WP-029-2020

Why DER cybersecurity is critical and how to protect DER systems

Version 0.9

20 November 2020

This document was produced in the European Network for Cybersecurity (ENCS) project on distributed energy resources (DER) security, which supports grid and DER operators in selecting and implementing technical and organizational security measures for DER systems and their components. The document is part of a series of requirements available through the ENCS portal (https://encs.eu/documents):

Smart metering	SM-301-2019: Security requirements for procuring smart meters and data concentrators
Distribution automation	DA-101-2019: Security risk assessment for distribution automation systems DA-201-2019: Security architecture for distribution automation systems DA-301-2019: Security requirements for procuring distribution automation RTUs DA-390-2019: Market survey on distribution automation RTU security DA-401-2019: Security test plan for distribution automation RTUs
Substation automation	SA-101-2019: Security risk assessment for substation automation systems SA-201-2019: Security architecture for substation automation systems SA-301-2019: Security requirements for procuring substation gateways SA-302-2019: Security requirements for procuring IEDs SA-303-2019: Security requirements for procuring HMI software
Electric vehicles	EV-101-2019: Security risk assessment for EC charging infrastructure EV-201-2019: Security architecture for EV charging infrastructure EV-301-2019: Security requirements for procuring EV charging stations EV-401-2019: Security test plan for EV charging stations

This document is shared under the Traffic Light Protocol classification:

TLP WHITE - public

The European Network for Cybersecurity (ENCS) is a non-profit membership organization that brings together critical infrastructure owners and security experts to deploy secure European energy grids.

Version History

Date	Version	Description
26 June 2020	0.1	Initial draft
20 November 2020	0.9	Final version for approval by partners

ENCS

Table of Contents

Version History 3

Why DER cybersecurity is critical and how to protect DER systems 5

When is a party critical to the electricity grid? 5

Attacks on critical parties can cause balancing problems 5

Advanced threat actors are targeting critical parties 6

Which DER parties are critical? 7

DER are generating a lot of power 7

Many parties are remotely controlling DER 7

What measures should critical parties take? 8

References 10

Why DER cybersecurity is critical and how to protect DER systems

There is increasing use of renewable energy in the European grid. In 2018, 32,1% of the electricity consumed in the EU-28 was generated from renewable sources. Much of the renewable energy is from wind and solar power, contributing 35,8% and 12,2% of electricity from renewable sources [1]. Much of the solar and wind generation takes place in Distributed Energy Resources (DER): smaller facilities connected to the distribution grid. In 2018, facilities with a capacity of less than 1 MW, for instance, contributed 76 GW[1] of solar power, while facilities with a capacity of more than 1 MW contributed 39,2 GW[1] [2] [3].

With the growth of DER, new parties have become involved in the electricity grid, as owners, equipment manufacturers, maintenance contractors or service providers [3]. However, these parties are often not ready to manage the societal risk of disruption to the European grid by a cyberattack. They need to compete in the market and are primarily concerned about the business risks to themselves. They do not have a legal obligation to mitigate societal risks. The NIS Directive for instance, which requires operators of essential services (OES) to take appropriate measures to mitigate cybersecurity risks [4], does not consider most DER parties as OES.

Yet, the cybersecurity of the European electricity grid is going to increasingly depend on these parties who own and operate DER. Many of them can control significant amounts of generation. If they are not secured as the critical infrastructures that they are, they will be targeted by attackers looking for the weakest link in the chain.

When is a party critical to the electricity grid?

Any party that controls hundreds of megawatts of electricity generation or consumption poses a cybersecurity risk to society unless they take the necessary measures to protect systems against advanced threats. Such parties should be considered critical for the cybersecurity of the electricity grid.

Attacks on critical parties can cause balancing problems

A cyber-attack on such a critical party that turns off or disconnects control systems can cause a large loss of electricity demand or supply, leading to balancing problems. Through a cascading effect in the grid, this can lead to a large-scale blackout.

[1] Result of multiplying the total solar PV capacity by the segment percentage presented in [2].

An example of such a cascading effect is the power outage in the UK in August 2019. In this case, the start of the cascade was a lightning strike. Automated reactions then caused a reduction of power at a large wind farm (737 MW), a gas plant (244 MW), and a large number of DER (500 MW), all within one second. The total reduction was 1,481 MW. The transmission system operator, National Grid, only had 1,000 MW of backup power available to compensate (as required by regulation). So, to keep the frequency of the grid in the allowed range, they started to disconnect customers in a reduced way. In the end, 1.1 million customers were without power for 15 to 45 minutes. The rail networks were disrupted for several days [5].

In theory, attackers can only disrupt the European grid by causing generation losses exceeding the reference incident defined in the System Operation Guideline. The guideline requires Transmission System Operators (TSOs) to ensure a reserve capacity that can compensate for a power imbalance equal to or lower than that reference, so that frequency deviations can be contained. For instance, the reference incident for continental Europe is 3 GW [6].

Still, in 2014, a study by ENTSO-E showed that the grid was likely to experience a blackout even for imbalances less than the reference 3 GW incident in certain scenarios. Consequently, ENTSO-E urged countries to set up and perform a retrofit program for the installed distributed generation [7].

Advanced threat actors are targeting critical parties

There are clear indications that some advanced threats, especially nation states, would be interested in attacking critical parties to cause such blackout scenarios. According to the Dutch intelligence agency [8], offensive cybersecurity programs are attractive to nation states, because they are low in cost and risk, yet, the range and results are large. Nation states can acquire the knowledge and skills to use advanced attack techniques and have the resources to launch persistent attack campaigns lasting for months or even years.

Countries like Australia, the United Kingdom or the United States of America publicly announced large-scale investments in their offensive capabilities as a response to the rising cyber threat [9] [10] [11]. US officials confirmed that their country and Israel jointly developed the *Stuxnet* worm that damaged a uranium enrichment facility in 2010 [12]. Security analysts suspect Russia caused the black-outs in Ukraine in 2015, affecting 225 thousand customers in several areas, and in 2016, affecting a part of Kyiv [13] [14].

Critical parties in the European grid have recently been targeted in cyber-attacks. In March 2020, ENTSO-E reported an intrusion in their office systems [15]. In May, ELEXON UK announced its internal IT systems were impacted by a cyber-attack [16].

Which DER parties are critical?

There are probably already several parties operating DER that can remotely control hundreds of megawatts of electricity, and hence should be considered critical. Many more parties will likely become critical in the near future.

DER are generating a lot of power

A party only needs to control a small fraction of solar and wind power to control hundreds of megawatts. In 2019, the solar PV capacity in the EU was 132 GW [2] and the wind capacity 192 GW [17]. For solar PV, the top countries were Germany, Italy and Spain, with 49,7 GW, 20,6 GW and 10,6 GW, respectively [18]. For wind, the top countries were Germany, Spain and the United Kingdom, with 61,4 GW, 25,8 GW and 23,5 GW, respectively [17].

For maximum effect, attackers need to time their attack to take place when the DER or the grid are close to maximum capacity. Wind and sunlight have an intermittent availability. Wind has an average capacity factor of around 30% [17] and Solar power is usually associated with even lower capacity factors. However, attackers can try to switch off power on a day with a good weather forecast, when the capacity factors are higher, or during scheduled grid works, when the grid can be more vulnerable. The attacker can easily find weather forecasts and a list of scheduled grid works with simple tools or on public websites.

Many parties are remotely controlling DER

Much of the power generated in DER is already remotely controlled by different types of parties and the numbers are expected to grow rapidly.

Larger facilities can be remotely controlled and maintained by their owner or a contractor. The owner can monitor the performance. The maintenance contractor can receive alerts and remotely diagnose failures. Sometimes aggregators can control the facilities to sell the flexibility in the system. For systems starting at tens of megawatts, grid operators can send curtailment orders to prevent problems in the grid [3].

Equipment manufacturers also often have remote access. In 2019, three turbine manufacturers represented 96% of all the offshore wind capacity, with one having 68,1%, another having 23,5% and the last having 4,4% in Europe [19]. Still, in 2019, four vendors shared 50% of the power capacity from PV inverter shipments in the global market [20].

Smaller facilities, especially residential solar panels, often have direct connections to internet servers of the equipment manufacturer. Some servers probably control many hundreds of thousands, if not millions of solar panels.

What measures should critical parties take?

Several parties have been developing their security capabilities for many years, including security in their processes, systems, or components. Some DER specific guidelines and requirement sets are already available, such as [22] or Section 10.8 of [3]. Yet, there are still many parties who need the right references and/or development in the security area. This showcases a need for harmonization.

All critical parties who can remotely control significant amounts of generation should be required to take measures like large grid operators and producers.

All critical parties should protect their own systems and processes against cyber-attacks. They can do this by setting up an information security management system to structurally manage the risks.

A harmonized, standard-based approach should be used throughout the electricity sector so that all parties have a minimum level of security and can more easily trust each other. We would recommend striving for ISO/IEC 27001 conformance for all critical parties. The scope of the management system should cover all processes critical to the electricity grid, as recommended for system operators in the Smart Grid Task Force Expert Group 2 report [21].

On top of this, some parties should take additional measures based on their role:

- **Manufacturers** must deliver components that are secure by design. The manufacture should support the components throughout their lifetime with security updates. Components that are managed by consumers or small businesses, such as residential PV inverters, should be delivered with security turned on by default. They should avoid using default password or insecure communication.
- **Maintenance contractors** must ensure that they deliver systems that are securely configured. For instance, they must replace default passwords with unique ones and configure strong settings (e.g., only secure protocols allowed). They must take strict measures to protect the systems they use to remotely access facilities that they maintain.
- **Electricity producers and aggregators** that control generation on many DER facilities must protect their control systems and communications in all stages of the life cycle.
- **Grid operators** (DSOs and TSOs) must protect the digital connection to DER systems together with the asset owners or operation contractors. They must also protect their systems against attacks coming from compromised DER systems.

To help achieve a chain with no weakest link, ENCS, WindEurope and SolarPower Europe have worked together to establish high-quality security requirement sets and best practices. These are ready for use in the design and procurement of DER systems, for manufacturers, DER operators and grid operators.

References

[1] Eurostat, "Wind and water provide most renewable electricity," 2020.

[2] SolarPower Europe, "EU Market Outlook for Solar Power 2020-2024," 2020.

[3] SolarPower Europe, "Operation & Maintenance. Best Practice Guidelines," 2009.

[4] The European Parliament and the Council of the European Union, "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," 2016.

[5] National Grid, Technical report on the events of 9 August 2019, 6 September 2019.

[6] European Commission (EC), "System Operation Guideline (SO GL)," 2017.

[7] ENTSO-E, "Dynamic Study on Dispersed Generation Impact on CE Region Security," 2014.

[8] Dutch General Intelligence and Security Service, "Offensive cyber-programmes - An ideal business model for states," 2020.

[9] The New York Times, "Australia Spending Nearly $1 Billion on Cyberdefense as China Tensions Rise," 2020.

[10] Independent, "UK is nearly ready to launch force to hit hostile countries with cyberattacks," 2020.

[11] NBC News, "Under Trump, U.S. military ramps up cyber offensive against other countries," 2019.

[12] The Washington Post, "Stuxnet was work of U.S. and Israeli experts, officials say," 2012.

[13] Wired, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," 2016.

[14] Wired, "'Crash Override': The Malware That Took Down a Power Grid," 2017.

[15] ENTSO-E, "ENTSO-E has recently found evidence of a successful cyber intrusion into its office network," 2020.

[16] ELEXON Portal, "BSC Bulletin 335 -ELEXON's internal IT systems have been impacted by a cyber attack," 2020.

[17] WindEurope, "Wind energy in Europe in 2019. Trends and statistics," 2020.

[18] SolarPower Europe, "Global Market Outlook for Solar Power 2020-2024," 2020.

[19] WindEurope, "Offshore Wind in Europe. Key trends and statistics 2019," 2020.

[20] PV Magazine, "Huawei, Sungrow and SMA dominate global inverter market," 2020.

[21] Smart Grid Task Force Expert Group 2, Recommendations for the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting, and Crisis Management, 2019.

[22] EPRI, "Security Architecture for the Distributed Energy Resources Integration Network," 2019.