Solar Systems: Protecting Inverters from Hacker Attacks

05/03/2018 | Cologne

TÜV Rheinland experts have succeeded in hacking commercially available PV inverters within a few minutes. This is all the more critical since storage systems typically communicate with the inverter, too. The possible impact of an attack ranges from manipulating the power output of the PV system to harming the battery or adversely influence electricity grids and maybe paralyze them completely. “In times of millions of renewable energy sources and the necessity of intelligent grids and in view of more than 75,000 home storage systems now installed, it is even more important to check whether the system is vulnerable,” emphasizes Dr. Daniel Hamburg, Head of the Global Center of Excellence Testing and Certification at TÜV Rheinland. “Solar systems must be able to communicate with the provider securely and without errors so that feeding in the electricity takes place within the allowed operating states.”

Inverter as a Communicator

Inverters convert the direct current generated by PV modules into alternating current that they feed into the distribution grid. By hacking the inverters, it is possible to

gain access to the battery management system, too. In doing so, it is possible to trick the battery into an unsafe status and, on a wider scale, to attack the entire electricity grid by specifically causing massive power fluctuations. “We were able to re-parametrize commercially available inverters without any problems,” said Roman-Alexander Brück, Laboratory Head for Solar Components at TÜV Rheinland, summarizing the tests. His colleagues had successfully penetrated inverters deploying several approaches among them a brute force attack or stealing passwords.

Inspection of Cyber Security Recommended

Cyber security and protection against hacker attacks is not included in the standard functional safety inspection of solar system components designed to ensure smooth operation. “Therefore, we recommend that manufacturers have their systems inspected and eliminate potential vulnerabilities,” explains Brück. “We use specifically developed security-by-design solutions and provide support to make the systems robust and protect them against unwanted interference,” adds Dr. Hamburg. “The aim is to ensure that the system cannot be driven into a dangerous state and that the communication with the grid operator takes place safely as planned.”

Find out more and visit us at the Intersolar in Munich, between the 20th and 22nd of June 2018, hall A2, booth 177. We look forward to seeing you.

Contact for media inquiries: Norman Hübner
Phone: +49 221 806 - 3060
E-Mail: norman.huebner@de.tuv.com

****

TÜV Rheinland is a global leader in independent inspection services, founded nearly 150 years ago. The group maintains a worldwide presence of more than 20,000 people; annual turnover is EUR 2 billion. The independent experts stand for quality and safety for people, technology and the environment in nearly all aspects of life. TÜV Rheinland inspects technical equipment, products and services, oversees projects, and helps to shape processes and information security for companies. Its experts train people in a wide range of careers and industries. To this end, TÜV Rheinland employs a global network of approved labs, testing and education centers. Since 2006, TÜV Rheinland has been a member of the United Nations Global Compact to promote sustainability and combat corruption.

Website: www.tuv.com