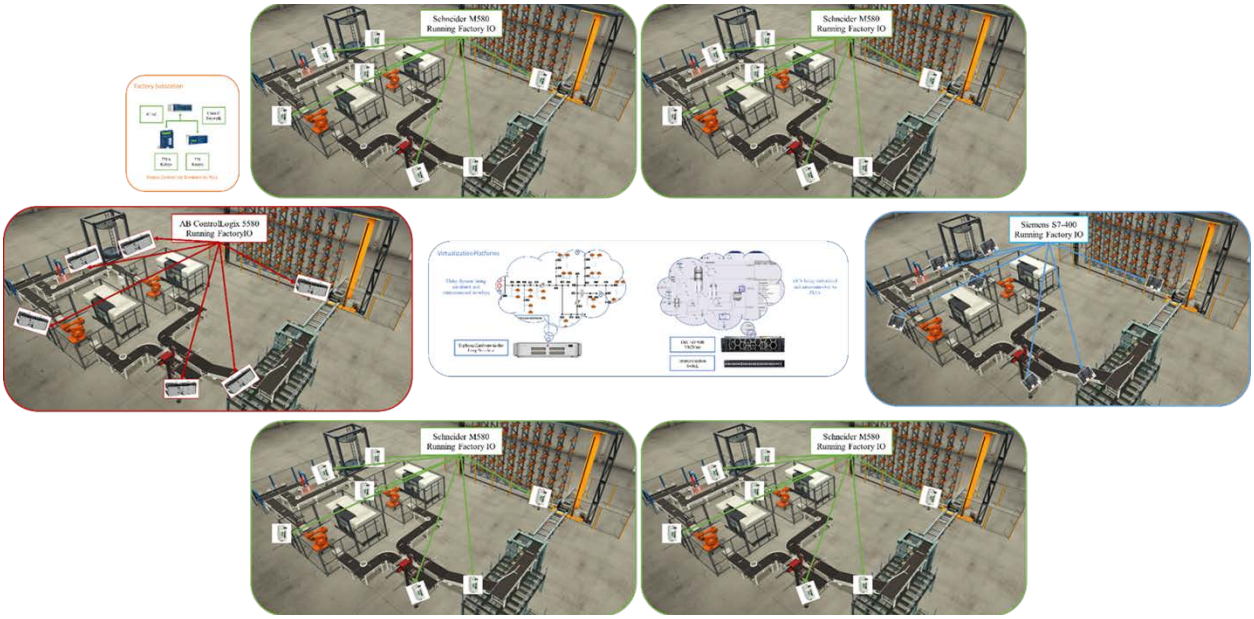
Contract No:

This document was prepared in conjunction with work accomplished under Contract No. DE-AC09-08SR22470 with the U.S. Department of Energy (DOE) Office of Environmental Management (EM).

Disclaimer:

Collaboration with USACyS for Signals Manipulation

SRNL and USACyS have entered a strategic partnership project (SPP) agreement in which SRNL builds an ICS training platform integrated with the S-CIIC, which the USACyS can invest resources to optimize their training requirements. This establishes SRNL as a key location for USACyS's hands-on training mission.



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

Signature **Date**

Collaboration with USACyS for Signals Manipulation

Project Team: Mackenzie Morris (Primary) Klaehn Burkes, and Jon Dollan

Subcontractor: None

Project Type: Standard

Project Start Date: October 1, 2018
Project End Date: September 30, 2020

Savannah River National Laboratory has been investing into cybersecurity capabilities since 2019. Cybersecurity has been a rapidly growing area for the CSRA in general and has included the consolidation of Cyber and Electronic Warfare units at Fort Gordon. This consolidation has been driven by the convergence of cyberwarfare and electronic warfare as the technologies underpinning Army Cyber Command's vision of Information Warfare. This convergence, investment by SRNL into cybersecurity for critical infrastructure, and the desire for collaboration between the Army and SRNL has resulted in an opportunity for SRNL to develop R&D capabilities in electronic warfare that will complement SRNL's cybersecurity efforts. Discussions between SRNL and the U.S. Army Cyber School (USACyS) has identified a general gap in ICS training lab capability in which both entities could contribute to solve. It is proposed to design and architecture that meets this need.

FY2020 Objectives

- Develop virtual ICS architecture that allows solders the ability to train with minimal hardware
- Establish encrypted GNSS capability into SRNL Critical Infrastructure, ICS and Cybersecurity (S-CIIC) lab
- Establish a Strategic Partnership Projects (SPP) Agreement with Cyber Center of Excellence

Introduction

The CSRA has seen a significant increase in investment into Cybersecurity over the last few years. Fort Gordon has been designated as the location that will consolidate the Army Cyber School, Army Cyber Command Headquarters, Information Warfare Operational Commands, and Electronic Warfare Units. SRNL is in the process of investing into developing capabilities and personnel who can tackle high level R&D projects in cybersecurity. The lab's focus has been industrial control system (ICS) security, which more broadly is part of critical infrastructure. This area is of interest to the Army, as critical infrastructure is important for national defense, but also because electronic warfare techniques are becoming increasingly applicable to cyber-attacks on ICS as these systems become more dependent on advanced electronics and communication systems. The proximity of SRNL and Fort Gordon, and mutual interests in national security, inevitably resulted in dialogue between the two entities.

In these discussions, the Army has expressed that they are seeking to advance their training laboratory capability in ICS security. They would like to work with SRNL Cyber Security Programs, which has experience in ICS equipment and laboratory implementation, to scope and execute a proof of concept for a novel method emulating an ICS environment with minimal hardware components that allow for cyber students to train. Development of this system will set SRNL apart since this capability is still being sought

by the Army. The Army's contributionto the collaboration will include rotating personnel to SRNL to work directly with engineers during all stages of this project.

With the completion of a successfully developed architecture, it is expected that fully implementing the architecture will be initiated via a SPP on the part of the Army. This initial investment will allow SRNL to build that trust and relationship as well as the capability and personnel to continue to engage in this area of research. Success in this area will define a new area of expertise for the lab and allow us to pursue funding opportunities in advanced signaling and communications.

Approach

SRNL and the USACyS identified that in order to do research into hardening systems from electronic warfare, training ranges with the equipment and capabilities of operational systems must be established. Therefore, SRNL identified and developed an architecture using equipment already owned by SRNL to create 8 interactive training ranges that cover multiple different ICS components. 6 of these ranges consist of factory floor ICS equipment, 1 range represents the electric grid feeding power to these factories, and finally a full virtualized SCADA system provides access into all of the previous developed ranges. This along with an encrypted GNSS simulator allows for SRNL to emulate many different environments the army is currently active.

Results/Discussion

Through this project SRNL built a working relationship with the USACyS and also established new capability within the S-CIIC for encrypted GNSS simulation, PLC programing, and virtual SCADA architecture design. These were all gaps in SRNL's capabilities before this LDRD. It was identified by the USACyS that GNSS simulation is very important for a controlled lab environment but to collaborate fully SRNL needed encrypted communication capability. This led to SRNL research and demonstrating several GNSS simulators' capabilities before identifying the BroadSim GNSS simulator as the most flexible and cost effective. BroadSim uses software defined radios to allow for the same radio to perform multiple GNSS constellation communication capabilities. This was the only system that did not use custom radios for each GNSS constellation and thus reducing the cost by a factor of 10. The BroadSim platform is an advanced jamming and spoofing Navigation Warfare (NAVWAR) system that can perform high dynamics, jamming, spoofing, and encrypted military codes. The system is capable of simulating multiple constellations through the software defined radios such as GPS, GLONASS, Galileo, BeiDou, and QZSS. This system is critical for any Army NAVWAR collaboration.

Figure 1: BroadSim NAVWAR GNSS simulator in the S-CIIC

Another achievement of this project was identifying a cost savings of $1.7M and executing the recovery of this equipment. Through the monitoring of the excess system at SRNS and with the closure of several projects and a mission at the SRS, a selection of equipment was identified that contained enough PLC and accessory components to build about 15 full ICS environment with redundant PLCs and over 1000 I/O modules.

Figure 2: Recovered Equipment Inside the S-CIIC

Through this recovery SRNL built the capability to program PLCs and emulate the factory floor utilizing a simulation platform called FactoryIO. With this gained expertise SRNL was then capable of executing the foundational objective of this project which was to develop the architecture for a training system for USACyS. Through one strategic hire and internal personnel developing new skill sets from the recovered equipment, SRNL designed a training platform that would consist of minimal hardware, 6 PLCs and 6 Relays with just two platforms used to simulate the SCADA system and the power grid. The architecture, which is emulating real world capability and functionality, resulted in overwhelming support from USACyS and also the desired replication by the Army Cyber Protection Brigade. USACyS executed a SPP with SRNL

to build the designed architecture and thus accomplishing the main objective of this project, thus establishing SRNL as the USACyS's location for ICS cybersecurity hands-on training.

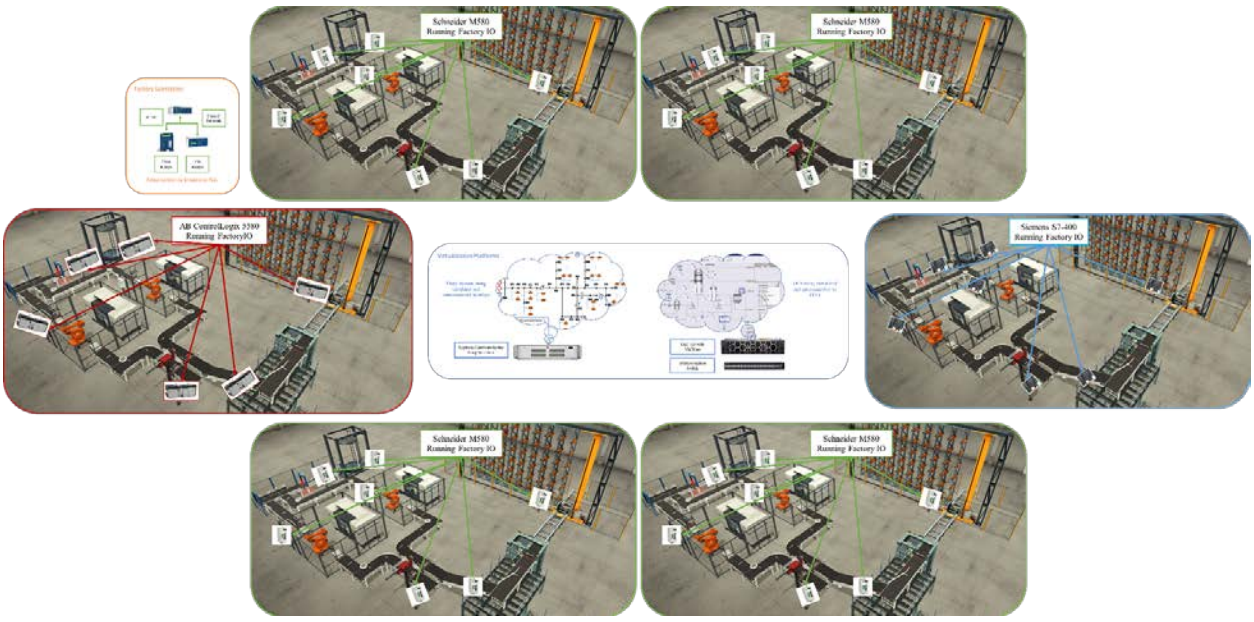


Figure 3: Proposed Architecture for USACyS Training System

FY2020 Accomplishments

- ✓ SRNL and USACyS have entered a strategic partnership project (SPP) agreement in which SRNL builds an ICS training platform integrated with the S-CIIC. This establishes SRNL as the location for USACyS's hands-on training mission.
- ✓ Received $300k follow-on funding for building the architecture developed in the project.
- ✓ Cost savings of $1.7M is Schneider PLC equipment recovery from excess.
- ✓ One strategic PLC programmer hire.

Future Directions

SRNL will execute J-SOW-A-00031 to build the architecture developed and get the system operational for the Army Cyber Center of Excellence.

FY 2020 Peer-reviewed/Non-peer reviewed Publications

None

Presentations

None

Works Cited

None

Acronyms

- GNSS – Global Navigation Satellite System
- NAVWAR – Navigation Warfare
- PLC – Programable Logical Controller
- S-CIIC – SRNL – Critical Infrastructure, ICS, and Cybersecurity
- SPP – Strategic Partnership Project
- USACyS – US Army Cyber School

Intellectual Property

- None

Total Number of Post-Doctoral Researchers

- None

Total Number of Student Researchers

- None

External Collaborators (Universities, etc.)

- None