Webinar: Cybersecurity and Distributed Energy Resources

July 9, 2020

Presented by the Resilient Energy Platform

Developed through the USAID-NREL Partnership, the Resilient Energy Platform provides expertly curated resources, training materials, data, tools, and direct technical assistance in planning resilient, sustainable, and secure power systems.

Responses to Attendee Questions

A recording of the webinar and the webinar slides are available at https://resilient-energy.org/training-and-resources/webinars.

While we were able to answer some attendee questions during the webinar, we did not have enough time to respond to all the great questions we received. Our presenter, Maurice Martin, Senior Cybersecurity Research Leader at National Renewable Energy Laboratory, kindly provided responses to those questions. We sent these responses directly to the attendees who asked the questions and compiled them in this document.

Question 1

What are the applications of distributed energy resources (DERs)?

Answer

Distributed energy resources (DERs) include wind, solar, battery storage, and other small-scale power devices connected at the grid edge. The deployment of DERs can support resilience through increasing overall and spatial diversity of generation resources.

Question 2

How many facilities with DERs have been the target of cyberattacks to date?

Answer

So far, only one renewable energy provider is known to have been hit by a cyber attack. However, as DERs are deployed in larger numbers, it is likely they will be targeted in future cyber attacks. It is important to secure these new devices from the first day, in order to prevent attackers from taking advantage of weak security (as happened with the Internet-of-Things devices).

Question 3

Could you please clarify what "cybersecurity tools" refers to and provide an example?

Answer

Different cybersecurity tools are useful for different cybersecurity functions (for instance, you'd use different tools for network defense vs. forensic analysis). For basic protection of networks, a good firewall is a good place to start, along with proper network segmentation and access control.

Question 4

Is there any standard for communication between the controllers and distributed generators (DGs) and what is the communication architecture?

Answer

If the controller and DG are on same site, then the power communication protocol (at the application layer level) is either Modbus (70%) or Proprietary (30%). The communication architecture would be TCP/IP (at the transport layer level).
If the controller and DG are NOT on the same site, then most likely they would use DNP3 or IEC 61850 to communicate.

Question 5

How does the DERCF tool work?

Answer

To use the Distributed Energy Resources Cybersecurity Framework (DERCF), visit http://www.dercf.nrel.gov. The online tool will guide you through the process of inputing data will produce cybersecurity scores for governance, technical management, and physical security. NOTE: You may register for an account with the Web site or use the tool in anonymous mode. However, anonymous mode does not store any data associated with the assessment. Anonymous mode requires that the full assessment be taken in one session, as there is no option to save the user's progress.

Question 6

Data storage technologies used during this era are dynamic. Kindly advise on the tradeoffs between local and cloud-based data storage.

Answer

Data storage is cheaper than ever before, enabling utilities to store large amounts of data locally and securely (look for a storage option that includes encryption). While cloud storage options offer many advantages, availability is only as good as your Internet connection to the cloud service. If Internet connectivity in your area is unreliable, focus on local storage options.

Question 7

Does the DERCF tool allow regulators to monitor profits made by the power producers or any false power characteristics?

Answer

No. The Distributed Energy Resources Cybersecurity Framework (DERCF) is a self-assessment tool. Users are not asked to input any financial data or power quality data. DERCF can be accessed at http://www.dercf.nrel.gov

Question 8

What is the role of cyber security for an energy regulator?

Answer

Because cybersecurity is important to the reliable delivery of electrical power, energy regulators have a role to play in advancing cybersecurity for utilities. Suggest beginning with a discussion with the utilities in order to hear their concerns regarding cybersecurity and the associated challenges. If a regulatory framework is needed, it should be developed with input from the utilities and based on meaningful, measurable outcomes. USAID and the National Association of Regulatory Utility Commissioners (NARUC) have put out an excellent guide that helps regulators evaluate cybersecurity investments: https://pubs.naruc.org/pub.cfm?id=9865ECB8-155D-0A36-311A-9FEFE6DBD077

If you are interested in exploring additional training materials, tools, data, case studies and other publications that support decision makers in assessing power sector vulnerabilities, identifying resilience solutions, and making informed decisions to enhance power sector resilience at all scales, please visit the Resilient Energy Platform at www.resilient-energy.org.