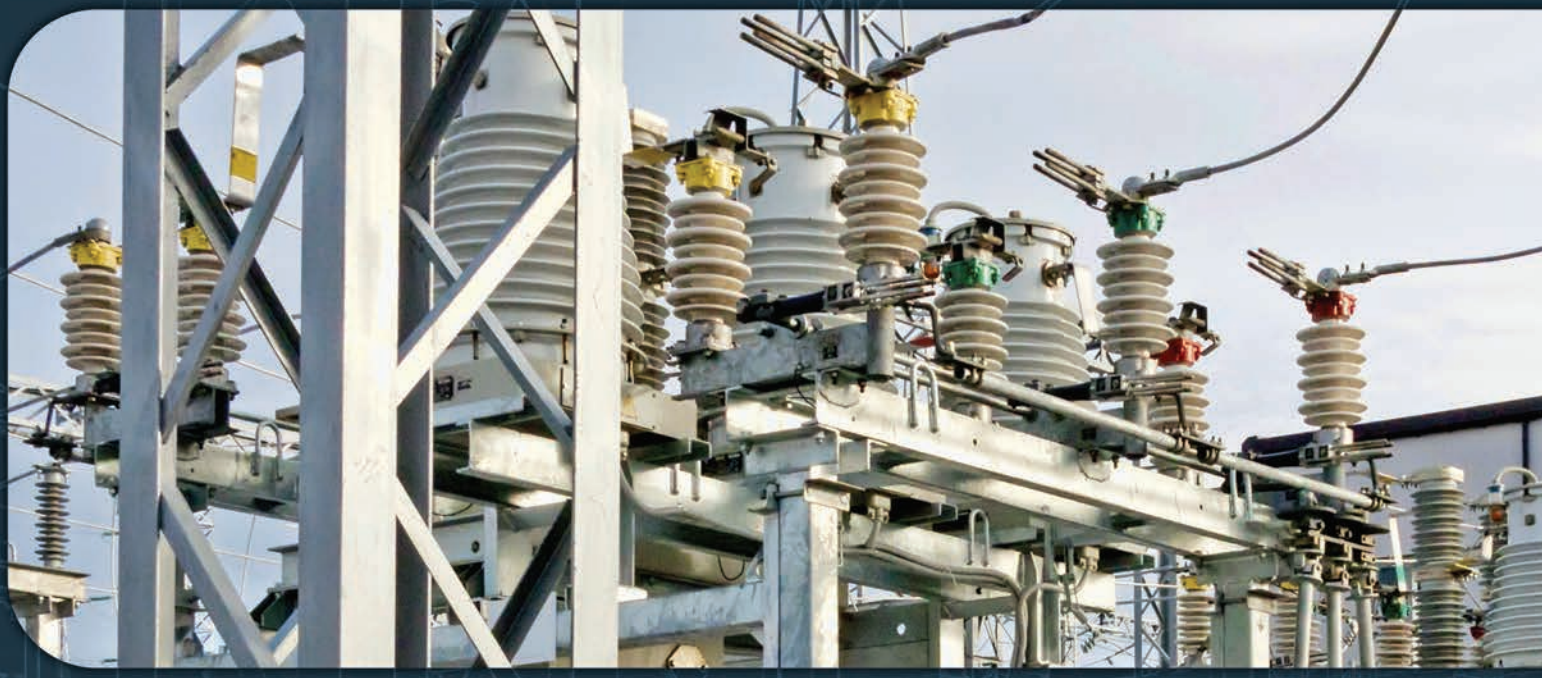
EPRI Integrates Transmission Security with Advanced System Threat Analysis

"We have defense in depth. We need defense in breadth."



An alarm rings at a utility security center signaling that a fence may have been cut at a substation. Another alarm rings at corporate cyber security offices, indicating an unauthorized attempt to access control equipment at the same substation. A third alarm at a grid dispatch center indicates that a transformer at the substation has failed. In most cases, each alarm would be handled separately, by personnel who have no way of knowing the larger picture that the three alarms could present if analyzed together. EPRI's Integrated Threat Analysis Framework (ITAF) would change that, analyzing the different alarms to create a comprehensive threat assessment for security personnel.

"EPRI had been researching how utilities can establish Integrated Security Operations Centers, or ISOCs, pulling together physical and cyber security events from various domains of operations," said EPRI Senior Program Manager Galen Rasche. "After the Metcalf incident, we began asking whether we could include events from grid operations in the ISOC."

In April 2013, saboteurs attacked the Metcalf, California, substation of Pacific Gas & Electric Co. They cut telephone cables and began shooting. It took 10 minutes for operators in a nearby building to realize what was happening and call for help. In 19 minutes, saboteurs knocked out 17 transformers and escaped. While grid operators rerouted power and avoided any blackouts, it took PG&E 27 days to restore service at the substation.

That event led to the ITAF, said Rasche. "Other utilities looked at how long it took for personnel to get a clear idea of what was happening, and asked if they could do better. Not many could. Metcalf was the catalyst for this project."

The ITAF project is identifying barriers to integrating data from grid events with data from physical and cyber security events. A major challenge is developing an automated system that can evaluate the data from power system sensors and detect which patterns represent threat scenarios. "We need to have a very intelligent, analytic system," said EPRI Principal Technical Leader Ralph King. Researchers must work closely with operations staff to achieve a solid understanding of grid operations, and then develop algorithms to recognize and analyze anomalies across multiple domains. The system must be aware of things such as maintenance schedules so that false alarms can be minimized. "Raw power system data don't integrate very well into existing security platforms. We have to transform the data into something useful," he said.

The project will test its event analysis frameworks in the laboratory and in real-world settings. Rasche said several utilities are building or planning ISOCs, and they see the ITAF project as "a logical progression." Adding the transmission system to the larger security mission requires broadening security concepts, he said. "We have defense in depth. Now we need defense in breadth."