Cyber Security in Photovoltaic System

(SA-E-20220908-001)

Why cyber security is becoming more important?

With the vigorous development of photovoltaic systems and the long-term goal of global carbon neutrality, the grid-connected capacity of photovoltaic systems in countries around the world has also increased, resulting in a gradual increase in the proportion of renewable energy in the national energy structure. At the same time, through the development and application of VPP technologies in both on-grid and off-grid systems including demand response, advanced metering infrastructure (AMI), and distributed energy (DER), the grid architecture is rapidly evolving from a structure at the center of a utility grid to a highly advanced smart grid with integrated distributed energy sources.

As a result, the number and sophistication of cyber-attacks against distributed energy resources is increasing. The resulting large-scale power outages and other events will bring serious consequences to the society, economy and market.

What is the breakthrough point of cyber-attacks in photovoltaic system?

In a solar photovoltaic system, the primary function of the inverter is to convert the DC energy generated by the solar panels into usable AC power. However, inverters can also play the role as IoT devices because they need to transmit data to a designated cloud server via the Internet, and most inverter companies have desktop or mobile applications available to users. Through these applications, users can obtain the data stored in the cloud server of the inverters they own within the scope of authority.

In addition to the demonstrate the data, many companies have now developed remote control functions and open them to authorized user to implement some control functions. For example, remotely control the opening and closing of the AC side relay of the photovoltaic grid-connected inverter to change the connection state with the grid. Although the opening of these functions reduces operation and maintenance costs to a certain extent and provides convenience to users, it also makes the inverter suffer greater risks and losses from cyber-attacks.

Therefore, as long as the user's inverter is connected to the Internet, hackers can launch network attacks on the inverter through the manufacturer's server or the home router connected to the inverter.

What are the impacts of cyber-attacks on PV systems?

The possible impacts of a cyber-attack on a solar energy system are mainly divided into individual users and the grid system. For the personal photovoltaic system, once the inverter is successfully hacked, the hacker can reduce the active output power of the inverter to cause economic loss of the user. If it is a energy storage system equipped with battery, a hacker can reduce the SOC of the battery by over-discharging the battery to an unhealthy state of charge, or change the working logic of the inverter to force the inverter to charge the battery from the grid instead of using abundant PV power, in order to increase the electricity cost of users. For the power grid system, the grid safety regulations of most countries do not allow the inverters in the grid-connected state to be

disconnected at will, because the large-scale disconnection of the inverter will have a huge impact on the frequency stability of the grid. So if the security is breached by the hacker, the massive shutdown of large amount of the PV systems under control by the hacker will bring serious impact and damage to the utility grid.

How does a PV system ensure cyber security?

In order to prevent cyber-attacks on photovoltaic systems to the greatest extent, inverter manufacturers usually deploy various security policies on the equipment side and server side. Taking GoodWe as an example, to ensure the security of data transmission between the inverter and the server, we use the transmission protocols of CRC+AES and TLS respectively for communication with servers with different functions.

At the cloud server level, the cloud service providers we choose also provide strong security strategies to ensure the security of the database, as well as the security and stability of customer data requests. Distributed Denial of Service, commonly known as DDoS, is the most common security threat. Usually, attackers use an illegal account to install the DDoS master program on one computer and install the agent program on multiple computers on the network. Within the set time, the main control program communicates with a large number of agent programs, and when the agent program receives an instruction, it launches an attack on the target. The main control program can even activate hundreds or thousands of agent programs within a few seconds. After a DDoS attack, the origin server may not be able to provide services, resulting in users being unable to access your corresponding data. At the same time, it may steal the core data of your business, resulting in huge economic losses.

Therefore, we configure security groups to avoid exposing service ports that are not necessary for business on the public network, so as to avoid requests and accesses that are not related to business. By configuring security groups, you can effectively prevent systems from being scanned or accidentally exposed.

Also, we deploy the bastion host, which is a management and control platform for core system operation and maintenance and security auditing provided by our cloud solution supplier. It can centrally manage asset permissions, control operation behaviors throughout the process, restore operation and maintenance scenarios in real time, and ensure that cloud operation and maintenance behaviors can be identified, permissions can be controlled, and operations can be audited. It is used to solve problems such as difficult management of many assets, unclear operation and maintenance responsibilities and authorities, and difficulty in tracing operation and maintenance events, helping enterprises to meet the requirements for compliance with the guarantee.

In addition, we use a SaaS (Software as a Service) firewall on the server side, which can manage north-south and east-west traffic in a unified manner, provide traffic monitoring, precise access control, real-time intrusion prevention and other functions, and comprehensively protect network boundaries.

Cyber Security in Photovoltaic System

(SA-E-20220908-001)

Summary

In the near future, renewable energy power generation will become one of the most important forms of energy in most countries or regions. The utility system is undergoing digital transformation, and related information technologies are introduced into the application of photovoltaic systems. The diversification and complexity of data brings new threats, which will prompt the photovoltaic industry to pay more attention to cyber security aspects to ensure the safe development of photovoltaic systems.

Welcome visiting **GoodWe Solar Community (community.goodwe.com)** to check all technical articles, guidance videos, webinars and activities released by GoodWe and GoodWe Solar Academy.