Essence™ Integration Pilot (EIP)

The cyber security landscape in the energy sector can be broadly categorized into Operational Technology (OT) and Information Technology (IT) systems. IT is comprised of the enterprise business systems necessary to manage business operations. OT is comprised of the operational systems necessary to monitor and control the power grid or refine and distribute energy products. The Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) recognizes that the nexus of these domains requires awareness to track adversarial cyber threats that target OT and IT environments.

To that end, DOE CESER engaged on a pilot project to integrate IT and OT information from live environments. The Cybersecurity Risk Information Sharing Program (CRISP) administered by the Electricity Information Sharing and Analysis Center (EISAC) and powered by the Pacific Northwest National Laboratory (PNNL) has developed analytics and processes to provide cyber “situational awareness” utilizing a system of sensors and bespoke analyst-driven algorithms for anomaly detection in the IT network space. The National Rural Electric Cooperative Association (NRECA) Essence™ research program provides cyber "situational awareness” through its collection and rules engine components for the electric OT network environment. Under this pilot project, PNNL and NRECA explored the opportunities presented by the combination of these two disparate data sets. To achieve the goals of the project the project team focused on the four major technical tasks:

- Instrumentation
- Data Management and Processing
- Analytics
- Engagement and Validation

Results

1. As a direct result of the CEIP Project:
   - CRISP gained 5 new participants from a generally underrepresented group within the electric sector,
   - developed, tested, and deployed the Operations Sharing Device (OSD) which can serve as a proof of concept for OT data sharing,
   - and new relationships were built between CRISP and NRECA, CRISP and new industry partners, and CRISP and OT organizations with current CRISP participants.

2. NRECA/Essence
   - The Essence program benefited from several successful outcomes from this project, including improved deployment procedures, insight into data quality issues and best practices for span/mirror port configuration on OT switches.
   - New utilities from rural distribution cooperatives to transmission ISOs learned about both the Essence and CRISP programs. New cross-organizational working relationships were created, and existing relationships were strengthened.

- New features were added, and stability issues were resolved. An automated process was created to correlate and publish this information for both teams so that, at a glance, every team member could be aware of what version of each component was installed, and if data was flowing between the Essence sensor and the OSD.

3. OT/IT Fusion
   - OT/IT fusion consisted of analyzing the available OT data to determine if it contained any external interactions and if those external interactions were observable in the IT data. Example interactions included DNS lookup and connections to cloud services showing that the OT environment had interactions with the IT environment, including access to the public internet.
   - When IT and OT interactions were seen, further analysis determined whether those interactions were legitimate. Legitimate interactions could include making OT data available to organizationally internal IT-based decision makers or providing it to other IT systems (e.g., energy accounting). If the OT data were made available outside the organization's IT environment, it could be legitimate, or it could represent a data exfiltration.
   - Interaction which involved reaching into the OT environment from the IT environment required additional analytics. If the access was from the organization's, IT environment to its OT environment, and it was engineering access (e.g., access by an engineer to update settings or extract ad hoc data), the interaction was probably legitimate. If the access used SCADA protocols and contained scan or control commands, or access was from outside the organization, the interaction was most likely not legitimate (although there are cases of legitimate use of the Internet as a transport for some OT protocols and functions).

EIP Summary

1. The key stakeholders included:
   - Department of Energy, Office of Cybersecurity, Energy Security and Emergency Response (DOE-CR): Program Manager and funding agent.
   - Pacific Northwest National Laboratory (PNNL): Project Manager and source of IT data for the pilot using CRISP capabilities.
   - NRECA: Subcontractor to PNNL and source of OT data for the pilot using Essence™.
   - North American Electric Reliability Corporation/Electricity Information Sharing and Analysis Center (NERC/E-ISAC): Collaborator and CRISP Program Manager.
   - Nine pilot electric utility partners.
2. The CRISP Essence™ Integration effort was a success in that the team demonstrated they could add experimental and rapidly changing 3rd party sensor data and integrate, transport, and provide baseline CRISP like Analytics securely into the existing "operating" architecture.
3. IT/OT fusion research is and will be of increasing importance as emerging communication networks are integrated in combination with increasing substation and

GRID complexity and the inevitable resulting increase in attack space (substations becoming data centers).

4. The CRISP platform provides unique and critical foundational capabilities that can allow visibility into the inside and outside communication traffic as well as correlation with other sensitive data sources.

Lessons Learned

1. Participant organizations (especially those with transmission or large generation assets) must comply with the NERC Critical Infrastructure Protection (CIP) standards, and they have developed policies and procedures to ensure compliance by organizations interacting with their systems.
   - The participant organization must protect its OT environments from external influences, which does include research endeavors such as the EIP.
   - The utility organization must understand the software that is running in their environment and its communications requirements, so autonomous software and firmware updates performed by NRECA or PNNL required oversight by the participant utilities.
   - The utility organization must document and justify all network interactions that cross an "electronic security perimeter—ESP", including data connections with EIP systems.
   - The teams had not adequately accounted for compliance with NERC CIP requirements, and the additional requirements that had to be met, resulting in longer lead times to tune systems.
2. Device Installations
   - Coordinating work with industry partner OT and IT staff, as well as PNNL, NRECA, and EISAC presented several challenges, as the level of integration necessary to conduct the research required all partner input.
   - Partly due to COVID-19, there were delays in installing Essence™ devices, OSDs and ISDs during the project. The installations needed to be coordinated with already busy industry staff during pandemic lockdown.
3. Time Synchronization
   - Early in the OT/IT Fusion analysis, it was determined that the Essence device and the ISD needed, at minimum, to be time synchronized to be able to compare OT and IT conversations. Additional capability to link conversations is a potential future research area.
4. Data Volume

   The large volume of OT data caused issues that had to be addressed by NRECA and PNNL over the course of the data exchange of the project. These issues included:
   - Essence device congestion (only on the very large sites).
   - If the Essence device was not directly connected to the OSD, flooding the site's OT network with Essence to OSD traffic.
   - OSD congestion (only on the very large sites).

Future Plans

1. Essence Version 3.x
   - This pilot implemented Essence 1.x, which is the research project funded in part by DOE. Essence 1.x had limitations in data that was provided. NRECA has since released Essence 3.x as a commercial product, investigating new functionality to address this lesson learned.
2. Data thinning/analytics at the edge
   - As field data volumes increase, the need to perform data thinning and analytics close to the edge becomes more important. Data thinning/analytics at the edge can radically reduce the volume of data and information without loss of information size. This also reduces the impact on the OT system as well as the network transport and storage requirements of the data warehouse. Data thinning at the warehouse side also allows for larger windows into the collected data for more effective analysis (greater temporal size). Data thinning approaches have a large combination of low hanging fruit as well as research areas that have large potential ROI.
3. Sensor Agnostic
   - Sensor selection should consider not only the data feed format, but also whether it can support the data thinning and distributed analytics. A data agnostic approach is the probable best way forward for analytics to allow for the use of nonproprietary collection technological solutions and a multitude of proven commercial capabilities. This approach also allows the analysis and reporting on of existing collections of data as well as near real time streams. The algorithms and approaches developed and to be developed can also be integrated into other systems, dashboards, and operational scenarios.
4. Testbed Development
   - When using actual field data to develop analytics, the field data shows only a small subset of possible network traffic. In most cases it should not include any malicious traffic, nor does it include infrequent or abnormal electric system conditions such as protection operations, impacts from lightning strikes, blackout, and blackstart, etc. Occasional normal operations such as SCADA dispatcher commanded breaker operations are also infrequent; therefore, generating analytics for such infrequent events may be difficult. Using a controlled laboratory emulation and simulation environment will allow a configurable and repeatable set of communications scenarios to be developed, sensed, and reported that will allow development and testing of these new and existing analytical methods, as well as to test any enhancements to a data collector that can support the new analytical methods or approaches. The controlled data generation in a lab will also provide critical training data for rare and catastrophic potential events that might be seen in a live GRID environment.