In Development

Who's Responsible for Security in a "Multi-Party Grid"?

EPRI Develops Guidelines and Methods to Strengthen Cyber Security for Distributed Energy Resources

By Brent Barker

Growing deployment of rooftop solar, energy storage, microgrids, and other distributed energy resources (DER) poses unique cyber security challenges. Traditionally, utilities have tightly controlled cyber security of grid assets, but DER occupy a looser space on the periphery of the distribution system. They are connected to the grid, yet are often privately owned by third parties.

"Some entities own the devices, while others manage them. Still others provide private communication networks or communicate with devices using the Internet, which nobody owns," said EPRI Principal Technical Leader Candace Suh-Lee. "The big question is, where should the responsibility for security lie in this multi-party grid? We need a model that resolves this question within a few years, or we are going to face various scenarios that threaten grid security. For example, we may not know how to respond to an active cyber attack because we don't have a collaborative incident response plan. If a device owned by a third party makes a suspicious connection request, we may not know whom to contact. Or, we may not have a solution to a known security flaw since the responsibility for the fix is not specified in any contract."

"The grid is especially vulnerable in areas with a high penetration of solar photovoltaic (PV) as more third parties become involved in controlling energy resources and transmitting data to and from them," said EPRI Senior Program Manager Galen Rasche. "Further deployment of DER could slow or stall if we don't address cyber security adequately."

Growing rooftop solar poses cyber security challenges for the distribution grid.

To address these concerns, Suh-Lee is developing guidelines for secure communication architectures. These would serve as a reference architecture for utilities, aggregators, solar component manufacturers, and other companies involved in DER communications. According to Suh-Lee, these guidelines can inform industry standards from organizations such as the National Institute of Standards and Technology and the Institute of Electrical and Electronics Engineers (IEEE). Jurisdictions can address cyber security by establishing regulations that refer to these standards.

"It takes years to develop industry standards. Our goal is to develop the guidelines rapidly, make them available to the public by the end of 2018, and engage with standards bodies," said Suh-Lee. "We're working collaboratively with the SunSpec Alliance—comprising solar component manufacturers and integrators—to develop reasonable, practical guidelines for a secure network architecture."

"This process has involved extensive discussions to sort out differences of opinion. Utilities and third parties initially had different perspectives on the need for a secure network architecture," Suh-Lee continued.

"At first, many third parties saw limited benefit to the guidelines and were concerned about the cost implications. Eventually, they came to recognize the importance of understanding the cyber risks in order to protect their investments in solar power infrastructure. If the systems are hacked and not producing power, there could be quick and steep financial consequences," said Suh-Lee.

Suh-Lee also is developing a white paper that outlines a methodology to assess security risks in a multi-party grid—and that suggests for stakeholders' consideration a potential manner in which to enforce security responsibilities appropriately. Participants in a multi-party grid include:

- **Customers:** Owners of houses with rooftop solar are often customers of several service providers, including utilities, aggregators that manage DER, and private communications networks.
- **Utilities:** DER data flows back to the utility, which manages demand response and provides customers with grid power as well as backup power when DER go offline.
- **Aggregators:** These private companies manage numerous DER and controls on their networks, compete for new business among DER owners, and sign up customers for services. They can provide utilities with demand response services and operational data on DER.
- **Manufacturers:** Smart inverters can communicate with the grid and are connected to the manufacturers' proprietary networks, enabling data collection and periodic software updates. Cyber security must be designed and built into inverters and other smart devices in the factory—not on a rooftop after they are installed.
- **Standards and certification bodies:** Standards organizations certify various functions and attributes of smart devices. Ideally, manufacturers build cyber security into their devices and then standards bodies certify these features. To make this process routine, manufacturers will need to implement cyber security features in parallel with efforts to develop their devices' functional requirements.
- **Industry trade groups:** Industry groups can serve an important role in facilitating DER cyber security. The SunSpec Alliance, comprising more than 100 solar and storage companies, is pursuing information standards to enable interoperability among grid assets and DER.

The forthcoming white paper will describe an idea for a "cooperative security model." This provides a way for a regulator, utility, or other entity to manage and track cyber security tasks among many different interconnected devices and systems owned or managed by multiple parties. Tasks of concern include secure communications, security patch updates, threat detection, and incident response.

As part of a project to support high solar PV penetration, the California Energy Commission is considering the use of a new communications protocol with smart inverters and has commissioned an EPRI "red team" to probe its vulnerabilities. The protocol, known as *IEEE 2030.5*, is intended to connect DER with grid operations.

"Our job as a red team will be to hack into smart inverters," said Suh-Lee. "We are working with highly skilled, reputable hackers who are very familiar with grid operations."

According to Suh-Lee, the central question guiding EPRI research in all these areas is, "How radically will cyber security change communications on the grid?"

KEY EPRI TECHNICAL EXPERTS

Candace Suh-Lee, Galen Rasche