EXECUTIVE SUMMARY

Critical Energy Infrastructure Cyber Defense-in-Depth

ESTCP Project EW-201607

AUGUST 2018

Distribution Statement A
This document has been cleared for public release

Page Intentionally Left Blank

This report was prepared under contract to the Department of Defense Environmental Security Technology Certification Program (ESTCP). The publication of this report does not indicate endorsement by the Department of Defense, nor should the contents be construed as reflecting the official policy or position of the Department of Defense. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the Department of Defense.

Page Intentionally Left Blank

EXECUTIVE SUMMARY

Project: # EW-201607

TABLE OF CONTENTS

Page

1. INTRODUCTION 1
   1.1. THE PROBLEM 1
   1.2. THE PROBLEM'S IMPACT 1
2. OBJECTIVES 3
3. TECHNOLOGY DESCRIPTION 5
   3.1. PHASE 1 – PNNL DEMONSTRATION 5
      3.1.1. Machine-Learning IDS 5
      3.1.2. CTAM-R 5
      3.1.3. Prime 6
      3.1.4. Spines 6
      3.1.5. Symbiote 6
   3.2. PHASE 2 – HECO POWER PLANT DEMONSTRATION 6
      3.2.1. Technology Notes 7
4. PERFORMANCE ASSESSMENT 9
   4.1. PHASE 1 – PNNL DEMONSTRATION 9
   4.2. PHASE 2 – HECO POWER PLANT DEMONSTRATION 9
5. COST ASSESSMENT 11
6. IMPLEMENTATION ISSUES 13
   6.1. RESULTS 13
      6.1.1. Overall Results 13
      6.1.2. MANA Results 14
      6.1.3. Spire Results 14
   6.2. CONCLUSION 14

LIST OF TABLES

Page

Table 1. All Runs Aggregate Attack Recall Scores 9

ACRONYMS AND ABBREVIATIONS

APT	Advanced Persistent Threat
CTAM-R	Cyber Threat Activity Matrix with Radiflow
DHS	U.S. Department of Homeland Security
DoD	U.S. Department of Defense
DoS	denial-of-service
ESTCP	Environmental Security Technology Certification Program
HECO	Hawaiian Electric Company
HMI	Human Machine Interface
ICS	industrial control system
IDS	intrusion detection system
IP	internet protocol
IT	information technology
MANA	Machine-learning Assisted Network Analyzer
NAVFAC EXWC	Naval Facilities Engineering and Expeditionary Warfare Center
NERC CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
OT	operational technology
PLC	programmable logic controller
PNNL	Pacific Northwest National Laboratory
RTU	remote terminal unit
SA	situational awareness
SCADA	Supervisory Control and Data Acquisition
SME	subject matter expert
TCP/IP	Transmission Control Protocol/Internet Protocol

ACKNOWLEDGEMENTS

Prime Contractor:	Kevin B. Jordan, Principal Investigator, Resurgo LLC
Subcontractors:	Imprimis Inc., Johns Hopkins University, and Spread Concepts LLC
Government Sponsors:	U.S. Northern Command (USNORTHCOM), U.S. Pacific Command (USPACOM), Naval Facilities Engineering Command (NAVFAC)
Industry Partner:	Hawaiian Electric Company, Inc.
Project Support:	Pacific Northwest National Laboratory (PNNL), Sandia National Laboratories

Technologies Provided:

Spire (Prime, Spines, +)	Johns Hopkins University, Spread Concepts LLC
MANA Intrusion Detection System (IDS)	Resurgo LLC
Security Information and Event Management (SIEM)	Resurgo LLC

1. INTRODUCTION

Resurgo LLC is a woman-owned, small business of 13 employees in the cybersecurity sector. Years of working with machine learners in U.S. Department of Defense (DoD) projects led to an understanding of machine learning's weaknesses and how to best harness its strengths. Machine learners work best in a simple environment that changes very little, such as industrial control systems (ICSs). However, it takes more than a new type of Network Intrusion Detection System (NIDS) to defend against today's threats to critical cyber infrastructure. Supervisory Control and Data Acquisition (SCADA) systems must ensure continuous availability and correct operation in the presence of compromises and attacks at both the system and network level. Unauthorized access to an operational technology (OT) network of a U.S. utility company by a cyber adversary represents a worst-case scenario from a critical infrastructure protection perspective. Yet, this existential threat is faced on a national scale. An active and aware cyber defense-in-depth of critical infrastructure is crucial to closing this vulnerability.

Based on National Institute of Standards and Technology (NIST) discussions, "defense-in-depth" (NIST Computer Security Division, 2013) is an information security strategy integrating people, technology, and operations capabilities. However, defense-in-depth stops at the firewalls before the OT networks. To address this capability gap, Resurgo LLC, as the Prime Contractor, partnered with Imprimis, Inc., Johns Hopkins University, and Spread Concepts LLC to address this national need. The Environmental Security Technology Certification Program (ESTCP) provided funding for the project. The project team received support from the Pacific Northwest National Laboratory (PNNL), Sandia National Laboratories, and the Hawaiian Electric Company (HECO). This team allowed Resurgo to demonstrate the first ever successful operation of a cyber-aware, fault-and-intrusion-tolerant defense of a utility control system in a functional power plant.

1.1. THE PROBLEM

The DoD lacks the ability to effectively defend the control system networks and SCADA systems of posts, bases, camps, installations, and related civilian critical-energy infrastructure against cyberattacks. The DoD's control system networks are subject to a broad spectrum of threats, the most serious of which are those associated with nation state actors and Advanced Persistent Threats (APTs). The DoD actively defends its information technology (IT) networks, but this active defense uses funding, manpower, and focused situational awareness (SA) that does not extend to DoD's OT networks. Commercial U.S. utility companies have a similar problem in that they do not have the tools, expertise, manpower, or budget to defend their OT networks from an APT.

1.2. THE PROBLEM'S IMPACT

The DoD's cyber systems, to include its energy production control systems, are probed every day by thousands of varied sources. DoD is well defended in its IT networks. However, the DoD is unable to identify new compromises in its OT systems or determine if any of its energy control systems are already compromised. The compromise or loss of one or more energy production facilities at the beginning of an attack on the Nation, or even on a single installation, will result in the loss of command, control communications, computers, and intelligence (C4I) at a crucial moment and could result in the loss of the opening battle of that war. This problem is compounded by the near total lack of tools made for the multi-protocol OT networks, the limited amount of IT

personnel with OT knowledge or OT personnel with knowledge of IT defensive technologies, and no budget to acquire the tools or expertise to close this massive vulnerability in the Nation's critical energy infrastructure. A NIST-compliant utility control system network is designed to deny and restrict cyber threats from reaching the OT networks from the internet. However, introduction of internet protocol (IP) devices and internet connectivity into SCADA spaces, and sometimes directly to field devices, creates vulnerabilities in previously non-IP, NIST-compliant areas. Once a cyber threat breaches a utility's defenses and gains access to the OT networks, being NIST-compliant does not adequately protect the critical devices and their associated data exchanges.

2. OBJECTIVES

The objective of this project was to implement and successfully demonstrate an aware, fault-and-intrusion-tolerant cyber defense-in-depth for a power plant's control system network. A power plant operating with the cyber defense-in-depth technologies used in this project will be cyber-secure, Byzantine-fault-tolerant, and aware. A plant thus protected would be able to withstand nation state equivalent cyberattacks. Demonstrating this cyber defense onsite in a commercial utility company's power plant shows a practical cyber-secure path forward for DoD, U.S. Department of Homeland Security (DHS), and commercial utilities.

Page Intentionally Left Blank

3. TECHNOLOGY DESCRIPTION

Phase 1 involved five technologies, though only four were demonstrated: two intrusion detection systems (IDSs) (a machine-learning IDS and the Cyber Threat Activity Matrix with Radiflow [CTAM-R] iSID) and two network defense technologies (Prime and Spines).

3.1. PHASE 1 – PNNL DEMONSTRATION

Five cyber defense-in-depth technologies (machine-learning IDS, CTAM-R, Prime, Spines, and Symbiote) went to PNNL. The technologies were layered in depth throughout the control system network. Only four of the technologies were tested by the cyber red team.

3.1.1. Machine-Learning IDS

The IDS used machine-learning-based tools to catch new and morphed (altered) attacks that traditional signature sensors could not catch. The IDS monitored all traffic entering and leaving the control system network and provided a crucial network layer of SA to the defense-in-depth architecture. Machine-learning-based systems have been proven to be particularly effective in detecting polymorphic versions of attacks on which the IDS has been trained. Machine learning systems have even shown the ability to catch true zero days or attacks on which it has not been trained. This machine-learning-based IDS was the initial prototype of the Machine-learning Assisted Network Analyzer (MANA) used in Phase 2.

3.1.2. CTAM-R

The CTAM-R is a prototype combined database and advanced, intelligent IDS for ICSs that uses both signature-based and anomaly detection. The technology also compiles threat information; threat tactics, techniques, and procedures (TTP); and detectable indicators from various open sources into a single, coherent, ICS-specific database of threats. CTAM-R compiles the threats it has detected and shares those confirmed detections externally using Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) formats, while simultaneously receiving threat intelligence updates. The technology uses the compiled observables and derived knowledge of the target network to guide IDS detection operations. Its Radiflow IDS component uses a modified Snort® IDS, combined with advanced smart packet inspection, to enable it to use both signature-based detection for known intrusion attempts and anomaly-based detection to identify variations from a derived model of normal network behavior. This gives the technology the ability to detect previously unknown attacks. The CTAM-R IDS evaluated the same traffic as the machine-learning IDS but used a completely different type of inspection method.

Although CTAM-R provided both IDS and operator SA functions, only the IDS component was tested. The SA component, actions taken by humans, and any other human or cognitive-based effect was not evaluated during testing.

3.1.3. Prime

Prime is an intrusion-tolerant replication engine that protected the SCADA Master of the SCADA architecture. Prime provides component and system performance guarantees even when the system is partially compromised by a sophisticated Byzantine replication protocol. Prime supports proactive recovery, diversity, and state transfer through its multiple Prime servers. Using its multi-compiler, Prime ensures that each of its replicas presents a different attack surface (different variation) to an attacker so that no single exploit can take down the entire system. Prime servers periodically rejuvenate to clean the system from potentially undetected intrusions. Prime seeks source congruency; that is, a strong majority of the Prime servers must have the same result or outcome for an operation to be congruent.

3.1.4. Spines

The Spines overlay communications architecture ensured delivery of SCADA traffic within very tight time constraints while blocking adversary positioning for man-in-the-middle attacks. Spines provided a highly reliable and fast messaging framework that overlaid the network structure connecting the Human Machine Interface (HMI) with the SCADA devices it manages. Speedy and reliable delivery of Spines-supported traffic is accomplished by multicasting network intelligence on the status of packets and availability of open routes across the overlay. A derivative of the Spines technology is in commercial use providing reliable and timely video delivery services worldwide for media enterprises such as Fox News, Cable News Network (CNN), National Public Radio (NPR), and Bloomberg Financial Services.

3.1.5. Symbiote

Symbiote completes the cyber defense-in-depth by providing host-based endpoint protection of remote terminal units (RTUs), programmable logic controllers (PLCs), and other devices. Symbiote detects and reverses firmware intrusions and modifications. Symbiote provides SCADA networks with critical endpoint device defense where none exists currently. Symbiote uses Automatic Binary Structure Randomization to protect the firmware by changing the structure and code. The result of this change is that the protected embedded device is no longer vulnerable to compromise. Symbiote is source-code agnostic and can be used on any device or by any manufacturer.

Symbiote is the ideal host (PLC, RTU, printer, etc.)-level defense to complete the defense-in-depth. Red Balloon Security (Symbiote's technology provider) withdrew from the project and did not provide the software to defend the PLCs or RTUs. Rather than not have Symbiote represented in the experiment, a commercial networked printer defended by Symbiote software was purchased and included within the defended OT network to see if it could be exploited by the cyber red team.

3.2. PHASE 2 – HECO POWER PLANT DEMONSTRATION

From the subject matter expert (SME) interactions and PNNL results, the machine-learning IDS, Spines, and Prime were determined to be strong enough to be used at HECO. The machine-learning IDS evolved into MANA, and Spines and Prime were upgraded, further hardened, and combined with other applications to become the Spire suite of technologies. In Phase 2, Spire defended the network and certain hardware and the MANA NIDS provided the plant operator the cyber SA missing from the Spire technologies.

Unfortunately, funding was not available to continue use of the CTAM-R NIDS. However, due to HECO security policies, the CTAM-R would not have been able to contribute to the demonstration since no connections external to the plant were permitted on networked equipment. Without the external connection, CTAM-R would not have been able to demonstrate the power of its database.

The MANA NIDS is an evolutionary upgrade of the Phase 1 machine-learning IDS components and processes. Different machine learning algorithms were integrated, training techniques were modified, correlation of alerts was moved internal to MANA, a new feature was added so that a confidence weighting was assigned to each alert, and the graphical user interface was simplified and improved so that the information displayed to the plant engineer was prioritized with links to the supporting data for further analysis. The MANA NIDS is passive and receives all traffic via a one-way network tap. The MANA NIDS is compatible with all networks using IP-based traffic to include variations such as Modbus over Transmission Control Protocol (TCP)/IP.

Spire is a suite of fault-and-intrusion-tolerant technologies based on the successful Spines and Prime technologies, with the addition of:

- A customized and hardened HMI derivative of the open-source pvbrowser (an application framework that provides a specialized browser for the client computer and an integrated development environment for the data acquisition programs that connect to the SCADA Master).
- A hardened PLC/RTU proxy (a device that relays Modbus or Distributed Network Protocol [DNP3] commands between the PLC or RTU and the SCADA Master).
- A SCADA Master designed from scratch to be intrusion-tolerant and compatible with replication using the Prime intrusion-tolerant replication engine. The SCADA Master is the core of a typical SCADA system. It collects data from the PLCs and RTUs in the field and sends commands to control the state of the field devices.

Spire is compatible with all networks using IP-based traffic to include Modbus over TCP/IP.

3.2.1. Technology Notes

Fault-and-intrusion-tolerant technologies, whether added to the network, installed alongside as complementary to network devices (as was done here), or integrated into a replacement device, are necessary to protect OT networks and SCADA devices and to ensure continuity of energy production despite existing or introduced vulnerabilities. Fault-and-intrusion-tolerant technologies significantly raise the cost of entry for APT but are not foolproof or a ‘silver bullet’ solution. The aware cyber defense-in-depth concept for utility control system defense also uses intrusion detection sensing. The NIDS is the only defensive technology that reports to the plant engineers and network defenders about what is happening on and to the control system and its networked devices.

The correlated, high-confidence alerts provided by the NIDS provide details about the threats attacking the formidable barriers provided by the fault-and-intrusion-tolerant technologies. The existence of fault-and-intrusion-tolerant systems on a utility OT network will force the attacker to adopt more intrusive measures, or adjust their attack timeline, as they attempt to overcome the defenses. This in turn exposes the attacker to a higher probability of detection by the aligned NIDS and permits plant personnel to respond sooner and limit the penetration and potential damage.

Note: These technologies complement the NIST and North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) requirements and add layers of defense where currently none exist. Both technologies are tested and shown not to induce latency or errors in plant equipment or networks.

4. PERFORMANCE ASSESSMENT

4.1. PHASE 1 – PNNL DEMONSTRATION

The designed experiment conducted in the PNNL produced the recall results shown in Table 1. The table shows the total number of Sandia National Laboratories cyber red team attacks (53) and the number of attacks identified and missed by the sensors.

Table 1. All Runs Aggregate Attack Recall Scores

Sensor	Total Number of Red Team Attacks	Total Number of Attacks Caught	Total Number of Attacks Missed	Recall
MANA (Machine Learning)	53	42	11	79.25%
MANA (Anomaly)	53	35	18	66.04%
CTAM-R (Anomaly)	53	15	38	28.30%
CTAM-R (Signature)	53	1	52	1.89%

Recall is defined as the number of attacks caught over the total number of attacks conducted:

$$Recall = \frac{Caught\ Attacks}{Missed + Caught\ Attacks} = \frac{Caught\ Attacks}{Total\ Attacks}$$

The Phase 1 aggregate attack recall results revealed some interesting insights:

1. MANA's machine learning detection did very well (comparatively) in catching the cyber red team attacks. MANA's anomaly-based detection performed adequately in detecting attacks; however, the previous precision results showed that the MANA anomaly alerts were not always accurate.
2. Signature-based detection is not appropriate for detecting advanced threats targeting SCADA systems. Based on the uniqueness of each plant's equipment composition and legacy networks, attackers only use known exploits (attacks with known signatures) during the initial "establish a foothold" phase of the attack. Once inside the OT network, attackers must improvise and craft specifically targeted attacks to achieve their objectives.
3. CTAM-R's anomaly-based detection did not catch many of the cyber red team attacks, although the alerts that were produced were the most accurate (as confirmed from the high precision results).

4.2. PHASE 2 – HECO POWER PLANT DEMONSTRATION

The MANA NIDS was able to detect 100% of the initial reconnaissance and all follow-on attacks that were later conducted. MANA's success was determined by comparing the high confidence correlated alerts (NIDS output) against the cyber red team's attack logs to provide ground truth that there was an attack, the type of attack, when it was launched, and against which IP address.

The cyber red team was unable to compromise any replicated device within the Spire-defended section of the network. Commands given to devices to exceed their safety parameters were ignored by the Prime multi-compiled replications. The cyber red team was also unable to isolate the defended devices from the control system or to perform denial-of-service (DoS) attacks on the ports that interfaced with the protected devices. This is consistent with results from the Phase 1 designed experiment at PNNL.

Additionally, data gathered by HECO showed that Spire did not induce latency or errors in control system's communications or devices. In fact, plant engineers observed that in some areas, Spire's response time was faster (approximately twice as fast) than the baseline system.

5. COST ASSESSMENT

Costs for acquiring, installing, and operating a cyber-aware, fault-and-intrusion-tolerant defense vary since the entire defense can be installed by the user/purchaser of the software and equipment. However, assuming all new equipment and installation by the technology providers, total cost for one installation is estimated to be $250,000, not including travel.

Page Intentionally Left Blank

6. IMPLEMENTATION ISSUES

The primary implementation issue for the technologies is inertia and resistance to change. For an IT professional, implementation of the critical energy infrastructure cyber defense-in-depth will be no harder than any standard day-to-day IT task using familiar tools and technology. The challenge will be installing in an unfamiliar power plant. Conversely, for the plant engineer or OT network professional, this will be all new, even though it has been done routinely in the enterprise part of the utility's network for decades. Plant personnel will also have an additional screen to monitor, but it will provide near-real-time, highly correlated, cyber SA of threats to the plant.

6.1. RESULTS

6.1.1. Overall Results

The Phase 1 results showed areas where all of the technologies needed improvement. Additionally, comments from the HECO, Naval Facilities Engineering and Expeditionary Warfare Center (NAVFAC EXWC), and PNNL SMEs suggested other areas for improvement in the technologies' displays and controls.

The Phase 2 operational validation reinforced the Phase 1 results that an aware cyber defense-in-depth using the Johns Hopkins' fault-and-intrusion-tolerant technologies and the aligned MANA NIDS provides significantly better protection for control systems than the NIST-compliant baseline architecture alone. HECO's plant network used the 18 control families of NIST SP 800-53.[1] However, to test the cyber defense-in-depth technologies, many of the regulatory access, physical, and training controls were set aside to permit a focused and timely demonstration. As in Phase 1, plant compliance with the cyber-specific portions of NIST offered no effective protection from a sophisticated threat. The results of the Phase 2 operational validation establish that fault-and-intrusion-tolerant technologies can protect a utility's OT networks from an advanced and determined cyber threat with insider access. The BlackEnergy and Stuxnet incidents show that even isolated ICS networks are subject to penetration when threats jump across air-gaps into the OT networks.

The results of the Phase 2 operational validation in a functional commercial power plant proved that the MANA and Spire technologies:

- Function in a power plant,
- Are compatible with power plant equipment,
- Do not induce latency or errors in plant networks or devices, and
- Are highly effective at identifying cyber penetrations and preventing their disruptive impact.

The results also strongly suggest that the DoD, the DHS, and commercial utilities should consider implementation of cyber defense-in-depth architectures using fault-and-intrusion-tolerant technologies combined with an aligned machine-learning NIDS to protect the control systems and SCADA systems of critical infrastructure.

[1] NIST Special Publication 800-53, Security Controls and Assessment Procedures for Federal Information Systems and Organizations, https://nvd.nist.gov/800-53.

6.1.2. MANA Results

The MANA NIDS performed bettered than anticipated, catching Network Mapper (NMAP) and reconnaissance conducted by the cyber red team, as well as the deliberate attacks done during the demonstration, with almost zero false positives and no false positives among the high confidence alerts. This was a marked improvement in MANA performance from the Phase 1 experiment results at PNNL.

In Phase 2, MANA had no false positives in the high-confidence-correlated alerts group. The MANA's patented correlation processes eliminated all false positives from the "high confidence" alerts forwarded to the human operator/plant defender for action. The high-confidence alerts had zero false positives. However, lower confidence level alerts did include some false positives. It is believed that refinement of the patented correlation process and other patented proprietary adjustments enabled this improvement in the NIDS performance.

6.1.3. Spire Results

The Spire fault-and-intrusion-tolerant technologies worked as intended without inducing latency, errors, or failure in the control system being defended or the devices connected to the control system. The fault-and-intrusion-tolerant technologies secured the control system's functionality, despite the presence of the cyber red team within the network. Additionally, data gathered by plant engineers showed that normal system latency was decreased in the areas defended by the Spire technologies. Note: HECO retained all network data due to confidentiality concerns regarding plant cybersecurity, equipment, and performance.

The cyber red team was unable to compromise any Prime-replicated device within the Spire-defended section of the network. Commands given to devices to exceed their safety parameters were ignored by the Prime multi-compiler replications defending the devices. The cyber red team was also unable to isolate the defended devices from the control system or to perform DoS attacks on the ports that interfaced with the protected devices. This is consistent with results from the Phase 1 designed experiment at PNNL. However, these same attacks were dramatically successful against the undefended portion of the plant network.

6.2. CONCLUSION

This operational validation showed that the two cybersecurity technologies, MANA and Spire, work as intended without inducing latency, errors, or failure in a functioning commercial power plant. The operational validation also confirmed that the Spire technologies, when combined with aligned machine learning sensing, provide better cybersecurity of a control system network than that of NIST-compliant architecture alone.

This project showed conclusively that the Spire fault-and-intrusion-tolerant technologies are powerful in and of themselves. But, combined with an aligned MANA NIDS (using heterogeneous sensor architecture and an internal correlation engine), the cyber-aware fault-and-intrusion-tolerant defense strips the initiative from the hackers and conveys it to the defenders in a way that delivers a true "fight through" capability for critical infrastructure dependent on ICSs.

It is recommended that the DoD, government agencies and organizations, and utility companies start employing the fault-and-intrusion-tolerant technologies with appropriate machine learning sensing methodologies so that the Nation's ICSs are able to operate unimpeded when—not if—intrusions occur. The combination of the Spire fault-and-intrusion-tolerant capabilities with the greatly enhanced SA provided by MANA offers the defenders of the Nation's critical infrastructure the opportunity to seize and hold the initiative in the cyber domain. These technologies complement NIST and NERC CIP and add layers of defense where currently there are none.