Cyber security: how prepared is the PV industry?

Cyber security | The digitalisation and distribution of the energy system is creating potentially more points of vulnerability for hackers to exploit. Catherine Early looks at how the PV industry is responding to ensure plants are kept safe from attack

Credit Flickr/blogtrepreneur.com/tech

A blackout forced by hackers from rogue states or criminal gangs may sound like a plot from a James Bond movie but the issue is high on the agenda of governments and electricity utilities worldwide.

Just last month – November 2017 – thousands of people working in industry or government in the US, Canada and Mexico took part in a large-scale exercise that simulated a cyber attack on electrical networks. Grid Ex IV was the fourth event of its kind run by the North American Electric Reliability Corporation (NERC) and is designed to test participants' preparation for such an event happening in reality.

Over in Europe, the EU Agency for Network and Information Security has co-ordinated similar exercises since 2010. The most recent simulation in 2016 imagined a blackout in a European country over the Christmas period, and used actors and social media to make the scenario more realistic. Over 300 organisations had to deal with a series of problems caused by malware, ransomware, drones and the Internet of Things.

The risk of cyber attacks on PV power plants and other smart grid infrastructure is attracting growing attention from industry and government

It is not just governments that are seeing the threat. In a survey of senior utility executives worldwide published by consultancy EY in November, 82% of respondents ranked business interruption from cyber attacks and storms in their top three threats.

Examples of cyber attacks specifically targeted against an electricity network so

far are rare. According to the International Energy Agency, the first such incident was in the Ukraine in 2015. Attackers accessed substations' supervisory control and data acquisition (SCADA) system and firmware with a combination of malware, personnel credentials obtained through of email phishing, and Denial of Service (DoS) to prevent customers from obtaining call centre information about the blackout. Around a quarter of a million people lost power. A similar attack followed in 2016.

The threat specifically to solar PV equipment is small, but should not be ignored, according to experts. Duncan Page, a cyber security specialist at consultancy PwC, says that at the most basic level, someone could take a site offline, preventing it from generating electricity and therefore earning revenue. Taking it a step further, they could corrupt the system, blocking the utility from getting it back up and running, he says.

This becomes more serious if a utility has contracts with a grid operator to provide services such as balancing or frequency response, he adds. In future, solar farms are likely to also incorporate storage equipment and batteries with local control systems, making them more complex. This not only increases the risk of an attack occurring, but also its potential impact.

"As the grid becomes smarter and more interrelated and utilities enter into more relationships that earn money from their assets, the implications of being hacked will become greater and more complicated," Page says.

Cyril Draffin, a cybersecurity expert who advises the Massachusetts Institute of Technology energy initiative, says that hackers wanting to take down a whole grid are most likely to be acting on behalf of nation states, as major attacks take time and resources to execute. Experts estimate that hackers would have spent around six months developing the attack in the Ukraine, which the country blamed on Russian security services.

Cyber security has been a concern in the wider energy sector for some time, but the growing use of renewable energy, batteries and electric vehicles has heightened the risks. By connecting such assets to their networks, utilities are effectively exposing them to third-party access, explains Daniel Arnold, researcher and engineer at the US-based Lawrence Berkeley National Laboratory (LBNL). "These devices could be co-opted to introduce problems into the electricity grid," he says.

A vulnerability hackers could exploit is the inverters used in PV systems, Arnold says. "There are autonomous control functions on these devices that are meant to regulate their power output for system safety and reliability. They can be changed in a way that could cause problems for the grid in terms of voltage oscillations if enough devices were affected," he says.

However, Arnold also sees the connection of third-party devices to the grid as an opportunity as well as a risk. He is leading a major government-funded project at the LBNL which is developing ways to use these devices to fight off attacks (see box, next page).

"There are autonomous control functions on inverters that are meant to regulate their power output for system safety and reliability. They can be changed in a way that could cause problems for the grid in terms of voltage oscillations if enough devices were affected"

Detlef Beister, business development manager at German inverter manufacturer SMA Solar Technology, says that distributed energy systems have advantages over traditional centralised power stations in terms of cyber security. "It's much harder for hackers to damage distributed supply as they would have to attack a large number of devices, which would take a lot of time and money to do," he says.

However, having multiple small sites can also be a challenge to protect, Page warns. When dealing with attacks, companies tend to fall down on the application of security, rather than lacking security tools and technologies, he says. For example, solar farms tend to be small and unmanned, so it is harder to keep up to date with security patches.

"Operators need to make sure that their security frameworks are just as good at protecting small sites as they are at controlling the central IT estate," he says. Once a vulnerability has been identified, it would be relatively easy to scale up an attack with a large number of small sites, he adds.

"There is no substitute for thinking about security at the design stage; then there should be enough tools and techniques available," he says. This is one advantage the solar power industry has over more traditional energy plants, since most equipment has been installed relatively recently, he says.

Industry and government action

Manufacturers also have a part to play. SMA has several strategies to deal with cyber security, according to its information security manager Marek Seeger. It has a team of people who work on ensuring that its products are certified to security standards and pass security tests. They are also tested by independent companies who employ hackers to test for vulnerabilities.

The company's products were recently criticised by Dutch cyber security engineer Willem Westerhof, who claimed that its inverters were vulnerable to attack. SMA acknowledges some problems exist with four older models of inverter, the Sunny Boy models TLST-21 and TL-21, and Sunny Tripower models TL-10 and TL-30.

However, the company stresses that even if operators use these inverters, a potential hacker would need to have extensive expertise to hack. It denies Westerhof's claims that there are a potential 17GW of solar inverter power at risk, saying that this figure represents its entire sales, not sales of the affected products, which is a fraction of this.

"We see absolutely no danger to grid stability even in the extremely unlikely event that all inverters should be successfully attacked at the same time," the company states.

The company publishes guidance for its customers to help them implement robust security measures. According to the guidance, when a PV system is being connected to the internet, the system operator or network administrator must have knowledge of all devices active in the network, including their communication requirements and features and possible vulnerabilities. They should also know all accounts that access the systems, how to limit access to the network and devices, and they should have installed all security tools such as a firewall and proxy server.

"Manufacturers and customers need to work together to stay up to date and secure on cyber security," Seeger says.

String inverter manufacturer SolarEdge says it is also taking the threat seriously. Lior Handelsman, vice president of marketing and product strategy at the company, explains that it embeds information

security into all product development, runs stress tests on its security systems and encrypts and authenticates communication channels. If an attack did take place, it has backup protection and restoration plans to minimise potential damage, he says.

However, Handelsman believes that more needs to be done industry-wide. "The entire energy industry, including solar, needs to view cyber security as a necessity. As such, we have called for the creation of an industry-wide body that includes all stakeholders to share information in order to prevent attacks and help prevent PV's collective brand from being damaged," he says.

Such a body would mean that the whole sector was working together to identify risks, and could create unified standards and regulations on encryption, backup, reporting breaches, protocols, endpoint security, penetration testing, server security and hardening, hosting security and database security, he says.

Other industry players have also been thinking about standards and regulations on cyber security. In Europe, PV trade association Solar Power Europe has set up a task force on digitalisation covering all aspects of how smart grids, buildings and meters will affect the sector's operations. The task force is being led by SMA, and its 30 members include manufacturers ABB, Siemens and utilities Centrica and RWE.

The task force has called on policy makers to support the PV industry in its transition to full digitalisation, and has highlighted cyber security as one of the 10 aspects of regulation that it wants addressed.

A lack of internationally binding standards or requirements mean that it is up to manufacturers how seriously they take cyber security and whether their products adhere to any of these standards, the task force says. It therefore wants internationally binding, consistent and modern cyber security regulation.

In turn, the task force has produced seven commitments on digitalisation that its members have signed up to, including championing data protection and putting in place stringent cyber security measures.

Meanwhile, the EU is working on strengthening its cyber security strategies and policies. The bloc's first legislation on cyber security, the Network and Information Security (NIS) Directive, was adopted by the European Parliament in July 2016. It requires member states to adopt a national strategy for NIS security and to designate responsibility for the issue to a national authority. It also enhances cooperation on cyber security among member states through a dedicated group on the issue.

In September 2017, the European Commission stepped up its action by proposing an EU cyber security agency to help member states in dealing with attacks, as well as a new European certification scheme to ensure that digital products and services are safe to use.

In the US, multiple organisations have responsibilities for cyber security, ranging from the Federal Bureau of Investigation to individual state government. Cyber security in the energy sector is led by the Department of Energy (DoE). It has developed strategies to coordinate public and private initiatives for resilient energy systems, and in 2013, launched public-private partnership the Cybersecurity Risk Information Sharing Programme to provide the electricity sector with near-time cyber threat information and analysis. The US also works with Canada on standards to maintain critical infrastructure within the North American Electric Reliability Corporation (NERC).

Some countries obligate organisations that provide critical infrastructure to comply with standards such as ISO/IEC 27001, which sets out best practice for management of information security. Product standards include ISO/IEC 27032, PAS 555, UL 2900 and IEC 62443. There is also the US National Institute of Standards and Technology (NIST) Cybersecurity Framework, which comprises voluntary guidance to organisations on reducing cyber security risks.

"There is a well organised overall direction, but responsibility for cyber security and response to attacks resides with companies, individual government agencies and organisations, and some are much better prepared than others," Draffin says.

Large solar PV systems owned by electric utilities do have to meet NERC critical infrastructure protection standards, but there are no regulations that apply to small solar PV. Draffin believes that regulations should be mandated for all solar PV systems connected to the grid, and all should use best practice.

However, he warns: "Just as it is impossible to stop all crimes, it is impossible to have fully effective cyber defences, because adversaries are constantly improving their attacks and approaches, and new software with vulnerabilities are being introduced." ■

Catherine Early is a freelance journalist specialising in energy and the environment

Inverters the focus of efforts to beat hackers at their own game

"Utilities connecting third-party devices to their systems are simultaneously creating a vulnerability and an opportunity for better defence," says Daniel Arnold, a researcher in the Grid Integration Group at the Lawrence Berkeley National Laboratory in America.

Arnold is exploring ways to use this theory to develop defences against cyber attacks on inverter technology. In September, his project was one of 20 awarded up to US$2.5 million funding by the US Department of Energy, which is seeking innovative, scalable and cost-effective solutions to deal with cyber security issues. The three-year project will test ways of enabling electricity grids to resist cyber attacks by developing adaptive control algorithms for distributed energy resources, voltage regulation and protection systems.

Industry and government are developing standards for how solar inverters communicate with the grid so that the PV modules can adjust their power levels accordingly. "It is this standardisation that presents a vulnerability," says Arnold.

The project will develop algorithms to use the system in the same way the hackers might do, but will nullify the attack by sending the opposite signals. "If an attacker tries to manipulate the settings in a number of PV inverters, we'll observe these manipulations, then identify the settings in PV inverters that have not been hacked, and finally, dispatch the appropriate settings to the inverters deemed safe in order to counter that attack," explains Arnold.

LBNL's approach is to consider what would happen if all existing cyber defence tools such as encryption fail and a hostile entity gains control of a PV system. "We're putting ourselves in the perspective of the hacker to understand what defences we should deploy to fight off these attacks," he says.

The team has discovered several methods by which control systems could be manipulated to create a problem, and it has also discovered ways in which it could counteract these attacks. One challenge for the project will be how to fully test the algorithms, Arnold says.

"It's very difficult to trial on a real system as we'd have to fall victim to an attack, and defend against it, or we'd have to simulate an attack ourselves, which utilities aren't exactly keen to do. So although we're going to deploy this on real networks, we'll have to be creative in how we test it," he says.

Partners on the project include trade bodies the SunSpec Alliance and HDPV Alliance, manufacturers SolarEdge and Siemens, and Arizona State University.

The ultimate aim is to develop algorithms that can monitor the grid to provide advanced warning to a utility operator of a possible emerging attack.