



UPDATES

Welcome to our bi-annual Installation Energy and Water newsletter, where we provide periodic updates about new information & products available from the Installation Energy and Water Program Area.

Critical Energy Infrastructure Cyber Defense In-Depth

Department of Defense (DoD) operates over 500,000 buildings and structures with diverse inventory encompassing barracks, commissaries, data centers, office buildings, laboratories, and aircraft maintenance depots. As DoD works towards incorporating more networked (“smart”) devices to improve building operational efficiency and increase capability, threat and vulnerability to cyber-attacks has also increased. In fact, it is one of the fastest growing threats to DoD installations’ information technology (IT) and operational technology (OT). SCADA (Supervisory Control and Data Acquisition) systems must ensure continuous availability and correct operation in the presence of compromises and attacks at both the system and network level. Currently, the most common approach to protecting OT from cyber-attack is to create a separate dedicated control system network that is “air gapped” from the business network and public internet. In many cases, this approach is cost prohibitive and still requires additional process security measures to ensure protection from the various threat vectors.

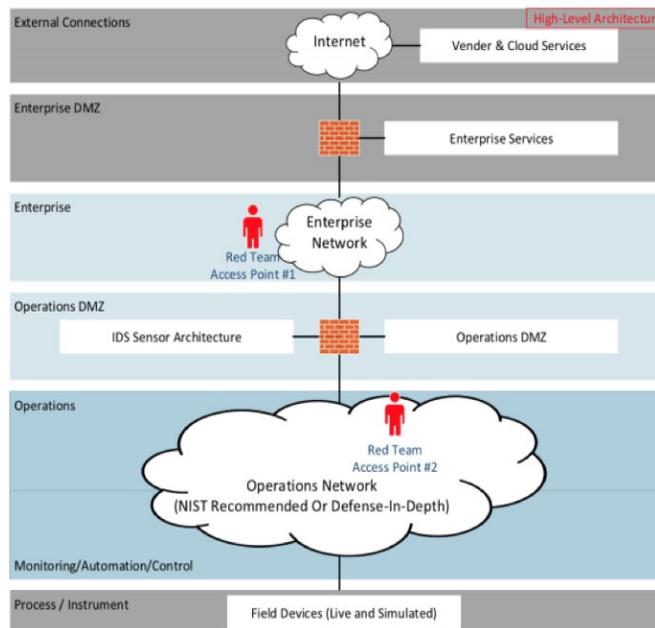


Figure 1 - (U) Depiction of Test Environment

To fully realize the benefits of smart technologies, new solutions for identifying and protecting against cyber threats need to be developed. To address this critical need, ESTCP issued a topic on cybersecurity, “Cybersecure Connectivity for Energy System Components and Military Installation Energy Infrastructure”, under its FY16 annual solicitation. The topic called for proposed solutions that would improve installation energy system’s cybersecurity by enabling components of building energy systems to use military networks to send/receive data and control signals and automatically sense and respond to ancillary service signals. These solutions are required to meet the DoD RMF requirements.

One of the proposed solutions selected under this topic was the project [EW-201607](#), Critical Energy Infrastructure Cyber Defense In-Depth, led by Mr. Kevin Jordan of Resurgo, LLC. The objective of this project was to successfully demonstrate an Intrusion Tolerant Cyber-secure defense-in-depth of an electrical power plant against attacks representative of Tier V/Nation-state actors. And, to demonstrate a new capability to mitigate and recover quickly from online and insider cyber activities directed against SCADA infrastructure.

In the demonstration, two technologies, Machine-learning Assisted Network Analyzer (MANA™) and Spire, were used to defend the Hawaiian Electric Company (HECO) power plant in an operational test. Spire is a suite of fault and intrusion tolerant technologies and MANA™ is an Intrusion Detection System (IDS) that uses machine-learning based tools to catch new and morphed (altered) attacks that traditional signature sensors cannot catch. Both Spire and MANA™ are compatible with all networks using IP based traffic to include variations such as MODBUS over Transmission Control Protocol/Internet Protocol (TCP/IP). Spire defended the network and certain hardware, while the MANA™ Network Intrusion Detection System (NIDS) provided the operator with cyber situational awareness (SA) missing from the Spire technologies. The MANA™ NIDS is passive and received all traffic via a one-way network tap. Together, both technologies successfully defended the HECO plant from intrusion attack.

The MANA™ NIDS was able to detect all attacks from initial reconnaissance through exploit and port denial of service to hide the exploits. Spire successfully protected all systems it was implemented on. Illegal commands given to Spire protected plant equipment were ignored by the multi-compiled Prime replications within Spire. Additionally, neither MANA™ nor Spire induced latency or errors in the plant's control systems, communications, or devices. Plant engineers observed that in some areas Spire's response time was faster (approximately twice as fast) than the baseline system.

Additional details on the performance and cost can be found in the Final Report, which will soon be posted on the project webpage.

Recently Released Documents Available for Download

- EW-201254 - “Optimizing Operational Efficiency: Integrating Energy Information Systems and Model-Based Diagnostics” - [Final Report and Cost & Performance Report](#)
- EW-201344 - “High Efficiency Dehumidification System (HEDS)” - [Final Report and Cost & Performance Report](#)
- EW-201346 - “Demonstration of the Zero Emission Distributed Generation and Storage System” - [Final Report](#)
- EW-201511 - “Automated Aerosol-Sealing of Building Envelopes” - [Final Report and Cost & Performance Report](#)
- EW-201512 - “Demonstration and Cost Analysis of a Building Retorfit Using High Performance Insulation” - [Final Report and Cost & Performance Report](#)
- EW18-5280 - “High Efficiency Dehumidification System (HEDS) Additional Proof of Concept” - [New Start Project Overview](#)
- EW18-5309 - “Military Energy Resilience Catalyst” - [New Start Project Overview](#)
- EW18-5329 - “Fast and Secure Integration of Industrial Controls using a Common Configuration” - [New Start Project Overview](#)

Key Events and Meetings

November 27-29, 2018 - SERDP & ESTCP 2018 Symposium

The 2018 Symposium will be held from November 27-29 at the Washington Hilton Hotel in Washington, D.C.

Out of the 16 sessions, EW program is hosting two technical sessions, one on Cybersecurity of Facility-Related Control Systems and one on Installation Resilience. The cybersecurity session, on Tuesday, November 27, 2018, 1:45 - 5:00 PM, will discuss the facility related control systems (FRCS) policy and legislation, gaps in cyber protection, R&D efforts and more. The Installation Resilience technical session, on Wednesday, November 28, 2018, 8:30 - 11:45 AM, will explore engineered systems developed to increase the resilience of specific systems or infrastructure. This session includes two distinguished panels, discussing the technology's role in installation resilience and metrics and approaches for modeling installation resilience.



In addition, EW will conduct a short course on the Risk Management Framework. The RMF How-To short course is geared to help ESTCP Investigators and Project Teams become familiar with the process of applying and obtaining and Authorization to Operate on the DoD Information Network. Registration for the short course is a separate modest fee. [Sign up here](#).

Register for this year's event at the [2018 Symposium Website](#).

Upcoming Conferences

January 12-16, 2019 - ASHRAE Winter Conference

The 2019 ASHRAE Winter Conference will be held in Atlanta, GA. Look for ESTCP Principal Investigators presenting on their projects at technical sessions. [MORE](#)

July 8-10, 2019 - ARPA-E Energy Innovation Summit

The ARPA-E Energy Innovation Summit's annual conference is heading to Denver, CO in 2019. Stay tuned for updates on ESTCP's presence at The Summit. [MORE](#)

Follow the [Installation Energy and Water LinkedIn](#) page for current news regarding the Program Area!