BACKGROUND
The primary focus of security analysts is to ensure correct behavior in operational technology and identify the connections between information technology (IT) data and unwanted operational behavior, such as disruptions to systems or services. The end goal is to improve detection and remediation of those unwanted behaviors. But analysts can only correct what they can actually see. Without proper sensors in place, an analyst might never see an event, either as it happens or after the fact.

THE CHALLENGE
Energy companies rely on operational technology to control the generation, transmission, and distribution of power. While there are a number of useful products on the market for monitoring enterprise networks for possible security events, these products tend to be imperfect fits for the unusual requirements of control system networks. A network monitoring solution that is tailored to the needs of control systems would reduce security blind spots.

GOALS
To improve the security of information and operational technology, including industrial control systems (ICS) and related networks, energy companies need mechanisms to capture, transmit, analyze and store real-time or near real-time data from across these networks and systems. The situational awareness project explores the methods by which energy providers can more readily detect and remediate anomalous conditions, investigate the chain of events that led to the anomalies, and share findings with other energy companies.

The goal of this project is to help energy companies:

• Integrate data visualization and analysis capabilities that help dispatchers and security analysts view control system behavior, network security events, and physical security events as a cohesive whole
• Allow dispatchers and security analysts to easily automate common, repetitive investigative tasks
• Facilitate the sharing and acquisition of new threat indicators, correlation rules, mitigations, and investigative techniques
• Create customizable interfaces that allow users to tailor the system to meet specific business needs
• Automate report generation to aid utilities in demonstrating compliance with relevant standards

BENEFITS
The potential business benefits of the situational awareness solution explored by this project include:

• Improves a company’s ability to detect cyber-related security breaches or anomalous behavior, likely resulting in earlier detection and less impact of such incidents on energy delivery, thereby lowering overall business risk
• Increases the probability that investigations of attacks or anomalous system behavior will reach successful conclusions
• Improves accountability and traceability, leading to valuable operational lessons learned
• Simplifies regulatory compliance by automating generation and collection of a variety of operational log data

SITUATIONAL AWARENESS
Securing Networked Infrastructure for the Energy Sector

The National Cybersecurity Center of Excellence (NCCoE) is addressing situational awareness for the energy sector through collaborative efforts with members of the sector and vendors of cybersecurity solutions. This fact sheet provides an overview of the background and challenge, goals, and proposed solution. For more information about the project, see the Situational Awareness project description on the NCCoE web site. The situational awareness solution we propose is not the only one available in the fast-moving cybersecurity technology market. If you would like to propose an alternative architecture or know of products that might be applicable to the challenge we are attempting to address, please contact us at energy_nccoe@nist.gov.
ARCHITECTURE

COMPONENTS
Situational awareness solutions for energy companies include but are not limited to the following components:

- security incident and event management (SIEM) or log analysis software
- ICS equipment, such as remote terminal units, programmable logic controllers, and relays, along with associated software and communications equipment (e.g., radios and encyptors)
- “bump-in-the-wire” devices for augmenting operational technology with encrypted communication and logging capabilities
- software for collecting, analyzing, visualizing, and storing operational control data (e.g., historians, outage management systems, distribution management systems, and human-machine interfaces)
- products that ensure the integrity and accuracy of data collected from remote facilities

DOWNLOAD THE PROJECT DESCRIPTION
For more information on this project, visit https://nccoe.nist.gov/projects/use_cases/situational_awareness

HOW TO PARTICIPATE
As a private-public partnership, we are always seeking collaborators, insights, and expertise from businesses, the public, and technology vendors. If you have questions about this project or would like to join the Energy Provider Community of Interest, please contact us at energy_nccoe@nist.gov.