U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Enabling Situation Awareness/Assessment for Utility Operators and Cybersecurity Professionals (Situation Awareness)

Pacific Northwest National Laboratory (PNNL)

Eric Andersen, PM/ Mark Rice, PI

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

Summary: Enabling Situation Awareness/Assessment for Utility Operators and Cybersecurity Professionals

Objective

- Develop visualizations that power system operators and/or cybersecurity professionals can use to make fast, accurate assessments of situations, enabling them to maintain situation awareness during unfolding events.

Schedule

- January 2015 – December 2018

Total Value of Award:	**$1,980,000**
Funds Expended to Date:	**93%**
Performer:	**Pacific Northwest National Laboratory**
Partners:	**Idaho National Laboratory** **Western Area Power Administration** **Peak RC** **General Electric (Alstom Grid)** **Total Reliability Solutions** **Excelsior Design, Inc.** **(Dr. Jodi Hientz-Obradovich)**

Advancing the State of the Art (SOA)

- Cybersecurity for electric grid critical infrastructure is an emerging field. Visualizations for control rooms and network security operations centers are being developed to aid decision making with increasing volumes of operations data. Some work has been done in the past in this area, but the tools developed have seen little use in utility operations.
- Our approach is different because we are engaging the primary stakeholders, the control room operators, and cybersecurity professionals, as part of our iterative design process.
- By engaging our primary stakeholders, we build credibility and ensure that our design is robust, and more importantly, that it will work in their environment and meet their needs.
- Utilities will benefit from having a visualization tool(s) to aid decision making when faced with cybersecurity concerns.

Challenges to Success

Understand the communication pathways for cyber information

- Conducting analyses to determine how to facilitate communications between appropriate parties so a shared awareness of the situation is quickly reached.

Designing useful visualizations

- Using the iterative design process with our stakeholders to understand the context in which the information needs to be displayed so a rapid, optimal decision is made by the appropriate personnel.

Coordination of Usability Testing with Utility

- Participation of utility cybersecurity professionals is problematic due to limited time availability.

Progress to Date

- Identified information that is essential for identifying potential cyber threats, as well as identifying who makes use of this information at a transmission utility
- Identified demonstration use cases for showcasing the visualization system developed as a part of the project
- Created a working proof of concept of the User Interface (UI) using SRS (PNNL developed capability) and Splunk
- Briefed the project to WAPA CISO and Regional Manager for Sierra Nevada
- Drafted a test plan for demonstrations at EIOC and WAPA
- Worked with Peak RC to use their Dynamic Training Simulator (DTS) to run our use cases for the usability testing

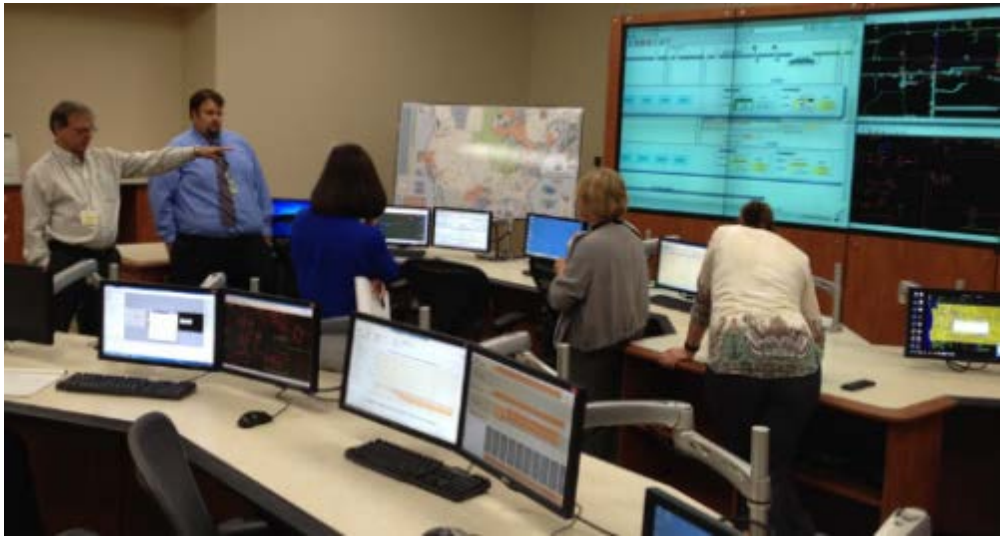
Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

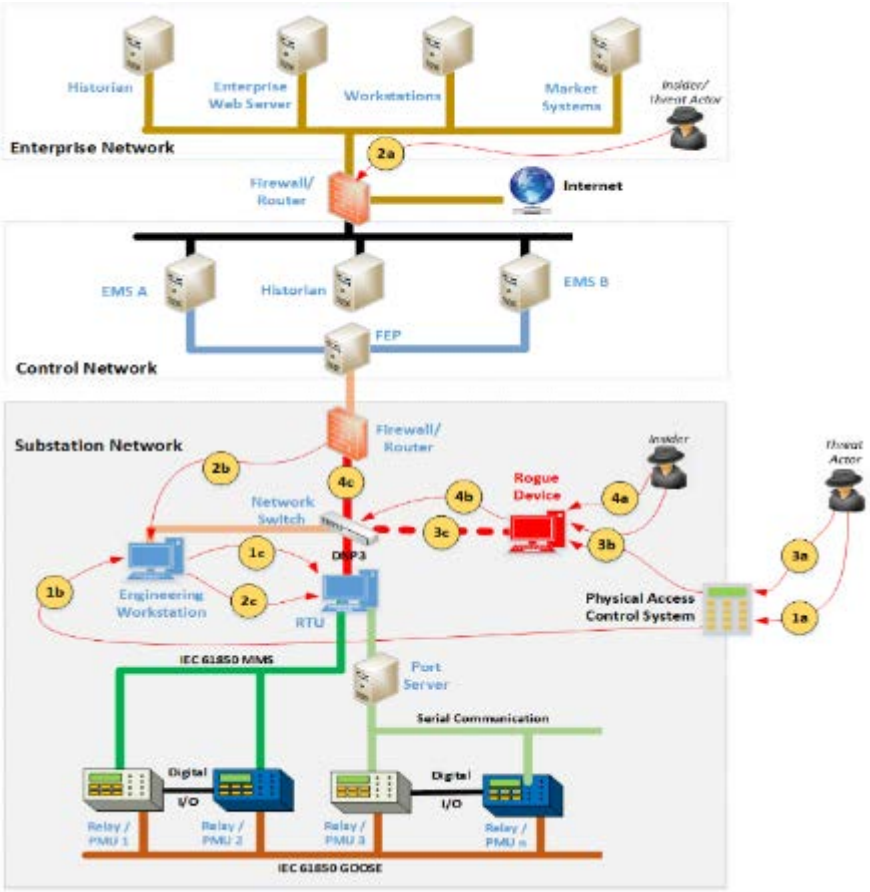
- This project will develop agnostic prototype visualizations that could be used by a wide variety of utility-based systems, including vendors for EMS, DMS, and NSOC applications.

What are your plans to gain industry acceptance?

- PNNL's EIOC is being configured with a GE EMS to prototype the visualizations as a testbed with real utility operators and cybersecurity professionals providing real-time feedback and input.



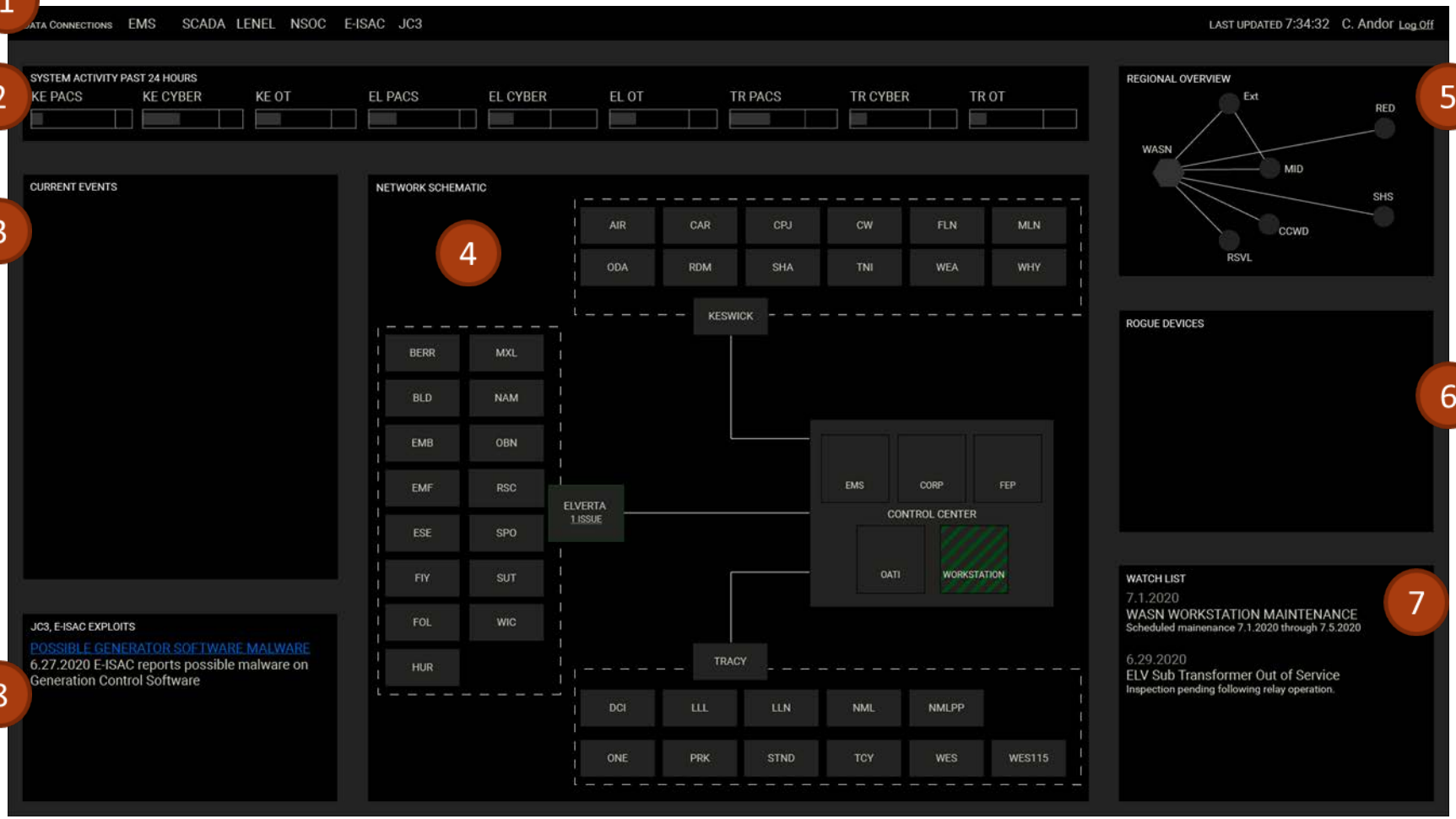
Demonstration Use Cases



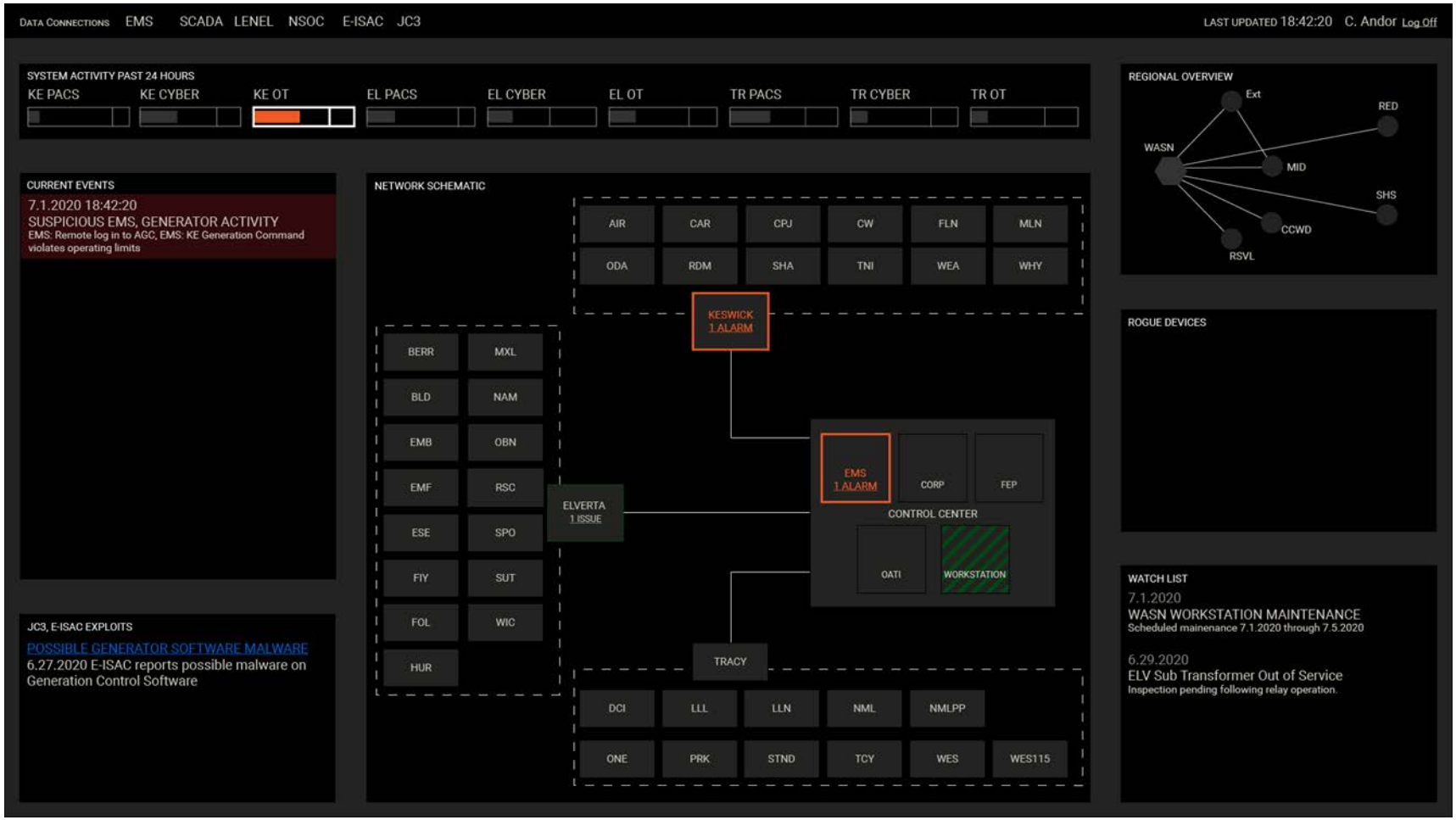
Use Cases

- **UC 1: Physical break-in, RTU Configuration Change, and Reboot**
- **UC 2: Unauthorized Remote Login to Change Critical Files**
- **UC 3: Unauthorized Network Configuration Change and Rogue device**
- **UC 4: Man-in-the-Middle Alters Telemetry/Control Data**

Top Level Dashboard
UC-001 Pre-Event Conditions FY18



Top-Level Dashboard
UC-002 KE Gen Low MW



Next Steps for this Project

Approach for the next year or to the end of project

- Project is winding down.
- Final testing planned in December with WAPA and SNR.