Environmental Security Technology Certification Program
Project EW-201607 Critical Energy Infrastructure Cyber Defense-in-Depth
under USACE contract W912HQ-16-C-0046

Modification (1) to above contract increased scope and funding for:

Cyber Transition to Practice
Defense-in-Depth for Industrial Control Systems (ICS):
Proposed Addition of an ICS Intrusion Detection System (IDS)

Summary Test Results from:

1. **Critical Energy Infrastructure Cyber Defense-in-Depth Experiment**
2. **Heterogeneous Sensor Experiment**

Prime Contractor:	Resurgo, LLC Kevin B. Jordan, Principal Investigator
Subcontractors:	Johns Hopkins University, Imprimis Inc, Spread Concepts LLC
Government Sponsors:	US Northern Command (NORTHCOM) U.S. Pacific Command (USPACOM) Naval Facilities Engineering Command (NAVFAC)
Industry Partner:	The Hawaiian Electric Company (HECO)
Technologies Provided:	
Spire (Prime, Spines, +)	Johns Hopkins University, Spread Concepts LLC
MANA IDS and SIEM	Resurgo, LLC
CTAM-R	Imprimis, Inc.

1. Executive Summary

Unauthorized access to an Operations Technology (OT) network of a US utility company by a cyber adversary is a worst-case scenario for critical infrastructure protection. And yet, we face this pervasive threat daily on a national scale. An active and aware cyber defense-in-depth of critical infrastructure is crucial to closing this vulnerability. To address this capability gap, Resurgo, LLC, as the Prime Contractor, and its partners: Johns Hopkins University, Spread Concepts LLC, Pacific Northwest National Laboratory, Sandia National Laboratories, and the Hawaiian Electric Company, conducted the first ever successful test of an aware, fault and intrusion tolerant defense of an OT network in a functional machine-in-the-loop emulation of a utility control system. This fault and intrusion tolerant experiment, sponsored by the Environmental Security Technology Certification Program (ESTCP) and entitled "Critical Energy Infrastructure Cyber Defense-in-Depth", was conducted at the Pacific Northwest National Laboratory (PNNL), 27 March through 7 April 2017. The aligned sensor experiment was conducted simultaneously with funding provided by the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)) Cyber Transition to Practice (CTP) Program.

The results of the two designed experiments demonstrated that the current standards for OT architectures published by the National Institute of Standards and Technology (NIST) do not offer effective protection against a cyber adversary who gains access to the OT network. While the NIST standards and the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) best practices make it harder for the cyber threat to establish itself within the OT network, compliance with these standards and practices does not prevent threat activities nor does it protect against the destructive consequences likely to follow should an adversary gain access. In time, a determined and capable adversary will eventually gain access. The phase 1 experiments at PNNL established that a fault and intrusion tolerant system enables continued functioning of the OT network despite being under attack by a sophisticated cyber threat. A necessary complement to all fault and intrusion tolerant defenses is a set of heterogeneous sensors employing different inspection methods to provide cyber situational awareness. With enough time, even fault and intrusion tolerant defenses can be overcome if advanced persistent threats are not detected and responded to appropriately. It is the addition of an aligned sensing architecture that elevates fault and intrusion tolerance defense to a true fight-through capability.

The defense-in-depth of the test architecture at PNNL was provided by a suite of fault and intrusion tolerant technologies called *Spir*e, developed by Johns Hopkins University and Spread Concepts, LLC. The Sandia National Laboratories cyber red team was unable to penetrate the secure communications overlay protecting information exchanges between the SCADA Master and the controlled endpoints of the Spire system during the designed experiment runs. The full results and conclusions are explained in *Volume 1 (of 2) Test Report on Electric Utility Control System Cyber Security at the Pacific Northwest National Laboratory - April 2017*.

The aligned sensor experiment, documented in the *Volume 2 (of 2) Test Report on Heterogeneous Sensor Experiment*, utilized sensors of different modalities to include Resurgo, LLC's prototype Machine-learning Assisted Network Analyzer (MANA) intrusion detection sensor (IDS) and Imprimis Inc.'s Cyber Threat Activity Matrix (CTAM) database with its Radiflow signature-based and anomaly detection sensor components. The results demonstrated

that a properly trained and focused machine-learning sensor, such as the MANA IDS, could detect a substantial percentage of the attacks that are undetectable by an up-to-date signature-based sensor on ICS/SCADA networks. This experiment demonstrated that signature-based sensing alone is woefully inadequate for detection of advanced cyber threats operating within ICS/SCADA networks. Signature-based sensors give a primarily retrospective view by alerting on known attacks that have been successful elsewhere. The signature-based portion of the Radiflow sensor registered only one alert, a true positive, on one of the 53 total attacks launched by the red team. By contrast, the MANA IDS' machine-learning sensor detected 42 of the 53 attacks. The reason for this disparity in detections is that most of the malicious actions taken by the red team, once inside the ICS/SCADA networks, were not activities associated with known signatures. The anomaly detection methods used by both Radiflow and MANA also alerted on attacks that were undetected by the signature-based sensor but neither were as effective in terms of recall (the percentage of actual (ground truth) attacks detected) as MANA IDS' machine learning method. The comparative results for the sensors of different inspection methods and the analysis of the results is available in the Volume 2 report.

The phase 1 designed experiment results summarized herein offers compelling evidence that an active and aware cyber defense provides significantly better protection for control systems than the NIST recommended architecture alone. The results also established that fault and intrusion tolerant technologies could protect a utility's OT networks from an advanced and determined cyber threat with remote or insider access. The *Black Energy* and *StuxNet* incidents confirmed that even isolated ICS networks are subject to penetration when malware jumps across air-gaps onto OT networks. The results of this experiment strongly suggest that the Department of Defense (DoD), the Department of Homeland Security (DHS), and commercial utilities should consider implementation of defense-in-depth architectures using fault and intrusion tolerant technologies combined with aligned sensing technologies to protect Supervisory Control and Data Acquisition (SCADA) control systems.

In Phase 2 of this project, in early 2018, we will demonstrate a fault and intrusion tolerant defense in combination with aligned sensors and correlation technologies in a layered cyber defense-in-depth of a Hawaiian Electric Company (HECO) power plant supporting Joint Base Pearl Harbor Hickam.

2. Technologies

The fault and intrusion tolerant technologies used were developed under the assumption that the OT network is already compromised, and that critical control system components need to resist or overcome attacks to continue functioning despite adversary efforts to disrupt them.

Spire System

The Spire system developed by Johns Hopkins University and Spread Concepts LLC, (www.dsn.jhu.edu/spire/) includes a SCADA Master, PLC/RTU Proxy, pvbrowser-based Human Machine Interface (HMI), Prime intrusion-tolerant replication engine, and the Spines intrusion-tolerant network overlay. Together, the Spire software components employ diversity and proactive recovery to increase the resilience of the system. Spire prevents a single exploit from compromising all instantiations of a particular software component by periodically resetting to a new state.

This removes any undetected intrusions from the protected host (SCADA Master). The Spire system is designed to scale to multiple field devices, sites, and operations centers, but was restricted to a small implementation for the ESTCP experiment.

Network IDS sensors were selected to ensure heterogeneous inspection methods and availability under project budget and timeline constraints. The addition of cyber SA to the powerful fault and intrusion tolerant defense elevates it to a true "fight-through" capability for critical infrastructure defense.

Machine-learning Assisted Network Analyzer (MANA) IDS

Resurgo, LLC's, prototype MANA IDS employs both machine learning-based, and anomaly-based, sensing methods. The MANA sensor uses many different algorithms during the training process for each type of sensing method. The best performing algorithms for a given network environment are then selected for sensor employment. The MANA IDS can be configured to employ one algorithm per instance or many algorithms of different modality per instance (i.e. one MANA sensor can perform the function of multiple heterogeneous sensors).

Cyber Threat Activity Matrix - Radiflow (CTAM-R)

Imprimis, Inc's, CTAM-R is designed to identify advanced persistent threat activity in industrial control systems and to report the resulting tailored threat intelligence information to national agencies. The system is intended for broad use throughout the Department of Defense, Department of Homeland Security, Department of Energy, as well as the commercial sector for use in energy and utilities, oil and gas, and many others. CTAM contains two major components, a threat database and intrusion detection sensor (Radiflow IDS). The Radiflow IDS component of CTAM uses modified versions of Suricata and Bro IDS, combined with advanced, tailored, and modular smart packet inspection to enable use of both signature-based detection for known intrusion attempts and anomaly-based detection to identify variations from a derived model of normal network behavior. The addition of the anomaly detection capability to Radiflow potentially offers the ability to detect previously unknown attacks.

3. Summarized Volume 1 Conclusion

Statistical analysis of the data (using several tests) confirmed the subjective assessment: that the Defense-in-Depth's cyber security of the critical data exchanges in the PNNL experiment was significantly better than that of the NIST-compliant architecture. The fault and intrusion tolerant technologies worked as intended; securing the Operations Technology (OT) network's functionality, despite the presence of a knowledgeable red team. The Supervisory Control and Data Acquisition (SCADA) devices found in OT networks are designed to perform in rugged environmental conditions without regard for cyber security. Introduction of internet protocol devices and internet connectivity into SCADA spaces creates vulnerabilities. Fault and intrusion tolerant technologies and cyber aware defenses, whether integrated with existing SCADA devices or installed alongside, are required on OT networks to ensure continuity of energy production in the presence of advanced cyber threats.

The NIST-compliant, standard utility control system network is designed to deny and restrict cyber threats from reaching the OT networks from the Internet. However, if that cyber threat breaches the utility's networks, then the NIST-compliant architecture does not protect the critical devices and the associated data exchanges. We recommend that government organizations and utility companies start employing fault and intrusion tolerant devices with appropriate sensing methodologies so that Industrial Control Systems (ICS) can operate unimpeded *when, and not if,* intrusions occur.

4. Summarized Volume 2 Conclusion

The results from this experiment show that machine-learning and anomaly detection methods are more successful at detecting attacks and therefore in providing cyber situational awareness. Signature-based detection alone is neither appropriate nor effective for utility company network defense. Utility company OT networks have specialized equipment that requires crafted attacks for which no signatures exist. Signature-based detection may be appropriate for IT/enterprise/corporate networks. However, as demonstrated in this experiment, an advanced threat can avoid using attacks that have known signatures on either network.

Anomaly detection results varied depending on method of implementation and utility network location. Anomaly detection should be carefully chosen based on attack recall and alert precision requirements, remembering that recall and precision are often inversely proportional. The experiment results showed that the two anomaly detection methods were on the opposite ends of the recall/precision spectrums (i.e. one had high alert precision with low attack recall and the other had lower alert precision with higher attack recall).

A properly trained and focused machine-learning sensor, such as the MANA IDS, can detect a substantial percentage of the attacks that are undetectable by an up-to-date signature-based sensor on ICS/SCADA networks. This experiment demonstrated that signature-based sensing alone is woefully inadequate for detection of advanced cyber threats operating within ICS/SCADA networks since most red team actions inside an ICS/SCADA network, are not associated with known signatures. Anomaly detection methods are better than the signature-based methods, but neither are as effective in terms of recall as the MANA IDS's machine learning method.

5. Conclusion

The phase 1 results offer compelling evidence that an active and aware cyber defense provides significantly better protection for control systems than the NIST recommended architecture alone. The results also establish that fault and intrusion tolerant technologies can protect a utility's OT networks from an advanced and determined cyber threat with remote or insider access. The *Black Energy* and *StuxNet* incidents confirmed that even isolated ICS networks are subject to penetration when malware jumps across air-gaps onto OT networks. Again, the results of this experiment strongly suggest that the DoD, the DHS, and commercial utilities should implement defense-in-depth architectures using fault and intrusion tolerant technologies combined with aligned sensing technologies to protect their control systems.

Machine-learning shows real potential as a powerful detection capability for a utility's OT, SCADA, and ICS networks. The prototype MANA IDS sensor was the only system that reliably caught red team attacks. For cyber intrusion defense against Advanced Persistent Threats and

nation-state actors, machine learning provides the cyber situational awareness necessary for a fault and intrusion tolerant OT network to succeed in a DoD or Industry implementation.