and research of SRNL customers or engineers and scientists at SRNL. This will allow the testbed to fit into a small form factor and interact with a simulator with minimum hardware components for easy transports and replication effort within the environment.

Objectives
- Every component will be virtualized except for the PLC.
- This will be accomplished through utilization of one server running HyperV.
- This will then create virtual servers for GE SCADA.
- Another Virtual PC will be running FactoryIO.
- A single software defined network switch will be utilized to define different access points within the network.
- A Schneider Modicon PLC will control FactoryIO through Modbus communication.
- Integrated into a portable rugged container that utilizes less that 10U rack space.

REVIEWS AND APPROVALS

1. Authors:

Klaehn Burkes _____

Harrison Howell _____

Ajay Tiwari _____

Dillon Tauscher _____

Signature Date

2. Technical Review:

_____

Name and Signature Date

3. PI's Manager Signature:

_____

Name and Signature Date

4. Intellectual Property Review:

This report has been reviewed by SRNL Legal Counsel for intellectual property considerations and is approved to be publicly published in its current form.

SRNL Legal Signature

_____

Name and Signature

Introduction

Industrial Control Systems (ICS) and Operational Technology (OT) merging as a unified system has become a target of foreign adversaries and a rapidly growing vulnerability for the United States. Our critical infrastructure, from chemical manufacturing to city street lights, are controlled by these technologies. Commercial entities have been racing to add intelligence to these systems to provide efficiency, better control, and better data acquisition from these networks. This race has historically left cybersecurity concerns absent or as an afterthought from rigorous integration. This has led the US to a situation where our critical infrastructure technology has become smarter but significant security omissions have exposed our national infrastructure to malicious hacking and a viable target to U.S. adversaries. Security awareness is improving among both the users and developers of these technologies, but we are living in a landscape of dubiously secure devices, and completely insecure legacy devices. The nature of these systems creates major hurdles for addressing their security issues.

Virtual commissioning (SAT/FAT) is a process which allows a comprehensive evaluation of production systems before performing physical commissioning. The programmable logic controller (PLC) code can be debugged before using it in a real production system. A growing number of companies have recently started taking interest in this technology related to Industry 4.0 as it reduces the time and cost of introducing new products and different scenarios can be performed to validate the manufacturing for pedagogical applications.

This project will give SRNL a tool to rapidly develop these ICS/OT networks to then perform vulnerability assessments without impacting the operational system. However, the current methods for virtualizing OT environments are nonexistent, mainly focusing on IT virtualization. SRNL will perform research to advance these methods to apply to ICS environments that require real time control. This will require OT vitalization architecture development and deployment placing SNRL in a leading position in ICS/OT network analysis. The results of which will allow SRNL to deploy environments for education and future.

Approach

To accomplish this goal SRNL will collaborate with SRPPF to identify existing methods for designing ICS/OT environments, and identify gaps where methods are needed. The project will then proceed two ways; (1) SRNL will build a portable ICS System Simulator that can simulate a broad range of ICS/OT devices, while (2) also working with SRPPF and USACyS to define incident response scenarios. Successful completion of these two will give SRNL a tool to rapidly deploy ICS/OT networks to then perform vulnerability assessments without impacting the operational system. Three existing techniques will be the primary focus for fingerprinting: passive collection of packet traffic that can be parsed for device information (packet sniffing with backend parsing), semi-passive which identifies protocol structure to ascertain the device maker and device type and then attempts to communicate with the device directly in a controlled manner, and lastly any safe active methods that can be deployed. Network mapping will further evaluate packet data to determine depth of devices from the collection point and the types of interfaces between the collection point and network edges (i.e. the identification of firewalls or aggregators between the point of collection and a PLC controlling a mixer).

FACTORY I/O can also be very useful in training HMI (Human Machine Interface) design and programming, SCADA (Supervisory Control and Data Acquisition), MES (Manufacturing Execution

Systems) and even ERP (Enterprise Resource Planning) systems. The total interactivity with the environment, allowing the introduction of disturbances on the controlled plant and faults in sensors and actuators, is an important feature of this software. The possibility to build virtual plants enables one to create systems similar to real ones to be deployed in research laboratory. Hence, pedagogical virtual commissioning becomes a new way of conducting research, enabling to test in a first stage, without risk, controllers.

These techniques will be implemented onto a prototype portable ICS System Simulator specialized for a factory floor. This prototype will deploy to a pilot network (the pilot to be identified during collaboration) to map and fingerprint the network. This information will be used by the simulator to develop a virtual model of the network. SRNL will host this model network on our SRNL – Critical Infrastructure, ICS, and Cybersecurity laboratory.

Accomplishments

- Built a fully functioning mini version of the SCIIC and marketed at the Portable – Critical Infrastructure, ICS, and Cybersecurity Training system (P-CIIC) Figure 1
- System consists of a server, switch, firewall, and PLC.
- OT protocols deployed include Modbus Plus, DNP3, and Open Process Control (OPC)
- Capable of virtualizing OT networks with HyperV
- Simulating factory floor with Factory IO Figure 2
- Utilizing SCADA system allowing for operator screens and control of factory floor Figure 3

Future Directions

- Present capabilities of portable system to New Mexico Air National Guard and customize to a grid focused ICS simulator.
- Build 4 customized systems for SRPPF for FAT, and SAT compliance
- USACyS interested in utilizing 1 or 2 as part of cyber training before full week capstone projects at S-CIIC.

FY 2021 Peer-reviewed/Non-peer reviewed Publications

Intellectual Property

Licensing on the Portable ICS Simulator is being submitted by SRNL legal

Total Number of Post-Doctoral Researchers

None

Total Number of Student Researchers

None

Include all images, charts and figures with captions, as shown below.

Figure 1: PCIIC connected to a Monitor in SCIIC

Figure 2: FactoryIO simulating a manufacturing process being controlled by a PLC

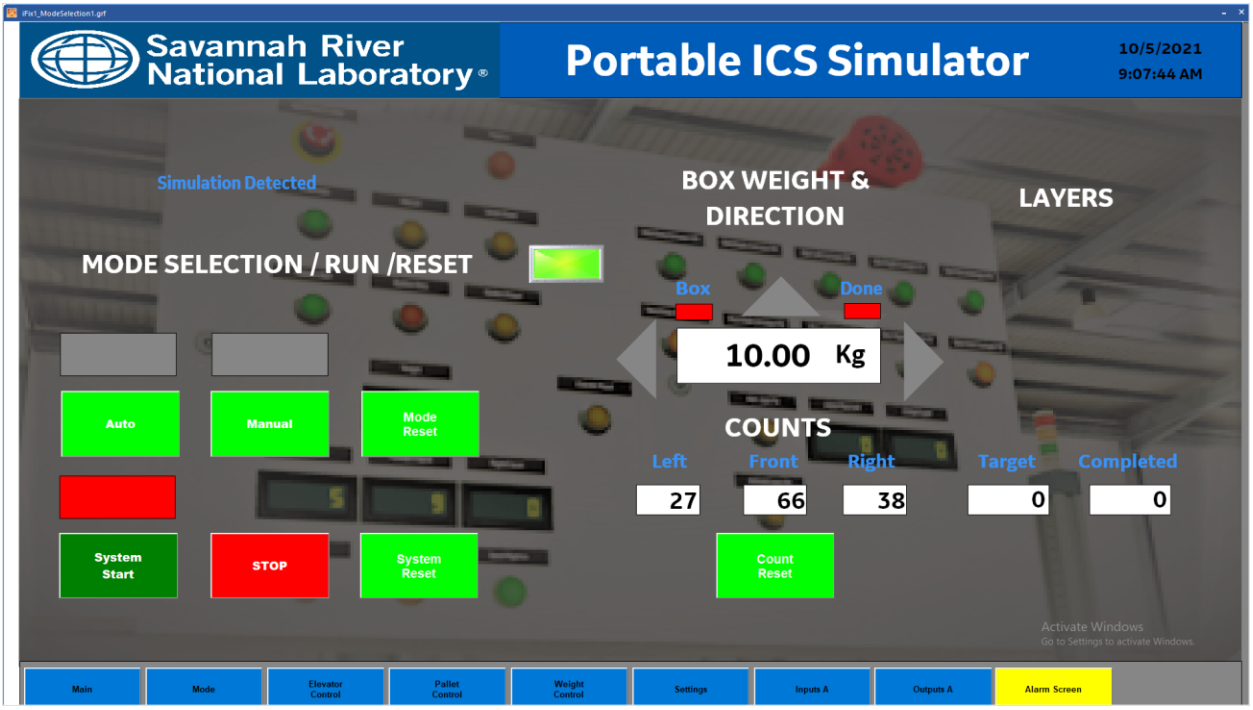

Figure 3: GE iFIX SCADA Human Machine Interface (HMI) Screen for PCIIC